POLYNOMIAL CLONES ON GROUPS OF ORDER pq

ERHARD AICHINGER AND PETER MAYR

Abstract. For two distinct primes p, q, we describe those clones on a set of size pq that contain a given group operation and all constants operations. We show that each such clone is determined by congruences and commutator relations. Thus we obtain that there is only a finite number of such clones on a fixed set.

1. Introduction

A *clone* [17, Definition 4.1] on a set A is a collection of finitary functions on A that contains all projections and is closed under all compositions. We will investigate those clones that contain all constant functions; such clones have been called *constantive* in [14]. From [2] we know that, if $|A| \geq 3$, there are $2^{\aleph_0}$ clones containing all constant functions on A. In [14] it was proved that for $|A| \geq 4$ infinitely many clones on A contain a ternary Mal'cev operation. Now given a finite set and a Mal'cev operation, one may ask how many constantive clones contain this operation. For example, if p is a prime, then there are precisely two constantive clones on $\mathbb{Z}_p$ that contain the ternary function $(x, y, z) \mapsto x - y + z$. By [9] there are countably infinitely many constantive clones on $\mathbb{Z}_p \times \mathbb{Z}_p$ that contain $(x, y, z) \mapsto x-y+z$. It is not known whether there is a Mal'cev operation on some finite set that is contained in more than countably many constantive clones. We will investigate this problem for the case when the Mal'cev operation is the Mal'cev operation of some abelian group.

Let $\langle V, +\rangle$ be a (not necessarily abelian) group, let F_1, F_2 be sets of finitary operations on V, and let $\mathbf{V}_1 := \langle V, \{+\} \cup F_1\rangle$ and $\mathbf{V}_2 := \langle V, \{+\} \cup F_2\rangle$ be two expansions of $\langle V, +\rangle$. Following [17, Definition 4.139], we call these expansions *polynomially equivalent* if $\mathrm{Pol}(\mathbf{V}_1) = \mathrm{Pol}(\mathbf{V}_2)$. Classifying the expansions of $\langle V, +\rangle$ modulo polynomial equivalence is a way to obtain a description of the constantive clones that extend the clone of polynomial functions of the group $\langle V, +\rangle$. In [14, Conjecture 9] P. M. Idziak has conjectured that for a squarefree n

Date: April 19, 2006.

2000 *Mathematics Subject Classification.* 08A40 (16Y30).

Key words and phrases. Mal'cev clones, polynomial functions, polynomial completeness, commutator theory.

Supported by the Austrian Science Foundation (FWF), grant P15691.

