University of Novi Sad
Faculty of Sciences
Department of Mathematics and Informatics

Nebojša Mudrinski

On Polynomials in Mal'cev Algebras

Doctoral dissertation

Novi Sad, 2009

Contents

Foreword

In this dissertation, we investigate polynomial functions on finite Mal'cev algebras. Mal'cev algebras are a special class of universal algebras that contains many well known classes of algebras such as groups and rings.

In general it is a difficult task to describe which functions on a given universal algebra are polynomials. We know a list of properties that are satisfied by polynomial functions: each polynomial function preserves all congruence relations; furthermore, if a polynomial function is added to an algebra as an additional fundamental operation, then the commutator operation of the new expanded algebra is the same as the commutator operation of the original algebra. In [**22**], the following natural problem is proposed: given such a list of properties, characterize those algebras in which every function that satisfies all of these properties is a polynomial function. One instance is the characterization of affine complete algebras. An algebra is called affine complete if every congruence preserving function is a polynomial function (cf. [**24**]). We will investigate this concept for algebras that have a group reduct; we call such algebras expanded groups. Of course, they are a special class of Mal'cev algebras.

However, it is hard to determine when a single algebra is affine complete. In [**30**], finite affine complete abelian groups are described. Except for the subvarieties of this variety, there is no other variety of groups for which the affine complete finite members have been determined. Thus, an interesting question is whether the property of affine completeness is a decidable property. We say that the property of an algebra is a decidable property if there is an algorithm that takes a given algebra on the input and gives back the answer whether the algebra has the property. In [**4**], it was proved that there is an algorithm that decides whether a given finite nilpotent group is affine complete. Here, we generalize this result for a subclass of Mal'cev algebras.

The second approach in our investigation of polynomials arises from the following observation. Composing fundamental operations of a finite Mal'cev algebra in two different ways one can obtain the same polynomial function. The problem is to determine whether two such different compositions of fundamental operations induce the same polynomial function. This problem is usually referred to as the polynomial equivalence problem. In [**15, 12**] it is proved that on finite nilpotent groups and finite nilpotent rings, it can be checked in polynomial time whether two given terms induce the same function. This dissertation provides a decidability result for a larger class of algebras.

The third problem we consider is: How many distinct sets of polynomial functions that are closed for composition and contain constant functions and projections can be obtained depending on a set of fundamental operations of a finite Mal'cev algebra. This set of functions is called a polynomial Mal'cev clone and therefore the problem is to count nonequivalent polynomial Mal'cev clones on a finite set. In [**21**] it was proved that for a finite set A with $|A| \geq 4$ infinitely many constantive clones (clones that contain all constant operations) on A contain a Mal'cev operation. In the case that the Mal'cev operation is the Mal'cev operation of some abelian group and p is a prime, there are precisely two constantive clones on $\mathbb{Z}_p$ that contain the ternary function $(x, y, z) \mapsto x - y + z$. Furthermore, E. Aichinger and P. Mayr have shown in [**6**] that there are precisely 17 different clones that contain the binary operation of the cyclic group $\mathbb{Z}_{pq}$, where p and q are two different prime numbers. In [**10**] it was shown that in the case of $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$, p a prime number, there are countably many clones that contain the Mal'cev operation and all the constant operations. It is not known whether there exists a finite set A such that there are uncountably many Mal'cev clones on A.

This dissertation is divided in three chapters. The first chapter is introductory. There, we define all fundamental notions and recall some fundamental properties about universal algebras, especially Mal'cev algebras, expanded groups, rings, nearrings, modules and lattices. We also introduce binary commutators, list some preliminaries from tame congruence theory and prove some properties of one special class of lattices. Most of the results concerning that class of lattices are original.

In the second chapter we develop our main technical tool which we use throughout the dissertation. Namely, we further develop the concept of higher commutators which was introduced by A. Bulatov in [**9**]. The paper [**9**] defines higher commutators as a generalization of usual binary commutators and exhibits some fundamental properties. Chapter 2 of this dissertation is a thorough study of the higher commutator operation and its connections to the polynomial functions of Mal'cev algebras. The techniques to prove the properties of higher commutators, and the actual proofs are the author's original contribution as well as the applications of higher commutators presented in this dissertation, which suggest that higher commutators could be a useful tool for further research in universal algebra. Thus we can say that the properties of higher commutators that allow effective manipulation of expressions containing higher commutators are one of the main contributions of this dissertation.

The main results of the dissertation are formulated and proved in Chapter 3. This chapter is divided in three sections: about affine completeness, about polynomial equivalence problem and about the number of Mal'cev clones on a finite set. We present a characterization of affine complete expanded groups whose congruence lattice has a special property (Theorem §3.1.10). This result is a part of the paper [**8**], which has appeared in Algebra Universalis. For a finite nilpotent algebra of finite type that is a product of algebras of prime power order and generates a congruence modular variety (this class of algebras is studied by K. Kearnes in [**25**]), we are able to show that the property of affine completeness is decidable (Theorem §3.1.18). Moreover, the polynomial equivalence problem has polynomial complexity in the length of the input polynomials (Theorem §3.2.3). A paper containing these two results together with the results on higher commutators from Chapter 2 is submitted and is under review. These results have been published in the form of a preprint in the Preprint series of the Departments of Mathematics at the Johannes Kepler University in Linz, Austria (Number 564, August 2008) under the title *Some Applications of Higher Commutators in Mal'cev Algebras*. As the final contribution of this dissertation, we prove that the polynomial functions of a finite Mal'cev algebra whose congruence lattice is of height at most 2 can be described by a finite set of relations (Theorem §3.3.22). This result can be found in [**7**] and will be published in Acta Mathematica Hungarica.

At the end I want to thank to my advisors Dozent Dr. Erhard Aichinger from Institute for Algebra at JKU Linz, Austria, for the fruitful collaboration in the research, and Professor Dragan Mašulović from Department of Mathematics and Informatics, University of Novi Sad, Serbia, for useful suggestions and help in the preparation of the papers and the dissertation. Furthermore, I want to thank Professor Siniša Crvenković, Professor Rozália Madarász-Szilágyi and dr Petar Marković as well as the Department of Mathematics and Informatics, University of Novi Sad, Serbia. I would also like to thank WUS Austria, Austrian Exchange Service (ÖAD), Professor Günter Pilz and JKU Linz in Austria, for the financial support for altogether 11 months long research stays during which the most of the investigation was realized and most of the results were obtained.

I would also thank my family for the inexhaustible support.

Novi Sad, 2009

Nebojša Mudrinski

CHAPTER 1

Introduction

In this chapter we recall some fundamental notions and their fundamental properties that we use throughout the dissertation. We suppose that the reader is familiar with elementary universal algebraic notions such as (universal) algebra, homomorphism, isomorphism, subalgebra, direct and subdirect product, isomorphism theorems and varieties. For these notions we refer to [**13, 29**].

1. Elementary Notions

Given an algebra $\mathbf{A}$ and $k \in \mathbb{N}$, a function f from A^k to A is called a *k-ary polynomial function* of $\mathbf{A}$ if there are a natural number l, elements $a_1, \ldots, a_l \in A$, and a $(k+l)$-ary term t in the language of $\mathbf{A}$ such that

$$f(x_1, \ldots, x_k) = \mathsf{t}^{\mathbf{A}}(x_1, \ldots, x_k, a_1, \ldots, a_l)$$

for all $x_1, \ldots, x_k \in A$. Here, we shall call polynomial functions shortly polynomials. By $\mathsf{Pol}_k\mathbf{A}$ we denote the set of all k-ary polynomials of $\mathbf{A}$ and $\mathsf{Pol}\,\mathbf{A} := \bigcup_{k\geq 0} \mathsf{Pol}_k\mathbf{A}$. We will usually denote a tuple (vector) $(x_0, \ldots, x_k)$ by $\mathbf{x}$ and its ith component by x_i or $\mathbf{x}^{(i)}$. For arbitrary tuples $\mathbf{x}, \mathbf{y} \in A^k$ and a congruence α of an algebra $\mathbf{A}$ we write $\mathbf{x} \equiv_\alpha \mathbf{y}$ if $\mathbf{x}^{(i)} \equiv_\alpha \mathbf{y}^{(i)}$ for every $i \in \{0, \ldots, k-1\}$. Also, for $f : A^{k+m+n} \to A$ and tuples $\mathbf{x} = (x_0, \ldots, x_{k-1}) \in A^k$, $\mathbf{y} = (y_0, \ldots, y_{m-1}) \in A^m$ and $\mathbf{z} = (z_0, \ldots, z_{n-1}) \in A^n$, we write $f(\mathbf{x}, \mathbf{y}, \mathbf{z})$ instead of $f(x_0, \ldots, x_{k-1}, y_0, \ldots, y_{m-1}, z_0, \ldots, z_{n-1})$.

We say that algebras $\mathbf{A}$ and $\mathbf{B}$, not necessarily with the same fundamental operations, are *polynomially equivalent* if they have the same set of polynomial functions.

Definition 1.1. A ternary operation m on a set A is said to be a *Mal'cev operation* if the equations

$$m(x, x, y) = y = m(y, x, x)$$

are valid for all $x, y \in A$. An algebra $\mathbf{A}$ is called a *Mal'cev algebra* if $\mathbf{A}$ has a Mal'cev term operation.

One of the most important classes of Mal'cev algebras are expanded groups.

Definition 1.2. We call an algebra $\mathbf{V}$ an *expanded group* if it has the operation symbols $+$ (binary), $-$ (unary) and 0 (nullary) and its reduct $(V, +, -, 0)$ is a group.

When we speak about the Mal'cev term of $\mathbf{V}$, we mean the operation $m(x,y,z) := x-y+z$, despite of the fact that other ternary term functions satisfying $m(x,x,y) = m(y,x,x) = y$ may exist. The following structure can be seen as an expanded group and will be mentioned several times in the sequel.

DEFINITION 1.3. Let $(M,+,-,0)$ be an Abelian group and let $\mathbf{R}$ be a ring with identity. We call an algebra $\mathbf{M} = (M,+,-,0,\{f_r : M \to M \mid r \in R\})$ an $\mathbf{R}$-*module* $\mathbf{M}$ if

(1) $f_r(x+y) = f_r(x) + f_r(y)$
(2) $f_{r+s}(x) = f_r(x) + f_s(x)$
(3) $f_r(f_s(x)) = f_{rs}(x)$
(4) $f_1(x) = x$

for all $x, y \in M$ and $r, s \in R$. We shortly denote $\mathbf{R}$-modules $\mathbf{M}$ by $(M,+,-,0,R)$.

Let $m, n \in \mathbb{N}$. For a field $\mathbf{D}$, let $\mathbf{M}_n(\mathbf{D})$ be the ring of $(n \times n)$-matrices over $\mathbf{D}$. For every $A \in \mathbf{M}_n(\mathbf{D})$ and every $(n \times m)$-matrix X with entries from $\mathbf{D}$ we define $f_A(X) := AX$. Then we have the $\mathbf{M}_n(\mathbf{D})$-module of all $(n \times m)$-matrices with entries from $\mathbf{D}$. We denote it by $\mathbf{D}^{(n \times m)}$.

We need one generalization of modules obtained using *near-rings* instead of rings. Here we give the definition, and more about this structure can be found in [**31**].

DEFINITION 1.4. Let $\mathbf{R} = (R,+,\cdot)$ be an algebra with two binary operations such that $(R,+)$ is a (not necessary abelian) group, $(R,\cdot)$ is a monoid and

$$(x+y) \cdot z = x \cdot z + y \cdot z$$

for all $x, y, z \in R$. Then, we say that $\mathbf{R}$ is a near-ring.

One of the first examples of near-rings is the following structure that we shall use several times in the sequel. Let $\mathbf{V}$ be an expanded group with a group reduct $(V,+,-,0)$. By $P_0(\mathbf{V})$ we denote the set of all unary polynomials p of $\mathbf{V}$ such that $p(0) = 0$. If we define

$$(p+q)(x) := p(x) + q(x),$$

for all $x \in V$ and for all $p, q \in \mathsf{Pol}_1\mathbf{V}$, and by $\circ$ we denote the usual composition of functions, then $(P_0(\mathbf{V}),+,\circ)$ is a near-ring.

DEFINITION 1.5. Let $\mathbf{R} = (R,+,\circ)$ be a near-ring and $(M,+)$ a group. The structure $\mathbf{M} = (M,+,-,0,\{f_r : M \to M \mid r \in R\})$ is a *near-ring module* if

(1) $f_{r \circ s}(x) = f_r(f_s(x))$;
(2) $f_{r+s}(x) = f_r(x) + f_s(x)$

for all $x \in M$ and $r, s \in R$. When it is clear from the context, a near-ring module $\mathbf{M}$ over $\mathbf{R}$ will be referred to as an $\mathbf{R}$-module and denoted by $(M,+,-,0,R)$, just like in the case of ring modules.

Let $\mathbf{V}$ be an expanded group with a group reduct $(V, +, -, 0)$. Using the previous example we can construct a near-ring module $\mathbf{M} = (V, +, -, 0, P_0(\mathbf{V}))$, where $f_p(v) := p(v)$ for all $p \in P_0(\mathbf{V})$ and all $v \in V$.

DEFINITION 1.6. A *partially ordered set* $(P, \leq)$ consists of a nonempty set P and binary relation $\leq$ that satisfies:

(1) $x \leq x$ (reflexivity);
(2) $(x \leq y) \wedge (y \leq x) \Rightarrow (x = y)$ (antisymmetry);
(3) $(x \leq y) \wedge (y \leq z) \Rightarrow x \leq z$ (transitivity)

for all $x, y, z \in P$. When the relation $\leq$ is clear from the context we call P partially ordered set. We shall shortly call a partially ordered set *poset*.

Let $(P, \leq)$ be a partially ordered set. Let $Q \subseteq P$. If there exists an element $z \in P$ such that

(1) $(\forall x \in Q)(z \leq x)$ and
(2) $(\forall y \in P)\Big(\big((\forall x \in Q)\, y \leq x\big) \Rightarrow (y \leq z)\Big)$

then one can easily show that z is unique. We call such an element *infimum of* Q and write $\inf Q$. Dually, we define *supremum of* Q, in abbreviation, $\sup Q$.

DEFINITION 1.7. An algebra $(L, \wedge, \vee)$ is called a *lattice* if L is a nonempty set, and $\wedge$ and $\vee$ are binary operations on L that satisfy the following conditions:

(L1) $x \wedge y = y \wedge x$; $x \vee y = y \vee x$ (commutative law)
(L2) $(x \wedge y) \wedge z = x \wedge (y \wedge z)$; $(x \vee y) \vee z = x \vee (y \vee z)$ (associative law)
(L3) $x \wedge x = x$; $x \vee x = x$ (idempotent law)
(L4) $x \wedge (x \vee y) = x$; $x \vee (x \wedge y) = x$ (absorption law)

for all $x, y, z \in L$.

We define a *lattice ordered set* as a partially ordered set L such that for every two elements $a, b \in L$ there exist $\inf\{a, b\}$ and $\sup\{a, b\}$. The following theorem describes how we switch from lattice to lattice ordered set and vice versa. The proof can be found in [**16**].

THEOREM 1.8. (i) *Let the poset* $(L, \leq)$ *be a lattice ordered set. Set*

$$a \wedge b = \inf\{a, b\},$$

$$a \vee b = \sup\{a, b\}$$

for all $a, b \in L$. *Then the algebra* $\mathbf{L}^a = (L, \wedge, \vee)$ *is a lattice.*

(ii) *Let the algebra* $(L, \wedge, \vee)$ *be a lattice. Set*

$$a \leq b \text{ if and only if } a \wedge b = a.$$

for all $a, b \in L$. *Then* $\mathbf{L}^p = (L, \leq)$ *is a lattice ordered set.*

(iii) *Let the poset* $(L, \leq)$ *be a lattice ordered set. Then* $(\mathbf{L}^a)^p = \mathbf{L}$.
(iv) *Let the algebra* $(L, \wedge, \vee)$ *be a lattice. Then* $(\mathbf{L}^p)^a = \mathbf{L}$.

We shall choose the more appropriate concept according to the context and situation.

In a lattice $\mathbf{L} = (L, \wedge, \vee)$ we write $a \prec b$ if $a \leq b$ and $a \leq x \leq b$ implies $x = a$ or $x = b$ for all $x \in L$. If $\mathbf{L}$ has a smallest element 0 and a largest element 1, then every $a \in L$ such that $0 \prec a$ is called an *atom* and every $b \in L$ such that $b \prec 1$ is called a *coatom*. We denote the finite lattices such that every atom is a coatom by $\mathbf{M}_i$, where i denotes the number of atoms (coatoms).

DEFINITION 1.9. Let $\mathbf{L} = (L, \wedge, \vee)$ be a lattice. We say that $\mathbf{L}$ is

(1) *modular* if $x \leq z$ implies $x \vee (y \wedge z) = (x \vee y) \wedge z$ for all $x, y, z \in L$,
(2) *distributive* if $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ for all $x, y, z \in L$.

DEFINITION 1.10. Let $\mathbf{L} = (L, \wedge, \vee)$ be a lattice. We say that $\mathbf{L}$ is a *complete lattice* if there exist $\inf X$ and $\sup X$ for every $X \subseteq L$. Usually, we denote $\inf X$ by $\bigwedge X$ and $\sup X$ by $\bigvee X$.

DEFINITION 1.11. Let $\mathbf{L} = (L, \wedge, \vee)$ be a complete lattice. An element $a \in L$ is called *compact* if for all $X \subseteq L$ the following holds: if $a \leq \bigvee X$, then $a \leq \bigvee Y$ for some finite $Y \subseteq X$. $\mathbf{L}$ is called *algebraic* if every element of L is the join of a set of compact elements of $\mathbf{L}$.

LEMMA 1.12. (cf. [**29**, Lemma 4.49(iii)]) *Let* $\mathbf{L}$ *be an algebraic lattice. If* $x, y \in L$ *such that* $x < y$, *then there exists* $a, b \in L$ *satisfying* $x \leq a \prec b \leq y$.

In a lattice $\mathbf{L}$ by $I[a, b]$ we denote the set $\{x \in L \mid a \leq x \leq b\}$ and call it an *interval* or *quotient*. The sublattice of $\mathbf{L}$ whose universe is $I[a, b]$ will be denoted by $\mathbf{I}[a, b]$. When an interval $I[a, b]$ contains only a and b we call it a *prime interval* or *prime quotient*.

DEFINITION 1.13. Let $\mathbf{L} = (L, \wedge, \vee)$ be a lattice and let $a, b, c, d \in L$.

(1) The interval $I[a, b]$ *transposes up to* $I[c, d]$ if $a = b \wedge c$ and $d = b \vee c$. We write $I[a, b] \nearrow I[c, d]$.
(1ω) The interval $I[a, b]$ *weakly transposes up to* $I[c, d]$ if $a = b \wedge c$ and $b \leq d$. We write $I[a, b] \nearrow_\omega I[c, d]$.
(2) The interval $I[a, b]$ *transposes down to* $I[c, d]$ if $c = a \wedge d$ and $b = a \vee d$. We write $I[a, b] \searrow I[c, d]$.
(2ω) The interval $I[a, b]$ *weakly transposes down to* $I[c, d]$ if $c \leq a$ and $b = a \vee d$. We write $I[a, b] \searrow_\omega I[c, d]$.

We say that intervals $I[a, b]$ and $I[c, d]$ *transpose* if either (1) or (2) is true, and that $I[a, b]$ and $I[c, d]$ *weakly transpose* if either (1ω) or (2ω) is true. The intervals $I[a, b]$ and $I[c, d]$ are *projective* (*weakly projective*) if there exists a finite sequence

$$I[a, b] = I[c_0, d_0], I[c_1, d_1], \ldots, I[c_n, d_n] = I[c, d]$$

in $\mathbf{L}$ such that $I[c_i, d_i]$ and $I[c_{i+1}, d_{i+1}]$ transpose (weakly transpose) for all $i \in \{0, \ldots, n-1\}$. We write $I[a, b] \leftrightsquigarrow I[c, d]$ ($I[a, b] \leftrightsquigarrow_\omega I[c, d]$).

Note that $\leftrightsquigarrow$ is the smallest equivalence relation that contains $\nearrow$. The following lemma makes a connection between these two concepts of projectivity.

LEMMA 1.14. (cf. [**16**, p. 171, Lemma 1]) *Let* $\mathbf{L}$ *be a lattice and let* $a, b, c, d \in L$ *such that* $a \leq b$ *and* $c \leq d$. *Then the following conditions are equivalent:*

(1) $I[a, b] \leftrightsquigarrow_\omega I[c, d]$
(2) *There is an* $n \in \mathbb{N}$ *and there are quotients*

$$I[a, b] = I[c_0, d_0], I[c_0', d_0'], I[c_1, d_1], I[c_1', d_1'] \ldots, I[c_n, d_n] = I[c, d]$$

in $\mathbf{L}$ *such that* $I[c_i, d_i]$ *and* $I[c_i', d_i']$ *transpose, and* $I[c_i', d_i']$ *is a subinterval of* $I[c_{i+1}, d_{i+1}]$ *for all* $i \in \{0, \ldots, n-1\}$.

DEFINITION 1.15 (G.Grätzer, E. T. Schmidt). Let us call a lattice $\mathbf{L}$ *weakly modular* if for every two weakly projective intervals $I[a, b]$ and $I[c, d]$ of $\mathbf{L}$ there exists a proper subinterval $I[c', d']$ of $I[c, d]$ such that $I[c', d'] \leftrightsquigarrow_\omega I[a, b]$.

PROPOSITION 1.16. (cf. [**16**, p.176. Corollary 9]) *Every modular lattice is weakly modular.*

DEFINITION 1.17. Let $\mathbf{L} = (L, \wedge, \vee)$ be a complete lattice. An element $a \in L$ is called *strictly meet irreducible* if $a < \bigwedge\{x \in L \mid a < x\}$. We define $a^+ := \bigwedge\{x \in L \mid a < x\}$. An element $b \in L$ is called *strictly join irreducible* if $\bigvee\{x \in L \mid x < b\} < b$. We define $b^- := \bigvee\{x \in L \mid x < b\}$.

Clearly, we have $a \prec a^+$ and $b^- \prec b$ for every strictly meet irreducible element a and every strictly join irreducible element b in a lattice $\mathbf{L}$.

PROPOSITION 1.18. (cf. [**29**, Theorem 2.19]) *In an algebraic lattice, every element is the meet of a set of strictly meet irreducible elements.*

We shall work mostly with finite lattices. In finite lattices strictly meet irreducible elements and meet irreducible elements are the same. We call an element a of a lattice $\mathbf{L}$ *meet irreducible* if $a \neq 1$ and

$$a = b \wedge c \text{ implies } a = b \text{ or } a = c$$

for all $b, c \in L$. Dually, we define *join irreducible* elements and they are precisely strictly join irreducible elements in finite lattices.

DEFINITION 1.19. Let $\mathbf{L}_1 = (L_1, \wedge_1, \vee_1)$ and $\mathbf{L}_2 = (L_2, \wedge_2, \vee_2)$ be two lattices. A bijective mapping $f : L_1 \to L_2$ is called an *isomorphism* if

$$f(x \wedge_1 y) = f(x) \wedge_2 f(y)$$
$$f(x \vee_1 y) = f(x) \vee_2 f(y)$$

for all $x, y \in L_1$.

DEFINITION 1.20. Let $\mathbf{L}$ be a lattice. We say that $\mathbf{L}$ satisfies the *descending chain condition* if, given any sequence $x_1 \geq x_2 \geq \cdots \geq x_n \geq \ldots$ of elements of L, there exists a $k \in \mathbb{N}$ such that $x_k = x_{k+1} = \ldots$..

2. Congruences and Ideals

DEFINITION 2.1. Let $\mathbf{A}$ be an algebra. A binary relation θ on A such that

(R) $x \equiv_\theta x$ (reflexivity)
(S) $x \equiv_\theta y \Longrightarrow y \equiv_\theta x$ (symmetry)
(T) $x \equiv_\theta y \wedge y \equiv_\theta z \Longrightarrow x \equiv_\theta z$ (transitivity) for all $x, y, z \in A$ and
(C) if f is n-ary operation of $\mathbf{A}$ and $x_1 \equiv_\theta y_1, \ldots, x_n \equiv_\theta y_n$ then $f(x_1, \ldots, x_n) \equiv_\theta f(y_1, \ldots, y_n)$ for all $x_1, \ldots, x_n, y_1, \ldots, y_n \in A$ (compatibility)

is called a *congruence* of $\mathbf{A}$. By $\mathsf{Con}\,\mathbf{A}$ we denote the set of all congruences of $\mathbf{A}$.

All nontrivial algebras have at least two congruences: by $0_\mathbf{A}$ we denote the equality relation (the smallest element in $\mathsf{Con}\,\mathbf{A}$) and by $1_\mathbf{A}$ we denote the full relation on the domain (the largest element in $\mathsf{Con}\,\mathbf{A}$). We omit the indices when the algebra is clear from the context. We say that an algebra $\mathbf{A}$ is *simple* if $0, 1$ are the only congruences of $\mathbf{A}$.

As it is mentioned in [**19**, p.25] to check whether an equivalence relation is a congruence of a given algebra $\mathbf{A}$ it is enough to check whether is it compatible with unary polynomials of $\mathbf{A}$.

Let $\mathbf{A}$ be an algebra and $k \in \mathbb{N}_0$. A function $f : A^k \to A$ preserves a congruence α of $\mathbf{A}$ if for every $\mathbf{a}, \mathbf{b} \in A^k$ such that $\mathbf{a} \equiv_\alpha \mathbf{b}$ we have $f(\mathbf{a}) \equiv_\alpha f(\mathbf{b})$. The function f is *congruence preserving* if it preserves all congruences of $\mathbf{A}$. Let us note that every constant function is a congruence preserving function.

In an algebra $\mathbf{A}$ for $\mathbf{x}, \mathbf{y} \in A^k$ we denote the congruence generated by $\{(\mathbf{x}^{(i)}, \mathbf{y}^{(i)}) \mid i \in \{0, \ldots, k-1\}\}$ by $\Theta_\mathbf{A}(\mathbf{x}, \mathbf{y})$. A congruence that is generated by a single pair in A^2 is called a *principal congruence* of $\mathbf{A}$ (see [**13**, Definition 5.6]). In Mal'cev algebras, we have a useful characterization of congruences generated by a pair of vectors:

PROPOSITION 2.2. *Let $k \geq 1$ and let $\mathbf{A}$ be a Mal'cev algebra. If $\mathbf{a}, \mathbf{b} \in A^k$, then*

$$\Theta_\mathbf{A}(\mathbf{a}, \mathbf{b}) = \{(p(\mathbf{a}), p(\mathbf{b})) \mid p \in \mathsf{Pol}_k\mathbf{A}\}.$$

Proof: Let m be a Mal'cev term of $\mathbf{A}$ and $\theta := \{(p(\mathbf{a}), p(\mathbf{b})) \mid p \in \mathsf{Pol}_k\mathbf{A}\}$. We have to prove $\Theta_\mathbf{A}(\mathbf{a}, \mathbf{b}) = \theta$. First, we show that θ is a congruence of $\mathbf{A}$. Clearly, $(\mathbf{a}^{(i)}, \mathbf{b}^{(i)}) \in \theta$ for all $i \in \{0, \ldots, k-1\}$, because the projections π_i are k-ary polynomials. All constant functions can be seen as k-ary polynomials and therefore θ is a reflexive relation. To show symmetry, suppose that $(p(\mathbf{a}), p(\mathbf{b})) \in \theta$, where $p \in \mathsf{Pol}_k\mathbf{A}$. We define $q \in \mathsf{Pol}_k\mathbf{A}$ such that $q(\mathbf{x}) := m(p(\mathbf{a}), p(\mathbf{x}), p(\mathbf{b}))$. Then $(q(\mathbf{a}), q(\mathbf{b})) \in \theta$. Hence, $(p(\mathbf{b}), p(\mathbf{a})) \in \theta$. Now we show the transitivity. Let $(p(\mathbf{a}), p(\mathbf{b})), (q(\mathbf{a}), q(\mathbf{b})) \in \theta$ where $p, q \in \mathsf{Pol}_k\mathbf{A}$ such that $p(\mathbf{b}) = q(\mathbf{a})$. We define $r \in \mathsf{Pol}_k\mathbf{A}$ such that $r(\mathbf{x}) := m(p(\mathbf{x}), q(\mathbf{a}), q(\mathbf{x}))$. Then $(r(\mathbf{a}), r(\mathbf{b})) \in \theta$ and hence $(p(\mathbf{a}), q(\mathbf{b})) \in \theta$. Composition of a unary and a k-ary polynomial is a k-ary polynomial and thus θ is a congruence of $\mathbf{A}$. Hence, $\Theta_\mathbf{A}(\mathbf{a}, \mathbf{b}) \subseteq \theta$. Now, let $\rho \in \mathsf{Con}\,\mathbf{A}$ be such that $(\mathbf{a}^{(i)}, \mathbf{b}^{(i)}) \in \rho$ for every $i \in \{0, \ldots, k-1\}$. Then by compatibility we have $(p(\mathbf{a}), p(\mathbf{b})) \in \rho$ for all $p \in \mathsf{Pol}_k\mathbf{A}$. Hence $\theta \subseteq \rho$ and therefore $\theta \subseteq \Theta_{\mathbf{A}}(\mathbf{a}, \mathbf{b})$. □

Let $\mathbf{A}$ be an algebra. For every $\alpha, \beta \in \mathsf{Con}\,\mathbf{A}$, we define $\alpha \vee \beta$ to be the smallest congruence of $\mathbf{A}$ that contains $\alpha \cup \beta$. By [**13**, Theorem 5.5], $(\mathsf{Con}\,\mathbf{A}, \cap, \vee)$ is an algebraic lattice. Mal'cev algebras are *congruence permutable* by [**13**, Theorem 12.2]. Hence, in Mal'cev algebras we have $\alpha \vee \beta = \alpha \circ \beta$ for every $\alpha, \beta \in \mathsf{Con}\,\mathbf{A}$. We say that an algebra $\mathbf{A}$ is *congruence modular* if the lattice $\mathsf{Con}\,\mathbf{A}$ is modular. The following characterization we use in Lemma §3.1.17.

PROPOSITION 2.3. (Gumm) *Let $\mathcal{V}$ be a variety. Then $\mathcal{V}$ is modular if and only if there exist terms p and $q_0, \dots, q_n$ for some $n \in \mathbb{N}$ such that in every $A \in \mathcal{V}$ the following is true:*

(1) $q_0(x, y, z) = x$;
(2) $q_i(x, y, x) = x$ *for* $i \leq n$;
(3) $q_i(x, y, y) = q_{i+1}(x, y, y)$ *for* i *even;*
(4) $q_i(x, x, y) = q_{i+1}(x, x, y)$ *for* i *odd;*
(5) $q_n(x, y, y) = p(x, y, y)$;
(6) $p(x, x, y) = y$

for every $x, y, z \in A$.

Proof: See [**14**, Theorem 6.4]. □

DEFINITION 2.4. Let $\mathbf{V}$ be an expanded group. A subset I of V is an *ideal* of $\mathbf{V}$ if I is a normal subgroup of $\mathbf{V}$, and for all $k \in \mathbb{N}$, for all k-ary fundamental operations f of $\mathbf{V}$, and for all $\mathbf{v} \in V^k$ and $\mathbf{i} \in I^k$, we have

$$f(\mathbf{v} + \mathbf{i}) - f(\mathbf{v}) \in I.$$

The set of all ideals of $\mathbf{V}$ is denoted by $\mathsf{Id}\,\mathbf{V}$.

Clearly, $\mathsf{Id}\,\mathbf{V}$ has at least two elements: 0 and V, in every expanded group $\mathbf{V}$. If $\mathsf{Id}\,\mathbf{V}$ has exactly two elements, we say that $\mathbf{V}$ is a simple expanded group. Modules and rings are called simple if they are simple as expanded groups.

We say that a ring $\mathbf{R}$ is *primitive* if there is a simple $\mathbf{R}$-module $\mathbf{M}$ such that $RM = \{f_r(m) \mid r \in R, m \in M\} \neq \{0_{\mathbf{M}}\}$.

PROPOSITION 2.5. *Every finite primitive ring is simple and has an identity element.*

Proof: The statement can be obtained directly from [**36**, Theorem 19, p.64]. □

A useful fact linking ideals with polynomial functions is given in the following proposition.

PROPOSITION 2.6. *Let $\mathbf{V}$ be an expanded group. A subset I of V is an* ideal *of $\mathbf{V}$ if and only if for all $a, b \in I$ and for all $p \in \mathsf{Pol}_1\mathbf{V}$ with $p(0) = 0$ we have $a + b \in I$ and $p(a) \in I$.*

Proof: See [**31**, Theorem 7.123]. □

In an expanded group $\mathbf{V}$, we define $I + J := \{i + j \mid i \in I, j \in J\}$ for every $I, J \in \mathsf{Id}\,\mathbf{V}$. One can easily show that $I+J$ is the smallest ideal of $\mathbf{V}$ that contains both I and J. Furthermore, $(\mathsf{Id}\,\mathbf{V}, \cap, +)$ is an algebraic lattice isomorphic to $(\mathsf{Con}\mathbf{V}, \cap, \vee)$ and the isomorphism $\gamma_V : \mathsf{Id}\,\mathbf{V} \to \mathsf{Con}\mathbf{V}$ is given by

$$\gamma_V(I) := \{(x, y) \mid x - y \in I\}$$

for every $I \in \mathsf{Id}\,\mathbf{V}$. Thus, for $I \in \mathsf{Id}\,\mathbf{V}$ and for $a, b \in V$ such that $a \equiv_{\gamma_V(I)} b$ we shall write $a \equiv_I b$.

3. Binary Commutators

In this section we recall the definition of the binary commutator and its important properties in universal algebras (cf. [**19, 29**]). We also give a proof of Gumm's result (Proposition 3.11) as a model for several proofs of our results in Chapters 2 and 3.

In [**3**, Proposition 2.1, Proposition 2.3] a proof is stated that the centralizing relation defined in [**29**] is the same as the following centralizing relation:

Definition 3.1. Let α, β, η be congruences of an algebra $\mathbf{A}$. We say that α *centralizes* β *modulo* η, written

$$C(\alpha, \beta; \eta),$$

if for all $n \geq 1$ and every $p \in \mathsf{Pol}_{n+1}\mathbf{A}$, $a, b \in A$ such that $a \equiv_\alpha b$ and $\mathbf{c}, \mathbf{d} \in A^n$ such that $\mathbf{c} \equiv_\beta \mathbf{d}$ we have

$$p(a, \mathbf{c}) \equiv_\eta p(a, \mathbf{d}) \text{ implies } p(b, \mathbf{c}) \equiv_\eta p(b, \mathbf{d}).$$

It follows immediately from the definition that for congruences α, β, $\{\eta_i \mid i \in I\}$ of an algebra $\mathbf{A}$, we have: if $C(\alpha, \beta; \eta_i)$ for each $i \in I$, then

$$C(\alpha, \beta; \bigwedge_{i \in I} \eta_i).$$

This justifies the following definition.

Definition 3.2. Let $\mathbf{A}$ be an algebra. For congruences α and β of $\mathbf{A}$ we define their *commutator*, denoted $[\alpha, \beta]$, to be the smallest congruence η of $\mathbf{A}$ for which α centralizes β modulo η. The *centralizer* of β *modulo* α, denoted $(\alpha : \beta)_{\mathbf{A}}$, is the largest congruence γ such that γ centralizes β modulo α. We omit the subscript when the algebra is clear from the context.

Example 3.3. Let $\mathbf{M} = (M, +, -, 0, R)$ be an $\mathbf{R}$-module and let us calculate $[1, 1]$. One can easily show, using inductive arguments, that for every $n \in \mathbb{N}$ and every polynomial $p \in \mathsf{Pol}_n\mathbf{M}$ there exist $\alpha \in M$ and $r_0, \ldots, r_{n-1} \in R$ such that

$$p(x_0, \ldots, x_{n-1}) = f_{r_0}(x_0) + \cdots + f_{r_{n-1}}(x_{n-1}) + \alpha$$

for all $x_0, \dots, x_{n-1} \in M$. If for $k \geq 0$, $a \in M$, $\mathbf{u}, \mathbf{v} \in M^k$ and $p \in \mathsf{Pol}_{k+1}\mathbf{M}$ we have $p(a, \mathbf{u}) = p(a, \mathbf{v})$, then $p(b, \mathbf{u}) = p(b, \mathbf{v})$ for every $b \in M$. This yields $C(1, 1; 0)$ and therefore $[1, 1] = 0$.

Let $\alpha, \beta, \eta \in \mathsf{Con}\mathbf{A}$. The following properties can be shown directly from the definition of centralizers and commutators:

(BC1) $[\alpha, \beta] \leq \alpha \wedge \beta$;

(BC2) for all $\gamma, \delta \in \mathsf{Con}\,\mathbf{A}$ such that $\alpha \leq \gamma, \beta \leq \delta$, we have

$$[\alpha, \beta] \leq [\gamma, \delta];$$

Furthermore, in [**3**, Proposition 2.4, Proposition 2.5] it has been proved that if **A** generates a congruence permutable variety, then, we have:

(BC4) $[\alpha, \beta] = [\beta, \alpha]$;

(BC5) $[\alpha, \beta] \leq \eta$ if and only if $C(\alpha, \beta; \eta)$;

(BC6) If $\eta \leq \alpha, \beta$, then in $\mathbf{A}/\eta$, we have $[\alpha/\eta, \beta/\eta] = ([\alpha, \beta] \vee \eta)/\eta$;

(BC7) If I is a nonempty set, and $\{\rho_i \mid i \in I\} \subseteq \mathsf{Con}\,\mathbf{A}$, then: $\bigvee_{i \in I}[\alpha, \rho_i] = [\alpha, \bigvee_{i \in I} \rho_i]$ and similarly $\bigvee_{i \in I}[\rho_i, \beta] = [\bigvee_{i \in I} \rho_i, \beta]$.

One can see that (BC4), (BC5), (BC6) and (BC7) are corollaries of results (HC4), (HC5), (HC6) and (HC7) shown in Chapter 2.

LEMMA 3.4. *Let $k \in \mathbb{N}$, let $\mathbf{A}$ be an algebra with a Mal'cev term m, let $\alpha, \beta \in \mathsf{Con}\,\mathbf{A}$ and let $p \in \mathsf{Pol}_k\mathbf{A}$. If $[\alpha, \beta] = 0$ and $\mathbf{a}, \mathbf{b}, \mathbf{c} \in A^k$ such that $\mathbf{a} \equiv_\alpha \mathbf{b} \equiv_\beta \mathbf{c}$, then we have*

$$m(p(\mathbf{a}), p(\mathbf{b}), p(\mathbf{c})) = p(m(\mathbf{a}^{(1)}, \mathbf{b}^{(1)}, \mathbf{c}^{(1)}), \dots, m(\mathbf{a}^{(k)}, \mathbf{b}^{(k)}, \mathbf{c}^{(k)})).$$

Proof: The statement can be obtained directly from [**3**, Proposition 2.6]. □

LEMMA 3.5. *Let $\mathbf{A}$ be an algebra with a Mal'cev term m, let $\alpha, \beta \in \mathsf{Con}\,\mathbf{A}$ and let $\theta, a, b \in A$. If $[\alpha, \beta] = 0$ and $a \equiv_\alpha b \equiv_\beta \theta$, then we have*

$$m(m(a, b, \theta), \theta, b) = a.$$

Proof: Using Lemma 3.4 we obtain

$$\begin{aligned} m(m(a, b, \theta), \theta, b) &= m(m(a, b, \theta), m(b, b, \theta), m(b, \theta, \theta)) \\ &= m(m(a, b, b), m(b, b, \theta), m(\theta, \theta, \theta)) = m(a, \theta, \theta) = a. \end{aligned}$$

□

LEMMA 3.6. *Let $k \in \mathbb{N}$, let $\mathbf{A}$ be an algebra with a Mal'cev term m, let θ be an arbitrary element of A, and let $\mathbf{a}, \mathbf{b} \in A^k$. Take any $p \in \mathsf{Pol}_k\mathbf{A}$ and let $\alpha \in \mathsf{Con}\,\mathbf{A}$. If $p|_{\theta/\alpha} = \theta$, $\mathbf{a} \equiv_\alpha \mathbf{b}$ and $[\alpha, 1] = 0$, then $p(\mathbf{a}) = p(\mathbf{b})$.*

Proof: The statement can be obtained from [**3**, Proposition 2.8.(1)] for $\beta = 1$. □

LEMMA 3.7. *Let $\mathbf{A}$ be an algebra with a Mal'cev term m, let $\alpha, \beta \in \mathsf{Con}\,\mathbf{A}$ and let $\theta, a, b \in A$. If $[\alpha, \beta] = 0$ and $a \equiv_\alpha b \equiv_\beta \theta$, then we have*

$$m(a, b, \theta) = m(a, \theta, m(\theta, b, \theta)).$$

Proof: Using Lemma 3.4 we obtain

$$m(a,b,\theta) = m(m(a,\theta,\theta), m(\theta,\theta,b), m(\theta,\theta,\theta))$$

$$= m(m(a,\theta,\theta), m(\theta,\theta,\theta), m(\theta,b,\theta)) = m(a,\theta,m(\theta,b,\theta)).$$

□

We say that $f : A^k \to A$, $k \geq 1$, is a *commutator preserving function* of $\mathbf{A}$ if f is congruence preserving function of $\mathbf{A}$ and for every two congruences α, β of $\mathbf{A}$ we have $[\alpha,\beta]_{\mathbf{A}} = [\alpha,\beta]_{\mathbf{A}+f}$, where $\mathbf{A}+f$ denotes the algebra obtained from $\mathbf{A}$ by adding the function f as a fundamental operation.

LEMMA 3.8. (cf.[**6**, Lemma 2.6.]) *Let $k \in \mathbb{N}$, let $\mathbf{A}$ be an algebra with a Mal'cev term m, and f a mapping $A^k \to A$. If we define*

$$\rho(\alpha,\beta,\eta,m) := \{(a,b,c,d) \in A^4 \mid a \equiv_\alpha b, b \equiv_\beta c, m(a,b,c) \equiv_\eta d\},$$

for every $\alpha,\beta,\eta \in \mathsf{Con}\,\mathbf{A}$, then the following are equivalent:

(1) *f is a commutator preserving function of $\mathbf{A}$*
(2) *f preserves all congruences of $\mathbf{A}$ and relations from the set*

$$\{\rho(\alpha,\beta,\eta,m) \mid \alpha,\beta,\eta \in \mathsf{Con}\,\mathbf{A}, C(\alpha,\beta;\eta)\}.$$

LEMMA 3.9. (cf.[**6**, Lemma 2.4.]) *Let $\mathbf{A}$ be an algebra with a Mal'cev term m, and $\alpha,\beta,\eta \in \mathsf{Con}\,\mathbf{A}$. Then the following are equivalent:*

(1) *Every $f \in \mathsf{Pol}\,\mathbf{A}$ preserves $\rho(\alpha,\beta,\eta,m)$.*
(2) *α centralizes β modulo η.*

The rest of this section is devoted to some special classes of algebras whose congruence lattices satisfy additional properties with respect to the binary commutator operation.

DEFINITION 3.10. (cf.[**2**, p. 106.]) An algebra $\mathbf{A}$ is called *TC-neutral* (*neutral with the respect to the term condition commutator) if $[\alpha,\beta] = \alpha \wedge \beta$ for all $\alpha,\beta \in \mathsf{Con}\mathbf{A}$.*

We say that an algebra $\mathbf{A}$ is *abelian* if $[1,1] = 0$. Abelian algebras are characterized by the following theorem.

