Central nilpotency of skew braces

Marco Bonatto & Přemysl Jedlička

Department of Mathematics
Faculty of Engineering (former Technical Faculty)
Czech University of Life Sciences (former Czech University of Agriculture) in Prague

Będlewo, 11th July 2022

Faculty of Engineering

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Expanded group

Definition

An algebra (A, Ω) is called an *expanded group*, if there exist a binary operation $+$, a unary operation $-$ and a constant 0 such that the retract $(A, +, -, 0)$ is a group.

Definition

Let A be an expanded group. A polynomial $f(x_1, \ldots, x_k)$, with $k > 1$, is called *absorbing*, if, for all $1 \leqslant i \leqslant k$, and for all $a_j \in A$, with $1 \leqslant j \leqslant k$,

$$f(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_k) = 0.$$

Expanded group

Definition

An algebra (A, Ω) is called an *expanded group*, if there exist a binary operation $+$, a unary operation $-$ and a constant 0 such that the retract $(A, +, -, 0)$ is a group.

Definition

Let A be an expanded group. A polynomial $f(x_1, \ldots, x_k)$, with $k > 1$, is called *absorbing*, if, for all $1 \leqslant i \leqslant k$, and for all $a_j \in A$, with $1 \leqslant j \leqslant k$,

$$f(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_k) = 0.$$

Absorbing polynomials

Groups:

$$-x-y+x+y=[x,y]$$

$$[[x,y],z]$$

Rings:

$$x \cdot y$$

Vector spaces:

$$0x+0y+0z$$

Lie algebras:

$$[x,y]$$

Loops:

$$((x+y)+z)-(x+(y+z))$$

Absorbing polynomials

Groups:

$$-x-y+x+y=[x,y]$$
$$[[x,y],z]$$

Rings:

$$x\cdot y$$

Vector spaces:

$$0x+0y+0z$$

Lie algebras:

$$[x,y]$$

Loops:

$$((x+y)+z)-(x+(y+z))$$

Absorbing polynomials

Groups:

$$-x-y+x+y=[x,y]$$

$$[[x,y],z]$$

Rings:

$$x\cdot y$$

Vector spaces:

$$0x+0y+0z$$

Lie algebras:

$$[x,y]$$

Loops:

$$((x+y)+z)-(x+(y+z))$$

Absorbing polynomials

Groups:

$$-x-y+x+y=[x,y]$$
$$[[x,y],z]$$

Rings:

$$x\cdot y$$

Vector spaces:

$$0x+0y+0z$$

Lie algebras:

$$[x,y]$$

Loops:

$$((x+y)+z)-(x+(y+z))$$

Absorbing polynomials

Groups:

$$-x - y + x + y = [x, y]$$
$$[[x, y], z]$$

Rings:

$$x \cdot y$$

Vector spaces:

$$0x + 0y + 0z$$

Lie algebras:

$$[x, y]$$

Loops:

$$((x + y) + z) - (x + (y + z))$$

Absorbing polynomials

Groups:

$$-x-y+x+y=[x,y]$$
$$[[x,y],z]$$

Rings:

$$x\cdot y$$

Vector spaces:

$$0x+0y+0z$$

Lie algebras:

$$[x,y]$$

Loops:

$$((x+y)+z)-(x+(y+z))$$

Center

Definition

Let A be an expanded group. An element $c \in A$ is called *central* if, for all binary absorbing polynomial f and for all $a \in A$,

$$f(a,c) = f(c,a) = 0.$$

The *center* $Z(A)$ of A is the subset of all central elements of A.

Definition

An expanded group A is called *abelian* if $Z(A) = A$.

Center

Definition

Let A be an expanded group. An element $c \in A$ is called *central* if, for all binary absorbing polynomial f and for all $a \in A$,

$$f(a,c) = f(c,a) = 0.$$

The *center* $Z(A)$ of A is the subset of all central elements of A.

Definition

An expanded group A is called *abelian* if $Z(A) = A$.