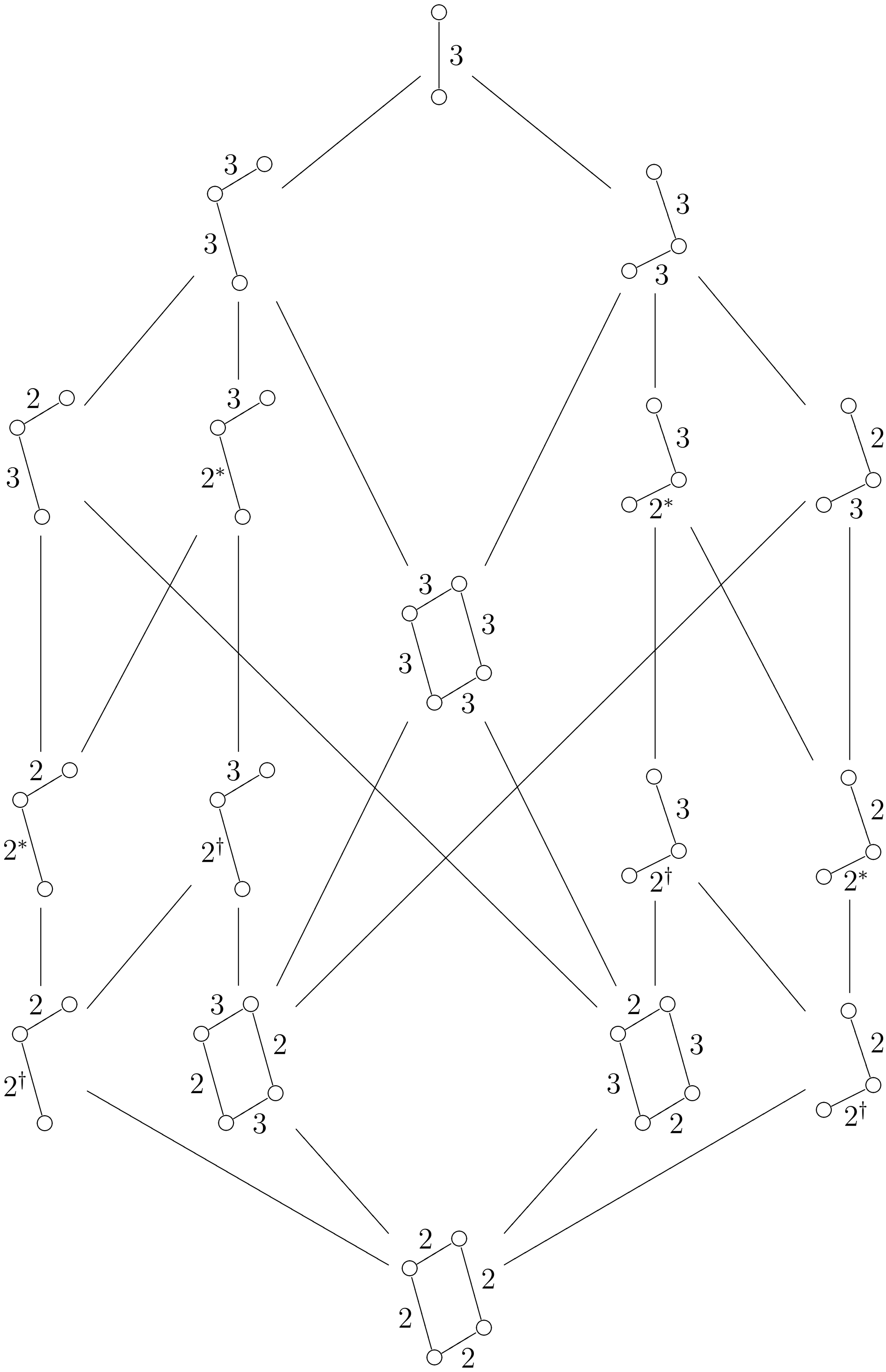

Figure 1. Polynomial clones on expansions $\mathbf{V}$ of $\langle \mathbb{Z}_{pq}, + \rangle$: Each clone $\mathrm{Pol}(\mathbf{V})$ is represented by $\mathbf{Con}^*(\mathbf{V})$. Simple factors are labelled 2 if they are abelian and 3 otherwise. A minimal factor which is labelled $2^\dagger$ is central; if it is labelled 2^*, it is not central.

the group $\langle \mathbb{Z}_n, +\rangle$ has only finitely many polynomially inequivalent expansions. Furthermore he conjectures that for each expansion $\mathbf{V}$ of $\langle \mathbb{Z}_n, +\rangle$ the clone of polynomial functions of $\mathbf{V}$ is uniquely determined by the congruences of $\mathbf{V}$ and their commutators. In the present paper we confirm this conjecture for the case when n is the product of two primes.

For any algebra $\mathbf{A}$ we will denote the set of its congruences by $\mathrm{Con}(\mathbf{A})$. By $\mathbf{Con}(\mathbf{A})$ we denote the lattice $\langle \mathrm{Con}(\mathbf{A}), \wedge, \vee\rangle$, and by $\mathbf{Con}^*(\mathbf{A})$ we denote the algebra $\langle \mathrm{Con}(\mathbf{A}), \wedge, \vee, [.,.]\rangle$, where $[.,.]$ is the term condition commutator on the congruences of $\mathbf{A}$ as defined in [17, Definition 4.150] (see also [11]). The main result of the present paper is the following theorem.