PROPOSITION 3.11 (Gumm). *Suppose that a variety $\mathcal{V}$ has permuting congruences. For $\mathbf{A} \in \mathcal{V}$ the following are equivalent.*

(1) *$\mathbf{A}$ is Abelian.*
(2) *$\mathbf{A}$ is polynomially equivalent to a module over a ring.*

Proof: Let m be a Mal'cev term for $\mathcal{V}$. Since (2)⇒(1) is already proved in Example 3.3 it remains to prove (1)⇒(2). Suppose that $\mathbf{A}$ is Abelian. Our task is to construct a module polynomially equivalent to $\mathbf{A}$.

We choose an arbitrary element of A, write it as 0, and hold it fixed throughout the argument. Then we put

$$x + y := m^{\mathbf{A}}(x, 0, y)$$
$$-x := m^{\mathbf{A}}(0, x, 0).$$

In order to establish that we have defined a commutative group $(A, +, -, 0)$, we use several times the facts that $m^{\mathbf{A}}$ commutes with itself, by Lemma 3.4, and obeys Mal'cev conditions. Let $x, y, z \in A$. Then we have:

$$\begin{aligned}
x + 0 &= m^{\mathbf{A}}(x, 0, 0) = x;\\
x + y &= m^{\mathbf{A}}(m^{\mathbf{A}}(0, 0, x), m^{\mathbf{A}}(0, 0, 0), m^{\mathbf{A}}(y, 0, 0))\\
&= m^{\mathbf{A}}(m^{\mathbf{A}}(0, 0, y), m^{\mathbf{A}}(0, 0, 0), m^{\mathbf{A}}(x, 0, 0)) = y + x;\\
x + (-x) &= m^{\mathbf{A}}(m^{\mathbf{A}}(x, 0, 0), m^{\mathbf{A}}(x, x, 0), m^{\mathbf{A}}(0, x, 0))\\
&= m^{\mathbf{A}}(m^{\mathbf{A}}(x, x, 0), m^{\mathbf{A}}(0, x, x), m^{\mathbf{A}}(0, 0, 0)) = 0;\\
(x + y) + z &= m^{\mathbf{A}}(m^{\mathbf{A}}(x, 0, y), m^{\mathbf{A}}(0, 0, 0), m^{\mathbf{A}}(0, 0, z))\\
&= m^{\mathbf{A}}(m^{\mathbf{A}}(x, 0, 0), m^{\mathbf{A}}(0, 0, 0), m^{\mathbf{A}}(y, 0, z)) = x + (y + z)
\end{aligned}$$

The ring we need is easily defined. We put

$$R := \{r \in \mathsf{Pol}_1\mathbf{A} \mid r(0) = 0\}.$$

For $r, s \in R$, we define

$$(r + s)(x) := r(x) + s(x) \text{ for all } x \in A.$$

Now, $(R, +)$ is an Abelian group. Clearly, R is closed under usual composition of functions denoted by $\circ$ and $\circ$ is right distributive with respect to $+$. Again, by Lemma 3.4 we have that every $r \in R$ commutes with $m^{\mathbf{A}}$. Hence, $r(x + y) = r(m^{\mathbf{A}}(x, 0, y)) = m^{\mathbf{A}}(r(x), r(0), r(y)) = r(x) + r(y)$ for every $x, y \in A$ and $r \in R$. One can easily show that $\circ$ is left distributive with respect to $+$. We obtain that $\mathbf{R} = (R, +, \circ, -, o, id_A)$ is a ring with identity, where the unary polynomial o is the constant with value 0. Thus, we have an $\mathbf{R}$-module $\mathbf{M} = (A, +, -, 0, R)$. It is easy to see that $\mathsf{Pol}\,\mathbf{M} \subseteq \mathsf{Pol}\,\mathbf{A}$ because the fundamental operations of $\mathbf{M}$ are polynomial operations of $\mathbf{A}$. Let us show that $\mathsf{Pol}\,\mathbf{A} \subseteq \mathsf{Pol}\,\mathbf{M}$. Let $f \in \mathsf{Pol}\,\mathbf{A}$. Then $g(\mathbf{x}) := f(\mathbf{x}) - f(0, \ldots, 0)$ defines a polynomial operation of $\mathbf{A}$. Now, $g(0, \ldots, 0) = 0$ and by Lemma 3.4, g commutes with $m^{\mathbf{A}}$. Therefore

$$g(x_0 + y_0, \ldots, x_{n-1} + y_{n-1}) = g(x_0, \ldots, x_{n-1}) + g(y_0, \ldots, y_{n-1}),$$

for all $x_i, y_i \in A$. An obvious inductive argument then gives that

$$g(x_0, \ldots, x_{n-1}) = r_0(x_0) + \cdots + r_{n-1}(x_{n-1})$$

where

$$r_i(x) = g(0, \ldots, 0, \overset{i\text{th}}{\overset{\downarrow}{x}}, 0, \ldots, 0)$$

and $r_i \in R$. This completes the proof. □

PROPOSITION 3.12. *Suppose that* $\mathsf{Con}\,\mathbf{A}$ *has a sublattice isomorphic to* $\mathbf{M}_3$ *consisting of permuting congruences. Then* $\mathbf{A}$ *is abelian.*

Proof: See [**29**, Lemma 4.153, p.254]. $\Box$

DEFINITION 3.13. (cf. [**14**]) Let $\mathbf{A}$ be an algebra. We say that $\mathbf{A}$ is k-*step nilpotent* or *nilpotent of class* k if

$$[\underbrace{1,\ldots,[1}_{k},1]] = 0.$$

We say that $\mathbf{A}$ is *nilpotent* if it is k-step nilpotent for a $k \in \mathbb{N}$.

Clearly, a 1-step nilpotent algebra is abelian.

LEMMA 3.14. (cf.[**14**, Corollary 7.4]) *Let* $\mathbf{A}$ *be a nilpotent Mal'cev algebra with Mal'cev term* m*, and let* $b, c \in A$*. Then the function* $x \to m(x, b, c)$ *is a bijection.*

LEMMA 3.15. (cf.[**25**, Theorem 2.7]) *A congruence modular variety generated by a nilpotent algebra is congruence permutable.*

In [**22**], the condition (SC1) has been isolated as an important condition in describing polynomials in a certain class of algebras.

DEFINITION 3.16. A finite algebra $\mathbf{A}$ in congruence modular variety satisfies the condition (SC1) if $(\mu : \mu^+) \leq \mu^+$ for every strictly meet irreducible congruence μ of $\mathbf{A}$.

DEFINITION 3.17. (cf. [**3**, Definition 1.1]) A Mal'cev algebra $\mathbf{A}$ is called a *central-by-simple-nonabelian* algebra if $\mathbf{A}$ has a congruence $\gamma \neq 1_{\mathbf{A}}$ such that $\mathbf{A}/\gamma$ is simple, $[1,1] = 1$ and $[\gamma, 1] = 0$.

4. Commutator Ideals in Expanded Groups

DEFINITION 4.1. (cf. [**34**]) Let $\mathbf{V}$ be an expanded group, and let A, B be ideals of $\mathbf{V}$. We define the commutator ideal $[A, B]_{\mathbf{V}}$ as the ideal of $\mathbf{V}$ that is generated by

$$\{p(a,b) \mid a \in A, b \in B, p \in \mathsf{Pol}_2(\mathbf{V}), p(x,0) = p(0,x) = 0 \text{ for all } x \in V\}.$$

LEMMA 4.2. *Let* $\mathbf{V}$ *be an expanded group, let* A, B *be ideals of* $\mathbf{V}$*,* $k \in \mathbb{N}$*,* $c \in \mathsf{Pol}_{k+1}\mathbf{V}$ *such that* $c(x, \mathbf{0}) = c(0, \mathbf{y}) = 0$ *for all* $x \in V, \mathbf{y} \in V^k$ *and* $a \in A, \mathbf{b} \in B^k$*. Then,* $c(a, \mathbf{b}) \in [A, B]$*.*

Proof: We proceed by induction on k. The case $k = 1$ is obvious from the definition. Now we assume $k \geq 2$. Defining

$$p(x,y) := c(x, b_1, \ldots, b_{k-1}, y) - c(x, b_1, \ldots, b_{k-1}, 0),$$

we see that $p(a, b_k) \in [A, B]$. By the induction hypothesis also $c(a, b_1, \ldots, b_{k-1}, 0)$ is in $[A, B]$. So $p(a, b_k) + c(a, b_1, \ldots, b_{k-1}, 0)$, which is $c(a, b_1, \ldots, b_k)$, is contained in $[A, B]$. $\Box$

Analogously, we can prove that $p(\mathbf{a},\mathbf{b})$ lies in $[A,B]_{\mathbf{V}}$ if $\mathbf{a}\in A^k$, $\mathbf{b}\in B^k$, $p\in \mathsf{Pol}_{2k}(\mathbf{V})$, and $p(\mathbf{0},\mathbf{y})=p(\mathbf{x},\mathbf{0})=0$ for all $\mathbf{x},\mathbf{y}\in V^k$.

PROPOSITION 4.3. *Let* $\mathbf{V}$ *be an expanded group, and let* A, B *be ideals of* $\mathbf{V}$*. Let* $\alpha := \gamma(A)$ *and* $\beta := \gamma(B)$ *be the congruences corresponding to* A *and* B*, respectively. Then,* $[\alpha,\beta] = \gamma([A,B])$*.*

Proof: See [**6**, Lemma 2.9]. □

DEFINITION 4.4. Let $\mathbf{V}$ be an expanded group. For two ideals A, B of $\mathbf{V}$, we write $\mathsf{C}_{\mathbf{V}}(A:B)$ for the largest ideal of $\mathbf{V}$ that satisfies $[B,C]_{\mathbf{V}} \leq A$; this ideal is called the *centralizer* of B modulo A.

The following proposition is the consequence of Propositions 2.2 and 6.1 in [**5**], but here, we give a direct proof.

PROPOSITION 4.5. *Let* $\mathbf{V}$ *be an expanded group, and let* A, B, C, D *be ideals of* $\mathbf{V}$ *such that* $A \prec B$ *and* $C \prec D$*. We assume that the intervals* $I[A,B]$ *and* $I[C,D]$ *are projective. Then,* $\mathsf{C}_{\mathbf{V}}(A:B) = \mathsf{C}_{\mathbf{V}}(C:D)$*.*

Proof: We consider $I[A,B] \nearrow I[C,D]$ without lost of generality. We show that for each ideal X of $\mathbf{V}$, we have $[X,D]_{\mathbf{V}} \leq C$ if and only if $[X,B]_{\mathbf{V}} \leq A$. To prove the "if"-direction of this statement, we compute $[X,D]_{\mathbf{V}} = [X, B\vee C]_{\mathbf{V}}$, which, by the distributivity of the commutator with respect to joins, is equal to $[X,B]_{\mathbf{V}} \vee [X,C]_{\mathbf{V}}$ and hence $[X,D]_{\mathbf{V}} \leq A \vee C = C$. In order to prove "only if", we observe that $[X,B]_{\mathbf{V}} \leq [X,D]_{\mathbf{V}}$, and hence $[X,B]_{\mathbf{V}} \leq C$. Thus, $[X,B]_{\mathbf{V}} \leq C \wedge B = A$. □

DEFINITION 4.6. (cf.[**5**]) An expanded group $\mathbf{V}$ satisfies the condition (SC1) if for every strictly meet irreducible ideal M of $\mathbf{V}$ we have $(M : M^+) \leq M^+$.

5. Tame Congruence Theory in Mal'cev Algebras

In this section we introduce the fundamental notions of tame congruence theory (cf. [**19**]). In this sense Mal'cev algebras have a simple local structure that is completely determined by binary commutators.

DEFINITION 5.1. Let $\mathbf{A}$ be an algebra, let $\theta \in \mathsf{Con}\,\mathbf{A}$, let $\emptyset \neq U \subseteq A$ and let $h : A^n \to A$. We define:

(1) $\theta|_U := \theta \cap (U\times U)$;
(2) $h|_U = h|_{U^n} := \{(x_0,\dots,x_{n-1}, h(x_0,\dots,x_{n-1})) | (x_0,\dots,x_{n-1}) \in U^n\}$;
(3) $(\mathsf{Pol}\,\mathbf{A})|_U$ is the set of all $h|_U$ such that $h \in \mathsf{Pol}_n\mathbf{A}$ for some $n\in\mathbb{N}$ and $h(U^n)\subseteq U$;
(4) $\mathbf{A}|_U := (U, (\mathsf{Pol}\,\mathbf{A})|_U)$, called the *algebra induced on* U *by* $\mathbf{A}$ (or an *induced algebra of* $\mathbf{A}$).

DEFINITION 5.2. Let $\mathbf{A}$ be a finite algebra and let $\alpha < \beta$ be two congruences of $\mathbf{A}$. We define $U_{\mathbf{A}}(\alpha,\beta)$ to be the set of all sets of the form $f(A)$ where $f \in \mathsf{Pol}_1\mathbf{A}$

and $f(\beta) \nsubseteq \alpha$. We define $M_{\mathbf{A}}(\alpha, \beta)$ to be the set of all minimal members of $U_{\mathbf{A}}(\alpha, \beta)$; i.e., $U \in M_{\mathbf{A}}(\alpha, \beta)$ if and only if $U \in U_{\mathbf{A}}(\alpha, \beta)$ and there does not exist a $V \in U_{\mathbf{A}}(\alpha, \beta)$ with $V \subseteq U$, $V \neq U$. The members of $M_{\mathbf{A}}(\alpha, \beta)$ are called $\langle \alpha, \beta \rangle$-*minimal sets* of $\mathbf{A}$.

DEFINITION 5.3. A finite algebra $\mathbf{C}$ will be called *minimal relative to its congruence quotient* $\langle \delta, \theta \rangle$, or simply $\langle \delta, \theta \rangle$-*minimal*, if $C \in M_{\mathbf{C}}(\delta, \theta)$.

A finite algebra $\mathbf{C}$ is called *minimal* if $\mathbf{C}$ is $\langle 0_C, 1_C \rangle$-minimal, or equivalently, $|C| > 1$ and every nonconstant $f \in \mathsf{Pol}_1\mathbf{C}$ is a permutation of C.

THEOREM 5.4 (P.P.Pálfy). *Every minimal algebra of at least three elements, that has a polynomial operation which depends on more than one variable, is polynomially equivalent to a vector space over a finite field.*

Proof: See [**19**, Theorem 4.7]. □

LEMMA 5.5 (D. Hobby, R. McKenzie). *Every algebra on the two element domain* $\{0, 1\}$ *is polynomially equivalent to one of the following, no two of which are polynomially equivalent:* $\mathbf{E}_0 = (\{0, 1\})$, $\mathbf{E}_1 = (\{0, 1\}, ')$, $\mathbf{E}_2 = (\{0, 1\}, +)$, $\mathbf{E}_3 = (\{0, 1\}, \vee, \wedge, ')$, $\mathbf{E}_4 = (\{0, 1\}, \vee, \wedge)$, $\mathbf{E}_5 = (\{0, 1\}, \vee)$, $\mathbf{E}_6 = (\{0, 1\}, \wedge)$.

Proof: See [**19**, Lemma 4.8]. □

The algebras $\mathbf{E}_5$ and $\mathbf{E}_6$ are isomorphic, and every algebra isomorphic to one of them is called a *two-element semilattice*. An algebra is a *two-element lattice* or *Boolean algebra* if it is isomorphic to $\mathbf{E}_4$ (or to $\mathbf{E}_3$, respectively).

DEFINITION 5.6. Let $\mathbf{M}$ be a minimal algebra.

(1) $\mathbf{M}$ is of *type 1* or *unary type*, if $\mathsf{Pol}\,\mathbf{M} = \mathsf{Pol}(M, \Pi)$ for a subgroup Π of the group of all permutations on set M.
(2) $\mathbf{M}$ is of *type 2* or *affine type*, if $\mathbf{M}$ is polynomially equivalent to a vector space.
(3) $\mathbf{M}$ is of *type 3* or *Boolean type*, if $\mathbf{M}$ is polynomially equivalent to a two-element Boolean algebra.
(4) $\mathbf{M}$ is of *type 4* or *lattice type*, if $\mathbf{M}$ is polynomially equivalent to a two-element lattice.
(5) $\mathbf{M}$ is of *type 5* or *semilattice type*, if $\mathbf{M}$ is polynomially equivalent to a two-element semilattice.

Now as a consequence of Theorem 5.4 and Lemma 5.5 we obtain the full classification of minimal algebras in the following corollary.

COROLLARY 5.7. *If a finite algebra is minimal, then it is of one of types 1-5.*

DEFINITION 5.8. Let $\mathbf{C}$ be an algebra and $\delta, \theta \in \mathsf{Con}\,\mathbf{C}$ such that $\mathbf{C}$ is $\langle \delta, \theta \rangle$-minimal. By a $\langle \delta, \theta \rangle$-*trace* in $\mathbf{C}$ we mean any set $N \subseteq C$ of the form x/θ such that $x/\theta \neq x/\delta$. The *body* and the *tail* of $\mathbf{C}$ (with respect to $\langle \delta, \theta \rangle$) are defined in this way:

$$\text{body} = \bigcup \{x/\theta \,|\, x/\theta \neq x/\delta\},$$
$$\text{tail} = C \backslash \text{body}.$$

DEFINITION 5.9. Let $\mathbf{A}$ be an algebra and $\alpha, \beta \in \mathsf{Con}\,\mathbf{A}$ such that $\alpha \prec \beta$. By an $\langle \alpha, \beta \rangle$-*trace* of $\mathbf{A}$ we mean any set $N \subseteq A$ such that for some $U \in M_{\mathbf{A}}(\alpha, \beta)$, $N \subseteq U$ and N is an $\langle \alpha|_U, \beta|_U \rangle$-trace of the $\langle \alpha|_U, \beta|_U \rangle$-minimal algebra $\mathbf{A}|_U$ (i.e., $N = x/\beta \cap U$ for some $x \in U$ such that $x/\beta \cap U \not\subseteq x/\alpha$). The *body* and the *tail* of $\mathbf{A}$ (with respect to $\langle \alpha|_U, \beta|_U \rangle$) are defined in this way:

$$\text{body} = \bigcup \{x/\beta \cap U \,|\, x/\beta \cap U \not\subseteq x/\alpha\},$$
$$\text{tail} = C \backslash \text{body}.$$

DEFINITION 5.10. Let $\mathbf{C}$ be an algebra and $\delta, \theta \in \mathsf{Con}\,\mathbf{C}$ such that $\mathbf{C}$ is minimal relative to $\langle \delta, \theta \rangle$. Let $i \in \{1, 2, 3, 4, 5\}$. We say that $\mathbf{C}$ has *type i relative to* $\langle \delta, \theta \rangle$ if for each $\langle \delta, \theta \rangle$-trace N, $(\mathbf{C}|_N)/(\delta|_N)$ is minimal algebra of type i.

THEOREM 5.11 (D. Hobby, R. McKenzie). *In every finite algebra $\mathbf{A}$ that is minimal with respect to its congruence quotient $\langle \alpha, \beta \rangle$, all $\langle \alpha, \beta \rangle$-traces induce minimal algebras of the same type.*

Proof: See [**19**, Theorem 4.23, Definition 4.21]. □

DEFINITION 5.12. Let $\mathbf{A}$ be an algebra, $\alpha, \beta, \gamma, \lambda \in \mathsf{Con}\,\mathbf{A}$ such that $\alpha \prec \beta$ and let $U \in M_{\mathbf{A}}(\alpha, \beta)$. We define the *type of* $\langle \alpha, \beta \rangle$, written $\text{typ}(\alpha, \beta)$, to be the type of $\mathbf{A}|_U$ relative to $\langle \alpha|_U, \beta|_U \rangle$. By $\text{typ}\{\gamma, \lambda\}$ we denote the set $\{\text{typ}(\alpha, \beta) \,|\, \gamma \leq \alpha \prec \beta \leq \gamma\}$. By $\text{typ}\{\mathbf{A}\}$ we denote the set $\text{typ}\{0_A, 1_A\}$. By $\text{typ}\{\mathcal{V}\}$ we denote the set $\bigcup \{\text{typ}\{\mathbf{A}\} \,|\, \mathbf{A} \in \mathcal{V}\}$.

THEOREM 5.13 (D. Hobby, R. McKenzie). *Let $\mathcal{V}$ be a locally finite variety. If $\mathcal{V}$ is congruence permutable then* $\text{typ}\{\mathcal{V}\} \in \{2, 3\}$.

Proof: See [**19**, Theorem 9.14(1)]. □

COROLLARY 5.14. *Let $\mathbf{A}$ be a finite Mal'cev algebra. Then* $\text{typ}\{\mathbf{A}\} \in \{2, 3\}$.

Proof: Since $\mathbf{A}$ is finite, $\mathcal{V}(\mathbf{A})$ is a locally finite variety by [**13**, Theorem 10.16]. By Theorem 5.13 we have $\text{typ}\{\mathcal{V}(\mathbf{A})\} \in \{2, 3\}$. Clearly, $\text{typ}\{\mathbf{A}\} \in \{2, 3\}$. □

THEOREM 5.15 (D. Hobby, R. McKenzie). *Let $\mathbf{A}$ be a finite Mal'cev algebra and let $\alpha, \beta \in \mathsf{Con}\,\mathbf{A}$ be such that $\alpha \prec \beta$. Then, $\langle \alpha, \beta \rangle$ has type 2 if and only if it is abelian.*

Proof: This is a consequence of Corollary 5.14 and [**19**, Theorem 5.7(3)]. □

In case of a type 2 quotient $\alpha \prec \beta$ in an algebra $\mathbf{A}$, we define $\text{subtyp}(\alpha, \beta)$ to be the cardinality of the scalar field for the appropriate vector space. If $\text{typ}(\alpha, \beta) =$

3 then subtype$(\alpha,\beta) = \emptyset$. Furthermore, by exttyp$(\alpha,\beta)$, we denote the pair (typ(α,β), subtyp(α,β)).

In the case of type 2 for congruences α and β of a given algebra $\mathbf{A}$, $\alpha \prec \beta$, we define subtyp(α,β) to be the cardinality of the scalar field for the appropriate vector space. If typ$(\alpha,\beta) = 3$ then subtype$(\alpha,\beta) = \emptyset$. Furthermore, by exttyp$(\alpha,\beta)$, we denote the pair (typ(α,β), subtyp(α,β)).

Let $\mathbf{A}$ be an algebra from a congruence permutable veriety. We say that a function $f : A^k \to A$ is $\mathbf{A}$-typ-*admissible* if f is a congruence preserving function and for every $\alpha, \beta \in \mathsf{Con}\,\mathbf{A}$ such that $\alpha \prec \beta$ we have $\mathrm{typ}_{\mathbf{A}+f}(\alpha,\beta) = \mathrm{typ}_{\mathbf{A}}(\alpha,\beta)$. We say that a function $f : A^k \to A$ is $\mathbf{A}$-exttyp-*admissible* if f is a congruence preserving function and for every $\alpha, \beta \in \mathsf{Con}\,\mathbf{A}$ such that $\alpha \prec \beta$ we have $\mathrm{exttyp}_{\mathbf{A}+f}(\alpha,\beta) = \mathrm{exttyp}_{\mathbf{A}}(\alpha,\beta)$.

6. Lattices With Special Properties

This section is devoted to one special class of complete lattices that we need in the first section of Chapter 3. We first demonstrate some advanced properties of homogeneous series in modular lattices which we then use to introduce and characterize (APMI) lattices. The section ends with a collection of results that are not needed for the rest of the thesis, but contribute to deeper understanding of (APMI) lattices.

6.1. Homogeneous series in modular lattices. In this subsection, we will investigate certain elements in modular lattices. In [**5**], *homogeneous* elements of a bounded lattice played an important role.

Definition 6.1. Let $\mathbf{L}$ be a bounded lattice. We call an element μ of L *homogeneous* if

(1) $\mu > 0$,
(2) for all $\alpha, \beta, \gamma, \delta \in L$ with $\alpha \prec \beta \leq \mu$ and $\gamma \prec \delta \leq \mu$, the intervals $I[\alpha,\beta]$ and $I[\gamma,\delta]$ are projective intervals of $\mathbf{L}$, and
(3) there are no $\alpha, \beta, \gamma, \delta \in L$ such that $\alpha \prec \beta \leq \mu \leq \gamma \prec \delta$, and $I[\alpha,\beta]$ and $I[\gamma,\delta]$ are projective.

It is not hard to show that this definition is equivalent to the definition of homogeneous elements of finite lattices given in [**5**, Definition 7.1]. We recall that an element μ of $\mathbf{L}$ is called *distributive* if $\mu \vee (\alpha \wedge \beta) = (\mu \vee \alpha) \wedge (\mu \vee \beta)$ for all $\alpha, \beta \in L$. For a lattice $\mathbf{L}$, let $D(\mathbf{L})$ denote the set of distributive elements of $\mathbf{L}$. In a modular lattice, $D(\mathbf{L})$ is closed under joins and meets, and therefore, it is the universe of a sublattice of $\mathbf{L}$ (this follows from [**16**, p. 187, Theorem 6, and p. 188, Theorem 9]). From [**16**, p. 176, Corollary 9] and [**16**, p. 186, Theorem 5, and p. 187, Theorem 6] we obtain that in a modular lattice $\mathbf{L}$, we have $\alpha \vee (\beta \wedge \gamma) = (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$ and $\alpha \wedge (\beta \vee \gamma) = (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$ if at least one of α, β, γ lies in $D(\mathbf{L})$.

THEOREM 6.2 (G.Grätzer, E. T. Schmidt). *In a weakly modular lattice* $\mathbf{L}$*, an element* $a \in L$ *is distributive if and only if*

$$(a \vee x) \wedge (x \vee y) \wedge (y \vee a) = (a \wedge x) \vee (x \wedge y) \vee (y \wedge a)$$

for all $x, y \in L$.

Proof: See [**16**, p. 187, Theorem 6]. □

COROLLARY 6.3. *In every modular lattice every distributive element is dually distributive.*

Proof: Every modular lattice is weakly modular by Proposition 1.16. One can easily see that the necessary and sufficient condition for distributivity in Theorem 6.2 is selfdual. □

LEMMA 6.4. (cf. [**8**, Lemma 7.3]) *Let* $\mathbf{L}$ *be an algebraic modular lattice. Then every homogeneous element of* $\mathbf{L}$ *is distributive.*

DEFINITION 6.5. Let $\mathbf{L}$ be an algebraic modular lattice with $|L| > 1$, and let $n \in \mathbb{N}$. A sequence $(\alpha_0, \alpha_1, \ldots, \alpha_n)$ is a *homogeneous series* for $\mathbf{L}$ if

(1) for each $i \in \{1, \ldots, n\}$, α_i is a homogeneous element of the lattice $\mathbf{I}[\alpha_{i-1}, 1]$, and
(2) $\alpha_0 = 0$ and $\alpha_n = 1$.

PROPOSITION 6.6. (cf. [**8**, Proposition 7.5]) *Let* $\mathbf{L}$ *be an algebraic modular lattice with* $|L| > 1$*, let* $n \in \mathbb{N}$*, and let* $(\alpha_0, \ldots, \alpha_n)$ *be a homogeneous series of* $\mathbf{L}$*. Then for all* $i \in \{0, \ldots, n\}$*,* α_i *is a distributive element of* $\mathbf{L}$.

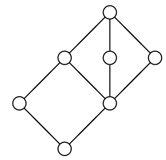
PROPOSITION 6.7. (cf. [**8**, Proposition 7.8]) *Let* $\mathbf{L}$ *be an algebraic modular lattice with* $|L| > 1$*. We assume that* $\mathbf{L}$ *has a homogeneous series* $(\alpha_0, \ldots, \alpha_n)$*. Let* $m \in \mathbb{N}$*, and let* $\beta_0, \ldots, \beta_m \in D(\mathbf{L})$ *be such that* $\beta_0 < \beta_1 < \cdots < \beta_m$*. Then the following are equivalent:*

(1) *The sequence* $(\beta_0, \ldots, \beta_m)$ *is a homogeneous series of* $\mathbf{L}$.
(2) *The sequence* $(\beta_0, \ldots, \beta_m)$ *is a maximal chain in the lattice* $D(\mathbf{L})$.

6.2. Modular lattices with adjacent projective meet irreducible elements.

DEFINITION 6.8. Let $\mathbf{L}$ be a complete lattice. We say that $\mathbf{L}$ has *adjacent projective meet irreducibles* if for all strictly meet irreducible elements α, β of $\mathbf{L}$ such that $I[\alpha, \alpha^+] \leftrightsquigarrow I[\beta, \beta^+]$, we have $\alpha^+ = \beta^+$.

As an abbreviation, we say that $\mathbf{L}$ satisfies the property (APMI) if it has adjacent projective meet irreducibles. As an example, we consider the following lattice $\mathbf{L} = \mathbf{M}_{2,3}$, which satisfies (APMI).



$\mathbf{M}_{2,3}$ satisfies (APMI)

We note that the dual of this lattice does not satisfy (APMI).

The following proposition provide us with a class of (APMI) lattices.

Proposition 6.9. (cf. [**8**, Proposition 8.2]) *Let* $\mathbf{V}$ *be an expanded group with* (SC1)*. Then the congruence lattice of* $\mathbf{V}$ *satisfies the property* (APMI)*.*

We will now see that several facts that were established in [**22**] for the congruence lattice of an algebra with (SC1) hold for all algebraic modular lattices with (APMI).

Proposition 6.10. (cf. [**8**, Proposition 8.3]) *Let* $\mathbf{L}$ *be an algebraic modular lattice with* (APMI)*, and let* α, β *be strictly join irreducible elements of* $\mathbf{L}$*. We assume* $I[\alpha^-, \alpha] \leftrightsquigarrow I[\beta^-, \beta]$ *and* $\alpha \leq \beta$*. Then* $\alpha = \beta$*.*

Proposition 6.11. (cf. [**8**, Proposition 8.4]) *Let* $\mathbf{L}$ *be an algebraic modular lattice with* (APMI)*, and let* α, β, γ *be strictly join irreducible elements of* $\mathbf{L}$ *such that* $I[\alpha^-, \alpha] \leftrightsquigarrow I[\beta^-, \beta]$*, and* $\beta < \gamma$*. Then we have* $\alpha < \gamma$*.*

For a lattice $\mathbf{L}$, we abbreviate the set of strictly join irreducible elements of $\mathbf{L}$ by $J(\mathbf{L})$. For $\alpha, \beta \in J(\mathbf{L})$, we define a relation $\sim$ by

$$\alpha \sim \beta :\Leftrightarrow I[\alpha^-, \alpha] \leftrightsquigarrow I[\beta^-, \beta].$$

On $J(\mathbf{L})/\!\sim$, we define a relation $\leq$ by

$$\leq \; := \{(\alpha/\!\sim, \; \beta/\!\sim) \,|\, \alpha, \beta \in J(\mathbf{L}) \text{ and } \alpha \leq \beta\}.$$

Hence, we have $\alpha/\!\sim \; \leq \; \beta/\!\sim$ if there are $\alpha', \beta' \in J(\mathbf{L})$ such that $\alpha' \sim \alpha$, $\beta' \sim \beta$, and $\alpha' \leq \beta'$.

Proposition 6.12. (cf. [**8**, Proposition 8.5]) *Let* $\mathbf{L}$ *be an algebraic modular lattice with* (APMI)*. Then* $\leq$ *is a partial order on* $J(\mathbf{L})/\!\sim$*.*

Following [**16**], we call a lattice $\mathbf{L}$ *atomic* if it has a 0, and for every $\alpha \in L \setminus \{0\}$ there is a $\gamma \in L$ such that $0 \prec \gamma \leq \alpha$.

Proposition 6.13. (cf. [**8**, Proposition 8.6]) *Let* $\mathbf{L}$ *be an atomic algebraic modular lattice with* (APMI)*, and let* $\alpha \in J(\mathbf{L})$ *be such that* $\alpha/\!\sim$ *is a minimal element of* $(J(\mathbf{L})/\!\sim, \leq)$*. Then every* $\alpha' \in \alpha/\!\sim$ *is an atom of* $\mathbf{L}$*.*

The next Proposition yields that in a modular lattice of finite height with (APMI), the partially ordered set $(J(\mathbf{L})/\!\sim, \leq)$ contains a minimal element.

Proposition 6.14. (cf. [**8**, Proposition 8.7]) *Let* $\mathbf{L}$ *be a modular lattice with* (APMI) *of finite height* n*, and let* $\alpha_1, \ldots, \alpha_m \in J(\mathbf{L})$ *be such that*

$$\alpha_1/\!\sim \;<\; \alpha_2/\!\sim \;<\; \cdots \;<\; \alpha_m/\!\sim.$$

Then $m \leq n$*.*

Proposition 6.15. (cf. [**8**, Proposition 8.8]) *Let* $\mathbf{L}$ *be an algebraic modular lattice with* (APMI) *that satisfies the descending chain condition. We assume that* $\alpha \in J(\mathbf{L})$ *is such that* $\alpha/\!\sim$ *is a minimal element of* $(J(\mathbf{L})/\!\sim, \leq)$*. Let* μ *be the element of* $\mathbf{L}$ *defined by*

$$\mu := \bigvee\{\beta \,|\, \beta \in \alpha/\!\sim\}.$$

Then μ *is a homogeneous element of* $\mathbf{L}$*.*

For an element μ of a complete lattice $\mathbf{L}$, we define

$$\Phi(\mu) := \mu \wedge \bigwedge\{\alpha \in L \,|\, \alpha \prec \mu\}.$$

Proposition 6.16. (cf. [**8**, Proposition 8.9]) *Let* $\mathbf{L}$ *be a modular lattice of finite height that satisfies* (APMI)*. Then* $\mathbf{L}$ *has a homogeneous element. Furthermore, for every homogeneous* $\mu \in L$*,* $I[0, \mu]$ *is a simple complemented modular lattice, and* $\Phi(\mu) = 0$*.*

We note that the structure of simple complemented modular lattices with finite height is well known by [**29**, Theorem 4.87].

For an element μ of a complete lattice $\mathbf{L}$, we define

$$\mu^* := \bigvee\{\alpha \in L \,|\, \alpha \wedge \mu = 0\}.$$

Proposition 6.17. (cf. [**8**, Proposition 8.10]) *Let* $\mathbf{L}$ *be a modular lattice of finite height with* (APMI)*, and let* μ *be a homogeneous element of* $\mathbf{L}$*. Then* $\mu \wedge \mu^* = 0$*, and for all* $\alpha \in L$*, we have* $\alpha \geq \mu$ *or* $\alpha \leq \mu \vee \mu^*$*.*

6.3. The Class of (APMI) Lattices. In this subsection we analyze the class of (APMI) lattices in universal algebraic and first order logic sense. Since the class is new we would like to know whether (APMI) property can be described using identities or first order predicate formulas.

Proposition 6.18.
(a) *The* (APMI) *property is not representable with a set of identities on the language of bounded lattices* $\wedge, \vee, 0, 1$*.*
(b) *The class of* (APMI) *lattices is not closed for subdirect products.*

Proof:

(a) It is not hard to see that the lattice $\mathbf{L}_1$ obtained as the direct product of the diamond $\mathbf{M}_3 = (\{0, a, b, c, 1\}, \wedge, \vee)$ and the two element lattice $\{\mathbf{0}, \mathbf{1}\} = (\{0, 1\}, \wedge, \vee)$ is an (APMI) lattice. The lattice

$$\mathbf{L}_2 = (\{(0,0), (a,0), (b,0), (c,0), (1,0), (a,1), (1,1)\}, \wedge, \vee)$$

is a sublattice of $\mathbf{L}_1$. The element $(b, 0)$ is (strictly) meet irreducible and $I[(b, 0), (1, 0)]$ is projective to $I[(a, 1), (1, 1)]$, where $(a, 1)$ is also (strictly) meet irreducible. Thus $\mathbf{L}_2$ does not satisfy the (APMI) property. Then we conclude that the class of (APMI) lattices is not closed for substructures and thus does not form a variety. By Theorem of Birkhoff (see [**29**]) this is not an equational class.

(b) Since $\pi_1(L_2) = M_3$ and $\pi_2(L_2) = \{0, 1\}$ we conclude that $\mathbf{L}_2$ is a subdirect product of $\mathbf{M}_3 \times \{\mathbf{0}, \mathbf{1}\}$. It is easy to verify that $\mathbf{M}_3$ and $\{\mathbf{0}, \mathbf{1}\}$ are (APMI) lattices and thus we obtain that a subdirect product of two (APMI) lattices is not necessarily an (APMI) lattice. □

In order to investigate the behavior of this class under other class operators such as the direct product, we first prove the following lemma.

LEMMA 6.19. *Let $I \neq \emptyset$ and let $\{\mathbf{L}_i | i \in I\}$ be a family of bounded lattices. An element $\mu \in \prod_{i\in I} L_i$ is a meet irreducible if $\mu(j)$ is meet irreducible element of $\mathbf{L}_j$ for precisely one $j \in I$ and $\mu(i) = 1$ for $i \neq j$.*

Proof: If $\mu \neq 1$ is meet irreducible in $\prod_{i\in I} \mathbf{L}_i$ then there is a $j \in I$ such that $\mu(j) \neq 1_{\mathbf{L}_j}$. If there exists an $i, i \neq j$ with this property then for $k \in \{i, j\}$ we define:

$$\mu_k(t) = \begin{cases} \mu(k), & t = k \\ 1, & t \neq k \end{cases}$$

It is clear that $\mu = \mu_i \wedge \mu_j$. Contradiction. Let $\mu(j)$ be a meet irreducible element of $\mathbf{L}_j$ for precisely one $j \in I$ and $\mu(i) = 1$ for $i \neq j$. Since $1_{\mathbf{L}_i}$ is meet irreducible in every $\mathbf{L}_i$, if $\mu(i) = \alpha(i) \wedge \beta(i)$ for every $i \in I$ and $\alpha, \beta \in \prod_{i\in I} L_i$, we conclude that $\mu = \alpha$ or $\mu = \beta$. □

Now, we can prove the following.

PROPOSITION 6.20. *The class of* (APMI) *lattices is closed for arbitrary direct products.*

Proof: If $\mu \in \prod_{i\in I} L_i$, where $\mathbf{L}_i$ satisfies the (APMI) property for every $i \in I$ and μ^+ is the unique cover of μ then μ is meet irreducible. By Lemma 6.19 for precisely one $j \in I$, $\mu(j) \neq 1_{\mathbf{L}_j}$ and for this j, $\mu(j)$ is meet irreducible in $\mathbf{L}_j$. Now, $\mu^+(j)$ is the unique cover of $\mu(j)$, since μ^+ is the unique cover of μ.

Let $\alpha, \beta \in \prod_{i\in I} L_i$, $\alpha, \beta \neq 1$ where $\mathbf{L}_i$ satisfies the (APMI) property for every $i \in I$, let α^+ be the unique cover of α and β^+ the unique cover of β such that $I[\alpha, \alpha^+]$ is projective to $I[\beta, \beta^+]$. We proved above that there exist $j, k \in I$ such that $\alpha^+(i) = 1_{\mathbf{L}_i}$, for every $i \in I, i \neq j$ and $\alpha^+(j)$ is the unique cover of $\alpha(j)$ in $\mathbf{L}_j$ and also, $\beta^+(i) = 1_{\mathbf{L}_i}$, for every $i \in I, i \neq k$ and $\beta^+(k)$ is unique cover of $\beta(k)$ in $\mathbf{L}_k$. Since $\alpha, \beta \neq 1$ and $I[\alpha(i), \alpha^+(i)]$ is projective to $I[\beta(i), \beta^+(i)]$ in $\mathbf{L}_i$, for every $i \in I$, while $I[\alpha, \alpha^+]$ is projective to $I[\beta, \beta^+]$, we conclude that $j = k$. Now, $I[\alpha(j), \alpha^+(j)]$ is projective to $I[\beta(j), \beta^+(j)]$ in $\mathbf{L}_j$ and $\mathbf{L}_j$ has the (APMI) property, thus $\alpha^+(j) = \beta^+(j)$. That implies $\alpha^+ = \beta^+$, while $\alpha^+(i) = 1_{\mathbf{L}_i} = \beta^+(i)$, for every $i \in I, i \neq j$. $\square$

PROPOSITION 6.21. *Class of* (APMI) *lattices is elementary class on the language of bounded lattices.*

Proof: Let us introduce the following notation.

(1) $\prec(x,y) \equiv (x \leq y \wedge \neg x = y \wedge (\forall z)(x \leq z \wedge z \leq y \Rightarrow z = x \vee z = y))$
(2) $HUC(x,y) \equiv (x \leq y \wedge (\forall z)(x \leq z \wedge \neg(x = z) \Rightarrow y \leq z))$
(3) $\nearrow(x,y,z,t) \equiv (\prec(x,y) \wedge \prec(z,t) \wedge (y \wedge z = x) \wedge (y \vee z = t))$
(4) $\searrow(x,y,z,t) \equiv (\prec(x,y) \wedge \prec(z,t) \wedge (x \wedge t = z) \wedge (x \vee t = y))$
(5) $T(x,y,z,t) \equiv \nearrow(x,y,z,t) \vee \searrow(x,y,z,t)$

Let

$$\Phi_0(x,y,z,t) \equiv (\forall x)(\forall y)(\forall z)(\forall t)(HUC(x,z) \& HUC(y,t) \& T(x,z,y,t) \Rightarrow z = t)$$

and

$$\Phi_k(x,y,z,t) \equiv (\forall x)(\forall y)(\forall z)(\forall t)\Big(HUC(x,z) \wedge HUC(y,t) \wedge$$
$$(\exists u_1)\dots(\exists u_k)(\exists v_1)\dots(\exists v_k)\big(\prec(u_1,v_1) \wedge \dots \wedge \prec(u_k,v_k) \wedge$$
$$T(x,z,u_1,v_1) \wedge \dots \wedge T(u_k,v_k,y,t)\big) \Rightarrow z = t\Big),$$

for every $k \geq 1$.

We will prove that the set of formulas $\{\Phi_0, \dots, \Phi_k, \dots\}$ together with formulas which define bounded lattices is the set of formulas which determine the class of (APMI) lattices.

Let $\mathbf{L}$ be a bounded lattice such that $\mathbf{L} \models \Phi_k$ for every $k \geq 0$ and let $\mu_1, \mu_2 \in L$ be such that they have unique covers $\mu_1^+, \mu_2^+ \in L$, such that $\mu_1 \prec \mu_1^+$, $\mu_2 \prec \mu_2^+$ and $I[\mu_1, \mu_1^+] \leftrightsquigarrow I[\mu_2, \mu_2^+]$.

(1) If $I[\mu_1, \mu_1^+] \nearrow I[\mu_2, \mu_2^+]$ or $I[\mu_1, \mu_1^+] \searrow I[\mu_2, \mu_2^+]$ then $\mu_1^+ = \mu_2^+$, since $\mathbf{L} \models \Phi_0$.
(2) If $I[\mu_1, \mu_1^+](\nearrow \cup \searrow)^k I[\mu_2, \mu_2^+]$, for some $k > 0$ then $\mu_1^+ = \mu_2^+$, since $\mathbf{L} \models \Phi_k$.

In both cases the (APMI) property is satisfied.

Now, suppose that a bounded lattice $\mathbf{L}$ is an (APMI) lattice. Let $k > 0$. If

$$\mathbf{L} \models HUC(x,z) \wedge HUC(y,t) \wedge$$
$$(\exists u_1)\dots(\exists u_k)(\exists v_1)\dots(\exists v_k)(\prec(u_1,v_1) \wedge \dots \wedge \prec(u_k,v_k) \wedge$$
$$T(x,z,u_1,v_1) \wedge \dots \wedge T(u_k,v_k,y,t))$$

for some x,y,z,t then $I[x,z] \leftrightsquigarrow I[y,t]$ which implies $z = t$ by (APMI), since z is the unique cover of x and t is the unique cover of y. Thus,

$$\mathbf{L} \models HUC(x,z) \wedge HUC(y,t) \wedge$$
$$(\exists u_1)\dots(\exists u_k)(\exists v_1)\dots(\exists v_k)(\prec(u_1,v_1) \wedge \dots \wedge \prec(u_k,v_k) \wedge$$

$$T(x,z,u_1,v_1) \wedge \cdots \wedge T(u_k,v_k,y,t)) \Rightarrow z = t.$$

So, $\mathbf{L} \models \Phi_k$. Similarly, $\mathbf{L} \models \Phi_0$. □

7. Polynomials and Clones

In this dissertation, we investigate polynomial functions on Mal'cev algebras. In this section we provide precise definitions of various types of affine completeness, clones and a few related notions.

