# Separating sets of invariant algebras

Schefler Barna

Eötvös Loránd University, Budapest
supervisor: Domokos Mátyás, Rényi Institute, Budapest

Conference on Rings and Polynomials, TU Graz
14-19.03.2025
The presentation contains results from joint work with K. Zhao and Q. Zhong

# Outline

# Outline

Let $\rho : G \to GL(V)$ be a finite dimensional complex representation of the finite group $G$. Denote by $x_1, x_2, \dots, x_n$ a basis of the dual space $V^*$. From now we suppress $\rho$ from the notation and use only $V$ to denote a representation.

Let $\rho : G \to GL(V)$ be a finite dimensional complex representation of the finite group $G$. Denote by $x_1, x_2, \dots, x_n$ a basis of the dual space $V^*$. From now we suppress $\rho$ from the notation and use only $V$ to denote a representation.
The representation induces $G$-action on the coordinate ring $\mathbb{C}[V] = \mathbb{C}[x_1, \dots, x_n]$ of $V$:

$$\text{for } g \in G \text{ and } f \in \mathbb{C}[V] \text{ we have: } g \cdot f(x_1, \dots, x_n) = f(g^{-1} \cdot x_1, \dots, g^{-1} \cdot x_n)$$

Let $\rho : G \to GL(V)$ be a finite dimensional complex representation of the finite group $G$. Denote by $x_1, x_2, \dots, x_n$ a basis of the dual space $V^*$. From now we suppress $\rho$ from the notation and use only $V$ to denote a representation.
The representation induces $G$-action on the coordinate ring $\mathbb{C}[V] = \mathbb{C}[x_1, ..., x_n]$ of $V$:

$$\text{for } g \in G \text{ and } f \in \mathbb{C}[V] \text{ we have: } g \cdot f(x_1, \dots, x_n) = f(g^{-1} \cdot x_1, \dots, g^{-1} \cdot x_n)$$

A theorem of Noether states that the invariant subalgebra

$$\mathbb{C}[V]^G := \{f \in \mathbb{C}[V] : g \cdot f = f \text{ for } \forall g \in G\}$$

is finitely generated by homogeneous polynomials of degree $\leq |G|$.

Let $\rho : G \to GL(V)$ be a finite dimensional complex representation of the finite group $G$. Denote by $x_1, x_2, \dots, x_n$ a basis of the dual space $V^*$. From now we suppress $\rho$ from the notation and use only $V$ to denote a representation.
The representation induces $G$-action on the coordinate ring $\mathbb{C}[V] = \mathbb{C}[x_1, \dots, x_n]$ of $V$:

$$\text{for } g \in G \text{ and } f \in \mathbb{C}[V] \text{ we have: } g \cdot f(x_1, \dots, x_n) = f(g^{-1} \cdot x_1, \dots, g^{-1} \cdot x_n)$$

A theorem of Noether states that the invariant subalgebra

$$\mathbb{C}[V]^G := \{f \in \mathbb{C}[V] : g \cdot f = f \text{ for } \forall g \in G\}$$

is finitely generated by homogeneous polynomials of degree $\leq |G|$.
One can raise two questions:

- What is a sharp upper bound for the degree of the generators?
- What is a sharp lower bound for the number of the generators?

## Definition

*Let $\beta(G,V)$ be the minimal positive integer $d$ such that $\mathbb{C}[V]^G$ is generated by homogeneous polynomials of degree at most $d$. The* **Noether number** *$\beta(G)$ of a finite group $G$ is*

$$\beta(G) := \max_V \{\beta(G,V) : V \text{ is a finite dimensional representation of } G\}$$

# Example

Consider the dihedral group $D_4$ and its two dimensional representation:

$$V: \quad r \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad s \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Then the algebra generators of $\mathbb{C}[V]^{D_4}$ are $\{xy, x^4 + y^4\}$.
(Check: $(-ix)(iy) = xy$, $yx = xy$ and $(-ix)^4 + (ix)^4 = x^4 + y^4$, $y^4 + x^4 = x^4 + y^4$.)