Theorem 1.1. *Let p, q be primes with $p \neq q$, let $\mathbf{G}$ be a group of order pq, and let $\mathbf{V}_1$ and $\mathbf{V}_2$ be two expansions of $\mathbf{G}$. Then the following are equivalent:*

(1) $\mathrm{Pol}(\mathbf{V}_1) = \mathrm{Pol}(\mathbf{V}_2)$.
(2) $\mathrm{Pol}_2(\mathbf{V}_1) = \mathrm{Pol}_2(\mathbf{V}_2)$.
(3) $\mathbf{Con}^*(\mathbf{V}_1) = \mathbf{Con}^*(\mathbf{V}_2)$.

The proof will be given in Section 7. From this result we will derive the following consequences.

Corollary 1.2. *Let p, q be primes with $p \neq q$. Then there are precisely 17 clones on $\mathbb{Z}_{pq}$ that contain the addition of $\mathbb{Z}_{pq}$ and all constant operations. The inclusions among these clones are given in Figure 1.*

Corollary 1.3. *Let p, q be primes with $p \neq q$. Then there are only finitely many constantive clones on a set with pq elements that have a group operation among their binary operations.*

2. Some facts about commutators

Our first goal in this section is to define and to investigate when a function preserves the commutators of an algebra $\mathbf{A}$. For an algebra $\mathbf{A} = \langle A, F\rangle$ and a finitary operation f on A we let $\mathbf{A} + f$ denote the algebra $\langle A, F \cup \{f\}\rangle$.

Definition 2.1. Let $\mathbf{A}$ be an algebra, let $k \in \mathbb{N}$, and let $f : A^k \to A$. Then f is *commutator preserving* if $\mathbf{Con}^*(\mathbf{A}) = \mathbf{Con}^*(\mathbf{A} + f)$.

By this definition a commutator preserving function is also congruence preserving. Based on [16] it is proved in [10, Lemma 4] that for an algebra in a congruence modular variety the set of commutator preserving functions is closed under all compositions and hence forms a clone. Actually the commutator preserving functions are described as those that preserve certain 5-ary relations on A. We give a brief self-contained account of this description, specialized to congruence permutable varieties. For a set A, a set R of finitary relations on A, and

$k \in \mathbb{N}$ we abbreviate the set of all k-ary functions on A that preserve all relations in R by $\mathrm{Comp}_k(A, R)$. Furthermore

$$\mathrm{Comp}(A, R) := \bigcup \{\mathrm{Comp}_k(A, R) \mid k \in \mathbb{N}\}.$$

We note that $\mathrm{Comp}(A, R)$ has also been called the set of polymorphisms of the relations in R and has often been denoted by $\mathrm{Pol}\, R$.

Definition 2.2. Let $\mathbf{A}$ be an algebra, let $m : A^3 \to A$, and let $\alpha, \beta, \eta \in \mathrm{Con}(\mathbf{A})$. Then we define a relation $\rho(\alpha, \beta, \eta, m)$ by

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

A ternary operation m on A is called a *Mal'cev operation* if $m(a, b, b) = m(b, b, a) = a$ for all $a, b \in A$. A *Mal'cev polynomial* of $\mathbf{A}$ is a Mal'cev operation that lies in $\mathrm{Pol}_3(\mathbf{A})$. The following proposition shows that in an algebra with a Mal'cev polynomial the centralizing relation from [17, Definition 4.148] is determined by the commutator operation.

Proposition 2.3. *Let $\mathbf{A}$ be an algebra that has a Mal'cev polynomial, and let $\alpha, \beta, \eta \in \mathrm{Con}(\mathbf{A})$. Then $[\alpha, \beta] \leq \eta$ if and only if α centralizes β modulo η.*

Proof: The "if"-direction follows from the definition of the commutator [17, Definition 4.150]. For the "only if"-direction we observe that α centralizes β modulo $[\alpha, \beta]$. By [17, Exercise 4.156 (13)] the congruence α then centralizes β modulo η. □

Lemma 2.4. *Let $\mathbf{A}$ be an algebra in a congruence permutable variety, let m be a Mal'cev polynomial on $\mathbf{A}$, and let $\alpha, \beta, \eta \in \mathrm{Con}(\mathbf{A})$. Then the following are equivalent:*

(1) *Every $f \in \mathrm{Pol}(\mathbf{A})$ preserves $\rho(\alpha, \beta, \eta, m)$.*
(2) *α centralizes β modulo η (as defined in* [17, Definition 4.148]*).*

Proof: We abbreviate $\rho(\alpha, \beta, \eta, m)$ by ρ.