Let $k \in \mathbb{N}$. An algebra $\mathbf{A}$ is *k-affine complete* if every k-ary congruence preserving function is a polynomial function. An algebra $\mathbf{A}$ is affine complete if it is k-affine complete for every k, $k \geq 1$. Among a number of classes of affine complete algebras, we will use affine complete $\mathbf{M}_n(\mathbf{D})$-modules to obtain the results in Chapter 3.

THEOREM 7.1. *Let $k, m, n \in \mathbb{N}$, let $\mathbf{D}$ be a finite field, let $\mathbf{M}_n(\mathbf{D})$ be the ring of $n \times n$-matrices over $\mathbf{D}$, and let $\mathbf{D}^{(n\times m)}$ denote the $\mathbf{M}_n(\mathbf{D})$-module of all $n \times m$-matrices with entries from $\mathbf{D}$. Then, $\mathbf{D}^{(n\times m)}$ is k-affine complete if and only if $m \geq 2$ or ($k = m = n = 1$ and $|\mathbf{D}| = 2$).*

Proof: See [**8**, Theorem 6.1(1)]. □

PROPOSITION 7.2. *Let $\mathbf{A}$ be a finite TC-neutral Mal'cev algebra and let $k \geq 2$. Then every homomorphic image of $\mathbf{A}$ is k-affine complete.*

Proof: The statement can be obtained from [**2**, Proposition 2.1] and [**2**, Proposition 5.2]. □

On several occcasions we use the following two generalizations of affine completeness, that are introduced in [**22**]. An algebra $\mathbf{A}$ is *k-polynomially rich* if every k-ary $\mathbf{A}$-typ-admissible function is a polynomial of $\mathbf{A}$. We say that $\mathbf{A}$ is polynomially rich if it is k-polynomially rich for every $k \in \mathbb{N}$. Moreover, $\mathbf{A}$ is *k-weakly polynomially rich* if every k-ary $\mathbf{A}$-exttyp-admissible function is a polynomial of $\mathbf{A}$. We say that $\mathbf{A}$ is weakly polynomially rich if it is k-polynomially rich for every $k \in \mathbb{N}$.

PROPOSITION 7.3. *Let $\mathbf{A}$ be a finite Mal'cev algebra such that $\mathbf{A}$ and all subdirectly irreducible members of $\mathsf{H}(\mathbf{A})$ satisfy the condition* (SC1). *Then, $\mathbf{A}$ is weakly polynomially rich.*

Proof: See [**22**, Theorem 24, Theorem 31]. □

The polynomial equivalence problem, also called identity checking problem with constants, for a Mal'cev algebra $\mathbf{A}$ is the problem of deciding whether the identity $s \approx t$ is satisfied by $\mathbf{A}$ for given polynomial terms s and t of $\mathbf{A}$. Here, a *polynomial term* is a term that is built up from variables and the elements of $\mathbf{A}$ using the operation symbols of $\mathbf{A}$.

A *clone* on a set A is a collection of finitary functions on A that contains all projections and is closed under all compositions. We investigate those clones that contain all constant functions; such clones have been called *constantive* in [**21**]. We shall also call such clones *polynomial clones*. If F be a set of polynomials of an algebra $\mathbf{A}$, we denote the clone generated by F by $\mathrm{Clo}(F)$.

Using the language of clone theory, the question of classifying algebras modulo polynomial equivalence can be rephrased as the question of describing all polynomial clones on a finite set; so the above results mean that there are 7 constantive clones on a two element set, and for $|A| \geq 3$, there are $2^{\aleph_0}$ clones containing all constant functions on A. A fundamental result in clone theory states that every clone on A can be described by a set of finitary relations on A [**32**, Satz 1.2.1, p. 53]. In this dissertation we exhibit a class of clones such that each clone can be described by a single relation.

In [**21**] it was proved that for a finite set A with $|A| \geq 4$ infinitely many constantive clones on A contain a Mal'cev operation. Now given a finite set and a Mal'cev operation on this set, one may ask in how many constantive clones this operation is contained. For a prime p, there are precisely two constantive clones on the cyclic group $\mathbb{Z}_p$ with p elements that contain the ternary function $(x, y, z) \mapsto x \cdot y^{-1} \cdot z$. On the cyclic group $\mathbb{Z}_{pq}$, where p and q are two different prime numbers, there are exactly 17 different constantive clones that contain the binary group multiplication [**6**], and in general, on every finite group of squarefree order, the number of constantive clones that contain the group multiplication is finite [**27**]. In [**10**] it was shown that in the case of $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$, p a prime number, there are countably many clones that contain the group multiplication and all the constant operations. It is not known whether there exists a finite set A such that there are uncountably many Mal'cev clones on A.

For $k \geq 0$, we denote the set of all k-ary polynomials on an algebra $\mathbf{A}$ by $\mathsf{Pol}_k\mathbf{A}$, and we let $\mathsf{Pol}\,\mathbf{A} := \cup_{k\geq 0}\mathsf{Pol}_k\mathbf{A}$ be the set of all polynomials on $\mathbf{A}$. For $k \geq 1$, we write $\mathsf{Inv}^k(A, \mathsf{Pol}\,\mathbf{A})$ for the set of all at most k-ary relations on the set A that are invariant under all polynomial functions of $\mathbf{A}$, and we let $\mathsf{Inv}(A, \mathsf{Pol}\,\mathbf{A}) := \cup_{k\geq 1}\mathsf{Inv}^k(A, \mathsf{Pol}\,\mathbf{A})$ be the set of all finitary relations that are invariant under $\mathsf{Pol}\mathbf{A}$. If R is a set of relations on A, we denote the set of all the operations on A that preserve all relations from the set R by $\mathsf{Comp}(A, R)$. As a consequence of [**32**, Satz 1.2.1, p. 53], if $\mathbf{A}$ is finite we have

$$\mathsf{Pol}\,\mathbf{A} = \mathsf{Comp}\,(A, \mathsf{Inv}(A, \mathsf{Pol}\,\mathbf{A})).$$

This tells that polynomials of $\mathbf{A}$ are completely determined by the infinite set $\mathsf{Inv}(A, \mathsf{Pol}\,\mathbf{A})$ of relations on A. For many Mal'cev algebras, though, we can actually give a finite subset R of $\mathsf{Inv}(A, \mathsf{Pol}\,\mathbf{A})$ that describes polynomials. In fact, it is not known whether the following conjecture is true.

Conjecture. *For every finite Mal'cev algebra* $\mathbf{A}$ *there is a finite set* R *of relations on* A *such that* $\mathsf{Pol}\,\mathbf{A} = \mathsf{Comp}(A, R)$.

By [**32**, p. 50] we know that for every finite set R of relations on a set A, there is a single finitary relation ρ on A such that $\mathsf{Comp}(A, R) = \mathsf{Comp}(A, \{\rho\})$. Hence the claim of the the conjecture is that for every finite Mal'cev algebra, the polynomials can be described by one single relation. If this conjecture holds, then it has two rather immediate consequences:

(1) On a finite set A, there are at most countably many constantive clones that contain a Mal'cev operation. Hence, there is a countable list of finite Mal'cev algebras such that every finite Mal'cev algebra is polynomially equivalent to an isomorphic copy of one of the algebras in the list.
(2) There is no infinitely descending chain of constantive Mal'cev clones on a finite base set.

We devote Section 3 of Chapter 3 to these questions. Actually, to test whether an n-ary function is contained in $\mathsf{Comp}(A, \mathsf{Inv}(A, \mathsf{Pol}\,\mathbf{A}))$ it is sufficient to check whether f preserves all the relations of arity at most $|A|^n$, as stated in the following lemma.

LEMMA 7.4. (cf. [**32**, Folgerung 1.1.18, p.49]) *Let* $\mathbf{A}$ *be a finite algebra,* $n \in \mathbb{N}$, *and* $f : A^n \to A$. *Then* $f \in \mathsf{Pol}_n\mathbf{A}$ *if and only if* $f \in \mathsf{Comp}(A, \mathsf{Inv}^{|A|^n}(A, \mathsf{Pol}\,\mathbf{A}))$.

LEMMA 7.5. *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term* m. *If* $f \in \mathsf{Comp}(A, \mathsf{Inv}^4(A, \mathsf{Pol}\,\mathbf{A}))$ *then* f *is a commutator preserving function of* $\mathbf{A}$.

Proof: We have $\{\rho(\alpha, \beta, \eta, m) \mid \alpha, \beta, \eta \in \mathsf{Con}\,\mathbf{A}, C(\alpha, \beta; \eta)\} \subseteq \mathsf{Inv}^4(A, \mathsf{Pol}\,\mathbf{A})$, by Lemma 3.9. Clearly, $\mathsf{Con}\,\mathbf{A} \subseteq \mathsf{Inv}^4(A, \mathsf{Pol}\,\mathbf{A})$ and thus f is a commutator preserving function by Lemma 3.8. $\square$

CHAPTER 2

Higher Commutators

Many properties of a universal algebra can be seen from its congruence lattice and the binary commutator operation on this lattice. The binary commutator operation for arbitrary universal algebras was introduced in [**35**] and studied further in [**3, 14, 17, 29**]. However, even in a congruence permutable variety, an algebra need not be determined up to polynomial equivalence by its unary polynomial functions, its congruences, and the commutator operation on these congruences. In [**9**], A. Bulatov generalized the binary commutator operation by introducing n-ary commutator operations for all $n \in \mathbb{N}$ and thereby provided a finer tool to distinguish between polynomially inequivalent algebras.

In this thesis we use n-ary commutator operations to obtain the main theorems of this thesis given in Chapter 3 (Theorem §3.2.3, Theorem §3.1.18 and Theorem §3.3.22). However, the main part of this chapter is devoted to proving several properties of Bulatov's higher commutator operations in congruence permutable varieties. While these properties seem quite natural, our proofs require a rather technical tool that we develop here, namely the difference operator on polynomial functions. The higher commutator operations are particularly interesting for expanded groups. In Corollary 4.11, we give a description of the higher commutator operations for expanded groups that resembles the description of the binary commutator operation stated in Definition 4.1.

1. Higher Commutators

In this section, we define the higher centralizers and the higher commutators and list their properties, which we will prove in this chapter.

Definition 1.1 (cf.[**9**]). Let $\mathbf{A}$ be an algebra, let $n \in \mathbb{N}$, and let $\alpha_1, \ldots, \alpha_n, \beta, \delta$ be congruences of $\mathbf{A}$. Then we say that $\alpha_1, \ldots, \alpha_n$ *centralize* β *modulo* δ if for all polynomials $f(\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{y})$ and vectors $\mathbf{a}_1, \mathbf{b}_1, \ldots, \mathbf{a}_n, \mathbf{b}_n, \mathbf{c}, \mathbf{d}$ from $\mathbf{A}$ satisfying:

(1) $\mathbf{a}_i \equiv_{\alpha_i} \mathbf{b}_i$ for all $i \in \{1, 2, \ldots, n\}$,
(2) $\mathbf{c} \equiv_{\beta} \mathbf{d}$, and
(3) $f(\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{c}) \equiv_{\delta} f(\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{d})$ for all $(\mathbf{x}_1, \ldots, \mathbf{x}_n) \in \{\mathbf{a}_1, \mathbf{b}_1\} \times \cdots \times \{\mathbf{a}_n, \mathbf{b}_n\} \backslash \{(\mathbf{b}_1, \ldots, \mathbf{b}_n)\}$

we have

$$f(\mathbf{b}_1, \ldots, \mathbf{b}_n, \mathbf{c}) \equiv_{\delta} f(\mathbf{b}_1, \ldots, \mathbf{b}_n, \mathbf{d}).$$

We abbreviate this property by $C(\alpha_1, \ldots, \alpha_n, \beta; \delta)$.

It follows immediately from the definition that for congruences $\alpha_1, \dots, \alpha_n, \beta$, $\{\delta_i \mid i \in I\}$, we have: if $C(\alpha_1, \dots, \alpha_n, \beta; \delta_i)$ for each $i \in I$, then

$$C(\alpha_1, \dots, \alpha_n, \beta; \bigwedge_{i \in I} \delta_i).$$

This justifies the following definition.

DEFINITION 1.2 (cf.[**9**]). Let $\mathbf{A}$ be an algebra, let $n \geq 2$, and let $\alpha_1, \dots, \alpha_n$ be congruences of $\mathbf{A}$. The smallest congruence δ such that $C(\alpha_1, \dots, \alpha_{n-1}, \alpha_n; \delta)$ holds is called the *(n-ary) commutator of* $\alpha_1, \dots, \alpha_n$. We abbreviate it by $[\alpha_1, \dots, \alpha_n]$.

Notice that for $n = 1$ in Definition 1.1 we obtain the definition of the (binary) centralizing relation that is used in [**14**]. For $n = 2$, Definition 1.2 yields the binary term-condition commutator ([**29**, Definition 4.150]).

PROPOSITION 1.3. (cf. [**9**, Proposition 1]) *Let $k \geq 1$ and let $\alpha_0, \dots, \alpha_k$ be congruences of an algebra $\mathbf{A}$. Then:*

(HC1) $[\alpha_0, \dots, \alpha_k] \leq \bigwedge_{0 \leq i \leq k} \alpha_i$;

(HC2) *for all $\beta_0, \dots, \beta_k \in \mathsf{Con}\,\mathbf{A}$ such that $\alpha_0 \leq \beta_0, \dots, \alpha_k \leq \beta_k$, we have*

$$[\alpha_0, \dots, \alpha_k] \leq [\beta_0, \dots, \beta_k];$$

(HC3) $[\alpha_0, \dots, \alpha_k] \leq [\alpha_1, \dots, \alpha_k]$.

Proof: (HC1) First, we prove $C(\alpha_0, \dots, \alpha_k; \alpha_i)$ for every $i \in \{0, \dots, k\}$. Let $j \in \{0, \dots, k\}$, $f(\mathbf{x}_0, \dots, \mathbf{x}_k)$ be a polynomial and vectors $\mathbf{a}_0, \mathbf{b}_0, \dots, \mathbf{a}_{k-1}, \mathbf{b}_{k-1}, \mathbf{c}, \mathbf{d}$ from $\mathbf{A}$ satisfying:

(1) $\mathbf{a}_i \equiv_{\alpha_i} \mathbf{b}_i$ for all $i \in \{0, 1, \dots, k-1\}$,
(2) $\mathbf{c} \equiv_{\alpha_k} \mathbf{d}$, and
(3) $f(\mathbf{x}_0, \dots, \mathbf{x}_{k-1}, \mathbf{c}) \equiv_{\alpha_j} f(\mathbf{x}_0, \dots, \mathbf{x}_{k-1}, \mathbf{d})$ for all $(\mathbf{x}_0, \dots, \mathbf{x}_{k-1}) \in \{\mathbf{a}_0, \mathbf{b}_0\} \times \dots \times \{\mathbf{a}_{k-1}, \mathbf{b}_{k-1}\} \backslash \{(\mathbf{b}_0, \dots, \mathbf{b}_{k-1})\}$.

Using (1) for $i := j$ and (3) for $(x_0, \dots, x_{k-1}) := (\mathbf{b}_0, \dots, \mathbf{b}_{j-1}, \mathbf{a}_j, \mathbf{b}_{j+1}, \dots, \mathbf{b}_{k-1})$ we obtain:

$$f(\mathbf{b}_0, \dots, \mathbf{b}_{k-1}, \mathbf{c}) \equiv_{\alpha_j} f(\mathbf{b}_0, \dots, \mathbf{b}_{j-1}, \mathbf{a}_j, \mathbf{b}_{j+1}, \dots, \mathbf{b}_{k-1}, \mathbf{c})$$

$$\equiv_{\alpha_j} f(\mathbf{b}_0, \dots, \mathbf{b}_{j-1}, \mathbf{a}_j, \mathbf{b}_{j+1}, \dots, \mathbf{b}_{k-1}, \mathbf{d}) \equiv_{\alpha_j} f(\mathbf{b}_0, \dots, \mathbf{b}_{k-1}, \mathbf{d}).$$

Therefore, we have $C(\alpha_0, \dots, \alpha_k; \alpha_j)$, by definition. Hence, $[\alpha_0, \dots, \alpha_k] \leq \alpha_j$. Now, we easily obtain $[\alpha_0, \dots, \alpha_k] \leq \bigwedge_{0 \leq i \leq k} \alpha_i$.

(HC2) We shall show that $C(\alpha_0, \dots, \alpha_k; [\beta_0, \dots, \beta_k])$. Let $f(\mathbf{x}_0, \dots, \mathbf{x}_k)$ be a polynomial and vectors $\mathbf{a}_0, \mathbf{b}_0, \dots, \mathbf{a}_{k-1}, \mathbf{b}_{k-1}, \mathbf{c}, \mathbf{d}$ from $\mathbf{A}$ and $j \in \{0, \dots, k\}$ satisfying:

(1) $\mathbf{a}_i \equiv_{\alpha_i} \mathbf{b}_i$ for all $i \in \{0, 1, \dots, k-1\}$,
(2) $\mathbf{c} \equiv_{\alpha_k} \mathbf{d}$, and
(3) $f(\mathbf{x}_0, \dots, \mathbf{x}_{k-1}, \mathbf{c}) \equiv_{[\beta_0, \dots, \beta_k]} f(\mathbf{x}_0, \dots, \mathbf{x}_{k-1}, \mathbf{d})$ for all $(\mathbf{x}_0, \dots, \mathbf{x}_{k-1}) \in \{\mathbf{a}_0, \mathbf{b}_0\} \times \dots \times \{\mathbf{a}_{k-1}, \mathbf{b}_{k-1}\} \backslash \{(\mathbf{b}_0, \dots, \mathbf{b}_{k-1})\}$.

Then by assumptions we have

(1') $\mathbf{a}_i \equiv_{\beta_i} \mathbf{b}_i$ for all $i \in \{0, 1, \ldots, k-1\}$ and

(2') $\mathbf{c} \equiv_{\beta_k} \mathbf{d}$.

We know that $C(\beta_0, \ldots, \beta_k; [\beta_0, \ldots, \beta_k])$ and then (1'), (2') and (3) yield

$$f(\mathbf{b}_0, \ldots, \mathbf{b}_{k-1}, \mathbf{c}) \equiv_{[\beta_0, \ldots, \beta_k]} f(\mathbf{b}_0, \ldots, \mathbf{b}_{k-1}, \mathbf{d}).$$

(HC3) Let us show that $C(\alpha_0, \ldots, \alpha_k; [\alpha_1, \ldots, \alpha_k])$. Let $f(\mathbf{x}_0, \ldots, \mathbf{x}_k)$ be a polynomial and vectors $\mathbf{a}_0, \mathbf{b}_0, \ldots, \mathbf{a}_{k-1}, \mathbf{b}_{k-1}, \mathbf{c}, \mathbf{d}$ from $\mathbf{A}$ satisfying:

(1) $\mathbf{a}_i \equiv_{\alpha_i} \mathbf{b}_i$ for all $i \in \{0, 1, \ldots, k-1\}$,

(2) $\mathbf{c} \equiv_{\alpha_k} \mathbf{d}$, and

(3) $f(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}, \mathbf{c}) \equiv_{[\alpha_1, \ldots, \alpha_k]} f(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}, \mathbf{d})$ for all $(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}) \in \{\mathbf{a}_0, \mathbf{b}_0\} \times \cdots \times \{\mathbf{a}_{k-1}, \mathbf{b}_{k-1}\} \backslash \{(\mathbf{b}_0, \ldots, \mathbf{b}_{k-1})\}$.

Now, we define a polynomial q of $\mathbf{A}$ by

$$g(\mathbf{x}_1, \ldots, \mathbf{x}_k) := f(\mathbf{b}_0, \mathbf{x}_1, \ldots, \mathbf{x}_k).$$

Then, using (3), we obtain

(3') $g(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{c}) \equiv_{[\alpha_1, \ldots, \alpha_k]} g(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{d})$ for all $(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}) \in \{\mathbf{a}_1, \mathbf{b}_1\} \times \cdots \times \{\mathbf{a}_{k-1}, \mathbf{b}_{k-1}\} \backslash \{(\mathbf{b}_1, \ldots, \mathbf{b}_{k-1})\}$.

We know that $C(\alpha_1, \ldots, \alpha_k; [\alpha_1, \ldots, \alpha_k])$ and therefore (1) for $i \neq 0$, (2) and (3') yield

$$g(\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{c}) \equiv_{[\alpha_1, \ldots, \alpha_k]} g(\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{d})$$

or equivalently, $f(\mathbf{b}_0, \ldots, \mathbf{b}_{k-1}, \mathbf{c}) \equiv_{[\alpha_1, \ldots, \alpha_k]} f(\mathbf{b}_0, \ldots, \mathbf{b}_{k-1}, \mathbf{d})$. □

Let $k \geq 1$ and let $\alpha_0, \ldots, \alpha_k, \eta$ be congruences of an algebra $\mathbf{A}$ that generates a congruence permutable variety. Then, we have:

(HC4) $[\alpha_0, \ldots, \alpha_k] = [\alpha_{\pi(0)}, \ldots, \alpha_{\pi(k)}]$ for every permutation π of the set $\{0, \ldots, k\}$;

(HC5) $[\alpha_0, \ldots, \alpha_k] \leq \eta$ if and only if $C(\alpha_0, \ldots, \alpha_k; \eta)$;

(HC6) If $\eta \leq \alpha_0, \ldots, \alpha_k$, then in $\mathbf{A}/\eta$, we have
$$[\alpha_0/\eta, \ldots, \alpha_k/\eta] = ([\alpha_0, \ldots, \alpha_k] \vee \eta)/\eta;$$

(HC7) If I is a nonempty set, $j \in \{0, \ldots, k\}$, and $\{\rho_i \mid i \in I\} \subseteq \mathsf{Con}\,\mathbf{A}$, then: $\bigvee_{i \in I} [\alpha_0, \ldots, \alpha_{j-1}, \rho_i, \alpha_{j+1}, \ldots, \alpha_k] = [\alpha_0, \ldots, \alpha_{j-1}, \bigvee_{i \in I} \rho_i, \alpha_{j+1}, \ldots, \alpha_k]$;

(HC8) $[\alpha_0, [\alpha_1, \ldots, \alpha_k]] \leq [\alpha_0, \alpha_1, \ldots, \alpha_k]$, and more generally
$$[\alpha_0, \ldots, \alpha_{i-1}, [\alpha_i, \ldots, \alpha_k]] \leq [\alpha_0, \ldots, \alpha_k] \text{ for all } i \in \{1, \ldots, k\}.$$

The proofs of properties (HC4)-(HC8) are given in Section 4. Actually, for $k = 1$, as a special case we obtain several properties of the binary commutator operation on Mal'cev algebras that have been listed in [**29**, Exercises 4.156(1),(11),(13)] and [**6**, Proposition 2.3].

We notice that the higher commutator operations of an algebra are not determined by its binary commutator operation. As examples, we consider the expansions of the cyclic group $(\mathbb{Z}_4, +)$ that were studied in [**10**]. For $n \geq 2$, let $\mathbf{A}_n$ be the algebra $(\mathbb{Z}_4, +, f_n)$, where f_n is the n-ary operation defined by $f_n(x_1, \ldots, x_n) := 2x_1 \cdots x_n$. $\mathbf{A}_n$ has exactly three congruences; we denote them by 0, α, and 1. Then from Lemma 2.4 of [**6**], one can easily infer that for $n \geq 2$, $\mathbf{A}_n$ satisfies $[1,1] = \alpha$ and $[1,\alpha] = 0$. Furthermore, in $\mathbf{A}_2$ we have $[1,1,1] = 0$, but in $\mathbf{A}_3$, we have $[1,1,1] = \alpha$. The property $[1,1,1]_{\mathbf{A}_2} = 0$ can be proved by observing that all ternary polynomial functions of $\mathbf{A}_2$ are of the form $(x,y,z) \mapsto a_0 + a_1x + a_2y + a_3z + 2a_4xy + 2a_5xz + 2a_6yz$ with $a_0,\dots,a_6 \in \mathbb{Z}_4$. Now one can use Corollary 4.11 to show that $[1,1,1]_{\mathbf{A}_2} = 0$. The property $[1,1,1]_{\mathbf{A}_3} = \alpha$ is easier to show: Since $[1,1,1]_{\mathbf{A}_3} \leq [1,1]_{\mathbf{A}_3}$ by (HC3), we have $[1,1,1]_{\mathbf{A}_3} \neq 1$. Now we show $[1,1,1]_{\mathbf{A}_3} \neq 0$. Seeking a contradiction, we assume $C(1,1,1;0)$. Since $f_3(\alpha_0,\alpha_1,0) = f_3(\alpha_0,\alpha_1,3)$ for all $(\alpha_0,\alpha_1) \in \{(0,0),(0,3),(3,0)\}$, $C(1,1,1;0)$ yields $f_3(3,3,0) = f_3(3,3,3)$, a contradiction. Thus $[1,1,1]_{\mathbf{A}_3} = \alpha$.

Similarly, if $k \geq 2$ and $n \geq 2$, one obtains $[1,[1,1]]_{\mathbf{A}_n} = 0$, $[\underbrace{1,\dots,1}_{k}]_{\mathbf{A}_n} = \alpha$ if $k \leq n$ and $[\underbrace{1,\dots,1}_{k}]_{\mathbf{A}_n} = 0$ if $k > n$.

2. The Difference Operator

The main tool for proving the properties of higher commutators will be the difference operator D defined in this section.

Definition 2.1. Let $\mathbf{A}$ be an algebra. Then for each $k \in \mathbb{N}_0$, $i \in \{0,1,\dots,k\}$, and $y \in A$, we define a mapping $\mathsf{E}_y^{(i)} : \mathsf{Pol}_{k+1}\mathbf{A} \to \mathsf{Pol}_k\mathbf{A}$ by:

$$\mathsf{E}_y^{(i)}(p)\,(x_0\dots,x_{i-1},x_{i+1},\dots,x_k) := p(x_0,\dots,x_{i-1},y,x_{i+1},\dots,x_k)$$

for all $p \in \mathsf{Pol}_{k+1}\mathbf{A}$ and $x_0,\dots,x_{i-1},x_{i+1},\dots,x_k \in A$.

Example 2.2. Let

$$p(x_0,x_1,x_2) = x_0x_1^2x_2$$

be a polynomial of the ring $\mathbb{Z}_8$. Then $\mathsf{E}_5^{(1)}(p)(x_0,x_2) = x_0x_2$.

Definition 2.3. Let $\mathbf{A}$ be a Mal'cev algebra with Mal'cev term m, let $\theta \in A$, and let $(a_i)_{i\in\mathbb{N}_0}$ be a sequence of elements of A. Then for each $k \in \mathbb{N}$, we define a mapping $\mathsf{D}^{(k)}_{\theta,(a_0,\dots,a_{k-1})} : \mathsf{Pol}_k\mathbf{A} \to \mathsf{Pol}_k\mathbf{A}$, by the following equations:

$$\mathsf{D}^{(1)}_{\theta,a_0}(f)(x_0) := m(f(x_0),f(a_0),\theta)$$

for every $f \in \mathsf{Pol}_1\mathbf{A}$, $x_0 \in A$ and

$$\mathsf{D}^{(k+1)}_{\theta,(a_0,\dots,a_k)}(p)(x_0,\dots,x_k) := m\begin{pmatrix} \mathsf{D}^{(k)}_{\theta,(a_0,\dots,a_{k-1})}\left(\mathsf{E}^{(k)}_{x_k}(p)\right)(x_0,\dots,x_{k-1}) \\ \mathsf{D}^{(k)}_{\theta,(a_0,\dots,a_{k-1})}\left(\mathsf{E}^{(k)}_{a_k}(p)\right)(x_0,\dots,x_{k-1}) \\ \theta \end{pmatrix}$$

for every $k \in \mathbb{N}$, $p \in \mathsf{Pol}_{k+1}\mathbf{A}$ and $x_0,\dots,x_k \in A$.

Note that the definition of D depends on the Mal'cev term m, which will always be clear from the context. Also, we use $m\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ instead of $m(a,b,c)$ if this improves readability.

EXAMPLE 2.4. Let p be a ternary polynomial of an expanded group $(V,+,-,0,F)$. For $\theta = 0$ and $a_0, a_1, a_2 \in V$ we obtain:

$$
\begin{aligned}
&\mathsf{D}^{(3)}_{0,(a_0,a_1,a_2)}(p)(x_0,x_1,x_2) = \\
&= \mathsf{D}^{(2)}_{0,(a_0,a_1)}\Big(\mathsf{E}^{(2)}_{x_2}(p)\Big)(x_0,x_1) - \mathsf{D}^{(2)}_{0,(a_0,a_1)}\Big(\mathsf{E}^{(2)}_{a_2}(p)\Big)(x_0,x_1) = \\
&= \mathsf{D}^{(1)}_{0,a_0}\Big(\mathsf{E}^{(1)}_{x_1}(\mathsf{E}^{(2)}_{x_2}(p))\Big)(x_0) - \mathsf{D}^{(1)}_{0,a_0}\Big(\mathsf{E}^{(1)}_{a_1}(\mathsf{E}^{(2)}_{x_2}(p))\Big)(x_0) \\
&-\Big(\mathsf{D}^{(1)}_{0,a_0}\Big(\mathsf{E}^{(1)}_{x_1}(\mathsf{E}^{(2)}_{a_2}(p))\Big)(x_0) - \mathsf{D}^{(1)}_{0,a_0}\Big(\mathsf{E}^{(1)}_{a_1}(\mathsf{E}^{(2)}_{a_2}(p))\Big)(x_0)\Big) = \\
&= \Big((\mathsf{E}^{(1)}_{x_1}(\mathsf{E}^{(2)}_{x_2}(p)))(x_0) - (\mathsf{E}^{(1)}_{x_1}(\mathsf{E}^{(2)}_{x_2}(p)))(a_0)\Big) \\
&-\Big((\mathsf{E}^{(1)}_{a_1}(\mathsf{E}^{(2)}_{x_2}(p)))(x_0) - (\mathsf{E}^{(1)}_{a_1}(\mathsf{E}^{(2)}_{x_2}(p)))(a_0)\Big) \\
&+\Big((\mathsf{E}^{(1)}_{a_1}(\mathsf{E}^{(2)}_{a_2}(p)))(x_0) - (\mathsf{E}^{(1)}_{a_1}(\mathsf{E}^{(2)}_{a_2}(p)))(a_0)\Big) \\
&-\Big((\mathsf{E}^{(1)}_{x_1}(\mathsf{E}^{(2)}_{a_2}(p)))(x_0) - (\mathsf{E}^{(1)}_{x_1}(\mathsf{E}^{(2)}_{a_2}(p)))(a_0)\Big) \\
&= (p(x_0,x_1,x_2) - p(a_0,x_1,x_2)) - (p(x_0,a_1,x_2) - p(a_0,a_1,x_2)) \\
&+(p(x_0,a_1,a_2) - p(a_0,a_1,a_2)) - (p(x_0,x_1,a_2) - p(a_0,x_1,a_2)) \\
&= p(x_0,x_1,x_2) - p(a_0,x_1,x_2) + p(a_0,a_1,x_2) - p(x_0,a_1,x_2) \\
&+p(x_0,a_1,a_2) - p(a_0,a_1,a_2) + p(a_0,x_1,a_2) - p(x_0,x_1,a_2)
\end{aligned}
$$

LEMMA 2.5. *Let $\mathbf{A}$ be a Mal'cev algebra with a Mal'cev term m, $\theta \in A$, $k \in \mathbb{N}$, and let α be a congruence of $\mathbf{A}$. Let $q \in \mathsf{Pol}_k\mathbf{A}$ such that $q(A^k) \subseteq \theta/\alpha$. Then for every $(x_0,\dots,x_{k-1}) \in A^k$, we have: $\mathsf{D}^{(k)}_{\theta,(\theta,\dots,\theta)}(q)(x_0,\dots,x_{k-1}) \in \theta/\alpha$.*

Proof: We show the statement by induction on k. For $k = 1$ and $x_0 \in A$, we have $q(x_0) \in \theta/\alpha$ and $q(\theta) \in \theta/\alpha$, and thus $\mathsf{D}^{(1)}_{\theta,\theta}(q)(x_0) = m(q(x_0), q(\theta), \theta) \equiv_\alpha m(\theta,\theta,\theta) = \theta \in \theta/\alpha$. Now let $k \geq 2$ and $x_0,\dots,x_{k-1} \in A$. Since $q(A^k) \subseteq \theta/\alpha$, we clearly have $\mathsf{E}^{(k-1)}_{x_{k-1}}(q)(A^{k-1}) \subseteq \theta/\alpha$ and $\mathsf{E}^{(k-1)}_{\theta}(q)(A^{k-1}) \subseteq \theta/\alpha$. Thus, by the induction hypothesis, both $a := \mathsf{D}^{(k-1)}_{\theta,(\theta,\dots,\theta)}(\mathsf{E}^{(k-1)}_{x_{k-1}}(q))(x_0,\dots,x_{k-2})$ and $b := \mathsf{D}^{(k-1)}_{\theta,(\theta,\dots,\theta)}(\mathsf{E}^{(k-1)}_{\theta}(q))(x_0,\dots,x_{k-2})$ lie in θ/α. Hence we have $m(a,b,\theta) \in \theta/\alpha$. This completes the proof. □

Definition 2.6. Let $\mathbf{A}$ be an algebra with a Mal'cev term m and let $k \in \mathbb{N}$. Then we define a mapping $\mathsf{F}_{\theta,u} : \mathsf{Pol}_k\mathbf{A} \to \mathsf{Pol}_k\mathbf{A}$ by:

$$\mathsf{F}_{\theta,u}(p)(x_0, \ldots, x_{k-1}) := m(p(x_0, \ldots, x_{k-2}, x_{k-1}), p(x_0, \ldots, x_{k-2}, u), \theta)$$

for all $p \in \mathsf{Pol}_k\mathbf{A}$ and $x_0, \ldots, x_{k-1}, \theta, u \in A$.

Example 2.7. Let p be a ternary polynomial of an expanded group $(V, +, -, 0, F)$. For $\theta = 0$ and $u \in V$ we obtain:

$$\mathsf{F}_{0,u}(p)(x_0, x_1, x_2) = p(x_0, x_1, x_2) - p(x_0, x_1, u).$$

We need the following technical lemma.

Lemma 2.8. *Let $\mathbf{A}$ be an algebra with a Mal'cev term m and $k \in \mathbb{N}$. Then for all $q \in \mathsf{Pol}_{k+1}\mathbf{A}$ and $x_0, \ldots, x_{k-2}, \theta, t, u, v \in A$, we have:*

$$\mathsf{E}_t^{(k-1)}(\mathsf{E}_v^{(k)}(\mathsf{F}_{\theta,u}(q)))(x_0, \ldots, x_{k-2}) = \mathsf{E}_v^{(k-1)}(\mathsf{F}_{\theta,u}(\mathsf{E}_t^{(k-1)}(q)))(x_0, \ldots, x_{k-2}).$$

Proof: Let $q \in \mathsf{Pol}_{k+1}\mathbf{A}$. We calculate the left hand side:

$$\mathsf{E}_t^{(k-1)}(\mathsf{E}_v^{(k)}(\mathsf{F}_{\theta,u}(q)))(x_0, \ldots, x_{k-2}) = \mathsf{E}_v^{(k)}(\mathsf{F}_{\theta,u}(q))(x_0, \ldots, x_{k-2}, t) =$$

$$= \mathsf{F}_{\theta,u}(q)(x_0, \ldots, x_{k-2}, t, v) = m(q(x_0, \ldots, x_{k-2}, t, v), q(x_0, \ldots, x_{k-2}, t, u), \theta).$$

Now, we compute the right hand side:

$$\mathsf{E}_v^{(k-1)}(\mathsf{F}_{\theta,u}(\mathsf{E}_t^{(k-1)}(q)))(x_0, \ldots, x_{k-2}) = \mathsf{F}_{\theta,u}(\mathsf{E}_t^{(k-1)}(q))(x_0, \ldots, x_{k-2}, v)$$

$$= m(\mathsf{E}_t^{(k-1)}(q)(x_0, \ldots, x_{k-2}, v), \mathsf{E}_t^{(k-1)}(q)(x_0, \ldots, x_{k-2}, u), \theta) =$$

$$= m(q(x_0, \ldots, x_{k-2}, t, v), q(x_0, \ldots, x_{k-2}, t, u), \theta).$$

□

Definition 2.9. Let $\mathbf{A}$ be an algebra, let $k \in \mathbb{N}$, let $p : A^k \to A$, let $(a_0, \ldots, a_{k-1}) \in A^k$, and let $\theta \in A$. Then p is *absorbing at* $(a_0, \ldots, a_{k-1})$ *with value* θ if for all $(x_0, \ldots, x_{k-1}) \in A^k$ we have: if there is an $i \in \{0, 1, \ldots, k-1\}$ such that $x_i = a_i$, then $p(x_0, \ldots, x_{k-1}) = \theta$. Note that $p(a_0, \ldots, a_{k-1}) = \theta$.

Example 2.10. In a ring $\mathbf{R}$, for $a, b, c, d \in R$, the function $f(x, y, z) := (x-a)(y-b)(z-c) + d$ is absorbing at (a, b, c) with value d.

Lemma 2.11. *Let $\mathbf{A}$ be a Mal'cev algebra with a Mal'cev term m, let $k \geq 1$, $(a_0, \ldots, a_{k-1}) \in A^k$ and $\theta \in A$. If $q \in \mathsf{Pol}_k\mathbf{A}$, then $\mathsf{D}^{(k)}_{\theta,(a_0,\ldots,a_{k-1})}(q)$ is absorbing at $(a_0, \ldots, a_{k-1})$ with value θ.*

Proof: We prove the statement by induction on k. Using Definition 2.3, we see that $\mathsf{D}^{(1)}_{\theta,a_0}(q)(a_0) = m(q(a_0), q(a_0), \theta) = \theta$. For the induction step, let $k \geq 2$, $(x_0, \ldots, x_{k-1}) \in A^k$ such that there is an $i \in \{0, 1, \ldots, k-1\}$ with $x_i = a_i$, and let $q \in \mathsf{Pol}_k\mathbf{A}$. We want to prove

$$\mathsf{D}^{(k)}_{\theta,(a_0,\ldots,a_{k-1})}(q)(x_0, \ldots, x_{k-1}) = \theta. \tag{2.1}$$

If $x_{k-1} = a_{k-1}$, then we obtain (2.1) directly from Definition 2.3. If there exists an $i \in \{0, \ldots, k-2\}$ such that $x_i = a_i$ then we reason as follows: Since $\mathsf{E}^{(k-1)}_{x_{k-1}}(q), \mathsf{E}^{(k-1)}_{a_{k-1}}(q) \in \mathsf{Pol}_{k-1}\mathbf{A}$, we have

$$\mathsf{D}^{(k-1)}_{\theta,(a_0,\ldots,a_{k-2})}(\mathsf{E}^{(k-1)}_{x_{k-1}}(q))(x_0, \ldots, x_{k-2}) = \mathsf{D}^{(k-1)}_{\theta,(a_0,\ldots,a_{k-2})}(\mathsf{E}^{(k-1)}_{a_{k-1}}(q))(x_0, \ldots, x_{k-2}) = \theta$$

by the induction hypothesis. Now, by Definition 2.3 we obtain (2.1). □

Example 2.12. Let p be a ternary polynomial of an expanded group $(V, +, -, 0, F)$. We already calculated in Example 2.4:

$$\mathsf{D}^{(3)}_{0,(a_0,a_1,a_2)}(p)(x_0, x_1, x_2) = p(x_0, x_1, x_2) - p(a_0, x_1, x_2) + p(a_0, a_1, x_2) - p(x_0, a_1, x_2)$$
$$+ p(x_0, a_1, a_2) - p(a_0, a_1, a_2) + p(a_0, x_1, a_2) - p(x_0, x_1, a_2)$$

and hence, $\mathsf{D}^{(3)}_{0,(a_0,a_1,a_2)}(p)(a_0, x_1, x_2) = \mathsf{D}^{(3)}_{0,(a_0,a_1,a_2)}(p)(x_0, a_1, x_2)$
$= \mathsf{D}^{(3)}_{0,(a_0,a_1,a_2)}(p)(x_0, x_1, a_2) = 0.$

Definition 2.13. Let $\mathbf{A}$ be an algebra and let $\theta \in A$. For each $n \in \mathbb{N}$ and $I \subseteq \{0, \ldots, n-1\}$, we define a function $S^{(n)}_{I,\theta} : A^n \to A^n$ by

$$S^{(n)}_{I,\theta}(x_0, \ldots, x_{n-1}) := (y_0, \ldots, y_{n-1})$$

for all $x_0, \ldots, x_{n-1} \in A$, where $y_j := x_j$ if $j \in I$, and $y_j := \theta$ if $j \notin I$.

In the previous definition, all entries whose indices are not listed in I are replaced with θ.

Definition 2.14. Let $\mathbf{A}$ be an algebra and let $\theta \in A$. For each $n \in \mathbb{N}$ and $I \subseteq \{0, \ldots, n-1\}$, we define a function $H^{(n)}_{I,\theta} : \mathsf{Pol}_n\mathbf{A} \to \mathsf{Pol}_n\mathbf{A}$ by

$$(H^{(n)}_{I,\theta}(p))(x_0, \ldots, x_{n-1}) := p(S^{(n)}_{I,\theta}(x_0, \ldots, x_{n-1}))$$

for all $(x_0, \ldots, x_{n-1}) \in A^n$.

Example 2.15. For $a_0, a_1, a_2 \in A$ we have $S^{(3)}_{\{0,2\},\theta}(a_0, a_1, a_2) = (a_0, \theta, a_2)$ and $H^{(3)}_{\{0,2\},\theta}(p)(a_0, a_1, a_2) = p(a_0, \theta, a_2)$.

Proposition 2.16. *Let* $\mathbf{A}$ *be an algebra, let* $\theta \in A$*, let* $\alpha \in \mathsf{Con}\,\mathbf{A}$ *and let* $k \geq 1$*. If* $p \in \mathsf{Pol}_k\mathbf{A}$ *such that* $p(A^k) \subseteq \theta/\alpha$ *then* $H^{(k)}_{I,\theta}(p)(A^k) \subseteq \theta/\alpha$ *for every* $I \subseteq \{0, \ldots, k-1\}$.

Proof: Obviously, we have $H^{(k)}_{I,\theta}(p)(A^k) = p(S^{(k)}_{I,\theta}(A^k)) \subseteq p(A^k)$. □

In a Mal'cev algebra $\mathbf{A}$ with a Mal'cev term m and $\theta \in A$ we define a binary polynomial $+_\theta$ and a unary polynomial $-_\theta$ such that:

$$a +_\theta b := m(a, \theta, b)$$

and

$$-_\theta(a) := m(\theta, a, \theta)$$

for all $a, b \in A$. We abbreviate $((a_1 +_\theta a_2) +_\theta \cdots +_\theta a_{n-1}) +_\theta a_n$ by ${}_\theta\sum_{i=1}^{n} a_i$. By $(-1)^k \cdot a$, we mean $-_\theta(a)$ if k is odd, and a if k is even.

