

Higher Commutators in Mal'cev Algebras— Properties and Applications

Erhard Aichinger, Nebojša Mudrinski

Department of Algebra
Johannes Kepler University Linz

July 16-20th, 2007, Szeged, Hungary

Outline

- 1 Introduction
- 2 Ternary Case
- 3 n-ary Case
- 4 Some Properties in Mal'cev Algebras
- 5 DEF Construction
- 6 Main Result

Some Known Results

E. Aichinger, P. Mayr

For different primes p, q there are precisely 17 clones on \mathbb{Z}_{pq} that contain the addition of \mathbb{Z}_{pq} and all constant operations.

Idziak's Conjecture

For a square-free natural number n , there are only finitely many polynomially inequivalent expansions of $\langle \mathbb{Z}_n, + \rangle$.

Some Known Results

E. Aichinger, P. Mayr

For different primes p, q there are precisely 17 clones on \mathbb{Z}_{pq} that contain the addition of \mathbb{Z}_{pq} and all constant operations.

Idziak's Conjecture

For a square-free natural number n , there are only finitely many polynomially inequivalent expansions of $\langle \mathbb{Z}_n, + \rangle$.

Some Known Results

A. Bulatov

There are countably many clones on $\mathbb{Z}_p \times \mathbb{Z}_p$ that contain $f(x, y, z) = x - y + z$ and all constant operations.

P. Idziak

For $|A| \geq 4$ there are infinitely many clones on A that contain a ternary Mal'cev operation.

Some Known Results

A. Bulatov

There are countably many clones on $\mathbb{Z}_p \times \mathbb{Z}_p$ that contain $f(x, y, z) = x - y + z$ and all constant operations.

P. Idziak

For $|A| \geq 4$ there are infinitely many clones on A that contain a ternary Mal'cev operation.

Our Goal

Question 1

Is there a finite set A such that there are uncountably many clones on A that contain a Mal'cev operation?

Question 2

Given a finite algebra \mathbf{A} with Mal'cev operation, is there an $n \in \mathbb{N}$ such that the following is true: if a function f preserves all n -ary relations that are invariant under all polynomial functions, then f is a polynomial function.

Our Goal

Question 1

Is there a finite set A such that there are uncountably many clones on A that contain a Mal'cev operation?

Question 2

Given a finite algebra \mathbf{A} with Mal'cev operation, is there an $n \in \mathbb{N}$ such that the following is true: if a function f preserves all n -ary relations that are invariant under all polynomial functions, then f is a polynomial function.

Expanded Groups

Ternary commutator ideal

If $A, B, C \in \text{Id } \mathbf{V}$, $\mathbf{V} = \langle V, +, F \rangle$ then the ideal $[A, B, C]$ is generated by the set

$$\{p(a, b, c) \mid a \in A, b \in B, c \in C, p \in \text{Pol}_3 \mathbf{V}$$

such that $p(x, y, z) = 0$ whenever $x = 0 \vee y = 0 \vee z = 0\}$.

Some properties

- $[A, [B, C]] \leq [A, B, C]$
- $[A, [B, C]] \neq [A, B, C]$,

Example: $[V, [V, V]] \neq [V, V, V]$ for $\mathbf{V} = \langle \mathbb{Z}_4, +, 2xyz \rangle$

Expanded Groups

Ternary commutator ideal

If $A, B, C \in \text{Id } \mathbf{V}$, $\mathbf{V} = \langle V, +, F \rangle$ then the ideal $[A, B, C]$ is generated by the set

$$\{p(a, b, c) \mid a \in A, b \in B, c \in C, p \in \text{Pol}_3 \mathbf{V}$$

such that $p(x, y, z) = 0$ whenever $x = 0 \vee y = 0 \vee z = 0\}$.

Some properties

- $[A, [B, C]] \leq [A, B, C]$
- $[A, [B, C]] \neq [A, B, C]$,

Example: $[V, [V, V]] \neq [V, V, V]$ for $\mathbf{V} = \langle \mathbb{Z}_4, +, 2xyz \rangle$

Expanded Groups

Ternary commutator ideal

If $A, B, C \in \text{Id } \mathbf{V}$, $\mathbf{V} = \langle V, +, F \rangle$ then the ideal $[A, B, C]$ is generated by the set

$$\{p(a, b, c) \mid a \in A, b \in B, c \in C, p \in \text{Pol}_3 \mathbf{V}$$

such that $p(x, y, z) = 0$ whenever $x = 0 \vee y = 0 \vee z = 0\}$.