(2)⇒(1): Let $k \in \mathbb{N}$, let $f \in \mathrm{Pol}_k(\mathbf{A})$, and let $(\overline{a}, \overline{b}, \overline{c}, \overline{d}) \in \rho^{[k]}$. Here $(\overline{a}, \overline{b}, \overline{c}, \overline{d}) \in \rho^{[k]}$ means $(a_i, b_i, c_i, d_i) \in \rho$ for each $i \in \{1, 2, \ldots, k\}$. We have to show

$$(f(\overline{a}), f(\overline{b}), f(\overline{c}), f(\overline{d})) \in \rho. \tag{2.1}$$

First we prove

$$m(f(\overline{a}), f(\overline{b}), f(\overline{c})) \equiv f(m(a_1, b_1, c_1), m(a_2, b_2, c_2), \ldots, m(a_k, b_k, c_k)) \pmod{\eta} \tag{2.2}$$

For $\overline{x}, \overline{y}, \overline{z} \in A^k$ we define $\overline{m}(\overline{x}, \overline{y}, \overline{z}) \in A^k$ by

$$\overline{m}(\overline{x}, \overline{y}, \overline{z}) := (m(x_1, y_1, z_1), m(x_2, y_2, z_2), \ldots, m(x_k, y_k, z_k)). \tag{2.3}$$

We define a function $t \in \mathrm{Pol}_{2k}(\mathbf{A})$ by

$$t(\overline{x}, \overline{y}) := m(m(f(\overline{x}), f(\overline{b}), f(\overline{y})), f(\overline{m}(\overline{x}, \overline{b}, \overline{y})), f(\overline{m}(\overline{a}, \overline{b}, \overline{c}))).$$

We have $t(\overline{b},\overline{b}) = t(\overline{b},\overline{c}) = f(\overline{m}(\overline{a},\overline{b},\overline{c}))$. Hence, applying [17, Exercise 4.156 (2)], we obtain $t(\overline{a},\overline{b}) \equiv t(\overline{a},\overline{c}) \pmod{\eta}$. This yields

$$f(\overline{m}(\overline{a},\overline{b},\overline{c})) \equiv m(f(\overline{a}), f(\overline{b}), f(\overline{c})) \pmod{\eta},$$

which completes the proof of (2.2). For the proof of (2.1) we note that f, as a polynomial function, preserves congruences. Hence we have

$$f(\overline{a})\,\alpha\, f(\overline{b}) \text{ and } f(\overline{b})\beta\, f(\overline{c}).$$

What remains to show is

$$m(f(\overline{a}), f(\overline{b}), f(\overline{c})) \equiv f(\overline{d}) \pmod{\eta}.$$

We observe that by (2.2) we have $m(f(\overline{a}), f(\overline{b}), f(\overline{c})) \equiv f(\overline{m}(\overline{a},\overline{b},\overline{c})) \pmod{\eta}$. Since $(\overline{a},\overline{b},\overline{c},\overline{d}) \in \rho^{[k]}$ and since f is congruence preserving, we have $f(\overline{m}(\overline{a},\overline{b},\overline{c})) \equiv f(\overline{d}) \pmod{\eta}$. This completes the proof of (2.1).

(1)⇒(2): We show that α centralizes β modulo η. To this end we let $k \in \mathbb{N}$, $t \in \mathrm{Clo}_{k+1}(\mathbf{A})$, and $a, b \in A$, $\overline{c}, \overline{d} \in A^k$ such that $a\,\alpha\, b$ and $\overline{c}\,\beta\,\overline{d}$. We assume $t(a,\overline{c})\,\eta\, t(a,\overline{d})$. We have $(b,a,a,b) \in \rho$, and $(\overline{d},\overline{d},\overline{c},\overline{c}) \in \rho^{[k]}$. Hence we have

$$(t(b,\overline{d}), t(a,\overline{d}), t(a,\overline{c}), t(b,\overline{c})) \in \rho.$$

