Separating Noether number of abelian groups

Schefler Barna

Eötvös Loránd University, Budapest
joint work with Domokos Mátyás, Rényi Institute, Budapest

Conference on Rings and Factorizations 2023
July 10–14, 2023 in Graz

"Out of nothing, I have created a strange new universe"

- Bolyai János -

Outline

Outline

Noether number of a group

Notation

G will always stand for a finite group; V for a finite dimensional vectorspace over $\mathbb{C}$.

Noether number of a group

Notation

G will always stand for a finite group; V for a finite dimensional vectorspace over $\mathbb{C}$.

A G-module structure on V is defined by a representation $\rho : G \to GL(V)$ of G. Let $x_1, x_2, \ldots, x_n$ be a basis in the dual space V^*. The G-action on the polynomial algebra $\mathbb{C}[V] = \mathbb{C}[x_1, x_2, \ldots, x_n]$ is the following:

$$g \cdot f(x_1, x_2, \ldots, x_n) = f(gx_1, gx_2, \ldots, gx_n)$$

Noether number of a group

Notation

G will always stand for a finite group; V for a finite dimensional vectorspace over $\mathbb{C}$.

A G-module structure on V is defined by a representation $\rho : G \to GL(V)$ of G. Let $x_1, x_2, \dots, x_n$ be a basis in the dual space V^*. The G-action on the polynomial algebra $\mathbb{C}[V] = \mathbb{C}[x_1, x_2, \dots, x_n]$ is the following:

$$g \cdot f(x_1, x_2, \dots, x_n) = f(gx_1, gx_2, \dots, gx_n)$$

By the theorem of Noether, the invariant subalgebra:

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

is generated by homogeneous elements of degree at most $|G|$.

Noether number of a group

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* is:

$$\beta(G) := \sup_V \{\beta(G, V) : V \text{ is a fin dim rep of } G\}$$

Noether number of a group

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* is:

$$\beta(G) := \sup_V \{\beta(G, V) : V \text{ is a fin dim rep of } G\}$$

Remark

By the theorem of Noether, $\beta(G) \leq |G|$.

Noether number of a group

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* is:

$$\beta(G) := \sup_V \{\beta(G,V) : V \text{ is a fin dim rep of } G\}$$

Remark

By the theorem of Noether, $\beta(G) \leq |G|$.

Example

For a cyclic group $\beta(C_n) = n$. *Moreover, for any other group* $\beta(G) < |G|$.

Separating Noether number of a group

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

if for $v_1, v_2 \in V$ there exists $h \in \mathbb{C}[V]^G$ such that $h(v_1) \neq h(v_2)$, then there exists $f \in S$, such that $f(v_1) \neq f(v_2)$

Separating Noether number of a group

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

if for $v_1, v_2 \in V$ there exists $h \in \mathbb{C}[V]^G$ such that $h(v_1) \neq h(v_2)$, then there exists $f \in S$, such that $f(v_1) \neq f(v_2)$

For a *finite* group G, the following is true:

Remark

A subset $S \subset \mathbb{C}[V]^G$ is a separating system if and only if:
$f(v_1) = f(v_2)$ for each $f \in S$ implies $Gv_1 = Gv_2$.

Separating Noether number of a group

Let $\beta_{sep}(G, V)$ 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* $\beta_{sep}(G)$ is:

$$\beta_{sep}(G) := \sup_V \{\beta_{sep}(G, V) : V \text{ is a fin dim rep of } G\}$$

Separating Noether number of a group

Let $\beta_{sep}(G,V)$ 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* $\beta_{sep}(G)$ is:

$$\beta_{sep}(G) := \sup_V \{\beta_{sep}(G,V) : V \text{ is a fin dim rep of } G\}$$

Every generating system is a separating system, which yields that:

Remark

$\beta_{sep}(G) \leq \beta(G)$.

Separating Noether number of a group

Let $\beta_{sep}(G, V)$ 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* $\beta_{sep}(G)$ is:

$$\beta_{sep}(G) := \sup_V \{\beta_{sep}(G, V) : V \text{ is a fin dim rep of } G\}$$

Every generating system is a separating system, which yields that:

Remark

$\beta_{sep}(G) \leq \beta(G)$.