Some properties

- $[A, [B, C]] \leq [A, B, C]$

- $[A, [B, C]] \neq [A, B, C]$,

Example: $[V, [V, V]] \neq [V, V, V]$ for $\mathbf{V} = \langle \mathbb{Z}_4, +, 2xyz \rangle$

Expanded Groups

Ternary commutator ideal

If $A, B, C \in \text{Id } \mathbf{V}$, $\mathbf{V} = \langle V, +, F \rangle$ then the ideal $[A, B, C]$ is generated by the set

$$\{p(a, b, c) \mid a \in A, b \in B, c \in C, p \in \text{Pol}_3 \mathbf{V}$$

such that $p(x, y, z) = 0$ whenever $x = 0 \vee y = 0 \vee z = 0\}$.

Some properties

- $[A, [B, C]] \leq [A, B, C]$
- $[A, [B, C]] \neq [A, B, C]$,

Example: $[V, [V, V]] \neq [V, V, V]$ for $\mathbf{V} = \langle \mathbb{Z}_4, +, 2xyz \rangle$

Bulatov's Definition

Definition (Ternary centralizer)

Let \mathbf{A} be an algebra and $\alpha, \beta, \gamma, \eta$ be congruences of \mathbf{A} . Then we say that α, β centralize γ modulo η if for every polynomial $f(\mathbf{x}, \mathbf{y}, \mathbf{z})$ and $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{u}, \mathbf{v}$ vectors from \mathbf{A} such that: $\mathbf{a} \equiv \mathbf{b} \pmod{\alpha}$, $\mathbf{c} \equiv \mathbf{d} \pmod{\beta}$, $\mathbf{u} \equiv \mathbf{v} \pmod{\gamma}$ and

$$\begin{aligned} f(\mathbf{a}, \mathbf{c}, \mathbf{u}) &\equiv f(\mathbf{a}, \mathbf{c}, \mathbf{v}) \pmod{\eta} \\ f(\mathbf{a}, \mathbf{d}, \mathbf{u}) &\equiv f(\mathbf{a}, \mathbf{d}, \mathbf{v}) \pmod{\eta} \\ f(\mathbf{b}, \mathbf{c}, \mathbf{u}) &\equiv f(\mathbf{b}, \mathbf{c}, \mathbf{v}) \pmod{\eta}, \end{aligned}$$

we have $f(\mathbf{b}, \mathbf{d}, \mathbf{u}) \equiv f(\mathbf{b}, \mathbf{d}, \mathbf{v}) \pmod{\eta}$.

Bulatov's Definition $[\alpha, \beta, \gamma]$

Definition (Ternary commutator)

$[\alpha, \beta, \gamma] :=$ the smallest congruence η such that $C(\alpha, \beta, \gamma; \eta)$.

Expanded Groups

Higher commutator ideal

If $A_1, \dots, A_n \in \text{Id } \mathbf{V}$, $\mathbf{V} = \langle V, +, F \rangle$ then $[A_1, \dots, A_n]$ is generated by the set

$$\{p(a_1, \dots, a_n) \mid a_i \in A_i, 1 \leq i \leq n, p \in \text{Pol}_n \mathbf{V}$$

such that $p(x_1, \dots, x_n) = 0$ whenever $\exists i$ such that $x_i = 0\}$.