Therefore we have $m(t(b,\overline{d}), t(a,\overline{d}), t(a,\overline{c})) \equiv t(b,\overline{c}) \pmod{\eta}$. Hence

$$m(t(b,\overline{d}), t(a,\overline{d}), t(a,\overline{d})) \equiv t(b,\overline{c}) \pmod{\eta},$$

and thus

$$t(b,\overline{d})\,\eta\, t(b,\overline{c}),$$

which completes the proof. □

Definition 2.5. Let $\mathbf{A}$ be an algebra, and let m be a Mal'cev polynomial on $\mathbf{A}$. We define a set $\mathrm{Cen}(\mathbf{A}, m)$ of 4-ary relations on A by

$$\mathrm{Cen}(\mathbf{A}, m) := \{\rho(\alpha,\beta,\eta,m) \mid \alpha,\beta,\eta \in \mathrm{Con}(\mathbf{A}) \text{ and } \alpha \text{ centralizes } \beta \text{ modulo } \eta \text{ in } \mathbf{A}\}.$$

Lemma 2.6. *Let $k \in \mathbb{N}$, let $\mathbf{A}$ be an algebra with Mal'cev polynomial m, and let f be a mapping from A^k to A. Then the following are equivalent:*

(1) *The function f is a commutator preserving function of $\mathbf{A}$.*
(2) *The function f preserves all relations in $\mathrm{Con}(\mathbf{A}) \cup \mathrm{Cen}(\mathbf{A}, m)$.*

Proof: (2)⇒(1): Since f is congruence preserving, we have $\mathrm{Con}(\mathbf{A}) = \mathrm{Con}(\mathbf{A}+f)$. Now we show that the commutators are the same. We claim that

> for all $\alpha,\beta,\eta \in \mathrm{Con}(\mathbf{A})$, α centralizes β modulo η in $\mathbf{A}$ if and only if α centralizes β modulo η in $\mathbf{A}+f$.

The "if"-direction is immediate from [17, Definition 4.148] since $\mathbf{A}$ is a reduct of $\mathbf{A}+f$. To show the "only if"-direction of this statement, we let α, β, η be such that α centralizes β modulo η in $\mathbf{A}$. By the assumption f preserves $\rho(\alpha, \beta, \eta, m)$. Using this fact and (2)⇒(1) of Lemma 2.4 for the algebra $\mathbf{A}$, we obtain that every fundamental operation of $\mathbf{A}+f$ is in $\mathrm{Comp}(A, \{\rho(\alpha,\beta,\eta,m)\})$. Thus we have

$$\mathrm{Pol}(\mathbf{A}+f) \subseteq \mathrm{Comp}(A, \{\rho(\alpha,\beta,\eta,m)\}).$$

Using (1)⇒(2) of Lemma 2.4 for the algebra $\mathbf{A}+f$, we obtain that α centralizes β modulo η in $\mathbf{A}+f$.

The commutator operation is completely determined by the set of all triples $(\alpha,\beta,\eta) \in (\mathrm{Con}(\mathbf{A}))^3$ such that α centralizes β modulo η. Therefore the commutator operations for $\mathbf{A}$ and $\mathbf{A}+f$ are the same.

(1)⇒(2): Let $\alpha, \beta, \eta \in \mathrm{Con}(\mathbf{A})$ be such that α centralizes β modulo η in $\mathbf{A}$. Hence $[\alpha,\beta]_{\mathbf{A}} \leq \eta$. By the assumption $\mathbf{A}$ and $\mathbf{A}+f$ have the same commutator operation, and therefore $[\alpha,\beta]_{\mathbf{A}+f} \leq \eta$. Hence α centralizes β modulo η in $\mathbf{A}+f$ by Proposition 2.3. Now by (2)⇒(1) of Lemma 2.4 every polynomial function of $\mathbf{A}+f$ preserves $\rho(\alpha,\beta,\eta,m)$, implying that f preserves $\rho(\alpha,\beta,\eta,m)$. □