Lemma 2.17. *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term* m*, let* $\theta \in A$*,* $k \in \mathbb{N}$*,* $\alpha \in \mathsf{Con}\,\mathbf{A}$ *and* $p \in \mathsf{Pol}_k\mathbf{A}$ *such that* $[\alpha, \alpha] = 0$ *and* $p(A^k) \subseteq \theta/\alpha$*. Then:*

(1) $(\theta/\alpha, +_\theta, -_\theta, \theta)$ *is an abelian group and* $m(a, b, \theta) = a +_\theta (-_\theta(b))$ *for all* $a, b \in \theta/\alpha$

(2) *there exists a bijective mapping* $\varphi_k : \{1, \ldots, 2^k\} \to \mathcal{P}(\{0, \ldots, k-1\})$ *such that* $\varphi_k(1) = \{0, \ldots, k-1\}$ *and*

$$\mathsf{D}^{(k)}_{\theta,(\theta,\ldots,\theta)}(p) = {}_\theta\sum_{i=1}^{2^k} (-1)^{k-|\varphi_k(i)|} \cdot H^{(k)}_{\varphi_k(i),\theta}(p).$$

Proof: (1) Since $a +_\theta b \in \theta/\alpha$ and $-_\theta(a) \in \theta/\alpha$ for all $a, b \in \theta/\alpha$, we know that $(\theta/\alpha, +_\theta, -_\theta, \theta)$ is an abelian group by Lemma §1.3.4 and the calculations in the proof of Proposition §1.3.11. By Lemma §1.3.7 we obtain $m(a, b, \theta) = m(a, \theta, m(\theta, b, \theta)) = a +_\theta (-_\theta(b))$ for all $a, b \in \theta/\alpha$.

(2) We proceed by induction on k. For $k = 1$ we define $\varphi_1(1) := \{0\}$ and $\varphi_1(2) := \emptyset$. Then, by Definition 2.3 and (1), for $x_0 \in A$, we have

$$\mathsf{D}^{(1)}_{\theta,\theta}(p)(x_0) = m(p(x_0), p(\theta), \theta) = p(x_0) +_\theta (-_\theta(p(\theta))) = {}_\theta\sum_{i=1}^{2} (-1)^{1-|\varphi_1(i)|} \cdot H^{(1)}_{\varphi_1(i),\theta}(p)(x_0).$$

For $k > 1$ we define $\varphi_k : \{1, \ldots, 2^k\} \to \mathcal{P}(\{0, \ldots, k-1\})$ by $\varphi_k(i) := \varphi_{k-1}(i) \cup \{k-1\}$ and $\varphi_k(2^k+1-i) := \varphi_{k-1}(i)$ for $i \in \{1, \ldots, 2^{k-1}\}$. Now, let $(x_0, \ldots, x_{k-1}) \in A^k$. Using item (1) we compute

$$\mathsf{D}^{(k)}_{\theta,(\theta,\ldots,\theta)}(p)(x_0, \ldots, x_{k-1}) = \tag{2.2}$$

$$\mathsf{D}^{(k-1)}_{\theta,(\theta,\ldots,\theta)}\left(\mathsf{E}^{(k-1)}_{x_{k-1}}(p)\right)(x_0, \ldots, x_{k-2}) +_\theta (-_\theta\left(\mathsf{D}^{(k-1)}_{\theta,(\theta,\ldots,\theta)}\left(\mathsf{E}^{(k-1)}_{\theta}(p)\right)(x_0, \ldots, x_{k-2})\right)).$$

Since $\mathsf{E}^{(k-1)}_{x_{k-1}}(p)(A^{k-1}) \subseteq \theta/\alpha$ and $\mathsf{E}^{(k-1)}_{\theta}(p)(A^{k-1}) \subseteq \theta/\alpha$, we may use the induction hypothesis and obtain that the last expresson is equal to

$$\begin{aligned}&{}_\theta\sum_{i=1}^{2^{k-1}} (-1)^{k-1-|\varphi_{k-1}(i)|} \cdot \left(H^{(k-1)}_{\varphi_{k-1}(i),\theta}(\mathsf{E}^{(k-1)}_{x_{k-1}}(p))\right)(x_0, \ldots, x_{k-2})\\ &+_\theta\big(-_\theta\left({}_\theta\sum_{i=1}^{2^{k-1}} (-1)^{k-1-|\varphi_{k-1}(i)|} \cdot \left(H^{(k-1)}_{\varphi_{k-1}(i),\theta}(\mathsf{E}^{(k-1)}_{\theta}(p))\right)(x_0, \ldots, x_{k-2})\right)\big).\end{aligned}$$

The last expression is equal to

$${}_\theta\sum_{i=1}^{2^{k-1}} (-1)^{k-1-|\varphi_{k-1}(i)|} \cdot \left(\mathsf{E}^{(k-1)}_{x_{k-1}}(p)\right)(S^{(k-1)}_{\varphi_{k-1}(i),\theta}(x_0, \ldots, x_{k-2}))$$

$$+_\theta\left({}_\theta\sum_{i=1}^{2^{k-1}}(-1)^{k-|\varphi_{k-1}(i)|}\cdot\left(\mathsf{E}_\theta^{(k-1)}(p)\right)(S^{(k-1)}_{\varphi_{k-1}(i),\theta}(x_0,\dots,x_{k-2}))\right)$$

$$= {}_\theta\sum_{i=1}^{2^{k-1}}(-1)^{k-1-|\varphi_{k-1}(i)|}\cdot p(S^{(k-1)}_{\varphi_{k-1}(i),\theta}(x_0,\dots,x_{k-2}),x_{k-1})$$

$$+_\theta\left({}_\theta\sum_{i=1}^{2^{k-1}}(-1)^{k-|\varphi_{k-1}(i)|}\cdot p(S^{(k-1)}_{\varphi_{k-1}(i),\theta}(x_0,\dots,x_{k-2}),\theta)\right)$$

$$= {}_\theta\sum_{i=1}^{2^{k-1}}(-1)^{k-|\varphi_k(i)|}\cdot p(S^{(k)}_{\varphi_k(i),\theta}(x_0,\dots,x_{k-1}))$$

$$+_\theta\left({}_\theta\sum_{i=2^{k-1}+1}^{2^k}(-1)^{k-|\varphi_k(i)|}\cdot p(S^{(k)}_{\varphi_k(i),\theta}(x_0\dots,x_{k-1}))\right)$$

$$= {}_\theta\sum_{i=1}^{2^k}(-1)^{k-|\varphi_k(i)|}\cdot H^{(k)}_{\varphi_k(i),\theta}(p)(x_0,\dots,x_{k-1}).$$

□

In an algebra $\mathbf{A}$ we say that a function $f : A^n \to A$ *depends on its* i *th argument* if there are $a, b \in A$ and $(x_1,\dots,x_n) \in A^n$ such that

$$p(x_1,\dots,x_{i-1},a,x_{i+1},\dots,x_n) \neq p(x_1,\dots,x_{i-1},b,x_{i+1},\dots,x_n).$$

The number of arguments on which p depends is called the *essential arity* of p. For $n \in \mathbb{N}$ and $\theta \in A$ we call a polynomial $p \in \mathsf{Pol}_n\mathbf{A}$ a *θ-polynomial* if for each $i \in \{1,\dots,n\}$ at least one of the following two conditions holds:

(1) p does not depend on its ith argument,
(2) $p(x_1,\dots,x_{i-1},\theta,x_{i+1},\dots,x_n) = p(\theta,\dots,\theta)$ for all $(x_1,\dots,x_n) \in A^n$.

Let $\mathbf{A}$ be a Mal'cev algebra with a Mal'cev term m and let $\theta \in A$. Then, for every $k \geq 0$, $\mathbf{P}(A,k,m,\theta) := (\mathsf{Pol}_k\mathbf{A}, m, \overline{\theta})$ is an algebra of type $(3,0)$ with Mal'cev operation m and a constant polynomial $\overline{\theta} \in \mathsf{Pol}_k\mathbf{A}$. For a nonempty set P of polynomials of $\mathbf{A}$, we denote the subuniverse of $\mathbf{P}(A,k,m,\theta)$ generated by P by $\mathrm{Sg}^{\mathbf{P}(A,k,m,\theta)}(P)$.

PROPOSITION 2.18. *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term* m*, let* $\theta \in A$*,* $n \in \mathbb{N}$*,* $\alpha \in \mathsf{Con}\,\mathbf{A}$ *and* $p \in \mathsf{Pol}_n\mathbf{A}$*. If* $[\alpha,\alpha] = 0$ *and* $p(A^n) \subseteq \theta/\alpha$ *then* $p \in \mathrm{Sg}^{\mathbf{P}(A,n,m,\theta)}(P)$*, where* $P := \{f \in \mathsf{Pol}_n\mathbf{A} \mid f$ *is a* θ*-polynomial and the essential arity of* f *is at most the essential arity of* $p\}$*.*

Proof: Let $k \in \mathbb{N}$ be the essential arity of the polynomial p. Then there exists a polynomial $q \in \mathsf{Pol}_k\mathbf{A}$ such that the essential arity of q is k and $p(x_0,\dots,x_{n-1}) = q(x_{i_0},\dots,x_{i_{k-1}})$ for all $(x_0,\dots,x_{n-1}) \in A^n$. To simplify the notation let us denote the arguments of q by $x_0,\dots,x_{k-1}$. We prove the statement of the proposition by induction on k. For $k = 1$ the statement is obvious because every unary polynomial function is a θ-polynomial function of essential arity at most 1. Now let $k \geq 2$. Since $[\alpha, \alpha] = 0$ and $q(A^k) \subseteq \theta/\alpha$, Lemma 2.17 yields a bijective mapping $\varphi_k : \{1, \dots, 2^k\} \to \mathcal{P}(\{0, \dots, k-1\})$ such that

$$q = \mathsf{D}^{(k)}_{\theta,(\theta,\dots,\theta)}(q) +_\theta (-_\theta \Bigg({}_\theta\sum_{i=2}^{2^k} (-1)^{k-|\varphi_k(i)|} \cdot H^{(k)}_{\varphi_k(i),\theta}(q) \Bigg)). \tag{2.3}$$

To prove (2.3), we observe that $\varphi_k(1) = \{0, \dots, k-1\}$ and

$$(-1)^{k-|\varphi_k(1)|} \cdot H^{(k)}_{\varphi_k(1),\theta}(q)(x_0, \dots, x_{k-1}) = q(x_0, \dots, x_{k-1}).$$

Therefore $q \in \mathrm{Sg}^{\mathbf{P}(A,k,m,\theta)}(\{\mathsf{D}^{(k)}_{\theta,(\theta,\dots,\theta)}(q)\} \cup \{H^{(k)}_{\varphi_k(i),\theta}(q) \,|2 \leq i \leq 2^k\})$. Now, by Lemma 2.11, we know that $\mathsf{D}^{(k)}_{\theta,(\theta,\dots,\theta)}(q)$ is a k-ary θ-polynomial. Obviously, its essential arity is at most k. Furthermore, for every $i \in \{2, 3, \dots, 2^{k-1}\}$, the polynomials $H^{(k)}_{\varphi_k(i),\theta}(q)$ depend on at most $k-1$ arguments and, by Proposition 2.16, $H^{(k)}_{\varphi_k(i),\theta}(q)(A^k) \subseteq \theta/\alpha$. Hence by the induction hypothesis $H^{(k)}_{\varphi_k(i),\theta}(q) \in \mathrm{Sg}^{\mathbf{P}(A,k-1,m,\theta)}(P)$ for $i \in \{2, 3, \dots, 2^{k-1}\}$, where P is the set of θ-polynomials of essential arities at most $k-1$. Therefore,

$$q \in \mathrm{Sg}^{\mathbf{P}(A,k,m,\theta)}(\{\mathsf{D}^{(k)}_{\theta,(\theta,\dots,\theta)}(q)\} \cup P).$$

This completes the induction step.□

LEMMA 2.19. *Let $\mathbf{A}$ be a Mal'cev algebra with a Mal'cev term m and let $k \geq 1$. Let $q \in \mathsf{Pol}_{k+1}\mathbf{A}$, $(a_0, \dots, a_{k-1}) \in A^k$, $\theta, u \in A$. Let $f \in \mathsf{Pol}_{k+1}\mathbf{A}$ be defined by*

$$f(x_0, \dots, x_k) := \mathsf{D}^{(k)}_{\theta,(a_0,\dots,a_{k-1})}(\mathsf{E}^{(k)}_{x_k}(\mathsf{F}_{\theta,u}(q)))(x_0, \dots, x_{k-1})$$

for all $x_0, \dots, x_k \in A$. Then f is absorbing at $(a_0, \dots, a_{k-1}, u)$ with value θ.

Proof: Let $(x_0, \dots, x_k) \in A^{k+1}$ such that $x_i = a_i$ for an $i \in \{0, 1, \dots, k-1\}$ or $x_k = u$. We first consider the case $x_k = u$. By the definitions of the operators E and F we know that $\mathsf{E}^{(k)}_u(\mathsf{F}_{\theta,u}(q))(y_0, \dots, y_{k-1}) = \theta$ for all $(y_0, \dots, y_{k-1}) \in A^k$. Then, $f(x_0, \dots, x_k) = \theta$ because the operator D, acting on a constant function, produces the constant function with value θ. In the case that there is an i with $a_i = x_i$, the assertion follows from Lemma 2.11. □

EXAMPLE 2.20. In this example we start with a ternary polynomial p of an expanded group $(V, +, -, 0, F)$. Since we have already computed $\mathsf{F}_{0,u}(p)$ in Example 2.7, we have

$$\begin{aligned}
&\mathsf{D}^{(2)}_{0,(a_0,a_1)}\left(\mathsf{E}^{(2)}_{x_2}(\mathsf{F}_{0,u}(p))\right)(x_0, x_1) = \\
&= \mathsf{D}^{(1)}_{0,a_0}\left(\mathsf{E}^{(1)}_{x_1}(\mathsf{E}^{(2)}_{x_2}(\mathsf{F}_{0,u}(p)))\right)(x_0) - \mathsf{D}^{(1)}_{0,a_0}\left(\mathsf{E}^{(1)}_{a_1}(\mathsf{E}^{(2)}_{x_2}(\mathsf{F}_{0,u}(p)))\right)(x_0) \\
&= \left(\mathsf{E}^{(1)}_{x_1}(\mathsf{E}^{(2)}_{x_2}(\mathsf{F}_{0,u}(p)))\right)(x_0) - \left(\mathsf{E}^{(1)}_{x_1}(\mathsf{E}^{(2)}_{x_2}(\mathsf{F}_{0,u}(p)))\right)(a_0)
\end{aligned}$$

$$-\Big(\big(\mathsf{E}^{(1)}_{a_1}(\mathsf{E}^{(2)}_{x_2}(\mathsf{F}_{0,u}(p)))\big)(x_0) - \big(\mathsf{E}^{(1)}_{a_1}(\mathsf{E}^{(2)}_{x_2}(\mathsf{F}_{0,u}(p)))\big)(a_0)\Big)$$
$$= (p(x_0,x_1,x_2) - p(x_0,x_1,u)) - (p(a_0,x_1,x_2) - p(a_0,x_1,u))$$
$$-\big((p(x_0,a_1,x_2) - p(x_0,a_1,u)) - (p(a_0,a_1,x_2) - p(a_0,a_1,u))\big)$$
$$= p(x_0,x_1,x_2) - p(x_0,x_1,u) + p(a_0,x_1,u) - p(a_0,x_1,x_2)$$
$$+p(a_0,a_1,x_2) - p(a_0,a_1,u) + p(x_0,a_1,u) - p(x_0,a_1,x_2).$$

Clearly, $\mathsf{D}^{(2)}_{0,(a_0,a_1)}\left(\mathsf{E}^{(2)}_u(\mathsf{F}_{0,u}(p))\right)(x_0,x_1) = \mathsf{D}^{(2)}_{0,(a_0,a_1)}\left(\mathsf{E}^{(2)}_{x_2}(\mathsf{F}_{0,u}(p))\right)(a_0,x_1)$

$$= \mathsf{D}^{(2)}_{0,(a_0,a_1)}\left(\mathsf{E}^{(2)}_{x_2}(\mathsf{F}_{0,u}(p))\right)(x_0,a_1) = 0.$$

LEMMA 2.21. *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term* m*, let* $\theta \in A$ *and let* $\eta \in \mathsf{Con}\,\mathbf{A}$*. If* $k \geq 1$*,* $(a_0,\dots,a_{k-1})$*,* $(b_0,\dots,b_{k-1}) \in A^k$*,* $u, v \in A$ *and* $q \in \mathsf{Pol}_{k+1}\mathbf{A}$ *such that*

$$q(\alpha_0,\dots,\alpha_{k-1},u) \equiv_\eta q(\alpha_0,\dots,\alpha_{k-1},v)$$

for every $(\alpha_0,\dots,\alpha_{k-1}) \in \{a_0,b_0\} \times \cdots \times \{a_{k-1},b_{k-1}\}$*, then*

$$\mathsf{D}^{(k)}_{\theta,(a_0,\dots,a_{k-1})}(\mathsf{E}^{(k)}_v(\mathsf{F}_{\theta,u}(q)))(b_0,\dots,b_{k-1}) \equiv_\eta \theta.$$

Proof: We prove the statement by induction on k. For $k=1$, we have

$$\mathsf{D}^{(1)}_{\theta,a_0}\left(\mathsf{E}^{(1)}_v(\mathsf{F}_{\theta,u}(q)\right)(b_0) =$$
$$= m(m(q(b_0,v),q(b_0,u),\theta), m(q(a_0,v),q(a_0,u),\theta),\theta) \equiv_\eta \theta,$$

using the assumptions on q. For $k \geq 2$ let $q \in \mathsf{Pol}_{k+2}\mathbf{A}$ such that

$$q(\alpha_0,\dots,\alpha_k,u) \equiv_\eta q(\alpha_0,\dots,\alpha_k,v)$$

for every $(\alpha_0,\dots,\alpha_k) \in \{a_0,b_0\}\times\cdots\times\{a_k,b_k\}$. Now we divide all possible choices of $(\alpha_0,\dots,\alpha_k)$ in two groups: $\{(\alpha_0,\dots,\alpha_k) \in \{a_0,b_0\}\times\cdots\times\{a_k,b_k\} \mid \alpha_k = a_k\}$ and $\{(\alpha_0,\dots,\alpha_k) \in \{a_0,b_0\}\times\cdots\times\{a_k,b_k\} \mid \alpha_k = b_k\}$. Hence we have

$$\mathsf{E}^{(k)}_{a_k}(q)(\alpha_0,\dots,\alpha_{k-1},u) \equiv_\eta \mathsf{E}^{(k)}_{a_k}(q)(\alpha_0,\dots,\alpha_{k-1},v)$$

and

$$\mathsf{E}^{(k)}_{b_k}(q)(\alpha_0,\dots,\alpha_{k-1},u) \equiv_\eta \mathsf{E}^{(k)}_{b_k}(q)(\alpha_0,\dots,\alpha_{k-1},v)$$

for every $(\alpha_0,\dots,\alpha_{k-1}) \in \{a_0,b_0\}\times\cdots\times\{a_{k-1},b_{k-1}\}$. By the induction hypothesis we obtain

$$\mathsf{D}^{(k)}_{\theta,(a_0,\dots,a_{k-1})}\left(\mathsf{E}^{(k)}_v(\mathsf{F}_{\theta,u}(\mathsf{E}^{(k)}_{a_k}(q)))\right)(b_0,\dots,b_{k-1}) \equiv_\eta \theta,$$

and then by Lemma 2.8 we have

$$\mathsf{D}^{(k)}_{\theta,(a_0,\dots,a_{k-1})}\left(\mathsf{E}^{(k)}_{a_k}(\mathsf{E}^{(k+1)}_v(\mathsf{F}_{\theta,u}(q)))\right)(b_0,\dots,b_{k-1}) \equiv_\eta \theta, \tag{2.4}$$

and in the same way we have

$$\mathsf{D}^{(k)}_{\theta,(a_0,\dots,a_{k-1})}\left(\mathsf{E}^{(k)}_{b_k}(\mathsf{E}^{(k+1)}_v(\mathsf{F}_{\theta,u}(q)))\right)(b_0,\dots,b_{k-1}) \equiv_\eta \theta. \tag{2.5}$$

Now, using equations (2.4) and (2.5) and the definition of the operator D for $p = \mathsf{E}_v^{(k+1)}(\mathsf{F}_{\theta,u}(q))$, we obtain:

$$\mathsf{D}^{(k+1)}_{\theta,(a_0,\ldots,a_k)}(\mathsf{E}_v^{(k+1)}(\mathsf{F}_{\theta,u}(q)))(b_0,\ldots,b_k) =$$

$$m\begin{pmatrix} \mathsf{D}^{(k)}_{\theta,(a_0,\ldots,a_{k-1})}\left(\mathsf{E}^{(k)}_{b_k}(\mathsf{E}_v^{(k+1)}(\mathsf{F}_{\theta,u}(p)))\right)(b_0,\ldots,b_{k-1}) \\ \mathsf{D}^{(k)}_{\theta,(a_0,\ldots,a_{k-1})}\left(\mathsf{E}^{(k)}_{a_k}(\mathsf{E}_v^{(k+1)}(\mathsf{F}_{\theta,u}(p)))\right)(b_0,\ldots,b_{k-1}) \\ \theta \end{pmatrix} \equiv_\eta \theta.$$

□

Example 2.22. Let $\mathbf{V} = (V, +, -, 0, F)$ be an expanded group and choose $a_0, a_1, u, b_0, b_1, v \in V$, $\theta = 0$. The relation η is the equality relation on V. Now, let p be a polynomial of $\mathbf{V}$ such that $p(a_0, a_1, u) = p(a_0, a_1, v)$, $p(a_0, b_1, u) = p(a_0, b_1, v)$, $p(b_0, a_1, u) = p(b_0, a_1, v)$, $p(b_0, b_1, u) = p(b_0, b_1, v)$. In Example 2.20, we have already calculated $\mathsf{D}^{(2)}_{0,(a_0,a_1)}\left(\mathsf{E}^{(2)}_{x_2}(\mathsf{F}_{0,u}(p))\right)(x_0, x_1)$, and thus $\mathsf{D}^{(2)}_{0,(a_0,a_1)}\left(\mathsf{E}^{(2)}_{v}(\mathsf{F}_{0,u}(p))\right)(b_0, b_1) = 0$.

Lemma 2.23. *Let $\mathbf{A}$ be a Mal'cev algebra with a Mal'cev term m, let $\eta \in \mathsf{Con}\,\mathbf{A}$ and let $k \geq 1$. If $(a_0, \ldots, a_{k-1})$, $(b_0, \ldots, b_{k-1})$ are vectors in A, $u, v \in A$ and $q \in \mathsf{Pol}_{k+1}\mathbf{A}$ such that*

$$q(\alpha_0, \ldots, \alpha_{k-1}, u) \equiv_\eta q(\alpha_0, \ldots, \alpha_{k-1}, v)$$

for every $(\alpha_0, \ldots, \alpha_{k-1}) \in \{a_0, b_0\} \times \cdots \times \{a_{k-1}, b_{k-1}\} \backslash \{(b_0, \ldots, b_{k-1})\}$, then for $\theta = q(b_0, \ldots, b_{k-1}, u)$ we have

$$\mathsf{D}^{(k)}_{\theta,(a_0,\ldots,a_{k-1})}(\mathsf{E}_v^{(k)}(\mathsf{F}_{\theta,u}(q)))(b_0,\ldots,b_{k-1}) \equiv_\eta q(b_0,\ldots,b_{k-1},v).$$

Proof: By induction on k. For $k = 1$, by the assumption $q(a_0, u) \equiv_\eta q(a_0, v)$, we have

$$\mathsf{D}^{(1)}_{q(b_0,u),a_0}\left(\mathsf{E}_v^{(1)}(\mathsf{F}_{q(b_0,u),u}(q)\right)(b_0) =$$
$$= m\big(m(q(b_0,v), q(b_0,u), q(b_0,u)), m(q(a_0,v), q(a_0,u), q(b_0,u)), q(b_0,u)\big)$$
$$= m\Big(q(b_0,v), m\Big(q(a_0,v), q(a_0,u), q(b_0,u)\Big), q(b_0,u)\Big) \equiv_\eta q(b_0,v).$$

For the induction step we let $k \geq 2$. We will now compute $\mathsf{D}^{(k+1)}_{q(b_0,\ldots,b_k,u),(a_0,\ldots,a_k)}\left(\mathsf{E}_v^{(k+1)}(\mathsf{F}_{q(b_0,\ldots,b_k,u),u}(q))\right)(b_0,\ldots,b_k)$. According to Definition 2.3 we have to compute $\mathsf{D}^{(k)}_{q(b_0,\ldots,b_k,u),(a_0,\ldots,a_{k-1})}\left(\mathsf{E}^{(k)}_{a_k}(\mathsf{E}_v^{(k+1)}(\mathsf{F}_{q(b_0,\ldots,b_k,u),u}(q))\right)(b_0,\ldots,b_{k-1})$ and $\mathsf{D}^{(k)}_{q(b_0,\ldots,b_k,u),(a_0,\ldots,a_{k-1})}\left(\mathsf{E}^{(k)}_{b_k}(\mathsf{E}_v^{(k+1)}(\mathsf{F}_{q(b_0,\ldots,b_k,u),u}(q))\right)(b_0,\ldots,b_{k-1})$. We assume that

$$q(\alpha_0, \ldots, \alpha_k, u) \equiv_\eta q(\alpha_0, \ldots, \alpha_k, v),$$

for every $(\alpha_0, \ldots, \alpha_k) \in \{a_0, b_0\} \times \cdots \times \{a_k, b_k\} \backslash \{(b_0, \ldots, b_k)\}$. Using Definition 2.1 we obtain $\mathsf{E}^{(k)}_{a_k}(q)(\alpha_0, \ldots, \alpha_{k-1}, u) \equiv_\eta \mathsf{E}^{(k)}_{a_k}(q)(\alpha_0, \ldots, \alpha_{k-1}, v)$ for all

$(\alpha_0, \dots, \alpha_{k-1}) \in \{a_0, b_0\} \times \cdots \times \{a_{k-1}, b_{k-1}\}$. Thus, by Lemma 2.8 and Lemma 2.21, for $\theta = q(b_0, \dots, b_k, u)$ and $\mathsf{E}^{(k)}_{a_k}(q)$, we have

$$\mathsf{D}^{(k)}_{q(b_0,\dots,b_k,u),(a_0,\dots,a_{k-1})}\left(\mathsf{E}^{(k)}_{a_k}(\mathsf{E}^{(k+1)}_v(\mathsf{F}_{q(b_0,\dots,b_k,u),u}(q)))\right)(b_0, \dots, b_{k-1}) \tag{2.6}$$

$$= \mathsf{D}^{(k)}_{q(b_0,\dots,b_k,u),(a_0,\dots,a_{k-1})}\left(\mathsf{E}^{(k)}_v(\mathsf{F}_{q(b_0,\dots,b_k,u),u}(\mathsf{E}^{(k)}_{a_k}(q)))\right)(b_0, \dots, b_{k-1})$$

$$\equiv_\eta q(b_0, \dots, b_k, u).$$

From the assumptions we know that

$$\mathsf{E}^{(k)}_{b_k}(q)(\alpha_0, \dots, \alpha_{k-1}, u) \equiv_\eta \mathsf{E}^{(k)}_{b_k}(q)(\alpha_0, \dots, \alpha_{k-1}, v)$$

for all $(\alpha_0, \dots, \alpha_{k-1}) \in \{a_0, b_0\} \times \cdots \times \{a_{k-1}, b_{k-1}\} \backslash \{(b_0, \dots, b_{k-1})\}$. By Lemma 2.8 and the induction hypothesis for $\mathsf{E}^{(k)}_{b_k}(q)$ and $\theta = \mathsf{E}^{(k)}_{b_k}(q)(b_0, \dots, b_{k-1}, u)$ we obtain

$$\mathsf{D}^{(k)}_{q(b_0,\dots,b_k,u),(a_0,\dots,a_{k-1})}\left(\mathsf{E}^{(k)}_{b_k}(\mathsf{E}^{(k+1)}_v(\mathsf{F}_{q(b_0,\dots,b_k,u),u}(q)))\right)(b_0, \dots, b_{k-1}) \tag{2.7}$$

$$= \mathsf{D}^{(k)}_{\mathsf{E}^{(k)}_{b_k}(q)(b_0,\dots,b_{k-1},u),(a_0,\dots,a_{k-1})}\left(\mathsf{E}^{(k)}_v(\mathsf{F}_{\mathsf{E}^{(k)}_{b_k}(q)(b_0,\dots,b_{k-1},u),u}(\mathsf{E}^{(k)}_{b_k}(q)))\right)(b_0, \dots, b_{k-1})$$

$$\equiv_\eta \mathsf{E}^{(k)}_{b_k}(q)(b_0, \dots, b_{k-1}, v)$$

$$= q(b_0, \dots, b_k, v).$$

Now using Definition 2.3 and the congruences (2.6) and (2.7), we compute

$$\mathsf{D}^{(k+1)}_{q(b_0,\dots,b_k,u),(a_0,\dots,a_k)}\left(\mathsf{E}^{(k+1)}_v(\mathsf{F}_{q(b_0,\dots,b_k,u),u}(q))\right)(b_0, \dots, b_k)$$

$$\equiv_\eta m\begin{pmatrix} q(b_0, \dots, b_k, v) \\ q(b_0, \dots, b_k, u) \\ q(b_0, \dots, b_k, u) \end{pmatrix}$$

$$= q(b_0, \dots, b_k, v).$$

□

EXAMPLE 2.24. Let $\mathbf{V} = (V, +, -, 0, F)$ be an expanded group and choose $a_0, a_1, u, b_0, b_1, v \in V$, $\theta = 0$. The relation η is the equality relation on V. Now let p be a polynomial of $\mathbf{V}$ such that $p(a_0, a_1, u) = p(a_0, a_1, v)$, $p(a_0, b_1, u) = p(a_0, b_1, v)$, $p(b_0, a_1, u) = p(b_0, a_1, v)$ and $p(b_0, b_1, u) = 0$. In Example 2.20, we have already calculated $\mathsf{D}^{(2)}_{0,(a_0,a_1)}\left(\mathsf{E}^{(2)}_{x_2}(\mathsf{F}_{0,u}(p))\right)(x_0, x_1)$, and thus obtain $\mathsf{D}^{(2)}_{0,(a_0,a_1)}\left(\mathsf{E}^{(2)}_v(\mathsf{F}_{0,u}(p))\right)(b_0, b_1) = p(b_0, b_1, v)$.

Remark: Definitions 2.1, 2.3, 2.6 and Lemmas 2.11, 2.19 and 2.23 can be formulated and proved analogously for arbitrary vectors, not just elements of the algebra. As an illustration we give the analogon of Lemma 2.19:

Let $\mathbf{A}$ be a Mal'cev algebra with a Mal'cev term m, let $k \geq 1$, and let $n_0, \dots, n_k \in \mathbb{N}$. Let $q \in \mathsf{Pol}_{n_0+\cdots+n_k}\mathbf{A}$, let $\mathbf{a}_i \in A^{n_i}$ for each $i \in \{0, 1, \dots, k-1\}$, let $\mathbf{u} \in A^{n_k}$, and let $\theta \in A$. Let $f \in \mathsf{Pol}_{n_0+\cdots+n_k}\mathbf{A}$ be defined by

$$f(\mathbf{x}_0, \dots, \mathbf{x}_k) := \mathsf{D}^{(k)}_{\theta,(\mathbf{a}_0,\dots,\mathbf{a}_{k-1})}(\mathsf{E}^{(k)}_{\mathbf{x}_k}(\mathsf{F}_{\theta,\mathbf{u}}(q)))(\mathbf{x}_0, \dots, \mathbf{x}_{k-1})$$

for all $\mathbf{x}_0 \in A^{n_0}, \dots, \mathbf{x}_k \in A^{n_k}$. Then f is absorbing at $(\mathbf{a}_0, \dots, \mathbf{a}_{k-1}, \mathbf{u})$ with value θ.

3. Some Properties of the Centralizing Relation

In Bulatov's definition of the n-ary commutator operation $[\bullet, \bullet, \dots, \bullet]$, polynomials of arbitrary arity are used. We will now show that in Mal'cev algebras, n-ary polynomials are enough. For the binary case, this has been proved in [**3**, Proposition 2.3].

DEFINITION 3.1. Let $\mathbf{A}$ be an algebra, $n_0, \dots, n_k \in \mathbb{N}$, $k \geq 0$ and let $\alpha_0, \dots, \alpha_k, \eta$ be arbitrary congruences of $\mathbf{A}$. Then we say that $C(n_0, \dots, n_k; \alpha_0, \dots, \alpha_k; \eta)$ holds if for all polynomials $p \in \mathsf{Pol}_{n_0+\cdots+n_k}\mathbf{A}$ and vectors $\mathbf{a}_0, \mathbf{b}_0 \in A^{n_0}, \dots, \mathbf{a}_{k-1}, \mathbf{b}_{k-1} \in A^{n_{k-1}}, \mathbf{u}, \mathbf{v} \in A^{n_k}$ that satisfy

(1) $\mathbf{a}_i \equiv_{\alpha_i} \mathbf{b}_i$, for all $i \in \{0, 1, \dots, k-1\}$,
(2) $\mathbf{u} \equiv_{\alpha_k} \mathbf{v}$,
(3) $p(\mathbf{x}_0, \dots, \mathbf{x}_{k-1}, \mathbf{u}) \equiv_\eta p(\mathbf{x}_0, \dots, \mathbf{x}_{k-1}, \mathbf{v})$, for all $(\mathbf{x}_0, \dots, \mathbf{x}_{k-1}) \in \{\mathbf{a}_0, \mathbf{b}_0\} \times \cdots \times \{\mathbf{a}_{k-1}, \mathbf{b}_{k-1}\} \backslash \{(\mathbf{b}_0, \dots, \mathbf{b}_{k-1})\}$,

we have

$$p(\mathbf{b}_0, \dots, \mathbf{b}_{k-1}, \mathbf{u}) \equiv_\eta p(\mathbf{b}_0, \dots, \mathbf{b}_{k-1}, \mathbf{v}).$$

LEMMA 3.2. *Let $\mathbf{A}$ be a Mal'cev algebra with a Mal'cev term m, let $k \geq 0$, let $n_0, \dots, n_k, n'_0, \dots, n'_k \in \mathbb{N}$ and let $\alpha_0, \alpha_1, \dots, \alpha_k, \eta$ be arbitrary congruences of $\mathbf{A}$. Then*

(a) *if $C(n_0, \dots, n_k; \alpha_0, \dots, \alpha_k; \eta)$ and $n'_0 \leq n_0, \dots, n'_k \leq n_k$, then $C(n'_0, \dots, n'_k; \alpha_0, \dots, \alpha_k; \eta)$;*
(b) *if $C(1, n_1, \dots, n_k; \alpha_0, \dots, \alpha_k; \eta)$ and $n_0 \geq 1$, then $C(n_0, n_1, \dots, n_k; \alpha_0, \dots, \alpha_k; \eta)$.*

Proof: (a) follows from the fact that every $(n'_0 + \cdots + n'_k)$-ary polynomial function can be seen as a $(n_0 + \cdots + n_k)$-ary polynomial function in a natural way.

In order to prove (b), we assume that $C(1, n_1, \dots, n_k; \alpha_0, \dots, \alpha_k; \eta)$ holds and we show by induction that $C(n_0, n_1, \dots, n_k; \alpha_0, \dots, \alpha_k; \eta)$ holds for all $n_0 \geq 1$. Let $p \in \mathsf{Pol}_{(n_0+1)+n_1+\cdots+n_k}\mathbf{A}$. Furthermore, take any $a, c \in A$, $\mathbf{b}, \mathbf{d} \in A^{n_0}$, $\mathbf{e}_i, \mathbf{f}_i \in A^{n_i}$, $i \in \{1, \dots, k-1\}$, and $\mathbf{u}, \mathbf{v} \in A^{n_k}$ such that

(1) $a \equiv_{\alpha_0} c$,
(2) $\mathbf{b} \equiv_{\alpha_0} \mathbf{d}$,
(3) $\mathbf{e}_i \equiv_{\alpha_i} \mathbf{f}_i$, for all $i \in \{1, \dots, k-1\}$,

(4) $\mathbf{u} \equiv_{\alpha_k} \mathbf{v}$
(5) $p(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}, \mathbf{u}) \equiv_\eta p(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}, \mathbf{v})$, for all $(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}) \in \{(a, \mathbf{b}), (c, \mathbf{d})\} \times \{\mathbf{e}_1, \mathbf{f}_1\} \times \cdots \times \{\mathbf{e}_{k-1}, \mathbf{f}_{k-1}\}$ and $(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}) \neq \{((c, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1})\}$.

We want to show that

$$p((c, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{u}) \equiv_\eta p((c, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{v}).$$

Now we define the polynomial $h \in \mathsf{Pol}_{(n_0+1)+n_1+\cdots+n_k}\mathbf{A}$ such that

$$h(\mathbf{x}_0, \ldots, \mathbf{x}_k) :=$$

$$\mathsf{D}^{(k)}_{p((c,\mathbf{d}),\mathbf{f}_1,\ldots,\mathbf{f}_{k-1},\mathbf{u}),((a,\mathbf{b}),\mathbf{e}_1,\ldots,\mathbf{e}_{k-1})} \left(\mathsf{E}^{(k)}_{\mathbf{x}_k}(\mathsf{F}_{p((c,\mathbf{d}),\mathbf{f}_1,\ldots,\mathbf{f}_{k-1},\mathbf{u}),\mathbf{u}}(p))\right)(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}).$$

We have

$$h((a, \mathbf{b}), \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{u}) = p((c, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{u}) = h((a, \mathbf{b}), \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{v}), \tag{3.1}$$

for all $(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}) \in \{\mathbf{e}_1, \mathbf{f}_1\} \times \cdots \times \{\mathbf{e}_{k-1}, \mathbf{f}_{k-1}\}$. This can be obtained from the analogon of Lemma 2.19 for vectors, by setting $\theta = p((c, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{u})$, $a_i = \mathbf{e}_i$, $b_i = \mathbf{f}_i$, for $i \in \{1, \ldots, k-1\}$, $a_0 = (a, \mathbf{b})$ and $b_0 = (c, \mathbf{d})$. In the same way we obtain

$$\begin{aligned} h((a, \mathbf{d}), \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{u}) &= p((c, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{u}) \\ &= h((a, \mathbf{d}), \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{v}), \end{aligned} \tag{3.2}$$

and

$$h((c, \mathbf{d}), \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{u}) = p((c, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{u}) = h((c, \mathbf{d}), \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{v}), \tag{3.3}$$

for all $(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}) \in \{\mathbf{e}_1, \mathbf{f}_1\} \times \cdots \times \{\mathbf{e}_{k-1}, \mathbf{f}_{k-1}\} \setminus \{(\mathbf{f}_1, \ldots, \mathbf{f}_{k-1})\}$. Now, we define a polynomial $q \in \mathsf{Pol}_{n_0+n_1+\cdots+n_k}\mathbf{A}$ by

$$q(\mathbf{y}, \mathbf{x}_1, \ldots, \mathbf{x}_k) := h((a, \mathbf{y}), \mathbf{x}_1, \ldots, \mathbf{x}_k).$$

Obviously, by (3.1) and (3.2) we have

$$q(\mathbf{y}, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{u}) \equiv_\eta q(\mathbf{y}, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{v})$$

for all $(\mathbf{y}, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}) \in \{\mathbf{b}, \mathbf{d}\} \times \{\mathbf{e}_1, \mathbf{f}_1\} \times \cdots \times \{\mathbf{e}_{k-1}, \mathbf{f}_{k-1}\}$ and $(\mathbf{y}, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}) \neq (\mathbf{d}, \mathbf{f}_1, \ldots, \mathbf{f}_{k-1})$. From the induction hypothesis we obtain

$$q(\mathbf{d}, \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{u}) \equiv_\eta q(\mathbf{d}, \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{v}),$$

or in other words

$$h((a, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{u}) \equiv_\eta h((a, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{v}). \tag{3.4}$$

If we introduce

$$s(x, \mathbf{x}_1, \ldots, \mathbf{x}_k) := h((x, \mathbf{d}), \mathbf{x}_1, \ldots, \mathbf{x}_k),$$

where $s \in \mathsf{Pol}_{1+n_1+\cdots+n_k}\mathbf{A}$ then (3.2), (3.3) and (3.4) yield

$$s(x, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{u}) \equiv_\eta s(x, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{v}),$$

for all $(x, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}) \in \{a, c\} \times \{\mathbf{e}_1, \mathbf{f}_1\} \times \cdots \times \{\mathbf{e}_{k-1}, \mathbf{f}_{k-1}\} \backslash \{(c, \mathbf{f}_1, \ldots, \mathbf{f}_{k-1})\}$. Using the assumption $C(1, n_0, \ldots, n_k; \alpha_0, \ldots, \alpha_k; \eta)$ we conclude

$$s(c, \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{u}) \equiv_\eta s(c, \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{v}),$$

or in other words

$$h((c, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{u}) \equiv_\eta h((c, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{v}).$$

We know from the analogon of Lemma 2.19 for vectors, where $a_i = \mathbf{e}_i$, $b_i = \mathbf{f}_i$, $1 \leq i \leq k-1$, $a_0 = (a, \mathbf{b})$, $b_0 = (c, \mathbf{d})$ and $\theta = p((c, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{u})$, that

$$h((c, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{u}) = p((c, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{u})$$

and, for the same parameters, from Lemma 2.23 that

$$h((c, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{v}) \equiv_\eta p((c, \mathbf{d}), \mathbf{f}_1, \ldots, \mathbf{f}_{k-1}, \mathbf{v}).$$

This completes the induction step. □

LEMMA 3.3. *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term* m, $\alpha_0, \ldots, \alpha_k, \eta \in \mathsf{Con}\,\mathbf{A}$, $k \geq 0$, $n_0, \ldots, n_k \in \mathbb{N}$, *and let* π *be a permutation of* $\{0, \ldots, k\}$. *Then if* $C(n_0, \ldots, n_k; \alpha_0, \ldots, \alpha_k; \eta)$, *we have*

$$C(n_{\pi(0)}, \ldots, n_{\pi(k)}; \alpha_{\pi(0)}, \ldots, \alpha_{\pi(k)}; \eta).$$

Proof: Since every permutation of $\{0, \ldots, k\}$ is generated by the transpositions, it suffices to consider the following two cases:

(i) $\pi = (i\ j)$, where $i, j \neq k$. Without loss of generality we can assume that $\pi = (0\ 1)$. Choose $p \in \mathsf{Pol}_{n_1+n_0+n_2\cdots+n_k}\mathbf{A}$, $\mathbf{a}_0, \mathbf{b}_0 \in A^{n_1}$, $\mathbf{a}_1, \mathbf{b}_1 \in A^{n_0}$, $\mathbf{a}_i, \mathbf{b}_i \in A^{n_i}$, $i \in \{2, \ldots, k-1\}$, and $\mathbf{u}, \mathbf{v} \in A^{n_k}$ so that

(1) $\mathbf{a}_0 \equiv_{\alpha_1} \mathbf{b}_0$,
(2) $\mathbf{a}_1 \equiv_{\alpha_0} \mathbf{b}_1$,
(3) $\mathbf{a}_i \equiv_{\alpha_i} \mathbf{b}_i$ for $i \in \{2, \ldots, k-1\}$,
(4) $\mathbf{u} \equiv_{\alpha_k} \mathbf{v}$,
(5) $p(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}, \mathbf{u}) \equiv_\eta p(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}, \mathbf{v})$ for all $(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}) \in \{\mathbf{a}_0, \mathbf{b}_0\} \times \cdots \times \{\mathbf{a}_{k-1}, \mathbf{b}_{k-1}\} \backslash \{(\mathbf{b}_0, \ldots, \mathbf{b}_{k-1})\}$.