Bulatov's Definition $C(\alpha_1, \dots, \alpha_n; \eta)$

Definition (Higher centralizer)

Let \mathbf{A} be an algebra, $\alpha_1, \dots, \alpha_n, \eta \in \text{Con } \mathbf{A}$. Then we say that $\alpha_1, \dots, \alpha_{n-1}$ centralize α_n modulo η if for all polynomials $f(\mathbf{x}_1, \dots, \mathbf{x}_n)$ and $\mathbf{a}_1, \dots, \mathbf{a}_{n-1}, \mathbf{b}_1, \dots, \mathbf{b}_{n-1}, \mathbf{u}, \mathbf{v}$ vectors from \mathbf{A} such that: $\mathbf{a}_i \equiv \mathbf{b}_i \pmod{\alpha_i}$, $1 \leq i \leq n$, $\mathbf{u} \equiv \mathbf{v} \pmod{\alpha_n}$ and

$$f(\mathbf{x}_1, \dots, \mathbf{x}_{n-1}, \mathbf{u}) \equiv f(\mathbf{x}_1, \dots, \mathbf{x}_{n-1}, \mathbf{v}) \pmod{\eta},$$

for all $(\mathbf{x}_1, \dots, \mathbf{x}_{n-1}) \in \{\mathbf{a}_1, \mathbf{b}_1\} \times \dots \times \{\mathbf{a}_{n-1}, \mathbf{b}_{n-1}\}$ and $(\mathbf{x}_1, \dots, \mathbf{x}_{n-1}) \neq (\mathbf{b}_1, \dots, \mathbf{b}_{n-1})$, we have

$$f(\mathbf{b}_1, \dots, \mathbf{b}_{n-1}, \mathbf{u}) \equiv f(\mathbf{b}_1, \dots, \mathbf{b}_{n-1}, \mathbf{v}) \pmod{\eta}.$$

Bulatov's Definition $[\alpha_1, \dots, \alpha_n]$

Definition (Higher commutator)

$[\alpha_1, \dots, \alpha_n] :=$ the smallest congruence η such that $\mathcal{C}(\alpha_1, \dots, \alpha_n; \eta)$.

Bulatov's Properties

Theorem

A an arbitrary algebra and $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \text{Con } \mathbf{A}$

- 1 $[\alpha_1, \dots, \alpha_n] \leq \bigwedge_{i=1}^n \alpha_i$
- 2 $\alpha_1 \leq \beta_1, \dots, \alpha_n \leq \beta_n \Rightarrow [\alpha_1, \dots, \alpha_n] \leq [\beta_1, \dots, \beta_n]$
- 3 $[\alpha_1, \dots, \alpha_n] \leq [\alpha_1, \dots, \alpha_{n-1}]$

Claim

If **A** is in congruence modular variety and π any permutation of the set $\{1, \dots, n\}$ then

$$[\alpha_1, \dots, \alpha_n] = [\alpha_{\pi(1)}, \dots, \alpha_{\pi(n)}].$$

Bulatov's Properties

Theorem

A an arbitrary algebra and $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \text{Con } \mathbf{A}$

- 1 $[\alpha_1, \dots, \alpha_n] \leq \bigwedge_{i=1}^n \alpha_i$
- 2 $\alpha_1 \leq \beta_1, \dots, \alpha_n \leq \beta_n \Rightarrow [\alpha_1, \dots, \alpha_n] \leq [\beta_1, \dots, \beta_n]$
- 3 $[\alpha_1, \dots, \alpha_n] \leq [\alpha_1, \dots, \alpha_{n-1}]$

Claim

If **A** is in congruence modular variety and π any permutation of the set $\{1, \dots, n\}$ then

$$[\alpha_1, \dots, \alpha_n] = [\alpha_{\pi(1)}, \dots, \alpha_{\pi(n)}].$$

Bulatov's Properties

Theorem

A an arbitrary algebra and $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \text{Con } \mathbf{A}$

- 1 $[\alpha_1, \dots, \alpha_n] \leq \bigwedge_{i=1}^n \alpha_i$
- 2 $\alpha_1 \leq \beta_1, \dots, \alpha_n \leq \beta_n \Rightarrow [\alpha_1, \dots, \alpha_n] \leq [\beta_1, \dots, \beta_n]$
- 3 $[\alpha_1, \dots, \alpha_n] \leq [\alpha_1, \dots, \alpha_{n-1}]$

Claim

If **A** is in congruence modular variety and π any permutation of the set $\{1, \dots, n\}$ then

$$[\alpha_1, \dots, \alpha_n] = [\alpha_{\pi(1)}, \dots, \alpha_{\pi(n)}].$$

Bulatov's Properties

Theorem

A an arbitrary algebra and $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \text{Con } \mathbf{A}$