Examples of centers

Groups:

$$Z(A) = \{c \mid \forall a \in A:\ a + c = c + a\}$$

Rings:

$$Z(A) = \{c \mid \forall a \in A:\ a \cdot c = c \cdot a = 0\} = \mathrm{Ann}_R(R)$$

Vector spaces:

$$Z(A) = A$$

Lie algebras:

$$Z(A) = \{c \mid \forall a \in A:\ [a, c] = 0\} = \mathrm{Rad}([,])$$

Loops:

$$Z(A) = \{c \mid \forall a, b \in A:\ a + c = c + a \;\&\; c + (a + b) = (c + a) + b\}$$

Examples of centers

Groups:

$$Z(A) = \{c \mid \forall a \in A:\ a + c = c + a\}$$

Rings:

$$Z(A) = \{c \mid \forall a \in A:\ a \cdot c = c \cdot a = 0\} = \mathrm{Ann}_R(R)$$

Vector spaces:

$$Z(A) = A$$

Lie algebras:

$$Z(A) = \{c \mid \forall a \in A:\ [a, c] = 0\} = \mathrm{Rad}([,])$$

Loops:

$$Z(A) = \{c \mid \forall a, b \in A:\ a + c = c + a \ \&\ c + (a + b) = (c + a) + b\}$$

Examples of centers

Groups:

$$Z(A) = \{c \mid \forall a \in A : \; a + c = c + a\}$$

Rings:

$$Z(A) = \{c \mid \forall a \in A : \; a \cdot c = c \cdot a = 0\} = \mathrm{Ann}_R(R)$$

Vector spaces:

$$Z(A) = A$$

Lie algebras:

$$Z(A) = \{c \mid \forall a \in A : \; [a, c] = 0\} = \mathrm{Rad}([,])$$

Loops:

$$Z(A) = \{c \mid \forall a, b \in A : \; a + c = c + a \;\&\; c + (a + b) = (c + a) + b\}$$

Examples of centers

Groups:

$$Z(A) = \{c \mid \forall a \in A: \ a + c = c + a\}$$

Rings:

$$Z(A) = \{c \mid \forall a \in A: \ a \cdot c = c \cdot a = 0\} = \mathrm{Ann}_R(R)$$

Vector spaces:

$$Z(A) = A$$

Lie algebras:

$$Z(A) = \{c \mid \forall a \in A: \ [a, c] = 0\} = \mathrm{Rad}([,])$$

Loops:

$$Z(A) = \{c \mid \forall a, b \in A: \ a + c = c + a \ \& \ c + (a + b) = (c + a) + b\}$$

Examples of centers

Groups:

$$Z(A) = \{c \mid \forall a \in A:\ a + c = c + a\}$$

Rings:

$$Z(A) = \{c \mid \forall a \in A:\ a \cdot c = c \cdot a = 0\} = \mathrm{Ann}_R(R)$$

Vector spaces:

$$Z(A) = A$$

Lie algebras:

$$Z(A) = \{c \mid \forall a \in A:\ [a, c] = 0\} = \mathrm{Rad}([,])$$

Loops:

$$Z(A) = \{c \mid \forall a, b \in A:\ a + c = c + a \ \&\ c + (a + b) = (c + a) + b\}$$

Nilpotency

Definition

A subalgebra I an expanded group A is called an *ideal* if there exists an endomorphism φ of A such that $\varphi(a) = 0$ if and only if $a \in I$.

Definition

An expanded group A is *nilpotent of class n* if there exists a chain of ideals

$$0 = I_0 \leqslant I_1 \leqslant \cdots \leqslant I_n = A,$$

such that $I_{j+1}/I_j \leqslant Z(A/I_j)$, for every $0 \leqslant j < n$.

Proposition

A commutative ring R is nilpotent of class n if and only if $R^{n+1} = 0$.

Nilpotency

Definition

A subalgebra I an expanded group A is called an *ideal* if there exists an endomorphism φ of A such that $\varphi(a) = 0$ if and only if $a \in I$.

Definition

An expanded group A is *nilpotent of class n* if there exists a chain of ideals

$$0 = I_0 \leqslant I_1 \leqslant \cdots \leqslant I_n = A,$$

such that $I_{j+1}/I_j \leqslant Z(A/I_j)$, for every $0 \leqslant j < n$.

Proposition

A commutative ring R is nilpotent of class n if and only if $R^{n+1} = 0$.

Nilpotency

Definition

A subalgebra I an expanded group A is called an *ideal* if there exists an endomorphism φ of A such that $\varphi(a) = 0$ if and only if $a \in I$.

Definition

An expanded group A is *nilpotent of class* n if there exists a chain of ideals

$$0 = I_0 \leqslant I_1 \leqslant \cdots \leqslant I_n = A,$$

such that $I_{j+1}/I_j \leqslant Z(A/I_j)$, for every $0 \leqslant j < n$.

Proposition

A commutative ring R is nilpotent of class n if and only if $R^{n+1} = 0$.