Next, consider the polynomial $q \in \mathsf{Pol}_{n_0+\cdots+n_k}\mathbf{A}$ defined as follows:

$$q(\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{k-1}, \mathbf{t}) := p(\mathbf{x}_1, \mathbf{x}_0, \mathbf{x}_2, \ldots, \mathbf{x}_{k-1}, \mathbf{t}).$$

Now, we have

$$q(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}, \mathbf{u}) \equiv_\eta q(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}, \mathbf{v})$$

for all $(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}) \in \{\mathbf{a}_1, \mathbf{b}_1\} \times \{\mathbf{a}_0, \mathbf{b}_0\} \times \{\mathbf{a}_2, \mathbf{b}_2\} \times \cdots \times \{\mathbf{a}_{k-1}, \mathbf{b}_{k-1}\}$ and $(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}) \neq (\mathbf{b}_1, \mathbf{b}_0, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1})$. From the assumption $C(n_0, \ldots, n_k; \alpha_0, \ldots, \alpha_k; \eta)$ we conclude that

$$q(\mathbf{b}_1, \mathbf{b}_0, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}, \mathbf{u}) \equiv_\eta q(\mathbf{b}_1, \mathbf{b}_0, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}, \mathbf{v})$$

and hence, we have $p(\mathbf{b}_0, \ldots, \mathbf{b}_{k-1}, \mathbf{u}) \equiv_\eta p(\mathbf{b}_0, \ldots, \mathbf{b}_{k-1}, \mathbf{v})$.

(ii) $\pi = (i\ j)$, where $i = k$ or $j = k$. Without loss of generality we can assume that $\pi = (0\ k)$. Let $p \in \mathsf{Pol}_{n_k+n_1+\cdots+n_{k-1}+n_0}\mathbf{A}$, $\mathbf{a}_0, \mathbf{b}_0 \in A^{n_k}$, $\mathbf{a}_0 \equiv_{\alpha_k} \mathbf{b}_0$, $\mathbf{a}_i, \mathbf{b}_i \in A^{n_i}$, $\mathbf{a}_i \equiv_{\alpha_i} \mathbf{b}_i$, $i \in \{1, \ldots, k-1\}$, and $\mathbf{u}, \mathbf{v} \in A^{n_0}$ such that $\mathbf{u} \equiv_{\alpha_0} \mathbf{v}$ and

$$p(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}, \mathbf{u}) \equiv_\eta p(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}, \mathbf{v})$$

for all $(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}) \in \{\mathbf{a}_0, \mathbf{b}_0\} \times \cdots \times \{\mathbf{a}_{k-1}, \mathbf{b}_{k-1}\} \backslash \{(\mathbf{b}_0, \ldots, \mathbf{b}_{k-1})\}$. Next, we define the polynomial $q \in \mathsf{Pol}_{n_0+\cdots+n_k}\mathbf{A}$ as follows:

$$q(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{t}) := m \begin{pmatrix} p(\mathbf{t}, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{u}) \\ p(\mathbf{t}, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{x}_0) \\ p(\mathbf{b}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{x}_0) \end{pmatrix}.$$

Then we calculate

$$q(\mathbf{u}, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{a}_0) = p(\mathbf{b}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{u}) = q(\mathbf{u}, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{b}_0), \tag{3.5}$$

$$q(\mathbf{v}, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{b}_0) = p(\mathbf{b}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{u}), \tag{3.6}$$

and by the assumption

$$p(\mathbf{a}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{v}) \equiv_\eta p(\mathbf{a}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{u}) \tag{3.7}$$

for all $(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}) \in \{\mathbf{a}_1, \mathbf{b}_1\} \times \cdots \times \{\mathbf{a}_{k-1}, \mathbf{b}_{k-1}\}$. Finally, if $(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}) \neq (\mathbf{b}_1, \ldots, \mathbf{b}_{k-1})$ then we have

$$p(\mathbf{b}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{v}) \equiv_\eta p(\mathbf{b}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{u}), \tag{3.8}$$

by the assumption. Thus, using (3.7), (3.8) and (3.6) we obtain

$$q(\mathbf{v}, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{a}_0) = m \begin{pmatrix} p(\mathbf{a}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{u}) \\ p(\mathbf{a}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{v}) \\ p(\mathbf{b}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{v}) \end{pmatrix} \equiv_\eta$$

$$p(\mathbf{b}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{v}) \equiv_\eta p(\mathbf{b}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{u}) = q(\mathbf{v}, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{b}_0)$$

for all $(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}) \in \{\mathbf{a}_1, \mathbf{b}_1\} \times \cdots \times \{\mathbf{a}_{k-1}, \mathbf{b}_{k-1}\} \backslash \{(\mathbf{b}_1, \ldots, \mathbf{b}_{k-1})\}$. Together with (3.5) we have

$$q(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{a}_0) \equiv_\eta q(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{b}_0),$$

for all $(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1}) \in \{\mathbf{u}, \mathbf{v}\} \times \{\mathbf{a}_1, \mathbf{b}_1\} \times \cdots \times \{\mathbf{a}_{k-1}, \mathbf{b}_{k-1}\} \backslash \{(\mathbf{v}, \mathbf{b}_1, \ldots, \mathbf{b}_{k-1})\}$ and we can conclude

$$q(\mathbf{v}, \mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{a}_0) \equiv_\eta q(\mathbf{v}, \mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{b}_0), \tag{3.9}$$

by the assumption $C(n_0, \ldots, n_k; \alpha_0, \ldots, \alpha_k; \eta)$. Finally, using (3.6), (3.9) and (3.7) we obtain

$$p(\mathbf{b}_0, \mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{u}) = q(\mathbf{v}, \mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{b}_0) \equiv_\eta q(\mathbf{v}, \mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{a}_0) =$$

$$= m \begin{pmatrix} p(\mathbf{a}_0, \mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{u}) \\ p(\mathbf{a}_0, \mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{v}) \\ p(\mathbf{b}_0, \mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{v}) \end{pmatrix} \equiv_\eta p(\mathbf{b}_0, \mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{v}).$$

This proves the statement. □

PROPOSITION 3.4. *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term m, let* $\alpha_0, \dots, \alpha_k$ *and* η *be congruences of* $\mathbf{A}$ *and* $k \geq 0$. *Then* $C(\alpha_0, \dots, \alpha_k; \eta)$ *if and only if* $C(1, \dots, 1; \alpha_0, \dots, \alpha_k; \eta)$.

Proof: If $C(\alpha_0, \dots, \alpha_k; \eta)$ then clearly from Definition 1.1 we have $C(n_0, \dots, n_k; \alpha_0, \dots, \alpha_k; \eta)$ for all $n_0, \dots, n_k \in \mathbb{N}$, thus for $n_0 = \dots = n_k = 1$ we obtain $C(1, \dots, 1; \alpha_0, \dots, \alpha_k; \eta)$. To prove the opposite direction suppose that $C(1, \dots, 1; \alpha_0, \dots, \alpha_k; \eta)$. Let $n_0, \dots, n_k \geq 1$. Then by Lemma 3.3 for $\pi = (0\ k)$ we obtain $C(1, \dots, 1; \alpha_k, \alpha_1, \dots, \alpha_{k-1}, \alpha_0; \eta)$ and by Lemma 3.2 (2), we obtain $C(n_k, 1, \dots, 1; \alpha_k, \alpha_1, \dots, \alpha_{k-1}, \alpha_0; \eta)$. When we apply Lemma 3.3 one more time for $\pi = (0\ k)$ we obtain

$$C(1, \dots, 1, n_k; \alpha_0, \dots, \alpha_k; \eta).$$

We can repeat the same procedure for each of the places from $k-1$ to 0 and obtain $C(n_0, \dots, n_k; \alpha_0, \dots, \alpha_k; \eta)$. Thus we have $C(\alpha_0, \dots, \alpha_k; \eta)$. □

4. Properties and Characterizations of Higher Commutators

Let $n \in \mathbb{N}$, $n \geq 2$. The aim of this section is to give a necessary and sufficient condition for $[\underbrace{1, \dots, 1}_{n}] \neq 0$ in Mal'cev algebras (Proposition 4.15) and to prove that a polynomial Mal'cev clone on a finite set is finitely generated whenever there exists an $n \in \mathbb{N}$ such that $[\underbrace{1, \dots, 1}_{n}] = 0$ (Proposition 4.17). Both results will be essential for proving Theorems §3.1.18, §3.2.3 and §3.3.22.

PROPOSITION 4.1 (HC4). *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term m,* $\alpha_0, \dots, \alpha_k$ *congruences of* $\mathbf{A}$, $k \geq 0$ *and* π *a permutation of* $\{0, \dots, k\}$. *Then*

$$[\alpha_0, \dots, \alpha_k] = [\alpha_{\pi(0)}, \dots, \alpha_{\pi(k)}].$$

Proof: From Definition 1.2 we know that $C(\alpha_0, \dots, \alpha_k; [\alpha_0, \dots, \alpha_k])$ holds and thus $C(1, \dots, 1; \alpha_0, \dots, \alpha_k; [\alpha_0, \dots, \alpha_k])$ holds by Proposition 3.4. Now, from Lemma 3.3 we obtain $C(1, \dots, 1; \alpha_{\pi(0)}, \dots, \alpha_{\pi(k)}; [\alpha_0, \dots, \alpha_k])$ and therefore $C(\alpha_{\pi(0)}, \dots, \alpha_{\pi(k)}; [\alpha_0, \dots, \alpha_k])$, again by Proposition 3.4. Now, by Definition 1.2 we have $[\alpha_{\pi(0)}, \dots, \alpha_{\pi(k)}] \leq [\alpha_0, \dots, \alpha_k]$. In order to prove the other inequality we start with $\alpha_{\pi(0)}, \dots, \alpha_{\pi(k)}$ and the permutation π^{-1}, and reason in the same way. □

LEMMA 4.2 (HC5). *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term m. Let* $\alpha_0, \dots, \alpha_k$ *and* η *be arbitrary congruences of* $\mathbf{A}$ $(k \geq 0)$. *Then* $[\alpha_0, \dots, \alpha_k] \leq \eta$ *if and only if* $C(\alpha_0, \dots, \alpha_k; \eta)$.

Proof: If $C(\alpha_0, \dots, \alpha_k; \eta)$ then by Definition 1.2, we have $[\alpha_0, \dots, \alpha_k] \leq \eta$. Now, suppose that $[\alpha_0, \dots, \alpha_k] \leq \eta$ for $\alpha_0, \dots, \alpha_k \in \mathsf{Con}\,\mathbf{A}$. We will show that $C(1, \dots, 1; \alpha_0, \dots, \alpha_k; \eta)$ by Definition 3.1. Choose $p \in \mathsf{Pol}_{k+1}\mathbf{A}$ and $a_0, \dots, a_{k-1}, u, b_0, \dots, b_{k-1}, v \in A$ so that:

(1) $a_i \equiv_{\alpha_i} b_i$ for $i \in \{0, \dots, k-1\}$,

(2) $u \equiv_{\alpha_k} v$
(3) $p(x_0, \ldots, x_{k-1}, u) \equiv_\eta p(x_0, \ldots, x_{k-1}, v)$, for all $(x_0, \ldots, x_{k-1}) \in \{a_0, b_0\} \times \cdots \times \{a_{k-1}, b_{k-1}\} \backslash \{(b_0, \ldots, b_{k-1})\}$.

We want to show that $p(b_0, \ldots, b_{k-1}, u) \equiv_\eta p(b_0, \ldots, b_{k-1}, v)$. We start by introducing a polynomial $s \in \mathsf{Pol}_{k+1}\mathbf{A}$ by

$$s(x_0, \ldots, x_k) :=$$
$$\mathsf{D}^{(k)}_{p(b_0,\ldots,b_{k-1},u),(a_0,\ldots,a_{k-1})} \left(\mathsf{E}^{(k)}_{x_k}(\mathsf{F}_{p(b_0,\ldots,b_{k-1},u),u}(p))\right)(x_0, \ldots, x_{k-1})$$

where $(x_0, \ldots, x_k) \in A^{k+1}$. Then we observe the following:

$$s(x_0, \ldots, x_{k-1}, u) = p(b_0, \ldots, b_{k-1}, u) = s(x_0, \ldots, x_{k-1}, v),$$

for all $(x_0, \ldots, x_{k-1}) \in \{a_0, b_0\} \times \cdots \times \{a_{k-1}, b_{k-1}\} \backslash \{(b_0, \ldots, b_{k-1})\}$, by Lemma 2.19 and thus

$$s(x_0, \ldots, x_{k-1}, u) \equiv_{[\alpha_0,\ldots,\alpha_k]} s(x_0, \ldots, x_{k-1}, v),$$

for all $(x_0, \ldots, x_{k-1}) \in \{a_0, b_0\} \times \cdots \times \{a_{k-1}, b_{k-1}\} \backslash \{(b_0, \ldots, b_{k-1})\}$. Now, we can conclude

$$s(b_0, \ldots, b_{k-1}, u) \equiv_{[\alpha_0,\ldots,\alpha_k]} s(b_0, \ldots, b_{k-1}, v),$$

and by the assumption we have

$$s(b_0, \ldots, b_{k-1}, u) \equiv_\eta s(b_0, \ldots, b_{k-1}, v).$$

The left side of the last congruence is equal to $p(b_0, \ldots, b_{k-1}, u)$ by Lemma 2.19 and the right side is congruent modulo η to $p(b_0, \ldots, b_{k-1}, v)$ by Lemma 2.23. Now, by Proposition 3.4 we obtain $C(\alpha_0, \ldots, \alpha_k; \eta)$. $\square$

Recall that for an algebra $\mathbf{A}$ and $\alpha, \beta \in \mathsf{Con}\,\mathbf{A}$ such that $\alpha \geq \beta$, α/β denotes the congruence of the factor algebra $\mathbf{A}/\beta$ which corresponds to α in $\mathbf{A}$.

COROLLARY 4.3 (HC6). *Let $\mathbf{A}$ be a Mal'cev algebra with a Mal'cev term m and choose $\alpha_1, \ldots, \alpha_n, \eta \in \mathsf{Con}\,\mathbf{A}$ such that $\eta \leq \alpha_1, \ldots, \alpha_n$. Then*

$$[\alpha_1/\eta, \ldots, \alpha_n/\eta] = ([\alpha_1, \ldots, \alpha_n] \vee \eta)/\eta.$$

Proof: We will show that $([\alpha_1, \ldots, \alpha_n] \vee \eta)/\eta$ is the smallest congruence θ/η with the property

$$C(\alpha_1/\eta, \ldots, \alpha_n/\eta; \theta/\eta).$$

Directly using Definition 1.2 we can check that for every $\eta \in \mathsf{Con}\,\mathbf{A}$, $\eta \leq \alpha_1, \ldots, \alpha_n, \theta$, we have

$$C(\alpha_1, \ldots, \alpha_n; \theta) \Leftrightarrow C(\alpha_1/\eta, \ldots, \alpha_n/\eta; \theta/\eta). \tag{4.1}$$

Since $[\alpha_1, \ldots, \alpha_n] \leq [\alpha_1, \ldots, \alpha_n] \vee \eta$ we have $C(\alpha_1, \ldots, \alpha_n; [\alpha_1, \ldots, \alpha_n] \vee \eta)$ by Lemma 4.2, and thus $C(\alpha_1/\eta, \ldots, \alpha_n/\eta; ([\alpha_1, \ldots, \alpha_n] \vee \eta)/\eta)$ using (4.1) for $\theta = [\alpha_1, \ldots, \alpha_n] \vee \eta$. Let us assume now

$$C(\alpha_1/\eta, \ldots, \alpha_n/\eta; \theta/\eta),$$

for a $\theta \in \mathsf{Con}\,\mathbf{A}$ such that $\eta \leq \theta$. Then by (4.1) we have $C(\alpha_1, \dots, \alpha_n; \theta)$ and thus $[\alpha_1, \dots, \alpha_n] \leq \theta$ by Lemma 4.2, whence $[\alpha_1, \dots, \alpha_n] \vee \eta \leq \theta$. Using the Correspondence Theorem we have $([\alpha_1, \dots, \alpha_n] \vee \eta)/\eta \leq \theta/\eta$. □

Lemma 4.4. *Let $\mathbf{A}$ be a Mal'cev algebra with a Mal'cev term m, let $\rho_1, \dots, \rho_n$, $\alpha_1, \dots, \alpha_k$ and η be arbitrary congruences of $\mathbf{A}$ and $k, n \geq 1$. If $C(\rho_i, \alpha_1, \dots, \alpha_k; \eta)$ for every $i \in \{1, \dots, n\}$, then $C(\bigvee_{1 \leq i \leq n} \rho_i, \alpha_1, \dots, \alpha_k; \eta)$.*

Proof: We know that $\bigvee_{1 \leq i \leq n} \rho_i = \rho_1 \circ \cdots \circ \rho_n$, since $\mathbf{A}$ is congruence permutable. We will prove the statement by induction. For $n = 1$ the statement is obvious. Let $n \geq 2$. We put $\theta_1 = \rho_1 \circ \cdots \circ \rho_{n-1}$ and $\theta_2 = \rho_n$. Now $\bigvee_{1 \leq i \leq n} \rho_i = \theta_1 \circ \theta_2$. We will prove that $C(1, \dots, 1; \theta_1 \circ \theta_2, \alpha_1, \dots, \alpha_k; \eta)$ by Definition 3.1. Let $p \in \mathsf{Pol}_{k+1}\mathbf{A}$ and choose $a_0, \dots, a_{k-1}, u, b_0, \dots, b_{k-1}, v \in A$ so that $a_0 \equiv_{\theta_1 \circ \theta_2} b_0$, $a_i \equiv_{\alpha_i} b_i$ for $i \in \{1, \dots, k-1\}$, $u \equiv_{\alpha_k} v$ and

$$p(x_0, \dots, x_{k-1}, u) \equiv_\eta p(x_0, \dots, x_{k-1}, v),$$

for all $(x_0, \dots, x_{k-1}) \in \{a_0, b_0\} \times \cdots \times \{a_{k-1}, b_{k-1}\} \backslash \{(b_0, \dots, b_{k-1})\}$. We have to show $p(b_0, \dots, b_{k-1}, u) \equiv_\eta p(b_0, \dots, b_{k-1}, v)$. From the assumption $a_0 \equiv_{\theta_1 \circ \theta_2} b_0$ we know that there exists a $c \in A$ such that $a_0 \equiv_{\theta_1} c$ and $c \equiv_{\theta_2} b_0$. We introduce a polynomial $s \in \mathsf{Pol}_{k+1}\mathbf{A}$ as follows:

$$s(x_0, \dots, x_k) :=$$

$$\mathsf{D}^{(k)}_{p(b_0, \dots, b_{k-1}, u), (a_0, \dots, a_{k-1})} \left(\mathsf{E}^{(k)}_{x_k} (\mathsf{F}_{p(b_0, \dots, b_{k-1}, u), u}(p)) \right) (x_0, \dots, x_{k-1})$$

and observe that by Lemma 2.19:

$$s(x_0, \dots, x_{k-1}, u) = p(b_0, \dots, b_{k-1}, u) = s(x_0, \dots, x_{k-1}, v),$$

for all $(x_0, x_1, \dots, x_{k-1}) \in \{a_0, c\} \times \{a_1, b_1\} \times \cdots \times \{a_{k-1}, b_{k-1}\}$ and $(x_0, x_1, \dots, x_{k-1}) \neq (c, b_1, \dots, b_{k-1})$ whence

$$s(x_0, \dots, x_{k-1}, u) \equiv_\eta s(x_0, \dots, x_{k-1}, v),$$

for all $(x_0, x_1, \dots, x_{k-1}) \in \{a_0, c\} \times \{a_1, b_1\} \times \cdots \times \{a_{k-1}, b_{k-1}\}$ and $(x_0, x_1, \dots, x_{k-1}) \neq (c, b_1, \dots, b_{k-1})$. Using the induction hypothesis we know that $C(\theta_1, \alpha_1, \dots, \alpha_k; \eta)$ and therefore we obtain

$$s(c, b_1, \dots, b_{k-1}, u) \equiv_\eta s(c, b_1, \dots, b_{k-1}, v). \tag{4.2}$$

Also, by Lemma 2.19 we have

$$s(x_0, \dots, x_{k-1}, u) = p(b_0, \dots, b_{k-1}, u) = s(x_0, \dots, x_{k-1}, v),$$

for all $(x_0, x_1, \dots, x_{k-1}) \in \{c, b_0\} \times \{a_1, b_1\} \times \cdots \times \{a_{k-1}, b_{k-1}\}$ and $(x_0, x_1, \dots, x_{k-1}) \notin \{(c, b_1, \dots, b_{k-1}), (b_0, b_1, \dots, b_{k-1})\}$, and thus

$$s(x_0, \dots, x_{k-1}, u) \equiv_\eta s(x_0, \dots, x_{k-1}, v), \tag{4.3}$$

for all $(x_0, x_1, \dots, x_{k-1}) \in \{c, b_0\} \times \{a_1, b_1\} \times \cdots \times \{a_{k-1}, b_{k-1}\}$ and

$(x_0, x_1, \ldots, x_{k-1}) \notin \{(c, b_1, \ldots, b_{k-1}), (b_0, b_1, \ldots, b_{k-1})\}$. From (4.2) and (4.3) we have

$$s(x_0, \ldots, x_{k-1}, u) \equiv_\eta s(x_0, \ldots, x_{k-1}, v),$$

for all $(x_0, x_1, \ldots, x_{k-1}) \in \{c, b_0\} \times \{a_1, b_1\} \times \cdots \times \{a_{k-1}, b_{k-1}\}$ and $(x_0, x_1, \ldots, x_{k-1}) \neq (b_0, b_1, \ldots, b_{k-1})$. Using assumption $C(\theta_2, \alpha_1, \ldots, \alpha_k; \eta)$ we obtain

$$s(b_0, \ldots, b_{k-1}, u) \equiv_\eta s(b_0, \ldots, b_{k-1}, v).$$

The left side of the last congruence is equal to $p(b_0, \ldots, b_{k-1}, u)$ by Lemma 2.19 and the right side is congruent modulo η to $p(b_0, \ldots, b_{k-1}, v)$ by Lemma 2.23. Now, by Proposition 3.4, we have $C(\theta_1 \circ \theta_2, \alpha_1, \ldots, \alpha_k; \eta)$. □

PROPOSITION 4.5. *Let* **A** *be a Mal'cev algebra with a Mal'cev term m, and let* $\rho_1, \ldots, \rho_n$, $\alpha_1, \ldots, \alpha_k$ *be congruences of* **A**, $k, n \geq 1$. *Then:*

$$\bigvee_{1 \leq i \leq n} [\rho_i, \alpha_1, \ldots, \alpha_k] = [\bigvee_{1 \leq i \leq n} \rho_i, \alpha_1, \ldots, \alpha_k].$$

Proof: Since $\rho_j \leq \bigvee_{1 \leq i \leq n} \rho_i$ we know from (HC2) that

$$[\rho_j, \alpha_1, \ldots, \alpha_k] \leq [\bigvee_{1 \leq i \leq n} \rho_i, \alpha_1, \ldots, \alpha_k],$$

for every $j \in \{1, \ldots, n\}$. Thus,

$$\bigvee_{1 \leq i \leq n} [\rho_i, \alpha_1, \ldots, \alpha_k] \leq [\bigvee_{1 \leq i \leq n} \rho_i, \alpha_1, \ldots, \alpha_k].$$

Let us show the other inequality. By Definition 1.2 we know that

$$C(\rho_j, \alpha_1, \ldots, \alpha_k; [\rho_j, \alpha_1, \ldots, \alpha_k]),$$

for every $j \in \{1, \ldots, n\}$, and thus using the inequality

$$[\rho_j, \alpha_1, \ldots, \alpha_k] \leq \bigvee_{1 \leq i \leq n} [\rho_i, \alpha_1, \ldots, \alpha_k]$$

and Lemma 4.2 we have

$$C(\rho_j, \alpha_1, \ldots, \alpha_k; \bigvee_{1 \leq i \leq n} [\rho_i, \alpha_1, \ldots, \alpha_k]),$$

for every $j \in \{1, \ldots, n\}$. By Lemma 4.4 we obtain

$$C(\bigvee_{1 \leq i \leq n} \rho_i, \alpha_1, \ldots, \alpha_k; \bigvee_{1 \leq i \leq n} [\rho_i, \alpha_1, \ldots, \alpha_k]).$$

Finally, by Definition 1.2 we have

$$[\bigvee_{1 \leq i \leq n} \rho_i, \alpha_1, \ldots, \alpha_k] \leq \bigvee_{1 \leq i \leq n} [\rho_i, \alpha_1, \ldots, \alpha_k].$$

□

Corollary 4.6. *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term* m*, and let* $\rho_1, \ldots, \rho_n$*,* $\alpha_0, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_k$ *be congruences of* $\mathbf{A}$*,* $j, k, n \geq 1$*. Then:*

$$\bigvee_{1 \leq i \leq n} [\alpha_0, \ldots, \alpha_{j-1}, \rho_i, \alpha_{j+1}, \ldots, \alpha_k] = [\alpha_0, \ldots, \alpha_{j-1}, \bigvee_{1 \leq i \leq n} \rho_i, \alpha_{j+1}, \ldots, \alpha_k].$$

Proof: We obtain the statement directly from Proposition 4.1 and Proposition 4.5. □

As a consequence we immediately obtain the following lemma which claims that distributivity holds for higher commutators in Mal'cev algebras.

Lemma 4.7 (HC7). *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term* m*. Let* $j, k \geq 1$*, let* $I \neq \emptyset$ *be a set and* $\{\alpha_0, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_k\} \cup \{\rho_i \mid i \in I\} \subseteq \mathsf{Con}\,\mathbf{A}$*. Then*

$$\bigvee_{i \in I} [\alpha_0, \ldots, \alpha_{j-1}, \rho_i, \alpha_{j+1}, \ldots, \alpha_k] = [\alpha_0, \ldots, \alpha_{j-1}, \bigvee_{i \in I} \rho_i, \alpha_{j+1}, \ldots, \alpha_k].$$

Proof: Obviously, $\rho_i \leq \bigvee_{i \in I} \rho_i$, for every $i \in I$ and thus we have

$$[\alpha_0, \ldots, \alpha_{j-1}, \rho_i, \alpha_{j+1}, \ldots, \alpha_k] \leq [\alpha_0, \ldots, \alpha_{j-1}, \bigvee_{i \in I} \rho_i, \alpha_{j+1}, \ldots, \alpha_k],$$

for every $i \in I$, by (HC2). Then

$$\bigvee_{i \in I} [\alpha_0, \ldots, \alpha_{j-1}, \rho_i, \alpha_{j+1}, \ldots, \alpha_k] \leq [\alpha_0, \ldots, \alpha_{j-1}, \bigvee_{i \in I} \rho_i, \alpha_{j+1}, \ldots, \alpha_k].$$

To show the other inequality we put $\eta = \bigvee_{i \in I} [\alpha_0, \ldots, \alpha_{j-1}, \rho_i, \alpha_{j+1}, \ldots, \alpha_k]$. Let us show that

$$C(\alpha_0, \ldots, \alpha_{j-1}, \bigvee_{i \in I} \rho_i, \alpha_{j+1}, \ldots, \alpha_k; \eta). \tag{4.4}$$

We use Proposition 3.4 to show (4.4). Thus, take $(a_0, \ldots, a_{k-1}), (b_0, \ldots, b_{k-1}) \in A^k$, $u, v \in A$ and $p \in \mathsf{Pol}_{k+1}\mathbf{A}$ such that

(1) $a_i \equiv_{\alpha_i} b_i$, for every $i \in \{0, \ldots, j-1, j+1, \ldots, k-1\}$,
(2) $a_j \equiv_{\bigvee_{i \in I} \rho_i} b_j$,
(3) $u \equiv_{\alpha_k} v$
(4) $p(x_0, \ldots, x_{k-1}, u) \equiv_\eta p(x_0, \ldots, x_{k-1}, v)$, for all $(x_0, \ldots, x_{k-1}) \in \{a_0, b_0\} \times \cdots \times \{a_{k-1}, b_{k-1}\} \backslash \{(b_0, \ldots, b_{k-1})\}$.

We have to show $p(b_0, \ldots, b_{k-1}, u) \equiv_\eta p(b_0, \ldots, b_{k-1}, v)$. It is well known that the join of an arbitrary set of congruences is the union of joins of its finite subsets. Condition (4) actually consists of $2^k - 1$ formulas, one for each choice of $(x_0, \ldots, x_{k-1})$. If we number all $2^k - 1$ choices of the vector $(x_0, \ldots, x_{k-1})$ with $1, \ldots, 2^k - 1$, then for the ℓ-th choice there is a *finite* subset J_ℓ of I such that the congruence (4) is true for $\bigvee_{i \in J_\ell} [\alpha_0, \ldots, \alpha_{j-1}, \rho_i, \alpha_{j+1}, \ldots, \alpha_k]$ instead of

η. Also there exists a finite set J_0, $J_0 \subseteq I$ such that $a_j \equiv_{\bigvee_{i\in J_0}\rho_i} b_j$. We take $J = \bigcup_{0\leq \ell \leq 2^k-1} J_\ell$. The set J is a finite subset of I. By Corollary 4.6 we know

$$\bigvee_{i\in J}[\alpha_0,\ldots,\alpha_{j-1},\rho_i,\alpha_{j+1},\ldots,\alpha_k] = [\alpha_0,\ldots,\alpha_{j-1},\bigvee_{i\in J}\rho_i,\alpha_{j+1},\ldots,\alpha_k]$$

and since $J_\ell \subseteq J$ for all $\ell \geq 1$ we obtain

$$\bigvee_{i\in J_\ell}[\alpha_0,\ldots,\alpha_{j-1},\rho_i,\alpha_{j+1},\ldots,\alpha_k] \leq [\alpha_0,\ldots,\alpha_{j-1},\bigvee_{i\in J}\rho_i,\alpha_{j+1},\ldots,\alpha_k], \tag{4.5}$$

for all $\ell \geq 1$. Now, we have

(1) $a_i \equiv_{\alpha_i} b_i$, for every $i \in \{0,\ldots,j-1,j+1,\ldots,k-1\}$,
(2) $a_j \equiv_{\bigvee_{i\in J}\rho_i} b_j$, (we know $\bigvee_{i\in J_0}\rho_i \subseteq \bigvee_{i\in J}\rho_i$),
(3) $u \equiv_{\alpha_k} v$,
(4) $p(x_0,\ldots,x_{k-1},u) \equiv_\theta p(x_0,\ldots,x_{k-1},v)$, for all $(x_0,\ldots,x_{k-1}) \in \{a_0,b_0\}\times\cdots\times\{a_{k-1},b_{k-1}\}\setminus\{(b_0,\ldots,b_{k-1})\}$ where $\theta = [\alpha_0,\ldots,\alpha_{j-1},\bigvee_{i\in J}\rho_i,\alpha_{j+1},\ldots,\alpha_k]$, because of inequality (4.5).

Thus, we obtain

$$p(b_0,\ldots,b_{k-1},u) \equiv_\theta p(b_0,\ldots,b_{k-1},v),$$

because $C(\alpha_0,\ldots,\alpha_{j-1},\bigvee_{i\in J}\rho_i,\alpha_{j+1},\ldots,\alpha_k;[\alpha_0,\ldots,\alpha_{j-1},\bigvee_{i\in J}\rho_i,\alpha_{j+1},\ldots,\alpha_k])$. Since

$$[\alpha_0,\ldots,\alpha_{j-1},\bigvee_{i\in J}\rho_i,\alpha_{j+1},\ldots,\alpha_k] = \bigvee_{i\in J}[\alpha_0,\ldots,\alpha_{j-1},\rho_i,\alpha_{j+1},\ldots,\alpha_k] \leq \eta,$$

we have

$$p(b_0,\ldots,b_{k-1},u) \equiv_\eta p(b_0,\ldots,b_{k-1},v).$$

This proves $C(1,\ldots,1;\alpha_0,\ldots,\alpha_{j-1},\bigvee_{i\in I}\rho_i,\alpha_{j+1},\ldots,\alpha_k;\eta)$, and hence concludes the proof of (4.4). $\square$

COROLLARY 4.8. *Let* $\mathbf{A}$ *be a Mal'cev algebra, let* α *be a congruence of* $\mathbf{A}$ *and let* $n \in \mathbb{N}$. *If* $[\underbrace{1,\ldots,[1}_{n},1]] \leq \alpha$ *then* $\mathbf{A}/\alpha$ *is nilpotent of class at most* n.

Proof: We prove

$$[\underbrace{1/\alpha,\ldots,[1/\alpha}_{k},1/\alpha]] \leq ([\underbrace{1,\ldots,[1}_{k},1]]\vee\alpha)/\alpha \text{ for all } k \in \mathbb{N} \tag{4.6}$$

by induction on k. For $k = 1$ the statement is a consequence of (HC6). Let $k > 1$. By the induction hypothesis we have

$$[1/\alpha,[\underbrace{1/\alpha,\ldots,[1/\alpha}_{k-1},1/\alpha]]] \leq [1/\alpha,([\underbrace{1,\ldots,[1}_{k-1},1]]\vee\alpha)/\alpha].$$

We now compute the righthand side of the last inequality. Applying (HC6), we obtain

$$[1/\alpha, ([\underbrace{1, \dots, [1}_{k-1}, 1]] \vee \alpha)/\alpha] = ([1, [\underbrace{1, \dots, [1}_{k-1}, 1]] \vee \alpha] \vee \alpha)/\alpha.$$

Using the distributivity of higher commutators (HC7), the last expression is equal to

$$([1, [\underbrace{1, \dots, [1}_{k-1}, 1]]] \vee [1, \alpha] \vee \alpha)/\alpha.$$

Since $[1, \alpha] \leq \alpha$, this is equal to

$$([\underbrace{1, \dots, [1}_{k}, 1]] \vee \alpha)/\alpha.$$

This completes the induction step. From (4.6), we obtain $[\underbrace{1/\alpha, \dots, [1/\alpha}_{n}, 1/\alpha]]_{\mathbf{A}/\alpha} = 0_{\mathbf{A}/\alpha}$ and hence $\mathbf{A}/\alpha$ is nilpotent of class at most n. ☐

LEMMA 4.9. *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term* m*,* $\alpha_0, \dots, \alpha_n$ *congruences of* $\mathbf{A}$ *and* $n \geq 0$*. Then* $[\alpha_0, \dots, \alpha_n]$ *is generated as a congruence by the set*

$$(4.7) \quad R = \{\big(c(b_0, \dots, b_n), c(a_0, \dots, a_n)\big) \mid b_0, \dots, b_n, a_0 \dots, a_n \in A,\ \forall i : a_i \equiv_{\alpha_i} b_i, \\ c \in \mathsf{Pol}_{n+1}\mathbf{A} \text{ and } c \text{ is absorbing at } (a_0, \dots, a_n)\}.$$

Proof: To prove the statement we will first show $R \subseteq [\alpha_0, \dots, \alpha_n]$. Let $n \geq 0$, $b_0, \dots, b_n, a_0, \dots, a_n \in A$ such that $b_i \equiv_{\alpha_i} a_i$, $i \in \{0, \dots, n\}$, and let $c \in \mathsf{Pol}_{n+1}\mathbf{A}$ be absorbing at $(a_0, \dots, a_n)$. Now it is clear that

$$c(x_0, \dots, x_{n-1}, a_n) = c(a_0, \dots, a_n) = c(x_0, \dots, x_{n-1}, b_n)$$

for all $(x_0, \dots, x_{n-1}) \in \{a_0, b_0\} \times \dots \times \{a_{n-1}, b_{n-1}\} \backslash \{(b_0, \dots, b_{n-1})\}$ and thus we have

$$c(x_0, \dots, x_{n-1}, a_n) \equiv_{[\alpha_0, \dots, \alpha_n]} c(x_0, \dots, x_{n-1}, b_n)$$

for all $(x_0, \dots, x_{n-1}) \in \{a_0, b_0\} \times \dots \times \{a_{n-1}, b_{n-1}\} \backslash \{(b_0, \dots, b_{n-1})\}$. Thus $c(b_0, \dots, b_{n-1}, a_n) \equiv_{[\alpha_0, \dots, \alpha_n]} c(b_0, \dots, b_n)$. Since c is absorbing at $(a_0, \dots, a_n)$, we obtain

$$(c(b_0, \dots, b_n), c(a_0, \dots, a_n)) \in [\alpha_0, \dots, \alpha_n].$$

This proves that every element of R is contained in $[\alpha_0, \dots, \alpha_n]$.

Now, let γ be a congruence of $\mathbf{A}$ such that $R \subseteq \gamma$. To finish the proof it will be enough to prove $[\alpha_0, \dots, \alpha_n] \leq \gamma$, which is equivalent to $C(\alpha_0, \dots, \alpha_n; \gamma)$ by Lemma 4.2. To this end, we take $b_0, \dots, b_n, a_0, \dots, a_n \in A$ such that $a_i \equiv_{\alpha_i} b_i$ for all $i \in \{0, \dots, n\}$ and $p \in \mathsf{Pol}_{n+1}\mathbf{A}$ such that

$$p(x_0, \dots, x_{n-1}, a_n) \equiv_\gamma p(x_0, \dots, x_{n-1}, b_n)$$

for all $(x_0, \ldots, x_{n-1}) \in \{a_0, b_0\} \times \cdots \times \{a_{n-1}, b_{n-1}\} \backslash \{(b_0, \ldots, b_{n-1})\}$. We will show $p(b_0, \ldots, b_{n-1}, a_n) \equiv_\gamma p(b_0, \ldots, b_{n-1}, b_n)$. We define a polynomial $t \in \mathsf{Pol}_{n+1}\mathbf{A}$ as follows:

$$t(x_0, \ldots, x_n) :=$$

$$\mathsf{D}^{(n)}_{p(b_0,\ldots,b_{n-1},a_n),(a_0,\ldots,a_{n-1})} \left(\mathsf{E}^{(n)}_{x_n}(\mathsf{F}_{p(b_0,\ldots,b_{n-1},a_n),a_n}(p))\right)(x_0, \ldots, x_{n-1}).$$

We can observe that by Lemma 2.19, t is absorbing at $(a_0, \ldots, a_n)$, and hence

$$t(x_0, \ldots, x_n) = p(b_0, \ldots, b_{n-1}, a_n) = t(a_0, \ldots, a_n) \tag{4.8}$$

for every $(x_0, \ldots, x_n) \in \{a_0, b_0\} \times \cdots \times \{a_n, b_n\} \backslash \{(b_0, \ldots, b_n)\}$. So, $(t(b_0, \ldots, b_n),$ $t(a_0, \ldots, a_n)) \in R$ and thus $(t(b_0, \ldots, b_n), t(a_0, \ldots, a_n)) \in \gamma$. By Lemma 2.23 we know that $t(b_0, \ldots, b_n) \equiv_\gamma p(b_0, \ldots, b_n)$, so we obtain

$$(p(b_0, \ldots, b_n), t(a_0, \ldots, a_n)) \in \gamma.$$

Therefore, using (4.8) we have $p(b_0, \ldots, b_{n-1}, a_n) \equiv_\gamma p(b_0, \ldots, b_n)$. ☐

Corollary 4.10. *Let $n \geq 2$. Let $\mathbf{A}$ and $\mathbf{B}$ be Mal'cev algebras, on the same set (with possibly different Mal'cev terms). If $\mathsf{Pol}_n\mathbf{A} = \mathsf{Pol}_n\mathbf{B}$, then $\mathbf{A}$ and $\mathbf{B}$ have the same n-ary commutator operation.*

Proof: If $\mathsf{Pol}_n\mathbf{A} = \mathsf{Pol}_n\mathbf{B}$ then $\mathsf{Con}\,\mathbf{A} = \mathsf{Con}\,\mathbf{B}$. Hence every n-ary commutator is generated by the same set on both $\mathbf{A}$ and $\mathbf{B}$. Since $\mathsf{Con}\,\mathbf{A} = \mathsf{Con}\,\mathbf{B}$, this set generates the same congruence on both $\mathbf{A}$ and $\mathbf{B}$. ☐

As another consequence of Lemma 4.9, we obtain a description of the commutator operation for expanded groups. Actually, for expanded groups, this description can be taken for a definition of the higher commutator operations.

Corollary 4.11. *Let $\mathbf{V}$ be an expanded group, let $n \in \mathbb{N}$, let $\alpha_0, \ldots, \alpha_n \in \mathsf{Con}\,\mathbf{V}$, and let $\gamma := [\alpha_0, \ldots, \alpha_n]$. For $i \in \{0, \ldots, n\}$, let A_i be the class $0/\alpha_i$, and let $C := 0/\gamma$. Then C is the subgroup of $(V, +, -, 0)$ that is generated by*

$$S := \{c(a_0, \ldots, a_n) \,|\, a_0 \in A_0, \ldots, a_n \in A_n, c \in \mathsf{Pol}_{n+1}\mathbf{V},$$
$$\text{and } c \text{ is absorbing at } (0, \ldots, 0) \text{ with value } 0\}.$$

Proof: Let S' be the subgroup of $(V, +, -, 0)$ that is generated by S. Since for all $p \in \mathsf{Pol}_1\mathbf{V}$ with $p(0) = 0$, we have $p(S) \subseteq S$, it is easy to show that for all $p \in \mathsf{Pol}_1\mathbf{V}$ with $p(0) = 0$, we have $p(S') \subseteq S'$. By Proposition §1.2.6, S' is an ideal of $\mathbf{V}$, and thus the relation σ' defined by

$$\sigma' := \{(v_0, v_1) \in V \times V \,|\, v_0 - v_1 \in S'\}$$

is a congruence of $\mathbf{V}$.

We will now prove $S' = C$. For proving $C \subseteq S'$, it is sufficient to prove $\gamma \subseteq \sigma'$. To prove this inclusion, we show that all of the generators of γ that are given in Lemma 4.9 lie in σ'. To this end, let $c \in \mathsf{Pol}_{n+1}\mathbf{V}$, $\mathbf{a} = (a_0, \ldots, a_n) \in V^{n+1}$, and

$\mathbf{b} = (b_0, \dots, b_n) \in V^{n+1}$ be such that c is absorbing at $\mathbf{a}$ and for all $i \in \{0, \dots, n\}$, we have $(a_i, b_i) \in \alpha_i$. We define $d \in \mathsf{Pol}_{n+1}\mathbf{V}$ by

$$d(\mathbf{x}) := c(\mathbf{a} + \mathbf{x}) - c(\mathbf{a}) \text{ for all } \mathbf{x} \in V^{n+1}.$$

Then d is absorbing at 0 with value 0, hence $d(-\mathbf{a}+\mathbf{b}) \in S$. Hence $(0, d(-\mathbf{a}+\mathbf{b})) \in \sigma'$, and thus, since σ' is a congruence of $\mathbf{V}$, $(0 + c(\mathbf{a}), d(-\mathbf{a} + \mathbf{b}) + c(\mathbf{a})) = (c(\mathbf{a}), c(\mathbf{b})) \in \sigma'$. This completes the proof of $\gamma \subseteq \sigma'$.

For proving $S' \subseteq C$, we first prove $S \subseteq C$. Let $s \in S$. Then there is a $c \in \mathsf{Pol}_{n+1}\mathbf{V}$ such that c is absorbing at 0 with value 0, and there are $a_0 \in A_0, \dots, a_n \in A_n$ such that $c(a_0, \dots, a_n) = s$. Lemma 4.9 yields $(0, c(a_0, \dots, a_n)) \in \gamma$, and hence $s \in 0/\gamma = C$. Since C is a subgroup of $(V, +, -, 0)$, we have $S' \subseteq C$. □

For the commutator of principal congruences we can avoid the congruence generation involved in Lemma 4.9.

Lemma 4.12. *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term* m*, let* $n \geq 0$*, let* $(u_0, \dots, u_n), (v_0, \dots, v_n) \in A^{n+1}$ *and for all* $i \in \{0, \dots, n\}$ *let* $\alpha_i = \Theta_{\mathbf{A}}(u_i, v_i)$*. Then*

$[\alpha_0, \dots, \alpha_n] = \{\big(c(v_0, \dots, v_n), c(u_0, \dots, u_n)\big) \mid c \in \mathsf{Pol}_{n+1}\mathbf{A}$*, c is absorbing at* $(u_0, \dots, u_n)\}$.