Example

$\beta_{sep}(C_n) = n$. *Moreover, for any other group* $\beta_{sep}(G) < |G|$.

Outline

Case of abelian groups

Question

Our goal is to determine the exact value of the separating Noether number of some infinite families of abelian groups.

Case of abelian groups

Question

Our goal is to determine the exact value of the separating Noether number of some infinite families of abelian groups.

This question is linked with the study of the zero-sum sequences over a finite abelian group. Take the subset $\{a_1, \dots, a_s\} \subset G$. Then

$$\mathcal{G}(a_1, \dots, a_s) := \{[m_1, \dots, m_s] \in \mathbb{Z}^s : \sum m_i a_i = 0 \in G\}$$

is a subgroup of $\mathbb{Z}^s$. It is true that $\mathcal{G}(a_1, \dots, a_s)$ is generated by the monoid

$$\mathcal{B}(a_1, \dots, a_s) := \mathbb{N}_0^n \cap \mathcal{G}(a_1, \dots, a_s)$$

Case of abelian groups

Question

Our goal is to determine the exact value of the separating Noether number of some infinite families of abelian groups.

This question is linked with the study of the zero-sum sequences over a finite abelian group. Take the subset $\{a_1, \dots, a_s\} \subset G$. Then

$$\mathcal{G}(a_1, \dots, a_s) := \{[m_1, \dots, m_s] \in \mathbb{Z}^s : \sum m_i a_i = 0 \in G\}$$

is a subgroup of $\mathbb{Z}^s$. It is true that $\mathcal{G}(a_1, \dots, a_s)$ is generated by the monoid

$$\mathcal{B}(a_1, \dots, a_s) := \mathbb{N}_0^n \cap \mathcal{G}(a_1, \dots, a_s)$$

If $\{a_1, \dots, a_n\} = G$, then we have the notation: $\mathcal{B}(a_1, \dots, a_n) := \mathcal{B}(G)$. For any subset $\{a_1, \dots, a_s\} \subset G$, we can interpret $\mathcal{B}(a_1, \dots, a_s)$ as a submonoid of $\mathcal{B}(G)$.

The Davenport constant

The *length* of $\mathrm{m} = [m_1, \ldots, m_n] \in \mathcal{B}(G)$ is: $|\mathrm{m}| = \sum_{i=1}^{n} m_i$.
$\mathrm{m} \in \mathcal{B}(G)$ is an *atom*, if it can not be written as the sum of two nonzero elements of $\mathcal{B}(G)$.
The *Davenport constant* of an abelian group is defined as:
$\mathrm{D}(G) := \max\{|\mathrm{m}| : \mathrm{m} \text{ is atom}\}$.

The Davenport constant

The *length* of $\mathrm{m} = [m_1, \dots, m_n] \in \mathcal{B}(G)$ is: $|\mathrm{m}| = \sum_{i=1}^{n} m_i$.
$\mathrm{m} \in \mathcal{B}(G)$ is an *atom*, if it can not be written as the sum of two nonzero elements of $\mathcal{B}(G)$.
The *Davenport constant* of an abelian group is defined as:
$\mathrm{D}(G) := \max\{|\mathrm{m}| : \mathrm{m} \text{ is atom}\}$.It is known that for an abelian group:

Lemma

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

The Davenport constant

The *length* of $\mathrm{m} = [m_1, ..., m_n] \in \mathcal{B}(G)$ is: $|\mathrm{m}| = \sum_{i=1}^{n} m_i$.
$\mathrm{m} \in \mathcal{B}(G)$ is an *atom*, if it can not be written as the sum of two nonzero elements of $\mathcal{B}(G)$.
The *Davenport constant* of an abelian group is defined as:
$\mathrm{D}(G) := \max\{|\mathrm{m}| : \mathrm{m} \text{ is atom}\}$.It is known that for an abelian group:

Lemma

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

Remark

$\beta(C_n) = \mathrm{D}(C_n) = n$. *For any generator* $g \in C_n$, $[n] \in \mathcal{B}(g)$ *is an atom of length* n.