Absorbing polynomials of a skew brace

Definition

An algebra $(A, +, \circ, 0)$ is called a *skew brace* if

- $(A, +, 0)$ is a group
- $(A, \circ, 0)$ is a group
- $a \circ (b + c) = a \circ b - a + a \circ c$, for all $a, b, c \in A$.

We denote

$$x * y = -x + (x \circ y) - y$$

Observation

Absorbing polynomials for a skew brace are

- $[x, y]_+$,
- $[x, y]_\circ$,
- $x * y$,
- $y * x$.

Absorbing polynomials of a skew brace

Definition

An algebra $(A, +, \circ, 0)$ is called a *skew brace* if

- $(A, +, 0)$ is a group
- $(A, \circ, 0)$ is a group
- $a \circ (b + c) = a \circ b - a + a \circ c$, for all $a, b, c \in A$.

We denote

$$x * y = -x + (x \circ y) - y$$

Observation

Absorbing polynomials for a skew brace are

- $[x, y]_+$,
- $[x, y]_\circ$,
- $x * y$,
- $y * x$.

Absorbing polynomials of a skew brace

Definition

An algebra $(A,+,\circ,0)$ is called a *skew brace* if

- $(A,+,0)$ is a group
- $(A,\circ,0)$ is a group
- $a\circ(b+c)=a\circ b-a+a\circ c$, for all $a,b,c\in A$.

We denote

$$x*y=-x+(x\circ y)-y$$

Observation

Absorbing polynomials for a skew brace are

- $[x,y]_+$,
- $[x,y]_\circ$,
- $x*y$,
- $y*x$.

Center of a skew brace

Theorem (M. B. & P. J.)

Let B be a skew brace. Then

$$Z(B) = \{c \mid \forall a \in B:\ c + a = a + c = c \circ a = a \circ c\}.$$

Corollary

A skew brace B is abelian if and only if $(B, +)$ is an abelian group and $a + b = a \circ b$, for all $a, b \in B$.

Center of a skew brace

Theorem (M. B. & P. J.)

Let B be a skew brace. Then

$$Z(B) = \{c \mid \forall a \in B: \ c + a = a + c = c \circ a = a \circ c\}.$$

Corollary

A skew brace B is abelian if and only if $(B, +)$ is an abelian group and $a + b = a \circ b$, for all $a, b \in B$.

(Central) nilpotency of skew braces

Upper central series:

$$\zeta_0(B) = 0$$
$$\zeta_n(B) = \{c \mid \forall a \in A:\ c * a, a * c, [a,c]_+ \in \zeta_{n-1}(B)\}$$

Lower central series:

$$\Gamma_0(B) = B$$
$$\Gamma_n(B) = \langle \Gamma_{n-1}(B) * B, B * \Gamma_{n-1}(B), [\Gamma_{n-1}(B), B]_+ \rangle_+$$

(Central) nilpotency of skew braces

Upper central series:

$$\zeta_0(B) = 0$$
$$\zeta_n(B) = \{c \mid \forall a \in A : \; c * a, a * c, [a, c]_+ \in \zeta_{n-1}(B)\}$$

Lower central series:

$$\Gamma_0(B) = B$$
$$\Gamma_n(B) = \langle \Gamma_{n-1}(B) * B, B * \Gamma_{n-1}(B), [\Gamma_{n-1}(B), B]_+ \rangle_+$$

Other notions of nilpotency

Definitions (W. Rump; Ag. Smoktunowicz)

Let B be a skew brace. We define

$$B^1 = B, \qquad B^{n+1} = B * B^n,$$
$$B^{(1)} = B, \qquad B^{(n+1)} = B^{(n)} * B,$$
$$B^{[1]} = B, \qquad B^{[n+1]} = \left\langle \bigcup_{i=1}^{n} B^{[i]} * B^{[n+1-i]} \right\rangle_+ .$$

We say that B is

- *left nilpotent* if $B^n = 0$,
- *right nilpotent* if $B^{(n)} = 0$,
- *nilpotent* if $B^{[n]} = 0$,

for some $n \in \mathbb{N}$.

Relations among nilpotencies

Theorem (F. Cedó, T. Gateva-Ivanova, Ag. Smoktunowicz)

A brace is right nilpotent of class n if and only if its associated set-theoretic solution of Yang-Baxter equation is multipermutational of level n.

Proposition (M. B. & P. J.)

Let B be a skew brace. Then the following properties are equivalent:

- *B is centrally nilpotent,*
- *B is a nilpotent brace and $(B, \circ)$ is a nilpotent group,*
- *B is a right nilpotent brace and both $(B, \circ)$ and $(B, +)$ are nilpotent groups.*

Relations among nilpotencies

Theorem (F. Cedó, T. Gateva-Ivanova, Ag. Smoktunowicz)

A brace is right nilpotent of class n if and only if its associated set-theoretic solution of Yang-Baxter equation is multipermutational of level n.