Proof: We denote the set on the right side of the equality by S. By Proposition §1.2.2 we have

$$\Theta_{\mathbf{A}}(u, v) = \{(p(u), p(v)) \mid p \in \mathsf{Pol}_1\mathbf{A}\}, \tag{4.9}$$

$u, v \in A$. First, we prove that the set of generators of $[\alpha_0, \dots, \alpha_n]$ from Lemma 4.9 is a subset of S. Take $a_0, \dots, a_n, b_0, \dots, b_n \in A$, $n \geq 0$, so that $a_i \equiv_{\alpha_i} b_i$, $i \in \{0, \dots, n\}$, and $c \in \mathsf{Pol}_{n+1}\mathbf{A}$ so that c is absorbing at $(a_0, \dots, a_n)$. Using statement (4.9) for $\alpha_i = \Theta_{\mathbf{A}}(u_i, v_i)$ we know that there exist polynomials $p_i \in \mathsf{Pol}_1\mathbf{A}$ such that $a_i = p_i(u_i)$ and $b_i = p_i(v_i)$, for every $i \in \{0, \dots, n\}$. Thus

$$(c(b_0, \dots, b_n), c(a_0, \dots, a_n)) = \Big(c\big(p_0(v_0), \dots, p_n(v_n)\big), c\big(p_0(u_0), \dots, p_n(u_n)\big)\Big).$$

Since c is absorbing at $(a_0, \dots, a_{n-1})$, $c(p_0(x_0), \dots, p_n(x_n))$ is absorbing at $(u_0, \dots, u_n)$. Then we know that

$$(c(b_0, \dots, b_n), c(a_0, \dots, a_n)) = \Big(c\big(p_0(v_0), \dots, p_n(v_n)\big), c\big(p_0(u_0), \dots, p_n(u_n)\big)\Big)$$

belongs to S. Since S is obviously a subset of the generating set of $[\alpha_0, \dots, \alpha_n]$ from Lemma 4.9, we conclude that S generates $[\alpha_0, \dots, \alpha_n]$. We will now show that S is a congruence relation of $\mathbf{A}$. Clearly, S is reflexive, since we can substitute constant functions for c. To prove the symmetry of S let $(c(v_0, \dots, v_n), c(u_0, \dots, u_n)) \in S$ for a polynomial $c \in \mathsf{Pol}_{n+1}\mathbf{A}$ absorbing at $(u_0, \dots, u_n)$. Now, we define the polynomial $e \in \mathsf{Pol}_{n+1}\mathbf{A}$ as follows

$$e(x_0, \dots, x_n) := m\big(c(u_0, \dots, u_n), c(x_0, \dots, x_n), c(v_0, \dots, v_n)\big).$$

We have that $(e(v_0,\dots,v_n), e(u_0,\dots,u_n)) \in S$, by the definition of S. Therefore $(c(u_0,\dots,u_n), c(v_0,\dots,v_n)) \in S$. To prove the transitivity of S we assume that $c, d \in \mathsf{Pol}_{n+1}\mathbf{A}$ are such that $(c(v_0,\dots,v_n), c(u_0,\dots,u_n)) \in S$, $(d(v_0,\dots,v_n), d(u_0,\dots,u_n)) \in S$ and $c(u_0,\dots,u_n) = d(v_0,\dots,v_n)$ for c and d absorbing at $(u_0,\dots,u_n)$, and we show

$$(c(v_0,\dots,v_n), d(u_0,\dots,u_n)) \in S.$$

We introduce the polynomial $e \in \mathsf{Pol}_{n+1}\mathbf{A}$ as follows

$$e(x_0,\dots,x_n) := m\big(c(x_0,\dots,x_n), c(u_0,\dots,u_n), d(x_0,\dots,x_n)\big).$$

It is not hard to see that e is absorbing at $(u_0,\dots,u_n)$. Thus, we conclude that $(e(v_0,\dots,v_n), e(u_0,\dots,u_n)) \in S$. Since $e(v_0,\dots,v_n) = c(v_0,\dots,v_n)$ and $e(u_0,\dots,u_n) = d(u_0,\dots,u_n)$, we have $(c(v_0,\dots,v_n), d(u_0,\dots,u_n)) \in S$. It remains to prove the compatibility property for S. As it is mentioned in [**19**, p. 9] it is enough to check the compatibility for unary polynomials. Let $f \in \mathsf{Pol}_1\mathbf{A}$ and $(c(v_0,\dots,v_n), c(u_0,\dots,u_n)) \in S$ for a polynomial $c \in \mathsf{Pol}_{n+1}\mathbf{A}$ absorbing at $(u_0,\dots,u_n)$. Then for a polynomial $t \in \mathsf{Pol}_{n+1}\mathbf{A}$, defined by

$$t(x_0,\dots,x_n) := f\big(c(x_0,\dots,x_n)\big),$$

we have that t is absorbing at $(u_0,\dots,u_n)$. Now we conclude that $(t(v_0,\dots,v_n), t(u_0,\dots,u_n)) \in S$ or, in other words, $(f\big(c(v_0,\dots,v_n)\big), f\big(c(u_0,\dots,u_n)\big)) \in S$. This completes the proof. □

Proposition 4.13. *Let $\mathbf{A}$ be a Mal'cev algebra with a Mal'cev term m, let $n, k \in \mathbb{N}$ be such that $k < n$, and let $\alpha_0,\dots,\alpha_n$ be congruences of $\mathbf{A}$. Then*

$$[\alpha_0,\dots,\alpha_{k-1},[\alpha_k,\dots,\alpha_n]] \le [\alpha_0,\dots,\alpha_n].$$

Proof: Since we know that every congruence is a join of principal congruences, it suffices to consider the case where $\alpha_k,\dots,\alpha_n$ are principal congruences. The general inequality then follows from Lemma 4.7. We will prove that each of the generators of $[\alpha_0,\dots,\alpha_{k-1},[\alpha_k,\dots,\alpha_n]]$ given in Lemma 4.9 belongs to $[\alpha_0,\dots,\alpha_n]$. Assume that $\alpha_i = \Theta_{\mathbf{A}}(a_i,b_i)$, where $(a_i,b_i) \in A^2$, $i \in \{k,\dots,n\}$. Let $(c(v_0,\dots,v_k), c(u_0,\dots,u_k))$ be an element in the generating set of $[\alpha_0,\dots,\alpha_{k-1},[\alpha_k,\dots,\alpha_n]]$ as in Lemma 4.9. Then $v_i \equiv_{\alpha_i} u_i$ for all $i \in \{0,\dots,k-1\}$, $v_k \equiv_{[\alpha_k,\dots,\alpha_n]} u_k$, and c is a k-ary polynomial of $\mathbf{A}$ that is absorbing at $(u_0,\dots,u_k)$. From Lemma 4.12 we know that there exists a $d \in \mathsf{Pol}_{n-k+1}\mathbf{A}$ such that $v_k = d(b_k,\dots,b_n)$ and $u_k = d(a_k,\dots,a_n)$ and d is absorbing at $(a_k,\dots,a_n)$. Now, we observe that the polynomial $e \in \mathsf{Pol}_{n+1}\mathbf{A}$ defined by

$$e(x_0,\dots,x_n) := c(x_0,\dots,x_{k-1}, d(x_k,\dots,x_n))$$

is absorbing at $(u_0,\dots,u_{k-1},a_k,\dots,a_n)$. Thus, from Lemma 4.9 we obtain that $(e(v_0,\dots,v_{k-1},b_k,\dots,b_n), e(u_0,\dots,u_{k-1},a_k,\dots,a_n))$ belongs to the generating set of the commutator $[\alpha_0,\dots,\alpha_n]$ or, in other words,

$$(c(v_0,\dots,v_k), c(u_0,\dots,u_k)) \in [\alpha_0,\dots,\alpha_n].$$

This completes the proof. □

COROLLARY 4.14 (HC8). *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term* m*, let* $n \in \mathbb{N}$*, and let* $\alpha_0, \ldots, \alpha_n$*, be congruences of* $\mathbf{A}$*. Then*

$$[\alpha_0, [\alpha_1, \ldots, \alpha_n]] \leq [\alpha_0, \alpha_1, \ldots, \alpha_n].$$

Proof: We obtain the inequality directly from Proposition 4.13 if we choose $k = 1$. □

PROPOSITION 4.15. *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term* m *and let* $n \geq 2$*. Then*

$$[\underbrace{1, \ldots, 1}_{n}] > 0$$

if and only if there exists a $c \in \mathsf{Pol}_n\mathbf{A}$ *and* $\theta, \theta_0, \ldots, \theta_{n-1} \in A$ *such that*

(1) c *is absorbing at* $(\theta_0, \ldots, \theta_{n-1})$ *with value* θ*, and*
(2) *there exists a vector* $(a_0, \ldots, a_{n-1}) \in A^n$ *such that* $c(a_0, \ldots, a_{n-1}) \neq \theta$*.*

Proof: ($\Rightarrow$) Let $[\underbrace{1, \ldots, 1}_{n}] > 0$. Then $C(\underbrace{1, \ldots, 1}_{n}; 0)$ is not true. By Proposition 3.4 and Definition 3.1 there exist $\theta_0, \ldots, \theta_{n-1}, a_0, \ldots, a_{n-1} \in A$ and a $p \in \mathsf{Pol}_n\mathbf{A}$ such that

$$p(x_0, \ldots, x_{n-2}, \theta_{n-1}) = p(x_0, \ldots, x_{n-2}, a_{n-1}),$$

for all $(x_0, \ldots, x_{n-2}) \in \{\theta_0, a_0\} \times \cdots \times \{\theta_{n-2}, a_{n-2}\} \backslash \{(a_0, \ldots, a_{n-2})\}$ and

$$p(a_0, \ldots, a_{n-2}, \theta_{n-1}) \neq p(a_0, \ldots, a_{n-2}, a_{n-1}).$$

Now, we put $\theta = p(a_0, \ldots, a_{n-2}, \theta_{n-1})$ and define $c \in \mathsf{Pol}_n\mathbf{A}$ as follows:

$$c(x_0, \ldots, x_{n-1}) :=$$
$$\mathsf{D}^{(n-1)}_{p(a_0,\ldots,a_{n-2},\theta_{n-1}),(\theta_0,\ldots,\theta_{n-2})}(\mathsf{E}^{(n-1)}_{x_{n-1}}(\mathsf{F}_{p(a_0,\ldots,a_{n-2},\theta_{n-1}),\theta_{n-1}}(p)))(x_0, \ldots, x_{n-2}).$$

By Lemma 2.19 we have that c is absorbing at $(\theta_0, \ldots, \theta_{n-1})$ with value θ, and by Lemma 2.23 we know that $c(a_0, \ldots, a_{n-1}) = p(a_0, \ldots, a_{n-1})$ and thus $c(a_0, \ldots, a_{n-1}) \neq \theta$.

($\Leftarrow$) Since

$$c(x_0, \ldots, x_{n-2}, \theta_{n-1}) = c(x_0, \ldots, x_{n-2}, a_{n-1}),$$

for all $(x_0, \ldots, x_{n-2}) \in \{\theta_0, a_0\} \times \cdots \times \{\theta_{n-2}, a_{n-2}\} \backslash \{(a_0, \ldots, a_{n-2})\}$ and

$$c(a_0, \ldots, a_{n-2}, \theta_{n-1}) = \theta \neq c(a_0, \ldots, a_{n-1}),$$

the condition $C(\underbrace{1, \ldots, 1}_{n}; 0)$ is false by Definition 1.1. Thus $[\underbrace{1, \ldots, 1}_{n}] = 0$ does not hold, by Definition 1.2. □

Note that the polynomial that satisfies the conditions (1) and (2) of Proposition 4.15 depends on each of its arguments, or, in other words, its essential arity equals its arity. In the sequel we will need θ-polynomials, which we have defined on page 39.

Corollary 4.16. *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term* m *and* $n \geq 2$. *If* $[\underbrace{1,\dots,1}_{n}] = 0$ *then for every* $\theta \in A$, *every* θ*-polynomial* p *of* $\mathbf{A}$ *has essential arity at most* $n-1$.

Proof: Let $\theta \in A$, and let $p \in \mathsf{Pol}_k\mathbf{A}$ be a θ-polynomial with essential arity k. Then p satisfies (1) from Proposition 4.15 for $(\theta', \theta'_0, \dots, \theta'_{k-1}) := (p(\theta,\dots,\theta), \theta, \dots, \theta)$. Since p depends on x_{k-1}, there exist $(a_0,\dots,a_{k-1}), (a_0,\dots,a_{k-2},b_{k-1}) \in A^k$ such that $p(a_0,\dots,a_{k-1}) \neq p(a_0,\dots,a_{k-2},b_{k-1})$. Clearly, $p(a_0,\dots,a_{k-1}) \neq p(\theta,\dots,\theta)$ or $p(a_0,\dots,a_{k-2},b_{k-1}) \neq p(\theta,\dots,\theta)$. Thus, p satisfies also (2) from Proposition 4.15. Thus we have $[\underbrace{1,\dots,1}_{k}] > 0$, and hence $k \leq n-1$. □

Proposition 4.17. *Let* $\mathbf{A}$ *be a Mal'cev algebra with a Mal'cev term* m *and* $n \geq 2$. *If* $[\underbrace{1,\dots,1}_{n}] = 0$ *then* $\mathrm{Clo}(\bigcup_{i=0}^{n-1} \mathsf{Pol}_i\,\mathbf{A} \cup \{m\}) = \mathsf{Pol}\,\mathbf{A}$.

Proof: By (HC8) $\mathbf{A}$ is nilpotent. We proceed by induction on the nilpotency class of $\mathbf{A}$.

In the case that $\mathbf{A}$ is abelian, Proposition §1.3.11 yields that the clone of all polynomials of $\mathbf{A}$ is generated by m and all the unary polynomials of $\mathbf{A}$.

For the induction step, we let $r \in \mathbb{N}$ such that $\mathbf{A}$ is of nilpotency class $r+1$. Then, we have $[\underbrace{1,\dots,[1}_{r+1},1]] = 0$, and for $\alpha := [\underbrace{1,\dots,[1}_{r},1]]$, we have $\alpha > 0$. Hence

$$[1,\alpha] = 0. \tag{4.10}$$

By Corollary 4.8, $\mathsf{Con}(\mathbf{A}/\alpha)$ is nilpotent of class at most r. Furthermore, by (HC6) we have $[\underbrace{1,\dots,1}_{n}]_{\mathbf{A}/\alpha} = 0_{\mathbf{A}/\alpha}$. We fix $p \in \mathsf{Pol}_k\mathbf{A}$, $k \geq n$, and let p_α be the corresponding polynomial from $\mathsf{Pol}(\mathbf{A}/\alpha)$ such that $p_\alpha(\mathbf{x}/\alpha) = p(\mathbf{x})/\alpha$ for all $\mathbf{x} \in A^k$. Thus, by the induction hypothesis we know that $p_\alpha \in \mathrm{Clo}(\bigcup_{i=0}^{n-1} \mathsf{Pol}_i(\mathbf{A}/\alpha) \cup \{m\})$. In other words, there exists a $p' \in \mathrm{Clo}(\bigcup_{i=0}^{n-1} \mathsf{Pol}_i\mathbf{A} \cup \{m\})$ such that $p_\alpha(\mathbf{x}/\alpha) = p'(\mathbf{x})/\alpha$. Now, we obtain $p(\mathbf{x}) \equiv_\alpha p'(\mathbf{x})$, for every $\mathbf{x} \in A^k$. We choose $\theta \in A$, and define $t \in \mathsf{Pol}_k\mathbf{A}$ as follows:

$$t(\mathbf{x}) := m(p(\mathbf{x}), p'(\mathbf{x}), \theta) \text{ for every } \mathbf{x} \in A^k.$$

We want to show $t \in \mathrm{Clo}(\bigcup_{i=0}^{n-1} \mathsf{Pol}_i\mathbf{A} \cup \{m\})$. First, we observe that $t(\mathbf{x}) \in \theta/\alpha$, for all $\mathbf{x} \in A^k$. From (4.10) we have $[\alpha,\alpha] = 0$ and thus we can apply Proposition 2.18 and obtain that $t \in \mathrm{Sg}^{\mathbf{P}(A,k,m,\theta)}(P)$, where P is a set of θ-polynomial functions of essential arities at most the essential arity of t. Using the assumption $[\underbrace{1,\dots,1}_{n}] = 0$ in $\mathbf{A}$ and Corollary 4.16 we conclude that all such θ-polynomial functions are of essential arities at most $n-1$ and thus we have $t \in \mathrm{Clo}(\bigcup_{i=0}^{n-1} \mathsf{Pol}_i\mathbf{A} \cup \{m\})$. Since $p(\mathbf{x}) \equiv_\alpha p'(\mathbf{x})$ and $[\alpha, 1] = 0$, Lemma §1.3.5

yields $p(\mathbf{x}) = m(t(\mathbf{x}), \theta, p'(\mathbf{x}))$. Since $t, p' \in \mathrm{Clo}(\bigcup_{i=0}^{n-1} \mathsf{Pol}_i \mathbf{A} \cup \{m\})$, we have $p \in \mathrm{Clo}(\bigcup_{i=0}^{n-1} \mathsf{Pol}_i \mathbf{A} \cup \{m\})$. $\square$

CHAPTER 3

On Polynomials in Various Types of Mal'cev Algebras

The main results of the dissertation are formulated and proved in this chapter which is divided in three sections: about affine completeness, about polynomial equivalence problem and about number of Mal'cev clones on a finite set. We present a characterization of affine complete expanded groups whose congruence lattice has the (APMI) property (Theorem §3.1.10). For a finite nilpotent algebra of finite type that is a product of algebras of prime power order and generates a congruence modular variety (studied by K. Kearnes in [**25**]), we are able to show that the property of affine completeness is decidable (Theorem §3.1.18). Moreover, the polynomial equivalence problem has polynomial complexity in the length of the input polynomials (Theorem §3.2.3). As the final contribution of this dissertation, we prove that the polynomial functions of a finite Mal'cev algebra whose congruence lattice is of height at most 2 can be described by a finite set of relations (Theorem §3.3.22).

1. Affine Completeness

In the first subsection we present the statements that lead to the characterization of affine complete expanded groups that satisfy the (APMI) property. The second subsection is devoted to the proof of the results about decidability of affine completeness for a subclass of Mal'cev algebras.

1.1. Congruence Preserving Functions in Expanded Groups and (APMI) Property. In this section, we will produce certain functions on $\mathbf{V}$ that preserve the extended types of an expanded group. We say that an ideal U of $\mathbf{V}$ is a *homogeneous ideal* if U is a homogeneous element of the lattice $\mathsf{Id}\,\mathbf{V}$. Our constructions of functions will work for those expanded groups that have a homogeneous ideal U such that every ideal of $\mathbf{V}$ is either above U or below $U \vee U^*$. By Propositions 6.16 and 6.17, each finite expanded group whose congruence lattice satisfies (APMI) has such an ideal.

For an expanded group $\mathbf{V}$ and an ideal I of $\mathbf{V}$, we say that S *is a transversal of* V *through the cosets of* I if $S \subseteq V$ and $|S \cap (v + I)| = 1$ for all $v \in V$.

Proposition 1.1 (Lifting of type preserving functions). *Let $k \in \mathbb{N}$, let $\mathbf{V}$ be a finite expanded group, and let U be a homogeneous ideal of $\mathbf{V}$ such that for all ideals A of $\mathbf{V}$, we have $A \geq U$ or $A \leq U \vee U^*$. Let $g : (V/U)^k \to V/U$, let T be a transversal of V through the cosets of $U \vee U^*$, and let $s_T : V \to T$, $s_U : V \to U$,*

$s_{U^*} : V \to U^*$ *be mappings such that*

$$v = s_T(v) + s_U(v) + s_{U^*}(v) \text{ for all } v \in V.$$

Now let h *be a function from* V^k *to* V *such that*

$$h(\mathbf{v}) \in g(\mathbf{v} + U^k) \text{ for all } \mathbf{v} \in V^k.$$

We define a function $f : V^k \to V$ *by*

$$f(\mathbf{v}) := s_T(h(\mathbf{v})) + s_{U^*}(h(\mathbf{v})) \text{ for all } \mathbf{v} \in V^k.$$

Then we have:

(1) *The function* f *is a lifting of* g*, i.e.,* $f(\mathbf{v}) \in g(\mathbf{v} + U^k)$ *for all* $\mathbf{v} \in V^k$*.*
(2) *The function* f *is constant on each coset of* U^k*.*
(3) *If* g *is a congruence preserving function of* $\mathbf{V}/U$*, then* f *is a congruence preserving function of* $\mathbf{V}$*.*

Proof: See [**8**, Proposition 9.2 (1)-(3)]. □

Proposition 1.2. (cf. [**5**, p. 90]) *Let* U *be a homogeneous ideal of the finite expanded group* $\mathbf{V}$*. We assume that we have* $\Phi(U) = 0$ *and* $[U, U] = 0$*. We take* $\mathbf{R}$ *to be an algebra with the universe*

$$R := \{p|_U \mid p \in P_0(\mathbf{V})\}$$

and the operations given by pointwise addition of functions and their composition. Then $\mathbf{R}$ *is a ring. Furthermore, we take* $\mathbf{U}$ *to be an* $\mathbf{R}$*-module* $(U, +, -, 0, R)$*. Then there exist a field* $\mathbf{D}$*, natural numbers* k, n*, a ring isomorphism* $\varepsilon_R : \mathbf{R} \to \mathbf{M}_k(\mathbf{D})$*, and a group isomorphism* $\varepsilon_U : (U, +) \to (\mathbf{D}^{(k\times n)}, +)$ *such that for* $r \in R$ *and* $u \in U$ *we have*

$$\varepsilon_U(r(u)) = \varepsilon_R(r)\varepsilon_U(u).$$

Proof: See [**5**, Proposition 8.1]. □

Proposition 1.3 (Extension of congrence preserving functions). *Let* $\mathbf{V}$ *be a finite expanded group, let* U *be a homogeneous ideal of* $\mathbf{V}$ *such that for all ideals* A *of* $\mathbf{V}$*, we have* $A \geq U$ *or* $A \leq U \vee U^*$*. Let* $\mathbf{U}$ *be the* $P_0(\mathbf{V})$*-module* $(U, +, -, 0, \{f_p \mid p \in P_0(\mathbf{V})\})$*, where*

$$f_p(u) := p(u) \text{ for all } u \in U.$$

Let $k \in \mathbb{N}$*, and let* $g : U^k \to U$ *be a function that preserves the congruences of* $\mathbf{U}$*. We define a function* $e : V^k \to V$ *by*

$$e(\mathbf{u} + \mathbf{u}^*) = g(\mathbf{u}) \text{ for all } \mathbf{u} \in U^k,\ \mathbf{u}^* \in (U^*)^k,$$
$$\text{and } e(\mathbf{v}) = 0 \text{ for all } \mathbf{v} \in V^k \setminus (U \vee U^*)^k.$$

Then, the function e *preserves the congruences of* $\mathbf{V}$*.*

Proof: See [**8**, Proposition 9.3(1)]. □

PROPOSITION 1.4. *Let* $\mathbf{V}$ *be a finite expanded group, and let* U *be a homogeneous ideal of* $\mathbf{V}$ *such that for all ideals* A *of* $\mathbf{V}$*, we have* $A \geq U$ *or* $A \leq U \vee U^*$*. If* $\mathbf{V}$ *is* 1*-affine complete, then the centralizer* $\mathsf{C}_{\mathbf{V}}(\Phi(U) : U)$ *of* U *modulo* $\Phi(U)$ *satisfies* $\mathsf{C}_{\mathbf{V}}(\Phi(U) : U) \leq U \vee U^*$*.*

Proof: Since every weakly 1-polynomially rich algebra is 1-affine complete algebra the statment can be obtained from Proposition 9.5 in [**8**]. □

We will need the following description of the centralizer $\mathsf{C}_{\mathbf{V}}(\Phi(U) : U)$ that appeared in Proposition 1.4.

PROPOSITION 1.5. *Let* $\mathbf{V}$ *be a finite expanded group, let* U *be a homogeneous ideal of* $\mathbf{V}$*, and let* A, B *be ideals of* $\mathbf{V}$ *with* $A \prec B \leq U$*.*

(1) *If* $[B,B]_{\mathbf{V}} \not\leq A$*, then* $A = 0$*,* $B = U$*, and hence* U *is an atom of* $\mathsf{Id}\,\mathbf{V}$*. Furthermore, in this case we have* $\mathsf{C}_{\mathbf{V}}(0 : U) = U^*$*.*
(2) *If* $[B,B]_{\mathbf{V}} \leq A$*, then we have* $\mathsf{C}_{\mathbf{V}}(A : B) = \mathsf{C}_{\mathbf{V}}(\Phi(U) : U) \geq U \vee U^*$*.*
(3) *Every atom* C *of* $\mathsf{Id}\,\mathbf{V}$ *with* $[C,C]_{\mathbf{V}} = C$ *is a homogeneous ideal of* $\mathbf{V}$*.*

Proof: See [**8**, Proposition 9.6]. □

LEMMA 1.6. (cf. [**8**, Lemma 9.7]) *Let* $\mathbf{V}$ *be a finite expanded group whose congruence lattice satisfies* (APMI)*. We assume that* $\mathbf{V}$ *is* 1*-affine complete. Then* $\mathbf{V}$ *satisfies the condition* (SC1)*.*

If the expanded group $\mathbf{V}$ satisfies (SC1), homogeneous ideals have several helpful properties.

PROPOSITION 1.7. *Let* $\mathbf{V}$ *be a finite expanded group with* (SC1)*, and let* U *be a homogeneous element of* $\mathbf{V}$*. Then we have:*

(1) $\Phi(U) = 0$*.*
(2) $\mathsf{C}_{\mathbf{V}}(\Phi(U) : U) \leq U \vee U^*$*.*
(3) *If* $\mathbf{V}$ *is finite, then* U *is the range of a unary idempotent polynomial function.*

Proof: See [**8**, Proposition 10.1]. □

In Section 7 of [**5**], one finds information on those unary polynomial functions whose range is contained in a homogeneous ideal. We will use straightforward generalizations of these results to k-ary functions.

PROPOSITION 1.8 (cf. [**5**, Proposition 7.16]). *Let* $k \in \mathbb{N}$*, let* $\mathbf{V}$ *be a finite expanded group, and let* U *be a homogeneous ideal of* $\mathbf{V}$ *with* $\mathsf{C}_{\mathbf{V}}(\Phi(U) : U) \leq U \vee U^*$*. Let* f *be a partial function on* V *with domain* $T \subseteq V^k$*. We assume* $f(T) \subseteq U$*. Then the following are equivalent.*

(1) *There is a polynomial* $p \in \mathsf{Pol}_k\mathbf{V}$ *with* $p(V^k) \subseteq U$ *and* $p(\mathbf{t}) = f(\mathbf{t})$ *for all* $\mathbf{t} \in T$*.*

(2) *For each coset* $C := \mathbf{v} + (\mathsf{C}_{\mathbf{V}}(\Phi(U) : U))^k$ *with* $\mathbf{v} \in V^k$ *there is a polynomial* $p_C \in \mathsf{Pol}_k\mathbf{V}$ *such that* $p_C(\mathbf{t}) = f(\mathbf{t})$ *for all* $\mathbf{t} \in T \cap C$*.*

The proof of this proposition is identical with the proof of Proposition 7.16 in [**5**] except that k-ary polynomial functions have to be used instead of unary polynomial functions.

PROPOSITION 1.9. *Let* $k \in \mathbb{N}$*, let* $\mathbf{V}$ *be a finite expanded group, and let* U *be an atom of* $\mathsf{Id}\,\mathbf{V}$*. We assume* $[U, U]_{\mathbf{V}} = U$*. Then*

$$\{p|_{U^k} \mid p \in \mathsf{Pol}_k(\mathbf{V}), p(V^k) \subseteq U\} = U^{(U^k)}. \tag{1.1}$$

Proof: See [**8**, Proposition 10.3] □

For an expanded group $\mathbf{V}$ and a homogeneous ideal U of $\mathbf{V}$ with $\Phi(U) = 0$, the structure of the $P_0(\mathbf{V})$-module U has been described in Theorem §1.7.1 and Proposition 1.2. Thus, if $(U_0, U_1, \ldots, U_n)$ is a homogeneous series of $\mathbf{V}$, and if i is such that $[U_{i+1}, U_{i+1}]_{\mathbf{V}} \leq U_i$, the $P_0(\mathbf{V})$-module U_{i+1}/U_i is polynomially equivalent to a module that is isomorphic to the $\mathbf{M}_n(\mathbf{D})$-module $\mathbf{D}^{(n \times m)}$, where $\mathbf{D}$, n and m can be recovered as follows: for an ideal A of $\mathbf{V}$ with $U_i \prec A \leq U_{i+1}$, $\mathbf{D}$ is the field of $P_0(\mathbf{V})$-endomorphisms of the module A/U_i, and n is the dimension of A/U_i over $\mathbf{D}$. The number m is the height of the lattice $\mathbf{I}[U_i, U_{i+1}]$.

Now, we can describe affine complete members of the class of finite expanded groups whose congruence lattice satisfies the condition (APMI).

THEOREM 1.10. (cf. [**8**, Theorem 11.2]) *Let* $\mathbf{V}$ *be a finite expanded group whose congruence lattice satisfies the condition* (APMI)*, let* $(U_0, U_1, \ldots, U_n)$ *be a homogeneous series of the lattice* $\mathsf{Id}\,\mathbf{V}$*, and let* $k \in \mathbb{N}$*. Then the following are equivalent:*

(1) $\mathbf{V}$ *is* k*-affine complete.*
(2) $\mathbf{V}$ *satisfies* (SC1)*, and for all* $i \in \{0, \ldots, n-1\}$ *with* $[U_{i+1}, U_{i+1}]_{\mathbf{V}} \leq U_i$*, the* $P_0(\mathbf{V})$*-module* U_{i+1}/U_i *is* k*-affine complete.*

1.2. Supernilpotent Algebras. In this section we investigate a class of Mal'cev algebras located between the class of abelian and the class of nilpotent Mal'cev algebras. The main result of this section we obtain when the class coincides with the class of nilpotent Mal'cev algebras.

DEFINITION 1.11. Let $k \in \mathbb{N}$. An algebra is called *k-supernilpotent* if

$$[\underbrace{1, \ldots, 1}_{k+1}] = 0.$$

An algebra $\mathbf{A}$ is called *supernilpotent* if there exists a $k \in \mathbb{N}$ such that $\mathbf{A}$ is k-supernilpotent.

DEFINITION 1.12. (cf. [**25**, p.179]) Let $\mathbf{A}$ be an algebra, and let $k \in \mathbb{N}$. The function $c \in \mathsf{Pol}_{k+1}\mathbf{A}$ is a *commutator polynomial of rank k* if the following conditions hold:

(1) For all $x_0, \dots, x_{k-1}, z \in A$: if $z \in \{x_0, \dots, x_{k-1}\}$, then

$$c(x_0, \dots, x_{k-1}, z) = z.$$

(2) There exist $y_0, \dots, y_{k-1}, u \in A$ such that

$$c(y_0, \dots, y_{k-1}, u) \neq u.$$

We can define commutator terms using term functions instead of polynomials in the previous definition. The following proposition will be used in Lemma 1.17.

Proposition 1.13. (cf.[**25**, Theorem 3.14(3),(4)]) *Let* $\mathbf{A}$ *be a finite nilpotent algebra of finite type that generates a congruence modular variety. The following conditions are equivalent:*

(1) $\mathbf{A}$ *factors as a direct product of algebras of prime power cardinality.*
(2) $\mathbf{A}$ *has a finite bound on the rank of nontrivial commutator terms.*

Proposition 1.14. *Let* $k \in \mathbb{N}$ *and let* $\mathbf{A}$ *be a* k*-supernilpotent Mal'cev algebra. If* $\mathbf{A}$ *is* $(k+1)$*-affine complete, then* $\mathbf{A}$ *is affine complete.*

Proof: We define an algebra $\mathbf{B}$ by $\mathbf{B} = (A, \mathcal{C})$ where $\mathcal{C}$ is the set of all functions on $\mathbf{A}$ that preserve all congruences of $\mathbf{A}$. We want to show that $\mathsf{Pol}\,\mathbf{B} = \mathsf{Pol}\,\mathbf{A}$. Since $\mathbf{A}$ is $(k+1)$-affine complete by the assumptions we have $\mathsf{Pol}_s\mathbf{B} = \mathsf{Pol}_s\mathbf{A}$ for every $s \leq k+1$. It is not hard to see that $\mathsf{Con}\,\mathbf{A} = \mathsf{Con}\,\mathbf{B}$. Then, from Corollary §2.4.10 we know that $[\underbrace{1, \dots, 1}_{k+1}] = 0$ is true in $\mathbf{B}$. Finally, from Proposition §2.4.17 we have

$$\mathsf{Pol}\,\mathbf{B} = \mathrm{Clo}(\bigcup_{i=0}^{k} \mathsf{Pol}_i\,\mathbf{B} \cup \{m\}) = \mathrm{Clo}(\bigcup_{i=0}^{k} \mathsf{Pol}_i\,\mathbf{A} \cup \{m\}) = \mathsf{Pol}\,\mathbf{A}.\square$$

Corollary 1.15. *There is an algorithm that decides whether a supernilpotent finite Mal'cev algebra of finite type, given by its operation tables, is affine complete.*

Proof: From Proposition §2.4.15, we obtain a way to compute a $k \in \mathbb{N}$ such that $\mathbf{A}$ is k-supernilpotent. Once such a k is known, it remains to check whether every $(k+1)$-ary congruence preserving function is a polynomial function. □

Lemma 1.16. *Let* $\mathbf{A}$ *be an algebra that generates a congruence permutable variety and let* $k \in \mathbb{N}$*. Then the following are equivalent:*

(1) $[\underbrace{1, \dots, 1}_{k+1}] = 0$*;*
(2) $\mathbf{A}$ *is nilpotent and all commutator polynomials have rank at most* k*.*

Proof: (1) $\Rightarrow$ (2) Let c be a commutator polynomial of rank $t \geq k+1$. From $[\underbrace{1, \ldots, 1}_{k+1}] = 0$ we have $[\underbrace{1, \ldots, 1}_{t}] = 0$ by (HC3), and thus

$$C(\underbrace{1, 1, \ldots, 1}_{t}; 0), \tag{1.2}$$

by Definition §2.1.2. Let $(y_0, \ldots, y_{t-1}, u) \in A^{t+1}$. We want to show that $c(y_0, \ldots, y_{t-1}, u) = u$. For every $(x_0, \ldots, x_{t-2}) \in \{u, y_0\} \times \cdots \times \{u, y_{t-2}\}$ and $(x_0, \ldots, x_{t-2}) \neq (y_0, \ldots, y_{t-2})$ we have $c(x_0, \ldots, x_{t-2}, y_{t-1}, u) = c(x_0, \ldots, x_{t-2}, u, u)$, by Definition 1.12. Thus, by Definition §2.1.1, we have $c(y_0, \ldots, y_{t-1}, u) = c(y_0, \ldots, y_{t-2}, u, u) = u$ because of (1.2). This contradicts the fact that c is a commutator polynomial. Clearly, by (HC8) $\mathbf{A}$ is nilpotent.

(2) $\Rightarrow$ (1) Let $c \in \mathsf{Pol}_n\mathbf{A}$, $\theta, \theta_0, \ldots, \theta_{n-1} \in A$ and $(a_0, \ldots, a_{n-1}) \in A^n$ be such that the following is satisfied:

(i) c is absorbing at $(\theta_0, \ldots, \theta_{n-1})$ with value θ

(ii) there exists a vector $(a_0, \ldots, a_{n-1}) \in A^n$ such that $c(a_0, \ldots, a_{n-1}) \neq \theta$.

By the assumptions of the lemma, $\mathbf{A}$ has a Mal'cev term. Let us denote this term by m. By Lemma §1.3.14, since $\mathbf{A}$ is nilpotent we know that the functions $f_i : A \to A$ defined by

$$f_i(x) := m(x, \theta, \theta_i),$$

for every $i \in \{0, \ldots, n-1\}$ are bijections. Thus there exist $b_0, \ldots, b_{n-1} \in A$ such that $f_i(b_i) = a_i$, for every $i \in \{0, \ldots, n-1\}$. Let us define a polynomial $d \in \mathsf{Pol}_{n+1}\mathbf{A}$ by

$$d(x_0, \ldots, x_{n-1}, z) := m(c(m(x_0, z, \theta_0), \ldots, m(x_{n-1}, z, \theta_{n-1})), \theta, z).$$

Clearly, we have $d(x_0, \ldots, \overset{i-th}{\overset{\downarrow}{z}}, \ldots, x_{n-1}, z) = z$, for every $i \in \{0, \ldots, n-1\}$. Also,

$$d(x_0, \ldots, x_{n-1}, \theta) = c(f_0(x_0), \ldots, f_{n-1}(x_{n-1})).$$

Therefore $d(b_0, \ldots, b_{n-1}, \theta) = c(a_0, \ldots, a_{n-1}) \neq \theta$. Now, the conditions (1) and (2) of Definition 1.12 are satisfied. Thus, d is a commutator polynomial of rank n. By the assumptions $n \leq k$, and thus by Proposition §2.4.15 we obtain $[\underbrace{1, \ldots, 1}_{k+1}] = 0$. $\square$

Lemma 1.17. *Let $\mathbf{A}$ be a finite nilpotent algebra of finite type that generates a congruence modular variety. If $\mathbf{A}$ factors as a direct product of algebras of prime power cardinality then $\mathbf{A}$ is a supernilpotent Mal'cev algebra.*

Proof: We define a new algebra $\mathbf{A}^\star$ in the following way: for each $c \in A$, we add a nullary operation $c^{\mathbf{A}^\star}$ defined by $c() := c$. Since A is finite we have that $\mathbf{A}^\star$ is a finite algebra of finite type. Furthermore Gumm's terms from Proposition §1.2.3 for $\mathbf{A}$ are also terms in $\mathbf{A}^\star$ and thus $\mathbf{A}^\star$ generates a congruence modular variety. By [**3**, Lemma 2.2] we know that the binary commutator in $\mathbf{A}$ and $\mathbf{A}^\star$

is the same. Thus we have that $\mathbf{A}^\star$ is nilpotent. By assumption we know that there is a natural number n such that $A = A_1 \times \cdots \times A_n$, where $|A_i| = p_i^{\alpha_i}$ for some primes p_i and some $\alpha_i \in \mathbb{N}$, $i \in \{1, \ldots, n\}$. We define an algebra $\mathbf{A}_i^\star$ in the following way: for each $c \in A$, we add a nullary operation $c^{\mathbf{A}_i{}^\star}$ defined by $c() := \pi_i(c)$ for every $i \in \{1, \ldots, n\}$. Now, $\mathbf{A}^\star = \mathbf{A}_1^\star \times \cdots \times \mathbf{A}_n^\star$ and $\mathbf{A}_i^\star$ has prime power cardinality. By Proposition 1.13 we have an $m \in \mathbb{N}$ such that the rank of every nontrivial commutator term of $\mathbf{A}^\star$ is at most m. Since these terms are precisely the commutator polynomials of $\mathbf{A}$, and since by Lemma §1.3.15 the algebra $\mathbf{A}$ generates a congruence permutable variety, Lemma 1.16 yields that $\mathbf{A}$ is m-supernilpotent. □

THEOREM 1.18. *There is an algorithm that decides whether a finite nilpotent algebra of finite type that is a product of algebras of prime power order and generates a congruence modular variety is affine complete.*

Proof: From Lemma 1.17 we know that a finite nilpotent algebra $\mathbf{A}$ of finite type which is a product of algebras of prime power order and generates a congruence modular variety is supernilpotent and generates a congruence permutable variety. Therefore $\mathbf{A}$ has a Mal'cev term. Then by Corollary 1.15 we have that the property of affine completeness for $\mathbf{A}$ is decidable. □

2. The Polynomial Equivalence Problem

The polynomial equivalence problem explained in the foreword can be formulated in the more appropriate way for nilpotent Mal'cev algebras. Again, when the nilpotent class of Mal'cev algebras coincides with the class of supernilpotent Mal'cev algebras, we obtain the result given in Theorem 2.3.

In a Mal'cev algebra $\mathbf{A}$, for $(x_0, \ldots, x_{k-1}) \in A^k$ and $\theta \in A$ we introduce the following notation:

$$\omega_\theta(x_0, \ldots, x_{k-1}) := |\{i : x_i \neq \theta\}|.$$

PROPOSITION 2.1. *Let $n, k \in \mathbb{N}$, let $\mathbf{A}$ be a k-supernilpotent Mal'cev algebra, and let $\theta \in A$. Let $p \in \mathsf{Pol}_n\mathbf{A}$ be such that for all $(x_0, \ldots, x_{n-1}) \in A^n$ with $\omega_\theta(x_0, \ldots, x_{n-1}) \leq k$, we have $p(x_0, \ldots, x_{n-1}) = \theta$. Then p is the constant function with value θ.*

Proof: Let $p \in \mathsf{Pol}_n\mathbf{A}$ be a polynomial with this property and let $(x_0, \ldots, x_{n-1}) \in A^n$. We prove $p(x_0, \ldots, x_{n-1}) = \theta$ by induction on $\omega_\theta(x_0, \ldots, x_{n-1})$. If $\omega_\theta(x_0, \ldots, x_{n-1}) < k+1$ then the statement is true by the assumption. Let us suppose that $\omega_\theta(x_0, \ldots, x_{n-1}) = m \geq k+1$. Let $\{i_1, \ldots, i_m\} = \{i \mid x_i \neq \theta\}$. We define a new polynomial q by

$$q(y_1, \ldots, y_{k+1}, z_{k+2}, \ldots, z_m) :=$$

$$p(\theta, \ldots, \theta, \overset{\overset{i_1}{\downarrow}}{y_1}, \theta, \ldots, \theta, \overset{\overset{i_{k+1}}{\downarrow}}{y_{k+1}}, \theta, \ldots, \theta, \overset{\overset{i_{k+2}}{\downarrow}}{z_{k+2}}, \theta, \ldots, \theta, \overset{\overset{i_m}{\downarrow}}{z_m}, \theta, \ldots, \theta)$$

for $y_1, \dots, y_{k+1}, z_{k+2}, \dots, z_m \in A^m$. By the induction hypothesis we have $q(y_1, \dots, y_{k+1}, x_{i_{k+2}}, \dots, x_{i_m}) = \theta$ for every $(y_1, \dots, y_{k+1}) \in \{x_{i_1}, \theta\} \times \dots \times \{x_{i_{k+1}}, \theta\} \backslash \{(x_{i_1}, \dots, x_{i_{k+1}})\}$. If we introduce a polynomial q' in the following way

$$q'(y_1, \dots, y_{k+1}) := q(y_1, \dots, y_{k+1}, x_{i_{k+2}}, \dots, x_{i_m}),$$

we have $q'(y_1, \dots, y_{k+1}) = \theta$ whenever there exists an $i \in \{1, \dots, k+1\}$, such that $y_i = \theta$. Therefore q' is a θ-polynomial, and hence the essential arity of q' is 0 or $k+1$. Since $\mathbf{A}$ is k-supernilpotent we know that $[\underbrace{1, \dots, 1}_{k+1}] = 0$, and thus the essential arity of q' is at most k by Corollary §2.4.16. Thus q is constant, so $q(x_{i_1}, \dots, x_{i_m}) = \theta$ and thus, $p(x_1, \dots, x_n) = \theta$. □

Lemma 2.2. *Let* $\mathbf{A}$ *be a nilpotent Mal'cev algebra* $\mathbf{A}$ *with a Mal'cev term* m *and let* $x, y, \theta \in A$. *Then if* $m(x, y, \theta) = \theta$, *we have* $x = y$.