We call an algebra $\mathbf{V}$ an *expanded group* if it has $+$ among its binary operation symbols, and $\langle V, +\rangle$ is a group. A normal subgroup I of $\langle V,+\rangle$ is called an *ideal* of $\mathbf{V}$ if $f(\overline{a}+\overline{i}) - f(\overline{a}) \in I$ for all $k \in \mathbb{N}$, all k-ary fundamental operations f of $\mathbf{V}$ and all $\overline{a} \in V^k, \overline{i} \in I^k$. A useful fact linking ideals with polynomial functions is the following: a set I of V is an ideal of $\mathbf{V}$ if and only if for all $i_1, i_2 \in I$ and for all $p \in \mathrm{Pol}_1(\mathbf{V})$ with $p(0)=0$ we have $i_1+i_2 \in I$ and $p(i_1) \in I$ [18, Theorem 7.123]. The set of all ideals of $\mathbf{V}$ is denoted by $\mathrm{Id}\,\mathbf{V}$. The mapping that sends each congruence to the congruence class of 0 is a bijective correspondence between congruences and ideals of $\mathbf{V}$. Its inverse will be denoted by γ: for every ideal I of $\mathbf{V}$ we have the congruence $\gamma(I)$ on $\mathbf{V}$ defined by

$$\gamma(I) = \{(v_1, v_2) \in V^2 \mid v_1 - v_2 \in I\}.$$

It is easy to see that γ is a lattice isomorphism from $\langle \mathrm{Id}\,(\mathbf{V}), \cap, +\rangle$ to $\langle \mathrm{Con}(\mathbf{V}), \wedge, \vee\rangle$. Of course the commutator operation for universal algebras can in particular be used for the congruences of expanded groups. However we want to have a commutator operation for ideals and not only for congruences. The commutator operation $[\![.,.]\!]_{\mathbf{V}}$ on ideals should behave in a way that the mapping γ is also a isomorphism from $\langle \mathrm{Id}\,(\mathbf{V}), \cap, +, [\![.,.]\!]_{\mathbf{V}}\rangle$ to $\mathbf{Con}^*(\mathbf{V})$. This can be accomplished with the following definition.

Definition 2.7. [19, p.77] 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

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

In Lemma 2.9 we will see that this commutator, which was introduced by S. D. Scott and used, e.g., in [5, 7], is essentially the same as the term condition commutator of universal algebra. For proving this lemma, we need the following easy observation.

Proposition 2.8. *Let* $\mathbf{V}$ *be an expanded group, let* A, B *be ideals of* $\mathbf{V}$*, let* $k \in \mathbb{N}$*, let* $c \in \mathrm{Pol}_{k+1}(\mathbf{V})$ *be such that* $c(x, \overline{0}) = c(0, \overline{y}) = 0$ *for all* $x \in V$*,* $\overline{y} \in V^k$*, and let* $a \in A$*,* $\overline{b} \in B^k$*. Then* $c(a, \overline{b})$ *is in* $[\![A, B]\!]_{\mathbf{V}}$*.*

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 $p(a, b_k) \in [\![A, B]\!]_{\mathbf{V}}$. By the induction hypothesis also $c(a, b_1, \ldots, b_{k-1}, 0)$ is in $[\![A, B]\!]_{\mathbf{V}}$. 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 $[\![A, B]\!]_{\mathbf{V}}$. □

Lemma 2.9. *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* $[\alpha, \beta] = \gamma([\![A, B]\!]_{\mathbf{V}})$*.*

Proof: We first show $[\alpha, \beta] \leq \gamma([\![A, B]\!]_{\mathbf{V}})$. By the definition of the commutator it suffices to show that α centralizes β modulo $\gamma([\![A, B]\!]_{\mathbf{V}})$. To this end we let $t \in \mathrm{Clo}_{k+1}(\mathbf{V})$, let $a, b \in V$ and $\overline{c}, \overline{d} \in V^k$ be such that $a - b \in A$ and $\overline{c} - \overline{d} \in B^k$, and we assume $t(a, \overline{c}) - t(a, \overline{d}) \in [\![A, B]\!]_{\mathbf{V}}$. We define $s \in \mathrm{Pol}_{k+1}(\mathbf{V})$ by

$$s(x, \overline{y}) := t(a + x, \overline{c} + \overline{y}) - t(a, \overline{c} + \overline{y}) + t(a, \overline{c}) - t(a + x, \overline{c}).$$

By Proposition 2.8 we have $s(-a + b, -\overline{c} + \overline{d}) \in [\![A, B]\!]_{\mathbf{V}}$. (Note that $-a + b = -b - (a - b) + b$, and the last expression is in A because A is a normal subgroup of $\mathbf{V}$). Hence $t(b, \overline{d}) - t(a, \overline{d}) + t(a, \overline{c}) - t(b, \overline{c})$ is in $[\![A, B]\!]_{\mathbf{V}}$. This implies that $t(b, \overline{d}) - t(b, \overline{c}) \in [\![A, B]\!]_{\mathbf{V}}$, which concludes the proof that α centralizes β modulo $\gamma([\![A, B]\!]_{\mathbf{V}})$.