# Example

Consider the dihedral group $D_4$ and its two dimensional representation:

$$V: \quad r \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad s \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Then the algebra generators of $\mathbb{C}[V]^{D_4}$ are $\{xy, x^4 + y^4\}$.
(Check: $(-ix)(iy) = xy$, $yx = xy$ and $(-ix)^4 + (ix)^4 = x^4 + y^4$, $y^4 + x^4 = x^4 + y^4$.)
For the three dimensional representation

$$V': \quad r \mapsto \begin{bmatrix} i & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad s \mapsto \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

the algebra generators of $\mathbb{C}[V']^{D_4}$ are $\{z^2, xy, x^4 + y^4, z(x^4 - y^4)\}$.

A subset $S \subset \mathbb{C}[V]^G$ is called *separating set* if the following holds:

$$\text{if for any } v_1 \neq v_2 \in V \text{ and } f \in S \text{ we have } f(v_1) = f(v_2), \text{ then } h(v_1) = h(v_2) \text{ holds for all } h \in \mathbb{C}[V]^G$$

For example: a generating set.

A subset $S \subset \mathbb{C}[V]^G$ is called *separating set* if the following holds:

if for any $v_1 \neq v_2 \in V$ and $f \in S$ we have $f(v_1) = f(v_2)$, then $h(v_1) = h(v_2)$ holds for all $h \in \mathbb{C}[V]^G$

For example: a generating set.
If $G$ is a *finite* group, then a subset $S \subset \mathbb{C}[V]^G$ is a separating set if and only if:

$$Gv_1 \neq Gv_2 \text{ implies that there exists } f \in S \text{ such that } f(v_1) \neq f(v_2)$$

A subset $S \subset \mathbb{C}[V]^G$ is called *separating set* if the following holds:

if for any $v_1 \neq v_2 \in V$ and $f \in S$ we have $f(v_1) = f(v_2)$, then $h(v_1) = h(v_2)$ holds for all $h \in \mathbb{C}[V]^G$

For example: a generating set.
If $G$ is a *finite* group, then a subset $S \subset \mathbb{C}[V]^G$ is a separating set if and only if:

$$Gv_1 \neq Gv_2 \text{ implies that there exists } f \in S \text{ such that } f(v_1) \neq f(v_2)$$

Again, we have the questions:

**Questions**

- What is a sharp upper bound for the degrees of the separating invariants?
- What is a sharp lower bound for the size of a separating set?

## Definition

*Let $\beta_{\mathrm{sep}}(G,V)$ be the minimal positive integer $d$ such that $\mathbb{C}[V]^G$ contains a separating set whose elements are homogeneous polynomials of degree at most $d$. The separating Noether number $\beta_{\mathrm{sep}}(G)$ of a finite group $G$ is*

$$\beta_{\mathrm{sep}}(G) := \max_V \{\beta_{\mathrm{sep}}(G,V) : V \text{ is a finite dimensional representation of } G\}$$

## Properties

- $\beta(G) \leq |G|$
- $\beta(G, V) \leq \beta(G, V \oplus V')$
- $\beta(G, V_{reg}) = \beta(G)$

## Properties

- $\beta(G) \leq |G|$
- $\beta(G, V) \leq \beta(G, V \oplus V')$
- $\beta(G, V_{reg}) = \beta(G)$

The same facts are also true for $\beta_{\mathrm{sep}}$. Moreover, we have:

- $\beta_{\mathrm{sep}}(G) \leq \beta(G)$
- $\beta_{\mathrm{sep}}(G, V_{mf}) = \beta_{\mathrm{sep}}(G)$

$\beta_{\mathrm{sep}}(C_n) = \beta(C_n) = n$. For any noncyclic finite group $G$: $\beta(G) < |G|$