Separating Noether number of an abelian group

An abelian group G can be written as: $G = C_{n_1} \times C_{n_2} \times ... \times C_{n_r}$ where $n_r \mid ... \mid n_2 \mid n_1$. Let g_i be a generator of C_{n_i}, and denote by $g := g_1 + ... + g_r$. Since $[n_1 - 1, n_2 - 1, ..., n_r - 1, 1] \in \mathcal{B}(g_1, g_2, ..., g_r, g)$ is an atom, we have:

$$1 + \sum_{i=1}^{r} (n_i - 1) \leq \mathrm{D}(G) \tag{1}$$

Separating Noether number of an abelian group

An abelian group G can be written as: $G = C_{n_1} \times C_{n_2} \times \ldots \times C_{n_r}$ where $n_r \mid \ldots \mid n_2 \mid n_1$. Let g_i be a generator of C_{n_i}, and denote by $g := g_1 + \ldots + g_r$. Since $[n_1 - 1, n_2 - 1, \ldots, n_r - 1, 1] \in \mathcal{B}(g_1, g_2, \ldots, g_r, g)$ is an atom, we have:

$$1 + \sum_{i=1}^{r} (n_i - 1) \leq \mathrm{D}(G) \tag{1}$$

Remark

$\beta(C_{n_1} \times C_{n_2}) = \mathrm{D}(C_{n_1} \times C_{n_2}) = n_1 + n_2 - 1.$
$\beta(C_{p^{n_1}} \times \ldots \times C_{p^{n_r}}) = \mathrm{D}(C_{p^{n_1}} \times \ldots \times C_{p^{n_r}}) = p^{n_1} + \ldots + p^{n_r} - (r-1).$

Separating Noether number of an abelian group

An abelian group G can be written as: $G = C_{n_1} \times C_{n_2} \times \ldots \times C_{n_r}$ where $n_r \mid \ldots \mid n_2 \mid n_1$. Let g_i be a generator of C_{n_i}, and denote by $g := g_1 + \ldots + g_r$. Since $[n_1 - 1, n_2 - 1, \ldots, n_r - 1, 1] \in \mathcal{B}(g_1, g_2, \ldots, g_r, g)$ is an atom, we have:

$$1 + \sum_{i=1}^{r}(n_i - 1) \leq \mathsf{D}(G) \tag{1}$$

Remark

$\beta(C_{n_1} \times C_{n_2}) = \mathsf{D}(C_{n_1} \times C_{n_2}) = n_1 + n_2 - 1.$
$\beta(C_{p^{n_1}} \times \ldots \times C_{p^{n_r}}) = \mathsf{D}(C_{p^{n_1}} \times \ldots \times C_{p^{n_r}}) = p^{n_1} + \ldots + p^{n_r} - (r-1).$

There are some infinite families of abelian groups for which the inequality is known to be strict. Beyond that, in general it is not known when equality holds.

Separating Noether number of an abelian group

Theorem (M. Domokos, 2017.)

For an abelian group G, $\beta_{sep}(G)$ is the minimal positive integer d such that for any positive integer $s \leq \mathrm{rank}(G) + 1$ and any finite sequence $a_1, \ldots, a_s$ of distinct elements of G the abelian group $\mathcal{G}(a_1, \ldots, a_s)$ is generated (as a group!) by $\{\mathrm{m} \in \mathcal{B}(a_1, \ldots, a_s) : |\mathrm{m}| \leq d\}$.

Separating Noether number of an abelian group

Theorem (M. Domokos, 2017.)

For an abelian group G, $\beta_{sep}(G)$ is the minimal positive integer d such that for any positive integer $s \leq \mathrm{rank}(G)+1$ and any finite sequence $a_1, \ldots, a_s$ of distinct elements of G the abelian group $\mathcal{G}(a_1, \ldots, a_s)$ is generated (as a group!) by $\{\mathrm{m} \in \mathcal{B}(a_1, \ldots, a_s) : |\mathrm{m}| \leq d\}$.