For proving $\gamma([\![A, B]\!]_{\mathbf{V}}) \leq [\alpha, \beta]$, we show that all generators of $[\![A, B]\!]_{\mathbf{V}}$ are congruent to 0 modulo $[\alpha, \beta]$. Let $c \in \mathrm{Pol}_2(\mathbf{V})$ be such that $c(x, 0) = c(0, x) = 0$ for all $x \in V$, and let $a \in A, b \in B$. Then we have $c(0, 0) \equiv c(0, b) \pmod{[\alpha, \beta]}$ and therefore $c(a, 0) \equiv c(a, b) \pmod{[\alpha, \beta]}$ by [17, Exercise 4.156 (2)]. This implies that $c(a, b)$ lies in the ideal $\gamma^{-1}([\alpha, \beta])$. Since all generators of $[\![A, B]\!]_{\mathbf{V}}$ are in $\gamma^{-1}([\alpha, \beta])$, we obtain $[\![A, B]\!]_{\mathbf{V}} \leq \gamma^{-1}([\alpha, \beta])$. Thus $\gamma([\![A, B]\!]_{\mathbf{V}}) \leq [\alpha, \beta]$. □

3. Some facts about polynomial functions

Lemma 3.1. *Let* $\mathbf{V}$ *be an expanded group such that* $\langle V, + \rangle$ *is a cyclic group and* $\mathbf{V}$ *is abelian, i.e.,* $[\![V, V]\!]_{\mathbf{V}} = 0$*. Then* $\mathbf{V}$ *is polynomially equivalent to* $\langle V, + \rangle$*.*

Proof: Since $\mathbf{V}$ is abelian, the clone of polynomial functions of $\mathbf{V}$ is determined by its unary members. Furthermore each unary polynomial function on

$\mathbf{V}$ is the sum of a constant function and an endomorphism of $\langle V,+\rangle$ (cf. [7, Proposition 2.3]). Every endomorphism of the cyclic group $\langle V,+\rangle$ is some multiple of the identity function. Hence $\mathrm{Pol}_1(\mathbf{V}) \subseteq \mathrm{Pol}_1(\langle V,+\rangle)$ and consequently $\mathrm{Pol}(\mathbf{V}) = \mathrm{Pol}(\langle V,+\rangle)$. □

Lemma 3.2. *Let p be a prime, and let $\mathbf{V}$ be an expansion of $\langle \mathbb{Z}_p,+\rangle$. Then $\mathbf{V}$ is either polynomially equivalent to $\langle \mathbb{Z}_p,+\rangle$ or polynomially complete.*

Proof: If $\mathbf{V}$ is simple and not abelian, then it is polynomially complete by [12]. If it is abelian, Lemma 3.1 yields that $\mathbf{V}$ is polynomially equivalent to $\langle \mathbb{Z}_p,+\rangle$. □

For many expanded groups of squarefree order the results in [15] can be used to obtain a description of the clone of polynomial functions. We will use the version given in [10, p.61, Theorem 2]. To apply this result, we will need the following lemma.