- 1 $[\alpha_1, \dots, \alpha_n] \leq \bigwedge_{i=1}^n \alpha_i$
- 2 $\alpha_1 \leq \beta_1, \dots, \alpha_n \leq \beta_n \Rightarrow [\alpha_1, \dots, \alpha_n] \leq [\beta_1, \dots, \beta_n]$
- 3 $[\alpha_1, \dots, \alpha_n] \leq [\alpha_1, \dots, \alpha_{n-1}]$

Claim

If **A** is in congruence modular variety and π any permutation of the set $\{1, \dots, n\}$ then

$$[\alpha_1, \dots, \alpha_n] = [\alpha_{\pi(1)}, \dots, \alpha_{\pi(n)}].$$

Bulatov's Properties

Theorem

A an arbitrary algebra and $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \text{Con } \mathbf{A}$

- 1 $[\alpha_1, \dots, \alpha_n] \leq \bigwedge_{i=1}^n \alpha_i$
- 2 $\alpha_1 \leq \beta_1, \dots, \alpha_n \leq \beta_n \Rightarrow [\alpha_1, \dots, \alpha_n] \leq [\beta_1, \dots, \beta_n]$
- 3 $[\alpha_1, \dots, \alpha_n] \leq [\alpha_1, \dots, \alpha_{n-1}]$

Claim

If **A** is in congruence modular variety and π any permutation of the set $\{1, \dots, n\}$ then

$$[\alpha_1, \dots, \alpha_n] = [\alpha_{\pi(1)}, \dots, \alpha_{\pi(n)}].$$

Improvement of Bulatov's Definition

Theorem

Let \mathbf{A} be an algebra, $\alpha_1, \dots, \alpha_n, \eta$ be congruences of \mathbf{A} . Then $C(\alpha_1, \dots, \alpha_n; \eta)$ if for every $f \in \text{Pol}_n \mathbf{A}$ and $a_1, \dots, a_{n-1}, b_1, \dots, b_{n-1}, u, v \in A$ such that: $a_i \equiv b_i \pmod{\alpha_i}$, $1 \leq i \leq n$, $u \equiv v \pmod{\alpha_n}$ and

$$f(x_1, \dots, x_{n-1}, u) \equiv f(x_1, \dots, x_{n-1}, v) \pmod{\eta},$$

for all $(x_1, \dots, x_{n-1}) \in \{a_1, b_1\} \times \dots \times \{a_{n-1}, b_{n-1}\}$ and $(x_1, \dots, x_{n-1}) \neq (b_1, \dots, b_{n-1})$, then we have

$$f(b_1, \dots, b_{n-1}, u) \equiv f(b_1, \dots, b_{n-1}, v) \pmod{\eta}.$$

Some Properties of Higher commutators

Theorem

- $[\alpha_0, \dots, \alpha_k] \leq \eta$ iff $C(\alpha_0, \dots, \alpha_k; \eta)$
- If $\eta \leq \alpha_0, \dots, \alpha_k$, then
$$[\alpha_0/\eta, \dots, \alpha_k/\eta] = ([\alpha_0, \dots, \alpha_k] \vee \eta)/\eta$$
- $\bigvee_{i \in I} [\alpha_0, \dots, \alpha_{j-1}, \rho_i, \alpha_{j+1}, \dots, \alpha_k] =$
 $[\alpha_0, \dots, \alpha_{j-1}, \bigvee_{i \in I} \rho_i, \alpha_{j+1}, \dots, \alpha_k].$
- $[\alpha_0, [\alpha_1, \dots, \alpha_k]] \leq [\alpha_0, \alpha_1, \dots, \alpha_k].$

Some Properties of Higher commutators

Theorem

- $[\alpha_0, \dots, \alpha_k] \leq \eta$ iff $\mathbf{C}(\alpha_0, \dots, \alpha_k; \eta)$
- If $\eta \leq \alpha_0, \dots, \alpha_k$, then
$$[\alpha_0/\eta, \dots, \alpha_k/\eta] = ([\alpha_0, \dots, \alpha_k] \vee \eta)/\eta$$
- $\bigvee_{i \in I} [\alpha_0, \dots, \alpha_{j-1}, \rho_i, \alpha_{j+1}, \dots, \alpha_k] =$
 $[\alpha_0, \dots, \alpha_{j-1}, \bigvee_{i \in I} \rho_i, \alpha_{j+1}, \dots, \alpha_k].$
- $[\alpha_0, [\alpha_1, \dots, \alpha_k]] \leq [\alpha_0, \alpha_1, \dots, \alpha_k].$