Proposition (M. B. & P. J.)

Let B be a skew brace. Then the following properties are equivalent:

- *B is centrally nilpotent,*
- *B is a nilpotent brace and $(B, \circ)$ is a nilpotent group,*
- *B is a right nilpotent brace and both $(B, \circ)$ and $(B, +)$ are nilpotent groups.*

Commutator of ideals

Definition

Let A be an expanded group and let I, J be two ideals. We define the *commutator* of I, J as the ideal

$$[\![I, J]\!] = \langle f(a,b) \mid a \in I, b \in J, f \text{ absorbing} \rangle.$$

Groups:

$$[\![I, J]\!] = [I, J] = \{[a,b] \mid a \in I, b \in J\}$$

Lie algebras:

$$[\![I, J]\!] = [I, J] = \{[a,b] \mid a \in I, b \in J\}$$

Rings:

$$[\![I, J]\!] = IJ + JI$$

Commutator of ideals

Definition

Let A be an expanded group and let I, J be two ideals. We define the *commutator* of I, J as the ideal

$$[\![I, J]\!] = \langle f(a, b) \mid a \in I, b \in J, f \text{ absorbing} \rangle.$$

Groups:

$$[\![I, J]\!] = [I, J] = \{[a, b] \mid a \in I, b \in J\}$$

Lie algebras:

$$[\![I, J]\!] = [I, J] = \{[a, b] \mid a \in I, b \in J\}$$

Rings:

$$[\![I, J]\!] = IJ + JI$$

Commutator of ideals

Definition

Let A be an expanded group and let I, J be two ideals. We define the *commutator* of I, J as the ideal

$$[\![I, J]\!] = \langle f(a, b) \mid a \in I, b \in J, f \text{ absorbing} \rangle.$$

Groups:

$$[\![I, J]\!] = [I, J] = \{[a, b] \mid a \in I, b \in J\}$$

Lie algebras:

$$[\![I, J]\!] = [I, J] = \{[a, b] \mid a \in I, b \in J\}$$

Rings:

$$[\![I, J]\!] = IJ + JI$$

Commutator of ideals

Definition

Let A be an expanded group and let I, J be two ideals. We define the *commutator* of I, J as the ideal

$$[\![I, J]\!] = \langle f(a, b) \mid a \in I, b \in J, f \text{ absorbing} \rangle.$$

Groups:

$$[\![I, J]\!] = [I, J] = \{[a, b] \mid a \in I, b \in J\}$$

Lie algebras:

$$[\![I, J]\!] = [I, J] = \{[a, b] \mid a \in I, b \in J\}$$

Rings:

$$[\![I, J]\!] = IJ + JI$$

Commutator of ideals 2

In general, absorbing polynomials may contain constants from $A \setminus (I \cup J)$.

Loops:

$$[\![I, J]\!] = \langle (a+b) - (b+a),\\ ((a+b)+c) - (a+(b+c)),\\ (c+(b+a)) - ((c+b)+a),\\ \text{some other elements} \mid a \in I, b \in J, c \in A \rangle$$

Skew braces:

$$[\![I, J]\!] = \langle [a, b]_+, a * b, b * a \mid a \in I, b \in J \rangle_+ \text{ ???}$$

Commutator of ideals 2

In general, absorbing polynomials may contain constants from $A \setminus (I \cup J)$.

Loops:

$$\begin{aligned}[\![I,J]\!] = \langle &(a+b)-(b+a), \\ &((a+b)+c)-(a+(b+c)), \\ &(c+(b+a))-((c+b)+a), \\ &\text{some other elements} \mid a \in I, b \in J, c \in A\rangle\end{aligned}$$

Skew braces:

$$[\![I,J]\!] = \langle [a,b]_+, a*b, b*a \mid a \in I, b \in J\rangle_+ \text{ ???}$$

Commutator of ideals 2

In general, absorbing polynomials may contain constants from $A \setminus (I \cup J)$.