Definition

For an abelian group G, $\mathrm{m} \in \mathcal{B}(G)$ is called a group atom if it can not be written as an integral linear combination of elements of length $< |\mathrm{m}|$.

Separating Noether number of an abelian group

Theorem (M. Domokos, 2017.)

For an abelian group G, $\beta_{sep}(G)$ is the minimal positive integer d such that for any positive integer $s \leq rank(G)+1$ and any finite sequence $a_1, \ldots, a_s$ of distinct elements of G the abelian group $\mathcal{G}(a_1, \ldots, a_s)$ is generated (as a group!) by $\{\mathrm{m} \in \mathcal{B}(a_1, \ldots, a_s) : |\mathrm{m}| \leq d\}$.

Definition

For an abelian group G, $\mathrm{m} \in \mathcal{B}(G)$ is called a group atom if it can not be written as an integral linear combination of elements of length $< |\mathrm{m}|$.

$\mathrm{m} \in \mathcal{B}(G)$ is an atom, if it can not be written as the sum of two nonzero elements of $\mathcal{B}(G)$. The maximal length of an atom is by definition $\mathsf{D}(G)$ (and $\mathsf{D}(G) = \beta(G)$).

Separating Noether number of an abelian group

Theorem (M. Domokos, 2017.)

For an abelian group G, $\beta_{sep}(G)$ is the minimal positive integer d such that for any positive integer $s \leq \mathrm{rank}(G) + 1$ and any finite sequence $a_1, \ldots, a_s$ of distinct elements of G the abelian group $\mathcal{G}(a_1, \ldots, a_s)$ is generated (as a group!) by $\{\mathrm{m} \in \mathcal{B}(a_1, \ldots, a_s) : |\mathrm{m}| \leq d\}$.

Definition

For an abelian group G, $\mathrm{m} \in \mathcal{B}(G)$ is called a group atom if it can not be written as an integral linear combination of elements of length $< |\mathrm{m}|$.

Note that the maximal length of a group atom is by definition the separating Noether number of the given abelian group.

Outline

New results

Theorem

$\beta_{sep}(C_n \times C_n) = n(1 + \frac{1}{p})$, where p is the minimal prime divisor of n.

New results

Theorem

$\beta_{sep}(C_n \times C_n) = n(1+\frac{1}{p})$, *where p is the minimal prime divisor of n.*

Lemma

Let $G = C_{n_1} \times C_{n_2} \times \ldots \times C_{n_r}$, where $n_r | n_{r-1} | \ldots | n_1$. Suppose that p is a prime divisor of n_r. For $r = 2s-1$, $\beta_{sep}(G) \geq n_1 + \ldots + n_s$, while for $r = 2s$, $\beta_{sep}(G) \geq n_1 + \ldots + n_s + \frac{n_{s+1}}{p}$.

New results

Theorem

$$\beta_{sep}(C_n^k) = \begin{cases} ns, & \text{for } k = 2s-1 \\ ns + \frac{n}{p}, & \text{for } k = 2s \end{cases}, \text{ where } p \text{ is the minimal prime divisor of } n.$$

New results

Theorem

$$\beta_{sep}(C_n^k) = \begin{cases} ns, & \text{for } k = 2s-1 \\ ns + \frac{n}{p}, & \text{for } k = 2s \end{cases}, \text{ where } p \text{ is the minimal prime divisor of } n.$$

This result is interesting since $\beta(C_n^k)$ is not known. Now we see a family of groups for which the separating Noether number is known, but the Noether number is not.

New results

The previous Theorem is a special case of this more general result:

Lemma

Let $G = C_{n_1} \times \ldots \times C_{n_s} \times C_{n_{s+1}} \times \ldots \times C_{n_r}$, where $n_r | n_{r-1} | \ldots n_{s+1} | n_s = n_{s-1} = \ldots = n_1$. Let $n := n_1$, and suppose that the least prime divisor of n_{2s} and n is the same, say p. For $r = 2s - 1$, $\beta_{sep}(G) = sn_1$, while for $r = 2s$, $\beta_{sep}(G) = sn + \frac{n}{p}$.