Some Properties of Higher commutators

Theorem

- $[\alpha_0, \dots, \alpha_k] \leq \eta$ iff $C(\alpha_0, \dots, \alpha_k; \eta)$
- If $\eta \leq \alpha_0, \dots, \alpha_k$, then

$$[\alpha_0/\eta, \dots, \alpha_k/\eta] = ([\alpha_0, \dots, \alpha_k] \vee \eta)/\eta$$
- $\bigvee_{i \in I} [\alpha_0, \dots, \alpha_{j-1}, \rho_i, \alpha_{j+1}, \dots, \alpha_k] =$
 $[\alpha_0, \dots, \alpha_{j-1}, \bigvee_{i \in I} \rho_i, \alpha_{j+1}, \dots, \alpha_k].$
- $[\alpha_0, [\alpha_1, \dots, \alpha_k]] \leq [\alpha_0, \alpha_1, \dots, \alpha_k].$

Some Properties of Higher commutators

Theorem

- $[\alpha_0, \dots, \alpha_k] \leq \eta$ iff $C(\alpha_0, \dots, \alpha_k; \eta)$
- If $\eta \leq \alpha_0, \dots, \alpha_k$, then

$$[\alpha_0/\eta, \dots, \alpha_k/\eta] = ([\alpha_0, \dots, \alpha_k] \vee \eta)/\eta$$
- $\bigvee_{i \in I} [\alpha_0, \dots, \alpha_{j-1}, \rho_i, \alpha_{j+1}, \dots, \alpha_k] =$
 $[\alpha_0, \dots, \alpha_{j-1}, \bigvee_{i \in I} \rho_i, \alpha_{j+1}, \dots, \alpha_k].$
- $[\alpha_0, [\alpha_1, \dots, \alpha_k]] \leq [\alpha_0, \alpha_1, \dots, \alpha_k].$

Some Properties of Higher commutators

Theorem

- $[\alpha_0, \dots, \alpha_k] \leq \eta$ iff $C(\alpha_0, \dots, \alpha_k; \eta)$
- If $\eta \leq \alpha_0, \dots, \alpha_k$, then

$$[\alpha_0/\eta, \dots, \alpha_k/\eta] = ([\alpha_0, \dots, \alpha_k] \vee \eta)/\eta$$
- $\bigvee_{i \in I} [\alpha_0, \dots, \alpha_{j-1}, \rho_i, \alpha_{j+1}, \dots, \alpha_k] =$
 $[\alpha_0, \dots, \alpha_{j-1}, \bigvee_{i \in I} \rho_i, \alpha_{j+1}, \dots, \alpha_k].$
- $[\alpha_0, [\alpha_1, \dots, \alpha_k]] \leq [\alpha_0, \alpha_1, \dots, \alpha_k].$

A Description of the Commutator

Theorem

$[\alpha_0, \dots, \alpha_n]$ is generated by

$\{(c(b_0, \dots, b_n), c(a_0, \dots, a_n)) \mid b_0, \dots, b_n, a_0, \dots, a_n \in \mathbf{A}, b_i \equiv_{\alpha_i} a_i, \\ c \in \text{Pol } \mathbf{A}, c(x_0, \dots, x_n) = c(a_0, \dots, a_n) \text{ if } \exists i \text{ such that } x_i = a_i\}.$

Theorem (For principal congruences)

$\alpha_i = \Theta_{\mathbf{A}} \langle (a_i, b_i) \rangle, 0 \leq i \leq n.$

$[\alpha_0, \dots, \alpha_n] = \{(c(b_0, \dots, b_n), c(a_0, \dots, a_n)) \mid$

$c \in \text{Pol } \mathbf{A}, c(x_0, \dots, x_n) = c(a_0, \dots, a_n) \text{ if } \exists i \text{ such that } x_i = a_i\}.$

A Description of the Commutator

Theorem

$[\alpha_0, \dots, \alpha_n]$ is generated by

$\{(c(b_0, \dots, b_n), c(a_0, \dots, a_n)) \mid b_0, \dots, b_n, a_0, \dots, a_n \in \mathbf{A}, b_i \equiv_{\alpha_i} a_i, c \in \text{Pol } \mathbf{A}, c(x_0, \dots, x_n) = c(a_0, \dots, a_n) \text{ if } \exists i \text{ such that } x_i = a_i\}$.