Loops:

$$\begin{aligned} [\![I,J]\!] = \langle & (a+b)-(b+a), \\ & ((a+b)+c)-(a+(b+c)), \\ & (c+(b+a))-((c+b)+a), \\ & \text{some other elements} \mid a \in I, b \in J, c \in A\rangle \end{aligned}$$

Skew braces:

$$[\![I,J]\!] = \langle [a,b]_+, a*b, b*a \mid a \in I, b \in J\rangle_+ \text{ ???}$$

Solvability

Definitions

Let A be an expanded group. We define

$$A_0 = A \qquad \text{and} \qquad A_{i+1} = [\![A_i, A]\!].$$

If there exists n such that $A_0 = 0$ then A is *nilpotent of class* n.

We define

$$A^{(0)} = A \qquad \text{and} \qquad A^{(i+1)} = [\![A^{(i)}, A^{(i)}]\!].$$

If there exists n such that $A_0 = 0$ then A is *solvable of class* n.

Solvability

Definitions

Let A be an expanded group. We define

$$A_0 = A \qquad \text{and} \qquad A_{i+1} = [\![A_i, A]\!].$$

If there exists n such that $A_0 = 0$ then A is *nilpotent of class* n.
We define

$$A^{(0)} = A \qquad \text{and} \qquad A^{(i+1)} = [\![A^{(i)}, A^{(i)}]\!].$$

If there exists n such that $A_0 = 0$ then A is *solvable of class* n.

Abelianess

Definition

An expanded group A is called *abelian* if $[\![A, A]\!] = 0$.

Definition

Let A be an expanded group and let I be an ideal of A. Then we say that *I is abelian in A* if $[\![I, I]\!] = 0$.

Definition

An expanded group A is *solvable of class n* if there exists a chain of ideals

$$0 = I_0 \leqslant I_1 \leqslant \cdots \leqslant I_n = A,$$

such that I_{j+1}/I_j is an abelian ideal in A/I_j, for every $0 \leqslant j < n$.

Abelianess

Definition

An expanded group A is called *abelian* if $[\![A, A]\!] = 0$.

Definition

Let A be an expanded group and let I be an ideal of A. Then we say that I *is abelian in* A if $[\![I, I]\!] = 0$.

Definition

An expanded group A is *solvable of class* n if there exists a chain of ideals

$$0 = I_0 \leqslant I_1 \leqslant \cdots \leqslant I_n = A,$$

such that I_{j+1}/I_j is an abelian ideal in A/I_j, for every $0 \leqslant j < n$.

Abelianess

Definition

An expanded group A is called *abelian* if $[\![A,A]\!] = 0$.

Definition

Let A be an expanded group and let I be an ideal of A. Then we say that I *is abelian in* A if $[\![I,I]\!] = 0$.

Definition

An expanded group A is *solvable of class* n if there exists a chain of ideals

$$0 = I_0 \leqslant I_1 \leqslant \cdots \leqslant I_n = A,$$

such that I_{j+1}/I_j is an abelian ideal in A/I_j, for every $0 \leqslant j < n$.

Supernilpotency

Definition

An expanded group A is called *supernilpotent of class n* if every $(n+1)$-ary absorbing polynomial is constant.

Theorem (E. Aichinger & J. Ecker)

A group is supernilpotent of class n if and only if it is nilpotent of class n.

Theorem (E. Aichinger & N. Mudrinski)

Every supernilpotent expanded group is nilpotent.

Theorem

Every finite supernilpotent expanded group is a product of expanded p-groups.

Supernilpotency

Definition

An expanded group A is called *supernilpotent of class n* if every $(n+1)$-ary absorbing polynomial is constant.

Theorem (E. Aichinger & J. Ecker)

A group is supernilpotent of class n if and only if it is nilpotent of class n.

Theorem (E. Aichinger & N. Mudrinski)

Every supernilpotent expanded group is nilpotent.

Theorem

Every finite supernilpotent expanded group is a product of expanded p-groups.

Supernilpotency

Definition

An expanded group A is called *supernilpotent of class n* if every $(n+1)$-ary absorbing polynomial is constant.

Theorem (E. Aichinger & J. Ecker)

A group is supernilpotent of class n if and only if it is nilpotent of class n.

Theorem (E. Aichinger & N. Mudrinski)

Every supernilpotent expanded group is nilpotent.

Theorem

Every finite supernilpotent expanded group is a product of expanded p-groups.

Supernilpotency

Definition

An expanded group A is called *supernilpotent of class n* if every $(n+1)$-ary absorbing polynomial is constant.

Theorem (E. Aichinger & J. Ecker)

A group is supernilpotent of class n if and only if it is nilpotent of class n.

Theorem (E. Aichinger & N. Mudrinski)

Every supernilpotent expanded group is nilpotent.

Theorem

Every finite supernilpotent expanded group is a product of expanded p-groups.