# Outline

# Historical background

- 1916 - Noether: degree bound for generators of the invariant algebra
- 1990 - Schmid: $\beta(G)$
- 2010 - Kohls-Kraft: $\beta_{\mathrm{sep}}(G)$
- 2012-2018 -Cziszter-Domokos: systematic study of $\beta(G)$
- 2017 - Domokos: $\beta_{\mathrm{sep}}(G)$ for abelian groups

# The separating Noether number of finite non-abelian groups

## Reminder

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

## Lemma

Let $V_1, \ldots, V_q$ be a complete list of representatives of the isomorphism classes of irreducible representations of $G$. Then for every $G$ there exists a positive integer $\kappa(G) << q$ such that

$$\beta_{sep}(G) = \max_{\substack{J \subset \{1,\ldots,q\} \\ |J| \leq \kappa(G)}} \{\beta_{sep}(G, \oplus_{j \in J} V_j)\}.$$

## Proposition [25+, Domokos, S.]

The exact value of the separating Noether number is calculated for any group $G$ with $|G| < 32$.

### Proposition [25+, Domokos, S.]

The exact value of the separating Noether number is calculated for any group $G$ with $|G| < 32$.

### Theorem [25+, Domokos, S.]

If $G$ is a non-cyclic finite group with a cyclic subgroup of index 2, then

$$\beta_{\mathrm{sep}}(G) = \frac{1}{2}|G| + \begin{cases} 2 & \text{if } G = \mathrm{Dic}_{4m},\ m > 1; \\ 1 & \text{otherwise.} \end{cases}$$

# Separating Noether number of finite abelian groups

Let $G_0$ be a subset of the (additively) written finite abelian group $G$. The elements of the (multiplicatively written) *free abelian monoid* $\mathcal{F}(G_0)$ with basis $G_0$ are written as

$$S = g_1 \dots g_k = \prod_{g \in G_0} g^{\mathsf{v}_g(S)}.$$

Consider the submonoid

$$\mathcal{B}(G_0) = \{ \prod_{g \in G_0} g^{\mathsf{v}_g(S)} \in \mathcal{F}(G_0) : \sum_{g \in G_0} \mathsf{v}_g(S) g = 0 \}$$

## Separating Noether number of finite abelian groups

Let $G_0$ be a subset of the (additively) written finite abelian group $G$. The elements of the (multiplicatively written) *free abelian monoid* $\mathcal{F}(G_0)$ with basis $G_0$ are written as

$$S = g_1 \dots g_k = \prod_{g \in G_0} g^{\mathsf{v}_g(S)}.$$

Consider the submonoid

$$\mathcal{B}(G_0) = \{ \prod_{g \in G_0} g^{\mathsf{v}_g(S)} \in \mathcal{F}(G_0) : \sum_{g \in G_0} \mathsf{v}_g(S) g = 0 \}$$

An element of $\mathcal{B}(G_0)$ that can not be written as a product of two non-invertible elements is called an *atom*.
The *length* of the element $S = \prod_{g \in G_0} g^{\mathsf{v}_g(S)} \in \mathcal{B}(G_0)$ is $|S| = \sum_{g \in G_0} \mathsf{v}_g(S)$.
The maximal length of the atoms of the monoid $\mathcal{B}(G)$ is called the *Davenport constant of the group* $G$ and is denoted by $\mathsf{D}(G)$.

# Example

Let us have $G = C_2 \oplus C_2$, and denote by $\{0, a, b, c\}$ the elements of the group.
$a + a = 0$, hence $A_1 = a^2 b^0 c^0 \in \mathcal{B}(\{a, b, c\})$ with $|A_1| = 2$
$b + b = 0$, hence $A_2 = a^0 b^2 c^0 \in \mathcal{B}(\{a, b, c\})$ with $|A_2| = 2$
$c + c = 0$, hence $A_3 = a^0 b^0 c^2 \in \mathcal{B}(\{a, b, c\})$ with $|A_3| = 2$
$a + b + c = 0$, hence $A_4 = a^1 b^1 c^1 \in \mathcal{B}(\{a, b, c\})$ with $|A_4| = 3$
Of course, the maximal length of the atoms is 3, so $\mathsf{D}(G) = 3$.