Proof: Suppose $m(x, y, \theta) = \theta$. By Lemma §1.3.14 we know that the function $f : A \to A$ defined by $f(t) := m(t, y, \theta)$ for $t \in A$ is one to one. Therefore if $x \neq y$ then $f(x) \neq f(y)$. Then we have $m(x, y, \theta) \neq m(y, y, \theta) = \theta$. This contradicts the assumption. □

On supernilpotent Mal'cev algebras, these results provide a method to determine whether two polynomial terms induce the same function. In particular, we can now prove the main result of the section.

Theorem 2.3. *The polynomial equivalence problem for a finite nilpotent algebra* $\mathbf{A}$ *of finite type that is a product of algebras of prime power order and generates a congruence modular variety has polynomial time complexity in the length of the input terms.*

Proof: Suppose that $s(x_0, \dots, x_{n-1}), t(x_0, \dots, x_{n-1})$ are polynomial terms of $\mathbf{A}$. By Lemma 1.17, there is a $k \in \mathbb{N}$ such that $\mathbf{A}$ is k-supernilpotent, and $\mathbf{A}$ has a Mal'cev term m. Since $\mathbf{A}$ is nilpotent, by Lemma 2.2, it suffices to check whether

$$m(s(x_0, \dots, x_{n-1}), t(x_0, \dots, x_{n-1}), \theta) \approx \theta$$

holds in $\mathbf{A}$. We define a polynomial term p of $\mathbf{A}$ by

$$p(x_0, \dots, x_{n-1}) := m(s(x_0, \dots, x_{n-1}), t(x_0, \dots, x_{n-1}), \theta).$$

By Proposition 2.1 we have to check $p^{\mathbf{A}}(a_0, \dots, a_{n-1}) = \theta$ only for those n-tuples from A^n that satisfy $\omega_\theta(a_0, \dots, a_{n-1}) < k+1$. There are precisely

$$1 + (|A| - 1)n + (|A| - 1)^2 \binom{n}{2} + \dots + (|A| - 1)^k \binom{n}{k}$$

such n-tuples. Clearly, this expression is a polynomial in n. Since n is the number of variables that occur in s and t, n is obviously bounded by the length of these terms.

Therefore the polynomial equivalence problem has polynomial complexity in the length of the input terms. □

3. On the Number of Mal'cev Clones

Here we will show that the assertion of Conjecture 1 in §1.7 is true for every finite Mal'cev algebra whose congruence lattice is of height at most 2.

Distinguishing cases according to the isomorphism class of the congruence lattice of the algebra and the commutator operation on this algebra, we will see that in most cases, the result can be inferred from existing results on polynomial completeness [**18, 22, 3**]. However, if the algebra is nilpotent and not abelian, we need a new argument to show that its polynomials can be described by finitely many relations. Actually, in this case (Subsection 3.3) we use higher commutators.

3.1. Abelian Algebras.

PROPOSITION 3.1. *Let* $\mathbf{A}$ *be a finite abelian Mal'cev algebra. Then,*

$$\mathsf{Pol}\,\mathbf{A} = \mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})).$$

Proof: We denote $\mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A}))$ by $\mathcal{C}$. Obviously, we have $\mathsf{Pol}\,\mathbf{A} \subseteq \mathcal{C}$. We will show that $\mathcal{C} \subseteq \mathsf{Pol}\,\mathbf{A}$. To this end we introduce a new algebra $\mathbf{B} = (A, \mathcal{C})$. Since $\mathsf{Inv}^4(A, \mathsf{Pol}\,\mathbf{A}) \subseteq \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})$ we know that every function from $\mathcal{C}$ is a commutator preserving function of $\mathbf{A}$ by Lemma §1.7.5. Thus, $[1,1]_{\mathbf{B}} = [1,1]_{\mathbf{A}} = 0$ and $\mathbf{B}$ is also abelian. Now, let $f \in \mathcal{C}$ be a unary function. Since $\mathsf{Inv}^{|A|}(A, \mathsf{Pol}\,\mathbf{A}) \subseteq \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})$ we know by Lemma §1.7.4 that $f \in \mathsf{Pol}_1\mathbf{A}$. Let $f \in \mathcal{C}$ be of arbitrary arity $k \geq 2$. To show that $f \in \mathsf{Pol}_k\mathbf{A}$ we proceed by induction on k. We have just proved the basis of the induction. For the induction step, we choose an arbitrary element $\theta \in A$. Then, we have

$$\begin{aligned} f(x_1, \ldots, x_k) &= f(m(x_1, \theta, \theta), \ldots, m(x_{k-1}, \theta, \theta), m(\theta, \theta, x_k)) \\ &= m(f(x_1, \ldots, x_{k-1}, \theta), f(\theta, \ldots, \theta), f(\theta, \ldots, \theta, x_k)) \end{aligned}$$

by Lemma §1.3.4 because $\mathbf{B}$ is abelian. Clearly, all constant functions belong to $\mathcal{C}$ and thus $f(x_1, \ldots, x_{k-1}, \theta)$ and $f(\theta, \ldots, \theta, x_k)$ can be seen as a $(k-1)$-ary and as a unary function from $\mathcal{C}$, respectively, and thus they are polynomials of $\mathbf{A}$ by the induction hypothesis. This proves the induction step. □

COROLLARY 3.2. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra such that* $\mathsf{Con}\,\mathbf{A} \cong \mathbf{M}_i$, $i \geq 3$*. Then, there is a finite set of relations* R *on* A *such that* $\mathsf{Pol}\,\mathbf{A} = \mathsf{Comp}(A, R)$.

Proof: By the assumptions $\mathsf{Con}\,\mathbf{A}$ has a sublattice consisting of permuting congruences and isomorphic to $\mathbf{M}_3$. Hence, by Proposition §1.3.12 $\mathbf{A}$ is abelian and the statement can be obtained from Proposition 3.1. □

3.2. Non-nilpotent Algebras.

PROPOSITION 3.3. *Let* $\mathbf{A}$ *be a finite simple Mal'cev algebra. Then,*

$$\mathsf{Pol}\,\mathbf{A} = \mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})).$$

Proof: If $[1,1]=0$ then $\mathbf{A}$ is abelian and we obtain the statement by Proposition 3.1. Thus we suppose $[1,1]=1$. Then $\mathbf{A}$ is TC-neutral and $\mathbf{A}$ has a Mal'cev term by assumptions. So, we have that $\mathbf{A}$ is affine complete by Proposition §1.7.2. □

LEMMA 3.4. *Let* $\mathbf{A}$ *be a finite weakly polynomially rich Mal'cev algebra. Then,*

$$\mathsf{Pol}\,\mathbf{A} = \mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})).$$

Proof: First, we observe that $\mathsf{typ}\{\mathbf{A}\} \in \{2,3\}$ by Corollary §1.5.14. Furthermore, we know by Theorem §1.5.15 that a prime quotient of congruences α and β, $\alpha \prec \beta$, denoted by $\langle\alpha,\beta\rangle$ is of type $\mathbf{2}$ if and only if $[\beta,\beta] \leq \alpha$. As we can see from Definition §1.5.2, $U_{\mathbf{A}}(\alpha,\beta)$ and thus $M_{\mathbf{A}}(\alpha,\beta)$ are completely determined by $\mathsf{Pol}_1\mathbf{A}$. For every prime quotient $\langle\alpha,\beta\rangle$ of type $\mathbf{2}$, the extended type consists of the type together with the corresponding finite field defined in the proof of Theorem §1.5.4. As we can see from this proof, this field is completely determined by unary polynomials of the induced algebra on U, $U \in M_{\mathbf{A}}(\alpha,\beta)$ and thus by $\mathsf{Pol}_1\mathbf{A}$. Now, we can conclude that the extended type of a given prime quotient in $\mathsf{Con}\,\mathbf{A}$ is completely determined by (binary) commutators and $\mathsf{Pol}_1\mathbf{A}$.

Now, we denote $\mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A}))$ by $\mathcal{C}$. If $\mathbf{B} = (A, \mathcal{C})$ then $\mathsf{Pol}_1\mathbf{B} = \mathsf{Pol}_1\mathbf{A}$, by Lemma §1.7.4 because $\mathsf{Inv}^{|A|}(A, \mathsf{Pol}\,\mathbf{A}) \subseteq \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})$. Since $\mathsf{Inv}^4(A, \mathsf{Pol}\,\mathbf{A}) \subseteq \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})$ the binary commutator is preserved by Lemma §1.7.5. So, every $f \in \mathcal{C}$ preserves extended types. Since $\mathbf{A}$ is weakly polynomially rich, every $f \in \mathcal{C}$ is a polynomial of $\mathbf{A}$. Clearly, $\mathsf{Pol}\,\mathbf{A} \subseteq \mathcal{C}$. □

PROPOSITION 3.5. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra such that* $\mathsf{Con}\,\mathbf{A} \cong \mathbf{M}_2$*. Then,*

$$\mathsf{Pol}\,\mathbf{A} = \mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})).$$

Proof: We know that $\mathbf{A}$ and all subdirectly irreducible members of $\mathsf{H}(\mathbf{A})$, which are simple algebras or isomorphic copies of $\mathbf{A}$, satisfy the condition (SC1). Thus by Proposition §1.7.3 we know that $\mathbf{A}$ is weakly polynomially rich. Now we obtain the statement by Lemma 3.4. □

We will now provide results that can be used for Mal'cev algebras whose congruence lattice is a three-element chain.

PROPOSITION 3.6. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra such that* $\mathsf{Con}\,\mathbf{A} = \{0,\alpha,1\}$ *and* $(0:\alpha)_{\mathbf{A}} \leq \alpha$*. Then,*

$$\mathsf{Pol}\,\mathbf{A} = \mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})).$$

Proof: Since $(0:\alpha)_{\mathbf{A}} \leq \alpha$, we know that $\mathbf{A}$ and all subdirectly irreducible members of $\mathsf{H}(\mathbf{A})$, which are simple algebras or isomorphic copies of $\mathbf{A}$, satisfy the condition (SC1). Thus by Proposition §1.7.3 we know that $\mathbf{A}$ is weakly polynomially rich. Now we obtain the statement by Lemma 3.4. □

PROPOSITION 3.7. *Let* $\mathbf{A}$ *be a finite central-by-simple-nonabelian Mal'cev algebra with center* γ *and let* $\theta \in A$. *Then there is a polynomial function* $e \in \mathsf{Pol}_1\mathbf{A}$ *such that* $e(A) \subseteq \theta/\gamma$ *and* $e(x) = x$ *for all* $x \in \theta/\gamma$.

Proof: See [**3**, Lemma 3.1]. □

PROPOSITION 3.8. *Let* $k \in \mathbb{N}$, *let* $\mathbf{A}$ *be a finite central-by-simple-nonabelian Mal'cev algebra and let* γ *be its center. Let* $f : A^k \to A$ *be a function that satisfies* $f(\mathbf{x}) = f(\mathbf{y})$ *for all* $\mathbf{x}, \mathbf{y} \in A^k$ *with* $\mathbf{x} \equiv_\gamma \mathbf{y}$. *Then* $f \in \mathsf{Pol}_k\mathbf{A}$.

Proof: See [**3**, Lemma 3.2]. □

LEMMA 3.9. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra such that* $\mathsf{Con}\,\mathbf{A} = \{0, \alpha, 1\}$, $[1, 1] = 1$, $[1, \alpha] = 0$ *and let* $\theta \in A$. *Then there is a polynomial function* $e \in \mathsf{Pol}_1\mathbf{A}$ *such that* $e(A) \subseteq \theta/\alpha$ *and* $e(x) = x$ *for all* $x \in \theta/\alpha$.

Proof: Since $\mathsf{Con}\,\mathbf{A} = \{0, \alpha, 1\}$, $[1, 1] = 1$ and $[1, \alpha] = 0$, the algebra $\mathbf{A}$ is a finite central-by-simple-nonabelian Mal'cev algebra with center α. The statement now follows by Proposition 3.7. □

LEMMA 3.10. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra such that* $\mathsf{Con}\,\mathbf{A} = \{0, \alpha, 1\}$, $[1, 1] = 1$ *and* $[1, \alpha] = 0$. *Let* $f : A^k \to A$ *be a function that satisfies* $f(\mathbf{x}) = f(\mathbf{y})$ *for all* $\mathbf{x}, \mathbf{y} \in A^k$ *with* $\mathbf{x} \equiv_\alpha \mathbf{y}$. *Then* $f \in \mathsf{Pol}_k\mathbf{A}$.

Proof: Since $\mathsf{Con}\,\mathbf{A} = \{0, \alpha, 1\}$, $[1, 1] = 1$ and $[1, \alpha] = 0$, the algebra $\mathbf{A}$ is a finite central-by-simple-nonabelian Mal'cev algebra with center α. The statement now follows by Proposition 3.8. □

DEFINITION 3.11. Let $n \in \mathbb{N}$, let $\mathbf{A}$ be an algebra and let $\theta \in A$. For each $f : A^n \to A$ and $i \in \{1, \ldots, n\}$, we define a function $f_{i,\theta} : A \to A$ by

$$f_{i,\theta}(x) := f(\theta, \ldots, \theta, \overset{i\text{th}}{\overset{\downarrow}{x}}, \theta, \ldots, \theta)$$

for all $x \in A$.

LEMMA 3.12. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra, let* $\alpha \in \mathsf{Con}\,\mathbf{A}$ *such that* $[\alpha, 1] = 0$ *and let us assume that there is a* $\theta \in A$ *such that*

(1) *there is a unary polynomial* e *such that* $e|_{\theta/\alpha} = id_{\theta/\alpha}$ *and* $e(A) \subseteq \theta/\alpha$,
(2) *every function* $f : A^k \to \theta/\alpha$ *that is constant on every* α*-class is a polynomial.*

If $k \geq 0$ *and* $f : A^k \to A$ *is such that*

$$f \in \mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})),$$

and if, furthermore, there is a polynomial $p : A^k \to A$ *such that* $f(\mathbf{x}) \equiv_\alpha p(\mathbf{x})$ *for all* $\mathbf{x} \in A^k$, *then* f *is a polynomial.*

Proof: Let $k \geq 0$, let $f : A^k \to A$ be such that $f \in \mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A}))$, and let $p : A^k \to A$ be a polynomial such that $f(\mathbf{x}) \equiv_\alpha p(\mathbf{x})$, for all $\mathbf{x} \in A^k$. We define

$$\mathbf{B} := (A, \mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A}))).$$

To simplify the notation we introduce a unary polynomial u on $\mathbf{A}$ by

$$u(x) := m(x, e(x), \theta) \text{ for } x \in A, \tag{3.1}$$

and let

$$g(\mathbf{x}) := m(f(u(\mathbf{x}^{(1)}), \ldots, u(\mathbf{x}^{(k)})), p(u(\mathbf{x}^{(1)}), \ldots, u(\mathbf{x}^{(k)})), \theta). \tag{3.2}$$

First, we notice that $g \in \mathsf{Pol}\,\mathbf{B}$ and $g|_{\theta/\alpha} = m(f(\theta, \ldots, \theta), p(\theta, \ldots, \theta), \theta)$. Thus, the function g' defined by $g'(\mathbf{x}) := m(g(\mathbf{x}), g(\theta, \ldots, \theta), \theta)$ for all $\mathbf{x} \in A^k$ satisfies $g'|_{\theta/\alpha} = \theta$. Since $\mathsf{Inv}^4(A, \mathsf{Pol}\,\mathbf{A}) \subseteq \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})$, Lemma §1.7.5 tells that all functions from $\mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A}))$ are commutator preserving functions and we obtain $[1, \alpha]_\mathbf{B} = 0$. Therefore, by Lemma 3.6, g' is constant on each α-class. Since $u(x) \equiv_\alpha x$ we have

$$f(u(\mathbf{x}^{(1)}), \ldots, u(\mathbf{x}^{(k)})) \equiv_\alpha f(\mathbf{x}) \equiv_\alpha p(\mathbf{x}) \equiv_\alpha p(u(\mathbf{x}^{(1)}), \ldots, u(\mathbf{x}^{(k)})).$$

Now from (3.2), we obtain $g(A^k) \subseteq \theta/\alpha$. Using Lemma §1.3.5 we obtain $g(\mathbf{x}) = m(g'(\mathbf{x}), \theta, g(\theta, \ldots, \theta))$. Therefore g is constant on each α-class and thus, $g \in \mathsf{Pol}_k\mathbf{A}$, by condition (2). Furthermore,

$$f(u(\mathbf{x}^{(1)}), \ldots, u(\mathbf{x}^{(k)})) = m(g(\mathbf{x}), \theta, p(u(\mathbf{x}^{(1)}), \ldots, u(\mathbf{x}^{(k)})))$$

by Lemma §1.3.5 and thus we know that $f(u(\mathbf{x}^{(1)}), \ldots, u(\mathbf{x}^{(k)})) \in \mathsf{Pol}_k\mathbf{A}$. Since $e(x) \equiv_\alpha \theta$ and $[1, \alpha]_\mathbf{B} = 0$, by Lemma §1.3.4 we have

$$f(u(\mathbf{x}^{(1)}), \ldots, u(\mathbf{x}^{(k)})) = m(f(\mathbf{x}), f(e(\mathbf{x}^{(1)}), \ldots, e(\mathbf{x}^{(k)})), f(\theta, \ldots, \theta)).$$

Since $f(e(\mathbf{x}^{(1)}), \ldots, e(\mathbf{x}^{(k)})) \equiv_\alpha f(\theta, \ldots, \theta)$, by Lemma §1.3.5 we have that

$$f(\mathbf{x}) = m(f(u(\mathbf{x}^{(1)}), \ldots, u(\mathbf{x}^{(k)})), f(\theta, \ldots, \theta), f(e(\mathbf{x}^{(1)}), \ldots, e(\mathbf{x}^{(k)}))).$$

In order to finish the proof that f is a polynomial it remains to prove that $f(e(\mathbf{x}^{(1)}), \ldots, e(\mathbf{x}^{(k)}))$ is a polynomial of $\mathbf{A}$. We will accomplish this by showing that $f|_{\theta/\alpha}$ is a polynomial of $\mathbf{A}$. Since all constant operations lie in $\mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A}))$, we know that $\{f_{i,\theta} \,|\, 1 \leq i \leq k\}$ is a subset of $\mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A}))$. Since $\mathsf{Inv}^{|A|}(A, \mathsf{Pol}\,\mathbf{A}) \subseteq \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})$ we have that all unary functions from $\mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A}))$ are polynomials, by Lemma §1.7.4. Therefore $\{f_{i,\theta} \,|\, 1 \leq i \leq k\} \subseteq \mathsf{Pol}_1\mathbf{A}$. If $x_1, \ldots, x_k \in \theta/\alpha$ then we have

$$f(x_1, \ldots, x_k) = m(f(\theta, \ldots, \theta, x_k), f(\theta, \ldots, \theta), f(x_1, \ldots, x_{k-1}, \theta)) = \cdots =$$

$$m(f(\theta, \ldots, \theta, x_k), f(\theta, \ldots, \theta), m(\ldots m(f(\theta, x_2, \theta, \ldots, \theta), f(\theta, \ldots, \theta), f(x_1, \theta, \ldots, \theta)) \ldots))$$

by Lemma §1.3.4, because $[\alpha, \alpha]_\mathbf{B} \leq [\alpha, 1]_\mathbf{B} = 0$. Now, we have that $f|_{\theta/\alpha}$ is a polynomial. This completes the proof. □

LEMMA 3.13. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra such that* $\mathsf{Con}\,\mathbf{A} = \{0, \alpha, 1\}$ *and let* $k \in \mathbb{N}$. *Then for every* k*-ary function* $f \in \mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A}))$, *there exists a polynomial* $p \in \mathsf{Pol}_k\mathbf{A}$ *such that* $f(\mathbf{x}) \equiv_\alpha p(\mathbf{x})$ *for all* $\mathbf{x} \in A^k$.

Proof: Let f be a k-ary function from $\mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A}))$. It is clear that $\mathbf{A}/\alpha$ is simple. Define a function f' on $\mathbf{A}/\alpha$ by: $f'(\mathbf{x}/\alpha) := f(\mathbf{x})/\alpha$ for all $\mathbf{x} \in A^k$. Since $\mathsf{Con}\,\mathbf{A} \subseteq \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})$, f' is well defined. We will now show that f' lies in $\mathsf{Comp}(A/\alpha, \mathsf{Inv}^{max\{|A/\alpha|,4\}}(A/\alpha, \mathsf{Pol}(\mathbf{A}/\alpha)))$. To this end, let ρ be a t-ary relation in $\mathsf{Inv}^{max\{|A/\alpha|,4\}}(A/\alpha, \mathsf{Pol}(\mathbf{A}/\alpha))$. We define a t-ary relation σ on A by

$$\sigma := \{(a_1, \dots, a_t) \,|\, (a_1/\alpha, \dots, a_t/\alpha) \in \rho\}.$$

We have $\sigma \in \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})$. Hence, f preserves σ. Therefore, f' preserves ρ. Now, we have proved that $f' \in \mathsf{Comp}(A/\alpha, \mathsf{Inv}^{max\{|A/\alpha|,4\}}(A/\alpha, \mathsf{Pol}(\mathbf{A}/\alpha)))$. Then, $f' \in \mathsf{Pol}(\mathbf{A}/\alpha)$, by Proposition 3.3. Thus, there exists a $p \in \mathsf{Pol}\,\mathbf{A}$ such that $f'(\mathbf{x}/\alpha) = p(\mathbf{x})/\alpha$, for all $\mathbf{x} \in A^k$. Therefore we have $f(\mathbf{x})/\alpha = p(\mathbf{x})/\alpha$ or in other words $f(\mathbf{x}) \equiv_\alpha p(\mathbf{x})$, for all $\mathbf{x} \in A^k$. □

PROPOSITION 3.14. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra such that* $\mathsf{Con}\,\mathbf{A} = \{0, \alpha, 1\}$, $[1, 1] = 1$ *and* $[1, \alpha] = 0$. *Then,*

$$\mathsf{Pol}\,\mathbf{A} = \mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})).$$

Proof: Let us denote $\mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A}))$ by $\mathcal{C}$ and $\mathbf{B} = (A, \mathcal{C})$. Obviously, $\mathsf{Pol}\,\mathbf{A} \subseteq \mathcal{C}$. Now, take any k-ary function $f \in \mathcal{C}$ and let us show that $f \in \mathsf{Pol}_k\mathbf{A}$. There exists a polynomial $p \in \mathsf{Pol}_k\mathbf{A}$ such that $f(\mathbf{x}) \equiv_\alpha p(\mathbf{x})$, for all $\mathbf{x} \in A^k$, by Lemma 3.13. Let $\theta \in A$ be arbitrary. We know that there exists an $e \in \mathsf{Pol}_1\mathbf{A}$ such that $e(A) \subseteq \theta/\alpha$ and $e(x) = x$ for all $x \in \theta/\alpha$ by Lemma 3.9. Thus Condition (1) of Lemma 3.12 is satisfied. Condition (2) of Lemma 3.12 is satisfied by Lemma 3.10. Therefore, we obtain $f \in \mathsf{Pol}_k\mathbf{A}$ by Lemma 3.12. □

3.3. Nilpotent Algebras. In this section we analyse nilpotent Mal'cev algebras whose congruence lattice is a three element chain.

DEFINITION 3.15. Let $\mathbf{A}$ be an algebra, let $\alpha \in \mathsf{Con}\,\mathbf{A}$ and let $\theta \in A$. We say that α is *stable at* θ if there exists a unary polynomial p of $\mathbf{A}$ such that $p(\theta) = \theta, p(A) \subseteq \theta/\alpha$ and p is not constant on θ/α.

LEMMA 3.16. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra such that* $\mathsf{Con}\,\mathbf{A} = \{0, \alpha, 1\}$ *where* $[1, \alpha] = 0$ *and* $k \geq 1$. *Let* $\theta \in A$ *be such that* α *is not stable at* θ. *If* $p \in \mathsf{Pol}_k\mathbf{A}$ *is such that* $p(A^k) \subseteq \theta/\alpha$ *then* p *is constant on every* α*-class.*

Proof: Choose $\mathbf{x}, \mathbf{t} \in A^k$ so that $\mathbf{x} \equiv_\alpha \mathbf{t}$ and let $J = \{s \in \{1, \dots, k\} \,|\, \mathbf{x}^{(s)} \neq \mathbf{t}^{(s)}\}$. We will prove that $p(\mathbf{x}) = p(\mathbf{t})$ by induction on $|J|$. For $|J| = 0$ the statement is obvious. Suppose now that the statement is true for all J with $|J| = \ell$. Let us consider $|J| = \ell + 1$ and $j \in J$. By the assumptions we have $\mathbf{x}^{(j)} \equiv_\alpha \mathbf{t}^{(j)}$. In order to show that $p(\mathbf{x}) = p(\mathbf{t})$ we define a unary polynomial p' on A in the following way:

$$p'(x) := p(\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(j-1)}, x, \mathbf{x}^{(j+1)}, \ldots, \mathbf{x}^{(k)}).$$

It is clear that $p'(A) \subseteq \theta/\alpha$. Therefore, $p''(A) \subseteq \theta/\alpha$ where $p''(x) = m(p'(x), p'(\theta), \theta)$ and $p''(\theta) = \theta$. Then p'' equals θ on the whole of θ/α by the assumptions of the lemma. Thus, p'' is constant on each α-class by Lemma §1.3.6 since $[\alpha, 1] = 0$. Then we conclude that p' is also constant on each α-class, because $p'(x) = m(p''(x), \theta, p'(\theta))$, by the condition $[\alpha, 1] = 0$ and Lemma §1.3.5. This proves $p'(\mathbf{x}^{(j)}) = p'(\mathbf{t}^{(j)})$. Now using the induction hypothesis we obtain

$$p(\mathbf{x}) = p'(\mathbf{x}^{(j)}) = p'(\mathbf{t}^{(j)}) = p(\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(j-1)}, \mathbf{t}^{(j)}, \mathbf{x}^{(j+1)}, \ldots, \mathbf{x}^{(k)}) = p(\mathbf{t}).$$

□

LEMMA 3.17. *Let $\mathbf{A}$ be a finite Mal'cev algebra with a Mal'cev term m. Let α be an atom of $\mathsf{Con}\,\mathbf{A}$ such that $[\alpha, \alpha] = 0$ and let $\theta \in A$. Consider the following algebra*

$$\mathbf{R} = (\{p|_{\theta/\alpha} \mid p \in \mathsf{Pol}_1\mathbf{A}, p(\theta) = \theta\}, +, \circ),$$

where $(p+q)(x) := m\,(p(x), \theta, q(x))$ for every $x \in A$, and $\circ$ is the usual function composition. Then $\mathbf{R}$ is a primitive ring. Moreover, if α is stable at θ, then there exists a unary polynomial e such that $e|_{\theta/\alpha} = id_{\theta/\alpha}$ and $e(A) \subseteq \theta/\alpha$.

Proof: We will denote θ/α by U. As in the proof of Proposition §1.3.11 we have that $\mathbf{R} = (\{p|_U \mid p \in \mathsf{Pol}_1\mathbf{A}, p(\theta) = \theta\}, +, \circ)$ is a ring with unit id_U. Since $[\alpha, \alpha] = 0$, $\mathbf{A}|_U$ is polynomially equivalent to the module $(U, +)$ over the ring $\mathbf{R}$, where $u_1 + u_2 := m(u_1, \theta, u_2)$ for all $u_1, u_2 \in U$ as in the proof of Proposition §1.3.11. Since α is an atom of $\mathsf{Con}\mathbf{A}$, the module $(U, +)$ satisfies $Ru = U$ for every $u \neq \theta$. Therefore the module $(U, +)$ over the ring $\mathbf{R}$ is simple, and thus $\mathbf{R}$ is a primitive ring.

Let us now assume that α is stable at θ. Then the ideal

$$I = \{p|_U \mid p \in \mathsf{Pol}_1\mathbf{A}, p(\theta) = \theta, p(A) \subseteq \theta/\alpha\}$$

of $\mathbf{R}$ contains more than one element. Since $\mathbf{R}$ is finite, we know that $\mathbf{R}$ is simple by Proposition §1.2.5. Therefore $I = R$, and thus $\mathrm{id}_U \in I$. This yields a unary polynomial e such that $e|_U = id_U$ and $e(A) \subseteq U$. □

LEMMA 3.18. *Let $\mathbf{A}$ be a Mal'cev algebra such that α is the unique coatom in $\mathsf{Con}\,\mathbf{A}$, and let $\mathbf{u}, \mathbf{v} \in A^k$, $k \geq 1$. If $\mathbf{u} \not\equiv_\alpha \mathbf{v}$ then for every $a, b \in A$ there exists a $p \in \mathsf{Pol}_k\mathbf{A}$ such that $a = p(\mathbf{u})$ and $b = p(\mathbf{v})$.*

Proof: Since $\mathbf{u} \not\equiv_\alpha \mathbf{v}$ and α is the unique coatom in $\mathsf{Con}\,\mathbf{A}$ we have $\Theta_{\mathbf{A}}(\mathbf{u}, \mathbf{v}) = 1$. Also, we have $\Theta_{\mathbf{A}}(\mathbf{u}, \mathbf{v}) = \{(p(\mathbf{u}), p(\mathbf{v})) \mid p \in \mathsf{Pol}_k\mathbf{A}\}$, by Proposition §1.2.2. Thus, we obtain the statement using the fact that $(a, b) \in 1$. □

LEMMA 3.19. *Let $\mathbf{A}$ be a finite Mal'cev algebra such that $\mathsf{Con}\,\mathbf{A} = \{0, \alpha, 1\}$, $\alpha \neq 0, \alpha \neq 1$, let $\theta \in A$ and $k \in \mathbb{N}$. Assume that $[\underbrace{1, \ldots, 1}_{n}] = \alpha$ for all $n \geq 2$ and*

$[1,\alpha]=0$. *Then every function* $f: A^k \to \theta/\alpha$ *which is constant on all* α*-classes is a polynomial.*

Proof: Let $r := |A/\alpha|^k - 1$. Since $[\underbrace{1,\dots,1}_{r+1}] > 0$, we know by Proposition §2.4.15 that there exist a $c' \in \mathsf{Pol}_{r+1}\mathbf{A}$, and $\psi_1, \psi_2, a_0, \dots, a_r \in A$ with the property: c' is absorbing at $(a_0,\dots,a_r)$ with value ψ_1 and there exists a vector $(b_0,\dots,b_r) \in A^{r+1}$ such that $c'(b_0,\dots,b_r) = \psi_2 \neq \psi_1$.

We will now show that there is a $\psi' \in A$ with $(\psi',\theta) \in \alpha$ and $\psi' \neq \theta$. To show this, let $(x_0,x_1) \in \alpha$ with $x_0 \neq x_1$. Now $m(x_1,x_0,\theta) \in \theta/\alpha$. If $m(x_1,x_0,\theta)=\theta$, we have $x_1 = m(x_1,x_0,x_0) = m(m(x_1,x_0,x_0), m(x_0,x_0,x_0), m(\theta,\theta,x_0))$. Since $[\alpha,1]=0$, this is equal to $m(m(x_1,x_0,\theta),\theta,x_0) = m(\theta,\theta,x_0) = x_0$, a contradiction. Hence $m(x_1,x_0,\theta) \neq \theta$. Therefore $\psi' := m(x_1,x_0,\theta)$ satisfies $\psi' \in \theta/\alpha$ and $\psi' \neq \theta$.

Since $\psi_1 \neq \psi_2$, we have $\Theta_{\mathbf{A}}(\psi_1,\psi_2) \geq \alpha$. Therefore there exists a $p \in \mathsf{Pol}_1\mathbf{A}$ with $p(\psi_1)=\theta$ and $p(\psi_2)=\psi'$. We define $c \in \mathsf{Pol}_{r+1}\mathbf{A}$ by $c := p \circ c'$. We note that c is absorbing at $(a_0,\dots,a_r)$ with value θ, and therefore, from Lemma §2.4.9 and $[1,1]=\alpha$ we obtain that the range of c is contained in θ/α.

Now, choose $j \in \{0,\dots,r\}$. We fix $\psi \in A$ such that $(\psi,\theta) \in \alpha$ and prove that the function $f: A^k \to \theta/\alpha$ defined by

$$f(\mathbf{x}) = \begin{cases} \psi & \text{if } \mathbf{x} \in \mathbf{t}_j/\alpha, \\ \theta & \text{otherwise} \end{cases}$$

is a polynomial function. Since $(\psi,\theta) \in \alpha \leq \Theta_{\mathbf{A}}(\psi',\theta)$ there exists an $f_\psi \in \mathsf{Pol}_1\mathbf{A}$ such that $f_\psi(\psi')=\psi$ and $f_\psi(\theta)=\theta$. We denote by $\mathbf{t}_0,\dots,\mathbf{t}_r$ a transversal of A^k through the classes of α, where $\mathbf{t}_0 := (\theta,\dots,\theta)$. There are two cases to consider.

– **Case** α *is not stable at* θ: Let $i \in \{0,\dots,r\}$ with $i \neq j$. Then there is an $s \in \{1,\dots,k\}$ such that $\mathbf{t}_i^{(s)} \not\equiv_\alpha \mathbf{t}_j^{(s)}$. Therefore, there exists a $p_i \in \mathsf{Pol}_k\mathbf{A}$ such that $p_i(\mathbf{t}_i)=a_i$, and $p_i(\mathbf{t}_j)=b_i$. We define p_j to be the constant polynomial with value b_j. Now let

$$q(\mathbf{x}) := f_\psi(c(p_0(\mathbf{x}),\dots,p_r(\mathbf{x}))),$$

and note that $q(\mathbf{t}_i) = f_\psi(c(p_0(\mathbf{t}_i),\dots,p_{i-1}(\mathbf{t}_i),a_i,p_{i+1}(\mathbf{t}_i),\dots,p_r(\mathbf{t}_i))) = f_\psi(\theta) = \theta$ for every $i \in \{0,\dots,r\}\backslash\{j\}$, and $q(\mathbf{t}_j) = f_\psi(c(b_0,\dots,b_r)) = f_\psi(\psi') = \psi$. Since $c(A^{k+1}) \subseteq \theta/\alpha$, we have that $q(A^k) \subseteq \theta/\alpha$. By Lemma 3.16, q is constant on each α-class. This proves $f=q$.

– **Case** α *is stable at* θ: Then we have a unary polynomial e such that $e|_{\theta/\alpha} = id_{\theta/\alpha}$ and $e(A) \subseteq \theta/\alpha$, by Lemma 3.17. If $i \neq j$ then there exists an $s \in \{1,\dots,k\}$ such that

$$m(\mathbf{t}_i^{(s)}, e(\mathbf{t}_i^{(s)}),\theta) \equiv_\alpha \mathbf{t}_i^{(s)} \not\equiv_\alpha \mathbf{t}_j^{(s)} \equiv_\alpha m(\mathbf{t}_j^{(s)}, e(\mathbf{t}_j^{(s)}),\theta).$$

Let u be defined by $u(x) := m(x,e(x),\theta)$. Then, from Lemma 3.18, we obtain that for each $i \in \{0,\dots,r\}\backslash\{j\}$, there exists a $p_i \in \mathsf{Pol}_k\mathbf{A}$ such that

$p_i(u(\mathbf{t}_i^{(1)}), \ldots, u(\mathbf{t}_i^{(k)})) = a_i$ and $p_i(u(\mathbf{t}_j^{(1)}), \ldots, u(\mathbf{t}_j^{(k)})) = b_i$. The polynomial p_j is defined to be the constant polynomial with value b_j. We define

$$q(\mathbf{x}) := f_\psi(c\big(p_0\big(u(\mathbf{x}^{(1)}), \ldots, u(\mathbf{x}^{(k)})\big), \ldots, p_r\big(u(\mathbf{x}^{(1)}), \ldots, u(\mathbf{x}^{(k)})\big)\big))$$

and observe that $q(\mathbf{t}_j) = \psi$ and $q(\mathbf{t}_i) = \theta$, $i \in \{0, \ldots, r\} \backslash \{j\}$. Since $e|_{\theta/\alpha}(x) = x$, directly from the definition of q and u we obtain that $q'|_{\theta/\alpha} = \theta$, where $q'(\mathbf{x}) := m(q(\mathbf{x}), q(\mathbf{t}_0), \theta)$. By Lemma §1.3.6 and the assumption $[\alpha, 1] = 0$ we have that q' is constant on each α-class. By Lemma §1.3.5 we have $q(\mathbf{x}) = m(q'(\mathbf{x}), \theta, q(\mathbf{t}_0))$. Hence, q is constant on each α-class. Therefore, we have proved $f = q$.

Now, we will prove the statement for an arbitrary function $F : A^k \to \theta/\alpha$ that is constant on each α-class. Define $F_i : A^k \to \theta/\alpha$ as follows:

$$F_i(\mathbf{x}) = \begin{cases} F(\mathbf{t}_i) & \text{if } \mathbf{x} \in \mathbf{t}_i/\alpha, \\ \theta & \text{otherwise,} \end{cases}$$

for $i \in \{0, \ldots, r\}$. Since we know that F_i are polynomials for all $i \in \{0, \ldots, r\}$, we can construct a polynomial function $h : A^k \to \theta/\alpha$ in the following way:

$$h(\mathbf{x}) := m\underbrace{(\ldots m(}_{r} F_0(\mathbf{x}), \theta, F_1(\mathbf{x})), \theta, \ldots), \theta, F_r(\mathbf{x})).$$

Obviously, $F = h$. □

Proposition 3.20. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra such that* $\mathsf{Con}\,\mathbf{A} = \{0, \alpha, 1\}$, $[\underbrace{1, \ldots, 1}_{n}] = \alpha$ *for all* $n \geq 2$, *and* $[1, \alpha] = 0$. *Then,*

$$\mathsf{Pol}\,\mathbf{A} = \mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})).$$

Proof: Let us denote $\mathsf{Comp}(A, \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A}))$ by $\mathcal{C}$, and let $\mathbf{B} = (A, \mathcal{C})$. Clearly, we have $\mathsf{Pol}\,\mathbf{A} \subseteq \mathcal{C}$. Let f be a k-ary function in $\mathcal{C}$. We want to show that $f \in \mathsf{Pol}\,\mathbf{A}$. There exists a polynomial $p \in \mathsf{Pol}_k\mathbf{A}$ such that $f(\mathbf{x}) \equiv_\alpha p(\mathbf{x})$, for all $\mathbf{x} \in A^k$, by Lemma 3.13. Let $\theta \in A$. There are two possibilities.

– **Case** *α is not stable at θ*: Then, the function $g(\mathbf{x}) = m(f(\mathbf{x}), p(\mathbf{x}), \theta)$ has the property $g : A^k \to \theta/\alpha$, because $f(\mathbf{x}) \equiv_\alpha p(\mathbf{x})$, for all $\mathbf{x} \in A^k$. Now, by Lemma 3.16, g is constant on each α-class. We conclude that $g \in \mathsf{Pol}_k\mathbf{A}$, by Lemma 3.19. We also observe that $[1, \alpha]_\mathbf{B} = 0$ by Lemma §1.7.5, because $\mathsf{Inv}^4(A, \mathsf{Pol}\,\mathbf{A}) \subseteq \mathsf{Inv}^{max\{|A|,4\}}(A, \mathsf{Pol}\,\mathbf{A})$. By Lemma §1.3.5 using $[1, \alpha]_\mathbf{B} = 0$ we have $f(\mathbf{x}) = m(g(\mathbf{x}), \theta, p(\mathbf{x}))$, and thus we obtain that $f \in \mathsf{Pol}_k\mathbf{A}$.

– **Case** *α is stable at θ*: Then we have a unary polynomial e such that $e|_{\theta/\alpha} = id_{\theta/\alpha}$ and $e(A) \subseteq \theta/\alpha$ by Lemma 3.17. Thus, Condition (1) of Lemma 3.12 is satisfied and also, by Lemma 3.19, Condition (2) of Lemma 3.12 is satisfied. Thus $f \in \mathsf{Pol}_k\mathbf{A}$, by Lemma 3.12. □

PROPOSITION 3.21. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra. If there exists an* $n \geq 2$ *such that* $[\underbrace{1,\dots,1}_{n}] = 0$, *then*

$$\mathsf{Pol}\,\mathbf{A} = \mathsf{Comp}(A, \mathsf{Inv}^{|A|^n}(A, \mathsf{Pol}\,\mathbf{A})).$$

Proof: Denote $\mathsf{Comp}(A, \mathsf{Inv}^{|A|^n}(A, \mathsf{Pol}\,\mathbf{A}))$ by $\mathcal{C}$. We will show that $\mathcal{C} = \mathsf{Pol}\,\mathbf{A}$. We introduce a new algebra $\mathbf{B} = (A, \mathcal{C})$. Clearly, $\mathsf{Pol}_n\mathbf{A} \subseteq \mathsf{Pol}_n\mathbf{B}$. Let f be an n-ary function from $\mathcal{C}$. We know that $f \in \mathsf{Pol}_n\mathbf{A}$ by Lemma §1.7.4. Thus, $\mathsf{Pol}_n\mathbf{B} = \mathsf{Pol}_n\mathbf{A}$. Hence, $[\underbrace{1,\dots,1}_{n}]_{\mathbf{B}} = [\underbrace{1,\dots,1}_{n}]_{\mathbf{A}}$, by Lemma §2.4.10. Therefore, we know $[\underbrace{1,\dots,1}_{n}]_{\mathbf{B}} = 0$. Furthermore, $\mathsf{Pol}_n\mathbf{B} = \mathsf{Pol}_n\mathbf{A}$ clearly entails $\mathsf{Pol}_k\mathbf{B} = \mathsf{Pol}_k\mathbf{A}$, for every $k \in \{0,\dots,n-1\}$. From Proposition §2.4.17 we have $\mathcal{C} = \mathsf{Pol}\,\mathbf{B} = \mathrm{Clo}(\bigcup_{k=0}^{n-1} \mathsf{Pol}_k(\mathbf{B}) \cup \{m\}) = \mathrm{Clo}(\bigcup_{k=0}^{n-1} \mathsf{Pol}_k(\mathbf{A}) \cup \{m\}) = \mathsf{Pol}\,\mathbf{A}$. □

3.4. The Main Result About the Number of Mal'cev Clones.

THEOREM 3.22. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra whose congruence lattice is of height at most two. Then there is a finite set of relations* R *on* A *such that* $\mathsf{Pol}\,\mathbf{A} = \mathsf{Comp}(A, R)$.

Proof: For simple algebras the statement follows from Proposition 3.3. If $\mathsf{Con}\,\mathbf{A} \cong \mathbf{M}_i$, $i \geq 3$, then the statement follows from Corollary 3.2. If $\mathsf{Con}\,\mathbf{A} \cong \mathbf{M}_2$ then the statement follows from Proposition 3.5. Now let $\mathsf{Con}\,\mathbf{A}$ be isomorphic to the three-element chain $\{0, \alpha, 1\}$. In case of $[1,1] = 0$ the statement follows directly from Proposition 3.1. If $[1,1] > 0$ the following cases are possible:

– **Case** $[1,1] = [1,\alpha] = \alpha$: In this case we have $(0 : \alpha)_{\mathbf{A}} \leq \alpha$ and the statement follows from Proposition 3.6.

– **Case** $[1,1] = \alpha$ *and* $[1,\alpha] = 0$: Since $[1,\dots,1] \leq [1,1] = \alpha$, by (HC3) we have the following two possibilities.

(i) There exists an $n \in \mathbb{N}$ such that $[\underbrace{1,\dots,1}_{n}] = 0$: Then the statement follows from Proposition 3.21.

(ii) $[\underbrace{1,\dots,1}_{r}] = \alpha$, for all $r \geq 2$: The statement follows from Proposition 3.20.

– **Case** $[1,1] = 1$ *and* $[1,\alpha] = \alpha$: As in the first case we have $(0 : \alpha)_{\mathbf{A}} \leq \alpha$ and the statement follows from Proposition 3.6.