New results

Lemma

Let $G = C_{p^{k_1}} \times \ldots \times C_{p^{k_r}}$ be a p-group.
For $r = 2s - 1$, $\beta_{sep}(C_{p^{k_1}} \times \ldots \times C_{p^{k_r}}) \geq p^{k_1} + \ldots + p^{k_s}$, while for $r = 2s$,
$\beta_{sep}(C_{p^{k_1}} \times \ldots \times C_{p^{k_r}}) \geq p^{k_1} + \ldots + p^{k_s} + p^{k_{s+1}-1}$.

New results

Lemma

Let $G = C_{p^{k_1}} \times \ldots \times C_{p^{k_r}}$ be a p-group.
For $r = 2s-1$, $\beta_{sep}(C_{p^{k_1}} \times \ldots \times C_{p^{k_r}}) \geq p^{k_1} + \ldots + p^{k_s}$, while for $r = 2s$, $\beta_{sep}(C_{p^{k_1}} \times \ldots \times C_{p^{k_r}}) \geq p^{k_1} + \ldots + p^{k_s} + p^{k_{s+1}-1}$.

Theorem

(i) $\beta_{sep}(C_{p^{k_1}} \times C_{p^{k_2}}) = p^{k_1} + p^{k_2-1}$, *where p is a prime.*

(ii) $\beta_{sep}(C_{p^{k_1}} \times C_{p^{k_2}} \times C_{p^{k_3}}) = p^{k_1} + p^{k_2}$, *where p is a prime.*

An example

Claim

Let $\mathcal{B}((1,0);(0,1);(1,\frac{p-1}{p}n)) \subset \mathcal{B}(C_n \times C_n)$ be denoted by $\mathcal{B}_0$. Then $[n-1, \frac{n}{p}, 1] \in \mathcal{B}_0$ is a group atom of length $n(1+\frac{1}{p})$.

An example

Claim

Let $\mathcal{B}((1,0);(0,1);(1,\frac{p-1}{p}n)) \subset \mathcal{B}(C_n \times C_n)$ be denoted by $\mathcal{B}_0$. Then $[n-1,\frac{n}{p},1] \in \mathcal{B}_0$ is a group atom of length $n(1+\frac{1}{p})$.

Outline of the proof. Atoms in which appear at least one 0 coordinate are: $[n,0,0]$, $[0,n,0]$, $[0,0,n]$, $[n-ip,0,ip]$ for $i \in \{1,2,...,\frac{n}{p}-1\}$. All the entries are divisible by p. If $m_i > 0$, then since $m_1+m_3 \equiv 0 \ (mod \ n)$ and $m_2 - m_3\frac{n}{p} \equiv 0 \ (mod \ n)$, we have $m_1+m_3 \geq n$ and $m_2 \geq \frac{n}{p}$. So $|\mathrm{m}| \geq n(1+\frac{1}{p})$. Of course, $|[n-1,\frac{n}{p},1]| = n(1+\frac{1}{p})$. If m is a linear combination of elements length strictly lower than $n(1+\frac{1}{p})$, then these elements must be among the previous ones. So all of their entries are divisible by p. Of course this holds for each linear combination of them. However, $[n-1,\frac{n}{p},1]$ has some entries not divisible by p. This contradiction shows that $[n-1,\frac{n}{p},1]$ is a group atom.

Bibliography

- M. Domokos, Degree bounds for separating invariants of abelian groups. Proceedings of the American Mathematical Society, 145:3695–3708, 2017.
- Weidong Gao and Alfred Geroldinger, Zero-sum problems in finite abelian groups: a survey, Expo. Math. 24 (2006), no. 4, 337–369, DOI 10.1016/j.exmath.2006.07.002. MR2313123
- E. Noether, Der Endlichketssatz der Invarianten endlicher Gruppen, Math. Ann. 77 (1916) 89-92.
- John E. Olson, A combinatorial problem on finite Abelian groups. I, J. Number Theory 1 (1969), 8–10. MR0237641
- John E. Olson, A combinatorial problem on finite Abelian groups. II, J. Number Theory 1 (1969), 195–199. MR0240200

Thank you for your attention!