A finite abelian group $G$ can be uniquely decomposed as $G = C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_r}$, where $2 \leq n_1 \mid n_2 \mid \cdots \mid n_r$. Here $r$ is the rank of the group. Setting

$$\mathrm{D}^*(G) := 1 + \sum_{i=1}^{r}(n_i - 1),$$

we have the inequality $\mathrm{D}^*(G) \leq \mathrm{D}(G)$.

Question: For which abelian groups $G$ do we have $\mathrm{D}^*(G) = \mathrm{D}(G)$?

A finite abelian group $G$ can be uniquely decomposed as $G = C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_r}$, where $2 \leq n_1 \mid n_2 \mid \cdots \mid n_r$. Here $r$ is the rank of the group. Setting

$$\mathrm{D}^*(G) := 1 + \sum_{i=1}^{r}(n_i - 1),$$

we have the inequality $\mathrm{D}^*(G) \leq \mathrm{D}(G)$.

Question: For which abelian groups $G$ do we have $\mathrm{D}^*(G) = \mathrm{D}(G)$?

## Theorems ['69, Olson]

- If $\operatorname{rank}(G) = 2$ (i.e. $G = C_{n_1} \oplus C_{n_2}$ with $1 < n_1 \mid n_2$), then $\mathrm{D}(G) = n_2 + n_1 - 1$.
- If $G$ is a finite abelian p-group, then $\mathrm{D}(G) = 1 + \sum_{i=1}^{r}(n_i - 1) + 1$.

## Conjectures

- For the direct sum $C_n^r = C_n \oplus \ldots \oplus C_n$ ($r$ copies) we have: $\mathrm{D}(C_n^r) = 1 + (n-1)r$
- If $\operatorname{rank}(G) = 3$ (i.e. $G = C_{n_1} \oplus C_{n_2} \oplus C_{n_3}$), then $\mathrm{D}(G) = n_1 + n_2 + n_3 - 2$.

## Fact

For a finite abelian group $G$, $\mathbb{C}[V]^G$ has a generating set consisting of monomials.

## Corollary

For a finite abelian group $G$, the value of the Noether number coincides with the value of the Davenport constant (the maximal length of an irreducible zero-sum sequence over $G$):

$$\beta(G) = \mathrm{D}(G)$$

## Fact

For a finite abelian group $G$, $\mathbb{C}[V]^G$ has a generating set consisting of monomials.

## Corollary

For a finite abelian group $G$, the value of the Noether number coincides with the value of the Davenport constant (the maximal length of an irreducible zero-sum sequence over $G$):

$$\beta(G) = \mathrm{D}(G)$$

## Theorem ['17, Domokos]

For a finite abelian group $G$, the number $\beta_{\mathrm{sep}}(G)$ can be given with the language of zero-sum sequences.

## Theorem ['25+, S., Zhao, Zhong]

Let $G = C_{n_1} \oplus \ldots \oplus C_{n_r}$ with $1 < n_1 \mid n_2 \ldots n_{r-1} \mid n_r$ and $r \geq 2$. Suppose $\mathrm{D}(n_s G) = \mathrm{D}^*(n_s G)$, where $s = \lfloor \frac{r+1}{2} \rfloor$. Then

$$\begin{cases} \beta_{\mathrm{sep}}(G) = n_s + n_{s+1} + \ldots + n_r, & \text{if } r \text{ is odd} \\ \beta_{\mathrm{sep}}(G) \leq \frac{n_s}{p} + n_{s+1} + \ldots + n_r, & \text{if } r \text{ is even,} \end{cases}$$

where $p$ is the minimal prime divisor of $n_s$.