– **Case** $[1,1] = 1$ *and* $[1,\alpha] = 0$: Then the statement follows from Proposition 3.14. □

Bibliography

[1] I. Ágoston, J. Demetrovics and L. Hannák, *On the number of clones containing all constants (a problem of R. McKenzie)*, in: Lectures in Universal Algebra (Szeged, 1983), Volume **43** of Colloq. Math. Soc. János Bolyai, North-Holland (Amsterdam, 1986), pp. 21–25.

[2] E. Aichinger, *On Hagemann's and Herrmann's characterization of strictly affine complete algebras*, Algebra Universalis, **44** (2000), no. 1-2, 105–121.

[3] E. Aichinger, *The polynomial functions of certain algebras that are simple modulo their center*, Contr. Gen. Alg. **17** (2006), 9–24.

[4] E. Aichinger, J. Ecker, *Every (k+1)-affine complete nilpotent group of class k is affine complete*, International Journal of Algebra and Computation, **16** (2006), no. 2, 259–274.

[5] E. Aichinger, P. M. Idziak, *Polynomial interpolation in expanded groups*, J. Algebra **271** (2004), no. 1, 65–107.

[6] E. Aichinger, P. Mayr, *Polynomial clones on groups of order pq*, Acta Math. Hungar., **114** (2007) no. 3, 267–285.

[7] E. Aichinger, N. Mudrinski, *Polynomial clones of Mal'cev algebras with small congruence lattices*, to appear in Acta Mathematica Hungarica

[8] E. Aichinger, N. Mudrinski, *Types of polynomial completeness in expanded groups*, Algebra Universalis, **60** (2009), 309–343.

[9] A. Bulatov, *On the number of finite Mal'tsev algebras*, Contr. Gen. Alg. **13**, Proceedings of the Dresden Conference 2000 (AAA 60) and the Summer School 1999, Verlag Johannes Heyn, Klagenfurt 2001, 41–54.

[10] A. Bulatov, *Polynomial clones containing the Mal'tsev operation of the groups* $\mathbb{Z}_{p^2}$ *and* $\mathbb{Z}_p \times \mathbb{Z}_p$, Mult.-Valued Log. **8** (2002), no. 2, 193–221.

[11] A. A. Bulatov and P. M. Idziak, *Counting Mal'tsev clones on small sets*, Discrete Math. **268** (2003), no. 1-3, 59–80.

[12] S. Burris and J. Lawrence, *The equivalence problem for finite rings*, J. Symbolic Comput. **15** (1993), no. 1, 67–71.

[13] S. Burris, H. P. Sankappanavar, *A Course in Universal Algebra*, Graduate Texts in Mathematics, Springer Verlag, 1981

[14] R. Freese, R. McKenzie, *Commutator Theory for Congruence Modular Varieties*, Cambridge University Press, Cambridge, 1987

[15] M. Goldmann and A. Russell, *The complexity of solving equations over finite groups*, Inform. and Comput. **178** (2002), no. 1, 253–262.

[16] G. Grätzer, *General lattice theory*, second ed., Birkhäuser Verlag, Basel, 1998, New appendices by the author with B. A. Davey, R. Freese, B. Ganter, M. Greferath, P. Jipsen, H. A. Priestley, H. Rose, E. T. Schmidt, S. E. Schmidt, F. Wehrung and R. Wille.

[17] J. Hagemann and C. Herrmann, *A concrete ideal multiplication for algebraic systems and its relations to congruence distributivity*, Arch. Math. (Basel) **32** (1979), 234–245.

[18] J. Hagemann and C. Herrmann, *Arithmetical locally equational classes and representation of partial functions*, Universal Algebra, Esztergom (Hungary), vol. 29, Colloq. Math. Soc. János Bolyai, 1982, pp. 345–360.

[19] D. Hobby, R. McKenzie, *The Structure of Finite Algebras*, Contemporary Mathematics, **76**, American Mathematical Society, Providence, Rhode Island, 1988

[20] H. B. Hunt, III and R. E. Stearns, *The complexity of equivalence for commutative rings*, J. Symbolic Comput. **10** (1990), no. 5, 411–436.

[21] P. M. Idziak, *Clones containing Mal'cev operations*, Internat. J. Algebra Comput. **9** (1999), 213–226.

[22] P. M. Idziak and K. Słomczyńska, *Polynomially rich algebras*, J. Pure Appl. Algebra **156** (2001), no. 1, 33–68.

[23] K. Kaarli, *Compatible function extension property*, Algebra Universalis **17** (1983), 200–207.

[24] K. Kaarli and A. F. Pixley, *Polynomial completeness in algebraic systems*, Chapman & Hall / CRC, Boca Raton, Florida, 2001.

[25] K. A. Kearnes, *Congruence modular varieties with small free spectra*, Algebra Universalis **42** (1999), no. 3, 165–181.

[26] E. W. Kiss, *Three remarks on the modular commutator*, Algebra Universalis **29** (1992), no. 4, 455–476.

[27] P. Mayr, *Polynomial clones on squarefree groups*, Internat. J. Algebra Comput. **18** (2008), no. 4, 759–777.

[28] J. D. P. Meldrum, *Near-rings and their links with groups*, Pitman (Advanced Publishing Program), Boston, Mass., 1985.

[29] R. N. McKenzie, G. F. McNulty, W. F. Taylor, *Algebras, Lattices, Varieties, Volume I*, Wadsworth & Brooks/Cole Advanced Books & Software Monterey, California, 1987

[30] W. Nöbauer, *Über die affin vollständigen, endlich erzeugbaren Moduln*, Monatshefte für Mathematik **82** (1976), 187–198.

[31] G. F. Pilz, *Near-rings*, 2nd ed., North-Holland Publishing Company – Amsterdam, New York, Oxford, 1983.

[32] R. Pöschel, L. Kalužnin, *Funktionen und Relationen-Algebren*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1979

[33] A. Saks, *Affine completeness of modules*, Tartu Riikl. Ül. Toimetised 700, University of Tartu, Estonia, 1985.

[34] S. D. Scott, *The structure of Ω-groups*, Near-rings, nearfields and K-loops (Hamburg, 1995), Kluwer Acad. Publ., Dordrecht, 1997, pp. 47–137.

[35] J.D.H. Smith, *Mal'cev varieties*, Lecture Notes in Math., vol. 554, Springer Verlag Berlin, 1976.

[36] B. L. van der Waerden, *Algebra, Volume II*, Springer-Verlag, New York, 1991.

Sažetak na srpskom jeziku

1. Motivacija

U ovoj disertaciji izučavaju se polinomi na konačnim Maljcevljevim algebrama. Maljcevljeve algebre su specijalna klasa univerzalnih algebri koja sadrži mnoge poznate klase algebri kao što su grupe i prsteni.

Za unapred zadatu algebru nije lako okarakterisati funkcije koje su polinomi na jeziku te algebre. Postoji čitava lista osobina koje zadovoljavaju polinomi kao što su očuvavanje kongruencija i komutatora, na primer. U [**22**] postavljen je sledeći problem: Za dati skup osobina, opisati sve algebre u kojima svaka funkcija koja zadovoljava sve date osobine jeste polinom. U takve probleme spada i karakterizacija *afino kompletnih* algebri. Algebra se naziva afino kompletna ako je svaka funkcija koja očuvava sve njene kongruencije polinom (videti [**24**]). Mi ćemo se baviti ovim konceptom u algebrama koje imaju grupni redukt (Ω-grupe) i koje su stoga svakako Maljcevljeve algebre.

Određivanje potrebnih i dovoljnih uslova koje treba da zadovoljava neka zadata algebra da bi bila afino kompletna je kompleksan problem. Do sada je ovaj problem rešen samo za konačne Abelove grupe ([**30**]) i neke podvarijetete varijeteta Abelovih grupa. Stoga je interesantno pitanje da li je osobina afine kompletnosti *odlučiva*. Za neku osobinu algebre kažemo da je odlučiva ako postoji efektivan algoritam koji za unapred datu algebru na ulazu daje na izlazu odgovor na pitanje da li je ulazna algebra afino kompletna. Za konačne nilpotentne grupe u [**12**] je dokazano da postoji algoritam koji odlučuje o afinoj kompletnosti. U ovoj disertaciji dajemo jedno uopštenje ovog rezultata, odnosno dajemo odgovor na pitanje odlučivosti afine kompletnosti za jednu širu potklasu Maljcevljevih algebri.

Drugi aspekt izučavanja polinoma inspirisan je sledećom činjenicom. Kompozicijom fundamentalnih operacija neke konačne Maljcevljeve algebre na različite načine može se dobiti isti polinom. Problem je odrediti da li takve unapred date kompozicije operacija određuju isti polinom. Ovaj problem je poznat pod imenom *problem polinomijalne ekvivalentnosti.* U slučaju nilpotentnih grupa i prstena pokazano je u [**15, 12**] da se u polinomnom vremenu može utvrditi da li dva unapred zadata polinomijalna terma indukuju isti polinom. U ovoj disertaciji dajemo isti rezultat za širu klasu algebri.

Treći problem kojim se bavimo u ovoj disertaciji je sledeći. Koliko različitih skupova polinoma, zatvorenih za kompoziciju i koji sadrže konstante i projekcije, se može dobiti menjajući skup fundamentalnih operacija konačne Maljcevljeve algebre? Takav skup funkcija se naziva *polinomijalni (ili konstantivni) Maljcevljev klon*. Zato nas ovde zanima koliko ima međusobno neekvivalentnih polinomijalnih Maljcevljevih klonova na konačnom skupu. U [**21**] je pokazano da postoji beskonačno mnogo takvih klonova ako je posmatrani skup najmanje četvoroelementni. U slučaju specijalnih podklasa Maljcevljevih algebri kao što su ciklične grupe poznato je sledeće. Ako je ciklična grupa prostog reda onda postoje tačno dva konstativna klona koji sadrže ternarnu funkciju $(x, y, z) \to x-y+z$. E. Aichinger i P. Mayr su u [**6**] pokazali da ako su p i q različiti prosti brojevi onda postoji tačno 17 različitih polinomijalnih klonova na cikličnoj grupi reda pq. Za slučaj direktnog proizvoda dve ciklične grupe istog prostog reda i cikličnu grupu čiji je red kvadrat prostog broja u [**10**] je pokazano da postoji prebrojivo mnogo polinomijalnih Maljcevljevih klonova koji sadrže odgovarajuću grupnu operaciju. Nije poznato da li postoji konačan skup A sa neprebrojivo mnogo polinomijalnih Maljcevljevih klonova na A.

2. Osnovni pojmovi i definicije

U disertaciji se pozivamo na notaciju i pojmove (univerzalne algebre, homomorfizmi, izomorfizmi, podalgebre, kongruencije, direktni i podirektni proizvodi i varijeteti) koji se pretežno uvode u [**13, 29**]. Radi bolje preciznosti u formulisanju glavnih rezultata navodimo definicije nekih pojmova kao i njihova osnovna svojstva.

Pre svega, polinomom neke algebre $\mathbf{A}$ nazivamo polinomijalnu funkciju koja je indukovana odgovarajućim polinomijalnim termom na jeziku uočene algebre $\mathbf{A}$. Skup svih polinoma neke algebre $\mathbf{A}$ označavaćemo sa $\mathsf{Pol}\,\mathbf{A}$. Za dve algebre $\mathbf{A}$ i $\mathbf{B}$ (sa različitim skupovima fundamentalnih operacija) kažemo da su *polinomijalno ekvivalentne* ako imaju isti skup polinoma.

Ternarnu operaciju m na skupu A zovemo Maljcevljevom operacijom ako za sve $x, y \in A$ važi:

$$m(x, x, y) = y = m(y, x, x).$$

Algebru $\mathbf{A}$ zovemo Maljcevljeva algebra ako ima Maljcevljevu term operaciju.

Proširena grupa (Ω-grupa) je algebra koja ima grupni redukt, odnosno među svojim fundamentalnim operacijama ima grupnu operaciju. U takve algebre spadaju svakako prsteni i moduli, ali i skoro-prsteni. Skoro-prsten (engl. *nearring*, vidi [**31**]) je algebra $\mathbf{R} = (R, +, \cdot)$ takva da je $(R, +)$ (ne obavezno Abelova) grupa, a $(R, \cdot)$ polugrupa sa jedinicom i za sve $x, y, z \in R$ važi:

$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

Glavni primer ovakve strukture, koji se i u disertaciji intenzivno koristi je skup svih unarnih polinoma p neke Ω-grupe $\mathbf{V}$ za koje važi $p(0) = 0$, gde je sa 0 označen neutralni element odgovarajuće grupne operacije u $\mathbf{V}$, sabiranje polinoma definisano je po tačkama, a množenje kao kompozicija funkcija. Slično kao u slučaju prstena definiše se *skoro-prstenski modul* (*near-ring module*) kao struktura $\mathbf{M} = (M, +, -, 0, \{f_r : M \to M \mid r \in R\})$ u kojoj je $(M, +, -, 0)$ grupa i za sve $x \in M$ i $r, s \in R$ važi:

(1) $f_{r \circ s}(x) = f_r(f_s(x))$;
(2) $f_{r+s}(x) = f_r(x) + f_s(x)$.

Za funkciju $f : A^k \to A$, gde je $\mathbf{A}$ neka algebra i $k \in \mathbb{N}_0$ kažemo da *očuvava kongruencije* ako za svaku kongruenciju α algebre $\mathbf{A}$ i sve vektore $\mathbf{a}, \mathbf{b} \in A^k$ kojima su odgovarajuće komponente u istoj klasi kongruencije α (što pišemo $\mathbf{a} \equiv_\alpha \mathbf{b}$) važi $f(\mathbf{a}) \equiv_\alpha f(\mathbf{b})$. Ako je za neko $k \in \mathbb{N}$, svaka k-arna funkcija na A koja očuvava sve kongruencije algebre $\mathbf{A}$ polinom, kažemo da je $\mathbf{A}$ *k-afino kompletna*. Algebra je afino kompletna ako je k-afino kompletna za sve $k \in \mathbb{N}$.

U Maljceveljevim algebrama koristi se sledeća karakterizacija kongruencije $\Theta_{\mathbf{A}}(\mathbf{a}, \mathbf{b})$ generisane dvama vektorima $\mathbf{a}$ i $\mathbf{b}$:

Propozicija §1.2.2 *Neka je $k \geq 1$ i $\mathbf{A}$ Maljcevljeva algebra. Ako $\mathbf{a}, \mathbf{b} \in A^k$, onda*

$$\Theta_{\mathbf{A}}(\mathbf{a}, \mathbf{b}) = \{(p(\mathbf{a}), p(\mathbf{b})) \mid p \in \mathsf{Pol}_k \mathbf{A}\}.$$

Komutatori predstavljaju ključno tehničko sredstvo za dobijanje glavnih rezultata ove disertacije. Njihove definicije i osnovne osobine koje ovde navodimo mogu se naći u [**19, 29**].

Definicija §1.3.1 Neka su α, β, η kongruencije algebre $\mathbf{A}$. Kažemo da α *centralizuje β modulo η*, i pišemo

$$C(\alpha, \beta; \eta),$$

ako za sve $n \geq 1$ i sve $p \in \mathsf{Pol}_{n+1}\mathbf{A}$, $a, b \in A$ takve da $a \equiv_\alpha b$ i $\mathbf{c}, \mathbf{d} \in A^n$ takve da $\mathbf{c} \equiv_\beta \mathbf{d}$ imamo

$$p(a, \mathbf{c}) \equiv_\eta p(a, \mathbf{d}) \text{ povlači } p(b, \mathbf{c}) \equiv_\eta p(b, \mathbf{d}).$$

Definicija §1.3.2 Neka je $\mathbf{A}$ neka algebra. Za kongruencije α i β algebre $\mathbf{A}$ definišemo *komutator*, u oznaci $[\alpha, \beta]$, kao najmanju kongruenciju η algebre $\mathbf{A}$ za koju važi da α centralizuje β modulo η. *Centralizator* kongruencije β *modulo* α, u oznaci $(\alpha : \beta)_{\mathbf{A}}$, je najveća kongruencija γ takva da γ centralizuje β modulo α.

Može se pokazati da u modulima važi $[1, 1] = 0$. Takve algebre nazivamo *Abelovim*.

Neka su α, β i η kongruencije algebre $\mathbf{A}$. Sledeće osobine slede direktno iz definicije centralizatora i komutatora:

(BC1) $[\alpha, \beta] \leq \alpha \wedge \beta$;
(BC2) za sve kongruencije γ, δ algebre $\mathbf{A}$ takve da $\alpha \leq \gamma, \beta \leq \delta$, imamo

$$[\alpha, \beta] \leq [\gamma, \delta];$$

U [**3**, Proposition 2.4, Proposition 2.5] je dokazano da ako $\mathbf{A}$ generiše kongruencijski permutabilan varijetet, onda važi:

(BC4) $[\alpha, \beta] = [\beta, \alpha]$;
(BC5) $[\alpha, \beta] \leq \eta$ ako i samo ako $C(\alpha, \beta; \eta)$;
(BC6) Ako $\eta \leq \alpha, \beta$, onda u $\mathbf{A}/\eta$, imamo $[\alpha/\eta, \beta/\eta] = ([\alpha, \beta] \vee \eta)/\eta$;
(BC7) Ako je $I \neq \emptyset$ i $\{\rho_i \,|\, i \in I\} \subseteq \mathsf{Con}\,\mathbf{A}$, onda: $\bigvee_{i \in I}[\alpha, \rho_i] = [\alpha, \bigvee_{i \in I} \rho_i]$ i slično $\bigvee_{i \in I}[\rho_i, \beta] = [\bigvee_{i \in I} \rho_i, \beta]$.

Osobine (BC4), (BC5), (BC6) i (BC7) su zapravo posledice resultata (HC4), (HC5), (HC6) i (HC7), redom, dobijenih u delu 2 ove disertacije.

Definicija §1.3.13(vidi [**14**]) Neka je $\mathbf{A}$ algebra. Kažemo da je $\mathbf{A}$ *nilpotentna* u k koraka ili *nilpotentna klase* k ako važi:

$$[\underbrace{1, \ldots, [1}_{k}, 1]] = 0.$$

Kažemo da je $\mathbf{A}$ *nilpotentna* ako je nilpotentna klase k za neko $k \in \mathbb{N}$.

Jasno, algebra koja je nilpotentna u jednom koraku je Abelova.

U disertaciji koristimo i osnove teorije pitomih kongruencija (Tame Congruence Theory), [**19**]. Ovde se parovima kongruencija koje čine prost interval u mreži kongruencija neke konačne algebre dodeljuje takozvani tip (broj) u zavisnosti od lokalnog ponašanja indukovane polinomijalne strukture. Teorija je zasnovana na teoremi P.P.Pálfy [**19**, Theorem 4.7] prema kojoj postoji samo pet polinomijalno neekvivalentnih indukovanih lokalnih struktura. Interesantno je da su u slučaju Maljcevljevih algebri zastupljeni samo tipovi 2 i 3 (Teorema §.1.5.13). Šta više tip zavisi od binarnog komutatora na sledeći način. Ako su α i β dve kongruencije konačne Maljcevljeve algebre $\mathbf{A}$ takve da je interval $[\alpha, \beta]$ prost (β "pokriva" α u mreži kongruencija algebre $\mathbf{A}$) onda je tip tog intervala 2 ako važi $[\beta, \beta] \leq \alpha$, inače je tip 3.

3. Viši komutatori

Mnoge osobine univerzalnih algebri se mogu videti iz mreže kongruencija i binarnog komutatora. Međutim, već u kongruencijski permutabilnom varijetetu (Maljcevljevim algebrama) algebra nije do na polinomijalnu ekvivalenciju određena svojim unarnim polinomima, kongruencijama i komutatorom na tim kongruencijama. U [**9**] A. Bulatov je uopštio binarni komutator uvođenjem

n-arnog komutatora za sve $n \in \mathbb{N}$ i time omogućio bolje razlikovanje polinomijalno neekvivalentnih algebri. U ovoj disertaciji n-arni komutatori predstavljaju moćno sredstvo pomoću koga su dobijeni ključni rezulati (Teorema §3.1.18, Teorema §3.2.3 i Teorema §3.3.22). Stoga je kompletna druga glava posvećena višim komutatorima i njihovim osobinama. To predstavlja takođe jedan od glavnih originalnih doprinosa ove disertacije jer je A. Bulatov koristio samo osnovne osobine. Iako tvrđenja o višim komutatorima izgledaju prirodno, dokazi zahtevaju uvođenje nove tehnike kao što je *operator razlike* (Difference operator). Kao i u slučaju binarnog komutatora vi ši komutator se definiše pomoću relacije n-arne centralizacije.

Definicija §2.1.1 (vidi [**9**]) Neka je $\mathbf{A}$ neka algebra, neka je $n \in \mathbb{N}$ i $\alpha_1, \ldots, \alpha_n, \beta, \delta$ kongruencije algebre $\mathbf{A}$. Kažemo da $\alpha_1, \ldots, \alpha_n$ *centralizuju* β *modulo* δ ako za sve polinome $f(\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{y})$ i vektore $\mathbf{a}_1, \mathbf{b}_1, \ldots, \mathbf{a}_n, \mathbf{b}_n, \mathbf{c}, \mathbf{d}$ iz $\mathbf{A}$ koji zadovoljavaju:

(1) $\mathbf{a}_i \equiv_{\alpha_i} \mathbf{b}_i$ za sve $i \in \{1, 2, \ldots, n\}$,
(2) $\mathbf{c} \equiv_\beta \mathbf{d}$ i
(3) $f(\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{c}) \equiv_\delta f(\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{d})$ za sve $(\mathbf{x}_1, \ldots, \mathbf{x}_n) \in \{\mathbf{a}_1, \mathbf{b}_1\} \times \cdots \times \{\mathbf{a}_n, \mathbf{b}_n\} \backslash \{(\mathbf{b}_1, \ldots, \mathbf{b}_n)\}$

važi:

$$f(\mathbf{b}_1, \ldots, \mathbf{b}_n, \mathbf{c}) \equiv_\delta f(\mathbf{b}_1, \ldots, \mathbf{b}_n, \mathbf{d}).$$

Ovo kraće zapisujemo kao $C(\alpha_1, \ldots, \alpha_n, \beta; \delta)$.

Definicija §2.1.2(vidi [**9**]) Neka je $\mathbf{A}$ neka algebra, $n \geq 2$ i neka su $\alpha_1, \ldots, \alpha_n$ kongruencije algebre $\mathbf{A}$. Najmanja kongruencija δ takva da važi $C(\alpha_1, \ldots \ldots, \alpha_{n-1}, \alpha_n; \delta)$ naziva se *(n-arni) komutator* kongruencija $\alpha_1, \ldots, \alpha_n$. Tu kongruenciju označavamo sa $[\alpha_1, \ldots, \alpha_n]$.

Uočimo da za $n = 1$ u definiciji §2.1.1 dobijamo definiciju (binarne) relacije centralizacije koja se koristi u [**14**]. Za $n = 2$, definicija §2.1.2 daje binarni komutator ([**29**, Definition 4.150]).

Propozicija §2.6.1(vidi [**9**, Proposition 1]) *Neka je $k \geq 1$ i neka su $\alpha_0, \ldots, \alpha_k$ kongruencije algebre* $\mathbf{A}$. *Tada važi:*

(HC1) $[\alpha_0, \ldots, \alpha_k] \leq \bigwedge_{0 \leq i \leq k} \alpha_i$;
(HC2) *za sve* $\beta_0, \ldots, \beta_k \in \mathsf{Con}\,\mathbf{A}$ *takve da je* $\alpha_0 \leq \beta_0, \ldots, \alpha_k \leq \beta_k$, *imamo*

$$[\alpha_0, \ldots, \alpha_k] \leq [\beta_0, \ldots, \beta_k];$$

(HC3) $[\alpha_0, \ldots, \alpha_k] \leq [\alpha_1, \ldots, \alpha_k]$.

Neka je $k \geq 1$ i neka su $\alpha_0, \ldots, \alpha_k, \eta$ kongruencije algebre $\mathbf{A}$ koje generišu kongruencijski permutabilan varijetet. Onda imamo:

(HC4) $[\alpha_0, \ldots, \alpha_k] = [\alpha_{\pi(0)}, \ldots, \alpha_{\pi(k)}]$ za sve permutacije π na skupu $\{0, \ldots, k\}$;
(HC5) $[\alpha_0, \ldots, \alpha_k] \leq \eta$ ako i samo ako $C(\alpha_0, \ldots, \alpha_k; \eta)$;

(HC6) Ako $\eta \leq \alpha_0, \ldots, \alpha_k$, onda u $\mathbf{A}/\eta$ važi:
$[\alpha_0/\eta, \ldots, \alpha_k/\eta] = ([\alpha_0, \ldots, \alpha_k] \vee \eta)/\eta$;

(HC7) Ako je I neprazan skup, $j \in \{0, \ldots, k\}$ i $\{\rho_i \mid i \in I\} \subseteq \mathsf{Con}\,\mathbf{A}$ onda:
$\bigvee_{i \in I}[\alpha_0, \ldots, \alpha_{j-1}, \rho_i, \alpha_{j+1}, \ldots, \alpha_k] = [\alpha_0, \ldots, \alpha_{j-1}, \bigvee_{i \in I} \rho_i, \alpha_{j+1}, \ldots, \alpha_k]$;

(HC8) $[\alpha_0, [\alpha_1, \ldots, \alpha_k]] \leq [\alpha_0, \alpha_1, \ldots, \alpha_k]$, ali i opštije:
$[\alpha_0, \ldots, \alpha_{i-1}, [\alpha_i, \ldots, \alpha_k]] \leq [\alpha_0, \ldots, \alpha_k]$ za sve $i \in \{1, \ldots, k\}$.

Viši komutator na kongruencijama neke algebre nije određen binarnim komutatorom. Primer se može naći u Ω-grupi ciklične grupe $(\mathbb{Z}_4, +)$, [**10**]. Za $n \geq 2$, neka je $\mathbf{A}_n$ algebra $(\mathbb{Z}_4, +, f_n)$, gde je f_n n-arna operacija definisana sa $f_n(x_1, \ldots, x_n) := 2x_1 \cdots x_n$. $\mathbf{A}_n$ ima tačno tri kongruencije; označimo ih sa 0, α i 1. Tada iz Leme 2.4 u [**6**], možemo lako dobiti da za $n \geq 2$, $\mathbf{A}_n$ zadovoljava $[1, 1] = \alpha$ i $[1, \alpha] = 0$. Dalje, u $\mathbf{A}_2$ imamo $[1, 1, 1] = 0$, ali u $\mathbf{A}_3$, imamo $[1, 1, 1] = \alpha$. Dakle, $[1, 1, 1]_{\mathbf{A}_3} = \alpha \neq 0 = [1, [1, 1]]_{\mathbf{A}_3}$. Generalno za $k \geq 2$ i $n \geq 2$, se može dobiti $[1, [1, 1]]_{\mathbf{A}_n} = 0$, $[\underbrace{1, \ldots, 1}_{k}]_{\mathbf{A}_n} = \alpha$ ako je $k \leq n$ i $[\underbrace{1, \ldots, 1}_{k}]_{\mathbf{A}_n} = 0$ ako je $k > n$. Odatle je $[\underbrace{1, \ldots, [1}_{k}, 1]]_{\mathbf{A}_n} = 0 \neq \alpha = [\underbrace{1, \ldots, 1}_{k}]_{\mathbf{A}_n}$, za $k \leq n$.

Viši komutatori za Ω-grupe opisani su u posledici §2.4.11. Naime, u slučaju Ω-grupa govorimo o komutator idealima, jer se mreži kongruencija obostrano jednoznačno pridružuje mreža ideala i to pridruživanje je izomorfizam. Međutim ne samo da se očuvavaju mrežne operacije nego i viši komutatori. Komutator ideal dužine k je ideal generisan skupom vrednosti svih polinoma koji se anuliraju kad god je jednom od argumenata pridružena 0 posmatrane Ω-grupe. Ovakvi polinomi igraju važnu ulogu uopšte u svim Maljcevljevim algebrama kada radimo sa komutatorima.

Definicija §2.2.9 Neka je $\mathbf{A}$ neka algebra, $k \in \mathbb{N}$, neka je dato preslikavanje $p : A^k \to A$, $(a_0, \ldots, a_{k-1}) \in A^k$, i neka $\theta \in A$. Tada za p kažemo da se *apsorbuje u* $(a_0, \ldots, a_{k-1})$ *sa vrednošću* θ ako za sve $(x_0, \ldots, x_{k-1}) \in A^k$ važi: ako postoji $i \in \{0, 1, \ldots, k-1\}$ tako da je $x_i = a_i$, onda $p(x_0, \ldots, x_{k-1}) = \theta$. Primetimo, $p(a_0, \ldots, a_{k-1}) = \theta$.

Koristeći apsorbujuće polinome dobijamo drugačiju karakterizaciju viših komutatora. Iz sledeće karakterizacije odmah sledi da polinomijalno ekvivalentne algebre imaju iste više komutatore (Posledica §2.4.10).

Lema §2.4.9 *Neka je* $\mathbf{A}$ *Maljcevljeva algebra sa Maljcevljevim termom* m, $\alpha_0, \ldots, \alpha_n$ *kongruencije od* $\mathbf{A}$ *i* $n \geq 0$. *Tada je* $[\alpha_0, \ldots, \alpha_n]$ *kongruencija generisana sa*

$$R = \{(c(b_0, \ldots, b_n), c(a_0, \ldots, a_n)) \mid b_0, \ldots, b_n, a_0 \ldots, a_n \in A,\ \forall i : a_i \equiv_{\alpha_i} b_i, \quad c \in \mathsf{Pol}_{n+1}\mathbf{A} \text{ i } c \text{ se apsorbuje u } (a_0, \ldots, a_n)\}. \tag{3.1}$$

Apsorbujući polinomi daju takođe i kriterijum kada se viši komutator anulira.

Propozicija §2.4.15 *Neka je* $\mathbf{A}$ *Maljcevljeva algebra sa Maljcevljevim termom* m *i* $n \geq 2$. *Tada je*

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

ako i samo ako postoji $c \in \mathsf{Pol}_n\mathbf{A}$ *i* $\theta, \theta_0, \dots, \theta_{n-1} \in A$ *tako da*

(1) c *se apsorbuje u* $(\theta_0, \dots, \theta_{n-1})$ *sa vrednošću* θ *i*
(2) *postoji vektor* $(a_0, \dots, a_{n-1}) \in A^n$ *takav da je* $c(a_0, \dots, a_{n-1}) \neq \theta$.

Klon generisan skupom operacija F označavaćemo sa $\mathrm{Clo}(F)$. U slučaju anuliranja višeg komutatora polinomijalni klon je generisan skupom polinoma ograničene arnosti.

Propozicija §2.4.17 *Neka je* $\mathbf{A}$ *Maljcevljeva algebra sa Maljcevljevim termom* m *i* $n \geq 2$. *Ako je* $[\underbrace{1, \dots, 1}_{n}] = 0$ *onda* $\mathrm{Clo}(\bigcup_{i=0}^{n-1} \mathsf{Pol}_i\,\mathbf{A} \cup \{m\}) = \mathsf{Pol}\,\mathbf{A}$.

4. Glavni rezultati

Prethodne propozicije sugerišu da klasa algebri kod kojih se viši komutator anulira ima posebna svojstva. Te algebre nazivamo *supernilpotentne* algebre. Preciznije, ako je $k \in \mathbb{N}$, algebra se naziva k-supernilpotentna ako je

$$[\underbrace{1, \dots, 1}_{k+1}] = 0.$$

Algebra $\mathbf{A}$ se naziva supernilpotentna ako je k-supernilpotentna za neko $k \in \mathbb{N}$. Jasno, na osnovu (HC8) sledi da je svaka supernilpotentna algebra i nilpotentna, a da su Abelove algebre 1-supernilpotentne, ali i k-supernilpotentne za sve $k \geq 1$ na osnovu nejednakosti (HC3). Dakle, klasa supernilpotentnih algebri je potklasa nilpotentnih algebri koja u sebi sadrži potklasu Abelovih algebri.

Propozicija §3.1.14 *Neka* $k \in \mathbb{N}$ *i neka je* $\mathbf{A}$ k*-supernilpotentna Maljcevljeva algebra. Ako je* $\mathbf{A}$ $(k+1)$*-afino kompletna, onda je* $\mathbf{A}$ *afino kompletna.*

Kao posledicu ove tvrdnje dobijamo da je afina kompletnost odlučiva osobina za supernilpotentne Maljcevljeve algebre. Pokazuje se da je neki polinom u k-supernilpotentnoj Maljcevljevoj algebri $\mathbf{A}$ jednak konstanti $\theta \in A$ ako i samo ako uzima vrednost θ za sve vektore koji se od θ razlikuju na najviše k mesta.

Lema §3.1.17 *Neka je* $\mathbf{A}$ *konačna nilpotentna algebra konačnog tipa koja generiše kongruencijski modularan varijetet. Ako je* $\mathbf{A}$ *direktan proizvod algebri* *čiji su redovi stepeni prostih brojeva onda je* $\mathbf{A}$ *supernilpotentna Maljcevljeva algebra.*

Prethodno tvrđenje razmatra jednu specijalnu klasu Maljcevljevih algebri koja je izučavana u [**25**] kod koje dolazi do poklapanja klase nilpotentnih Maljcevljevih algebri sa klasom supernilpotentnih Maljcevljevih algebri. Tako dobijamo sledeće rezultate.

Teorema §3.1.18 *Postoji algoritam koji odlučuje da li je konačna nilpotentna algebra konačnog tipa koja je direktan proizvod algebri čiji su redovi stepeni prostih brojeva i koja generiše kongruencijski modularan varijetet afino kompletna.*

Teorema §3.2.3 *Problem polinomijalne ekvivalentnosti za konačnu nilpotentnu algebru konačnog tipa koja je direktan proizvod algebri čiji su redovi stepeni prostih brojeva i koja generiše kongruencijski modularan varijetet ima polinomijalnu složenost u zavisnosti od dužine unetih polinomijalnih termova.*

Finalni doprinos ove disertacije je vezan za pitanje broja polinomijalno neekvivalentnih Maljcevljevih klonova na konačnom skupu.

Za $k \geq 1$ pišemo $\mathsf{Inv}^k(A, \mathsf{Pol}\,\mathbf{A})$ za skup svih najviše k-arnih relacija na skupu A invarijantnih u odnosu na sve polinome iz $\mathbf{A}$. Dalje, neka je $\mathsf{Inv}(A, \mathsf{Pol}\,\mathbf{A}) := \cup_{k\geq 1}\mathsf{Inv}^k(A, \mathsf{Pol}\,\mathbf{A})$ skup svih konačnih relacija koje su invarijantne u odnosu na sve polinome iz $\mathbf{A}$. Ako je R skup relacija na A, označimo skup svih operacija na A koje očuvavaju sve relacije iz skupa R sa $\mathsf{Comp}(A, R)$. Kao posledicu od [**32**, Satz 1.2.1, p. 53], ako je $\mathbf{A}$ konačan, imamo:

$$\mathsf{Pol}\,\mathbf{A} = \mathsf{Comp}\,(A, \mathsf{Inv}(A, \mathsf{Pol}\,\mathbf{A})).$$

Prema tome skup polinoma na $\mathbf{A}$ je kompletno određen beskonačnim skupom $\mathsf{Inv}(A, \mathsf{Pol}\,\mathbf{A})$ relacija na A. Za mnoge Maljcevljeve algebre možemo tačno navesti konačan podskup R od $\mathsf{Inv}(A, \mathsf{Pol}\,\mathbf{A})$ koji opisuje polinome. Ipak nije poznato da li je sledeća hipoteza tačna.

Hipoteza. *Za svaku konačnu Maljcevljevu algebru* $\mathbf{A}$ *postoji konačan skup* R *relacija na* A *takav da važi:* $\mathsf{Pol}\,\mathbf{A} = \mathsf{Comp}(A, R)$.

Prema [**32**, p. 50] znamo da za svaki konačan skup R relacija na A, postoji jedna konačna relacija ρ na A takva da je $\mathsf{Comp}(A, R) = \mathsf{Comp}(A, \{\rho\})$. Pa se navedena hipoteza može formulisati na sledeći način. U svakoj konačnoj Maljcevljevoj algebri, polinomi se mogu opisati pomoću samo jedne relacije. Ako je ova hipoteza tačna onda ona ima sledeće posledice:

(1) Na konačnom skupu A, postoji najviše prebrojivo mnogo polinomijalnih Maljcevljevih klonova. Stoga, postoji prebrojiva lista konačnih Maljcevljevih algebri takvih da je svaka konačna Maljcevljeva algebra polinomijalno ekvivalentna izomorfnoj kopiji neke od algebri sa liste.
(2) Ne postoji beskonačan opadajući niz polinomijalnih Maljcevljevih klonova na konačnom skupu.

Koristeći [**32**, Folgerung 1.1.18, p.49] znamo da je dovoljno proveriti da li n-arna funkcija očuvava sve relacije arnosti najviše $|A|^n$, da bi utvrdili da li je f sadržana u $\mathsf{Comp}(A, \mathsf{Inv}(A, \mathsf{Pol}\,\mathbf{A}))$. To i jeste glavna ideja za pokazivanje sledećeg parcijalnog rezultata ove hipoteze.

TEOREMA §3.3.22 *Neka je* $\mathbf{A}$ *konačna Maljcevljeva algebra kod koje je mreža kongruencija visine najviše dva. Tada postoji konačan skup relacija* R *na* A *takav da je* $\mathsf{Pol}\,\mathbf{A} = \mathsf{Comp}(A, R)$.

Kratka biografija

Nebojša Mudrinski je rođen u Novom Sadu 16. 01. 1978. godine gde je završio osnovnu školu. Matematička odeljenja gimnazije ,,Jovan Jovanović Zmaj" u Novom Sadu završio je kao učenik generacije 1997. godine. Iste godine je upisao Prirodno-matematički fakultet u Novom Sadu, smer Profesor matematike. Fakultet je završio 2001. godine sa prosekom 9,93 i upisao poslediplomske studije na Departmanu za matematiku i informatiku PMF-a, smer Algebra i matematička logika. Sve ispite na magistarskim studijama položio je sa ocenom 10. Magistarsku tezu pod naslovom ,,Monoidi endomorfizama prebrojivih homogenih grafova" odbranio je 2005. godine. Tema za doktorsku disertaciju ,,O polinomima u algebrama Maljceva" prihvaćena mu je 15. januara 2009. godine.

Kao asistent na Departmanu za matematiku i informatiku PMF-a radi od 01. 10. 2001. godine. Član je katedre za Opštu algebru i teorijsko računarstvo.

Od 2002. godine je angažovan na projektu 1227 ,,Algebarske i kombinatorne metode u informacio-nim i komunikacionim tehnologijama", a od 2005. godine je angažovan na projektu 144011 ,,Algebarske strukture u procesuiranju informacija" Ministarstva za nauku i zaštitu životne sredine Republike Srbije.

Svoje naučne rezultate izlagao je na domaćim i međunarodnim konferencijama u Austriji, Finskoj, Italiji, Mađarskoj i Nemačkoj. Dva puta je izlagao na Seminaru iz algebre Tehničkog univerziteta u Beču, Austrija. Ministarstvo Republike Austrije za obrazovanje, nauku i kulturu dodelilo mu je istraivačku stipendiju u aprilu 2005., oktobru 2006. i junu 2008. godine za finansiranje jednomesečnih naučno-istraivačkih boravka na Institutu za algebru Johannes Kepler univerziteta u Lincu, gde je takođe 2007. godine od januara do septembra bio angažovan kao istraživač saradnik.

Autor je i koautor 5 naučnih radova u domaćim i međunarodnim časopisima.

FO
Naučna oblast: Matematika
NO
Naučna disciplina: Algebra
ND
Ključne reči: Polinomi, klonovi, Maljcevljeve algebre, komutatori
PO
UDK:
Čuva se
ČU
Važna napomena:
VN

Izvod: Ustanovljavamo osobine viših komutatora, koje je uveo A. Bulatov, u kongruencijki permutabilnim varijetetima. Te komutatore koristimo da bi dokazali da se klon polinomijalnih funkcija konačne Maljcevljeve algebre čija je mreža kongruencija visine najviše dva može opisati konačnim skupom relacija. Za konačne nilpotentne algebre konačnog tipa koje su proizvod algebri koje imaju red stepena prostog broja i koje generišu kongruencijki modularan varijetet pokazujemo da je osobina afine kompletnosti odlučiva. Takođe, pokazujemo za istu klasu da problem polinomijalne ekvivalencije ima polinomnu složenost u zavisnosti od dužine unetih polinomijalnih terma.

IZ
Datum prihvatanja teme od strane NN veća: 15. 01. 2009.
DP
Datum odbrane:
DO
Članovi komisije:
KO
Predsednik: dr Siniša Crvenković, redovni profesor
član: dr Dragan Mašulović, vanredni profesor - mentor
član: Doz.dr Erhard Aichinger - mentor
član: dr Rozália Madarász-Szilágyi, redovni profesor
član: dr Petar Marković, docent

Scientific field: Mathematics
SF
Scientific discipline: Algebra
Key words: Polynomials, clones, Mal'cev algebra, commutators
Holding data:
HD Note:
Abstract: We establish several properties of higher commutators, which were introduced by A. Bulatov, in congruence permutable varieties. We use these commutators to prove that the clone of polynomial functions of a finite Mal'cev algebra whose congruence lattice is of height at most 2, can be described by a finite set of relations. For a finite nilpotent algebra of finite type that is a product of algebras of prime power order and generates congruence modular variety, we are able to show that the property of affine completeness is decidable. Moreover, polynomial equivalence problem has polynomial complexity in the length of the input polynomials.
AB
Accepted by the Scientific Board on: 15^{th} January 2009
Defended:
Thesis defend board:
Member: dr Siniša Crvenković, full professor, (head)
Member: dr Dragan Mašulović, associated professor - mentor
Member: Doz.dr Erhard Aichinger - mentor
Member: dr Rozália Madarász-Szilágyi, full professor
Member: dr Petar Marković, docent

UNIVERSITY OF NOVI SAD
FACULTY OF SCIENCES
KEY DOCUMENTATION

Accession number:
ANO
Identification number:
INO
Document type: Monograph type
DT
Type of record: Printed text
TR
Contents Code: Doctoral dissertation
CC
Author: mr Nebojša Mudrinski
AU
Mentor: Doz.dr Erhard Aichinger and dr Dragan Mašulović
MN
Title: On Polynomials in Mal'cev Algebras
XL
Language of text: English
LT
Language of abstract: Serbian
LA
Country of publication: Republic of Serbia
CP
Locality of publication: Vojvodina
LP
Publication year: 2009
PY
Publisher: Author's reprint
PU
Publ. place: Novi Sad, Trg Dositeja Obradovića 4
PP
Physical description: three chapters, 91 pages, 36 references, 0 tables, one picture, 0 graphics and one appendix
PD

UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
KLJUČNA DOKUMENTACIJSKA INFORMACIJA

Redni broj:
Identifikacioni broj:
IBR
Tip dokumentacije: Monografska dokumentacija
TD
Tipe zapisa: Tekstualni štampani materijal
TZ
Vrsta rada: Doktorska disertacija
VR
Autor: mr Nebojša Mudrinski
AU
Mentor: Doz.dr Erhard Aichinger i dr Dragan Mašulović
MN
Naslov rada: O polinomima u algebrama Maljceva
MR
Jezik publikacije: Engleski
JP
Jezik izvoda: Srpski
JI
Zemlja publikovanja: Republika Srbija
ZP
Uže geografsko područje: Vojvodina
UGP
Godina: 2009
GO
Izdavač: Autorski reprint
IZ
Mesto i adresa: Novi Sad, Trg Dositeja Obradovića 4
MA
Fizički opis rada: tri dela, 91 strana, 36 referenci, 0 tablica, jedna slika, 0 grafika i jedan dodatak
PD