Theorem (For principal congruences)

$\alpha_i = \Theta_{\mathbf{A}} \langle (a_i, b_i) \rangle, 0 \leq i \leq n$.

$[\alpha_0, \dots, \alpha_n] = \{(c(b_0, \dots, b_n), c(a_0, \dots, a_n)) \mid$

$c \in \text{Pol } \mathbf{A}, c(x_0, \dots, x_n) = c(a_0, \dots, a_n) \text{ if } \exists i \text{ such that } x_i = a_i\}$.

Two Important Properties

Theorem

If

$$\underbrace{[1, \dots, 1]}_n > 0$$

then $\exists c \in \text{Pol}_n \mathbf{A}$ and $\theta, \theta_0, \dots, \theta_{n-1} \in \mathbf{A}$ such that
 $c(x_0, \dots, x_{n-1}) = \theta$ whenever $\exists i : x_i = \theta_i$, and
 $\exists (a_0, \dots, a_{n-1}) \in \mathbf{A}^n$ such that $c(a_0, \dots, a_{n-1}) \neq \theta$.

Theorem

If $\underbrace{[1, \dots, 1]}_n = 0$, then $\langle \text{Pol}_{n-1} \mathbf{A} \cup \{m\} \rangle = \text{Pol } \mathbf{A}$.

Two Important Properties

Theorem

If

$$\underbrace{[1, \dots, 1]}_n > 0$$

then $\exists c \in \text{Pol}_n \mathbf{A}$ and $\theta, \theta_0, \dots, \theta_{n-1} \in A$ such that $c(x_0, \dots, x_{n-1}) = \theta$ whenever $\exists i : x_i = \theta_i$, and $\exists (a_0, \dots, a_{n-1}) \in A^n$ such that $c(a_0, \dots, a_{n-1}) \neq \theta$.

Theorem

If $\underbrace{[1, \dots, 1]}_n = 0$, then $\langle \text{Pol}_{n-1} \mathbf{A} \cup \{m\} \rangle = \text{Pol } \mathbf{A}$.

Example For One Proof

$$\begin{aligned}
 & D_{\rho(b_0, b_1, a_2), (a_0, a_1)}^{(2)} (E_{x_2}^{(2)} (F_{\rho(b_0, b_1, a_2), a_2}(\rho)))(x_0, x_1) = \\
 & m \left(\begin{array}{c} m \left(\begin{array}{c} \rho(x_0, x_1, x_2) \\ \rho(x_0, x_1, a_2) \\ \rho(b_0, b_1, a_2) \end{array} \right), m \left(\begin{array}{c} \rho(a_0, x_1, x_2) \\ \rho(a_0, x_1, a_2) \\ \rho(b_0, b_1, a_2) \end{array} \right), \rho(b_0, b_1, a_2) \\ \\ m \left(\begin{array}{c} \rho(x_0, a_1, x_2) \\ \rho(x_0, a_1, a_2) \\ \rho(b_0, b_1, a_2) \end{array} \right), m \left(\begin{array}{c} \rho(a_0, a_1, x_2) \\ \rho(a_0, a_1, a_2) \\ \rho(b_0, b_1, a_2) \end{array} \right) \rho(b_0, b_1, a_2) \\ \\ \rho(b_0, b_1, a_2) \end{array} \right)
 \end{aligned}$$

One Partial Solution

Theorem

Let \mathbf{A} be a finite Mal'cev algebra with congruence lattice of height two. Then there is an $n \in \mathbb{N}$ such that: if a function f preserves all n -ary relations that are invariant under all polynomial functions, then f is a polynomial function.