### Corollary ['25+, S., Zhao, Zhong]

Let $G = C_{n_1} \oplus \ldots \oplus C_{n_r}$ with $1 < n_1 \mid n_2 \ldots n_{r-1} \mid n_r$ and $r \geq 2$, and let $p$ be the minimal prime divisor of $n_s$. We have

$$\begin{cases} \beta_{\mathrm{sep}}(G) = n_s + n_{s+1} + \ldots + n_r, & \text{if } r \text{ is odd} \\ \beta_{\mathrm{sep}}(G) = \frac{n_s}{p} + n_{s+1} + \ldots + n_r, & \text{if } r \text{ is even,} \end{cases}$$

for the following infinite families of finite abelian groups:

- groups of rank $r \leq 5$,
- $p$-groups,
- groups of type $C_n^r$.

# Outline

**Proposition ['08, Dufresne]**

If $V$ is a $n$-dimensional representation of $G$, then a separating set of size $2n+1$ exists.

### Proposition ['08, Dufresne]

If $V$ is a $n$-dimensional representation of $G$, then a separating set of size $2n+1$ exists.

### Corollary ['24, Cahill, Contreras, Hip]

Let $G$ be a finite abelian group of rank $r$ and of order $n$. Then there exists a separating set of $\mathbb{C}[V_{\mathrm{reg}}]^G$ size $\sum_{i=1}^{\kappa(G)+1} \binom{n}{i}$ consisting of monomials.

## Proposition ['25+, S., Zhao, Zhong]

Let $C_n$ be the cyclic group of order $n$. The minimal size of a separating set of $\mathbb{C}[V_{\mathrm{reg}}]^{C_n}$ consisting of monomials is

$$n + \sum_{\substack{d|n \\ 1<d}} \frac{2^{\omega(d)}-2}{2}\phi(d),$$

where $\phi$ denotes the Euler totient function, and $\omega$ the number of distinct prime divisors.

## Proposition ['25+, S., Zhao, Zhong]

Let $C_n$ be the cyclic group of order $n$. The minimal size of a separating set of $\mathbb{C}[V_{\mathrm{reg}}]^{C_n}$ consisting of monomials is

$$n + \sum_{\substack{d|n \\ 1<d}} \frac{2^{\omega(d)}-2}{2}\phi(d),$$

where $\phi$ denotes the Euler totient function, and $\omega$ the number of distinct prime divisors.

## Proposition ['25+, S., Zhao, Zhong]

The size of a minimal separating set of $\mathbb{C}[V_{\mathrm{reg}}]^{C_p^k}$ consisting of monomials is

$$|S| = p^k + \frac{(p^k-1)(p-2)}{2} + \sum_{i=2}^{k} \frac{(p^k-1)(p^k-p)\dots(p^k-p^{i-1})(p-1)^i}{(i+1)!}$$

# Summarizing

**Question**

What is a sharp upper bound for the degrees of the separating invariants?

Answers for non-commutative groups:

- $|G| < 32$
- $G$ has a cyclic subgroup of index 2

Answers for abelian groups:

- $C_n^r$
- $\mathrm{rank}(G) \leq 5$
- $p$-groups

**Question**

What is a sharp lower bound for the size of a separating set?

-

- $\mathrm{rank}(G) = 1$
- elementary abelian $p$-groups

- M. Domokos, B. Schefler, The separating Noether number of small groups, https://doi.org/10.48550/arXiv.2412.08621
- B. Schefler, The separating Noether number of the direct sum of several copies of a cyclic group, Proc. Amer. Math. Soc. 153 (2025), 69–79.
- B. Schefler, The separating Noether number of abelian groups of rank two, J. Comb. Theory, Ser. A 209 (2025), Paper no. 105951.
- B., Schefler, K. Zhao, Q. Zhong, On the separating Noether number of finite abelian groups, Preprint, arXiv:2503.01296 [math.AC], (2025)
- B., Schefler, K. Zhao, Q. Zhong, On separating systems of polynomial invariants for finite abelian groups, Work in progress

Thank you for your attention!