Lemma 3.3. *Let $\mathbf{V}$ be a subdirectly irreducible expanded group, and let A be the unique minimal ideal of $\mathbf{V}$. We assume that $|A|$ is a prime, that $[\![A,A]\!]_{\mathbf{V}} = 0$, and that there is an idempotent polynomial function $e \in \mathrm{Pol}_1(\mathbf{V})$ such that $e(V) \subseteq A$ and $e(a) = a$ for all $a \in A$. Let $\alpha := \gamma(A)$, and let $q := |A|$. Then A is a $\langle 0,\alpha\rangle$-minimal set of $\mathbf{V}$, and it is polynomially equivalent to the group $\langle \mathbb{Z}_q,+\rangle$.*

Proof: Let $a \in A$ be such that $a \neq 0$. Since $e(a) = a$, [13, Definition 2.5] yields $A \in U_{\mathbf{V}}(0,\alpha)$. Hence there is a set $U \in M_{\mathbf{V}}(0,\alpha)$ such that $U \subseteq A$. By [13, Theorem 2.8 (2)] there is an idempotent polynomial function $f \in \mathrm{Pol}_1(\mathbf{V})$ such that $f(V) = U$. Since $[\![A,A]\!]_{\mathbf{V}} = 0$, the fact that $|A|$ is a prime number and [7, Proposition 2.3] yield that there are $u \in \mathbb{Z}$ and $b \in A$ such that $f(a) = ua + b$ for all $a \in A$, and q does not divide u. Then $f(A) = A$ and therefore $A \subseteq U$. Thus $\mathbf{V}|_U$ (see [13, Definition 2.2]) is an expanded group of prime order. Since $[\![A,A]\!]_{\mathbf{V}} = 0$, there is no $f \in \mathrm{Pol}_2(\mathbf{V})$ with $f(0,0) = f(a,0) = f(0,a) = 0$ and $f(a,a) = a$. Hence $\mathbf{V}|_U$ is not polynomially complete, and therefore it is polynomially equivalent to $\langle \mathbb{Z}_q,+\rangle$ by Lemma 3.2. □

4. Consequences of known results

In the following lemma we combine several already available results. We note that all expansions of non-abelian groups of order pq are covered by its assumptions.

Lemma 4.1. *Let p,q be primes with $p \neq q$, and let $\mathbf{V}$ be an expanded group with $|V| = pq$. We assume that the following holds:*

> *If $\mathbf{Con}(\mathbf{V})$ is isomorphic to a three element chain, then the monolith μ of $\mathbf{V}$ is not central.*

Then every commutator preserving function of $\mathbf{V}$ is in $\mathrm{Pol}(\mathbf{V})$.

Proof: We let $\alpha := \{(v_1, v_2) \in V^2 \,|\, v_1 - v_2 \in pV\}$ and $\beta := \{(v_1, v_2) \in V^2 \,|\, v_1 - v_2 \in qV\}$. Since $\{0\}, 0/\alpha, 0/\beta$ and V are the only subgroups of $\langle V, +\rangle$, we have $\mathrm{Con}(\mathbf{V}) \subseteq \{0, \alpha, \beta, 1\}$. We will now distinguish several cases.

$\mathrm{Con}(\mathbf{V}) = \{0, 1\}$: If $[1, 1] = 0$, then $\langle V, +\rangle$ is a cyclic group. Now Lemma 3.1 yields that $\mathbf{V}$ is polynomially equivalent to $\langle V, +\rangle$ and therefore $\mathrm{Con}(\mathbf{V}) = \{0, \alpha, \beta, 1\}$, a contradiction. If $[1, 1] = 1$, then [12] (cf. [3, Proposition 5.2]) yields that $\mathbf{V}$ is polynomially complete.

$\mathrm{Con}(\mathbf{V}) = \{0, \alpha, \beta, 1\}$: In this case all subdirectly irreducible homomorphic images of $\mathbf{V}$ satisfy the condition (SC1) (see [15], [10, p.62]). Both subdirectly irreducible quotients are expanded groups of prime order. Therefore Lemma 3.3 (with e equal to the identity function) implies that each subdirectly irreducible quotient satisfies (GFp) (see [10, p.62]). Hence $\mathbf{V}$ is polynomially rich by [10, Theorem 2]. Now let f be a commutator preserving function. For expanded groups the type of each prime interval in the congruence lattice of $\mathbf{V}$ is determined by the commutator operation. Therefore, by preserving commutators, f also preserves the types of the prime intervals. Since $\mathbf{V}$ is polynomially rich, f is a polynomial function. — We note that the structure of polynomial functions on direct products of expanded groups can be determined from [4, Corollary 2.2]. This provides an alternative proof for the present case.

$\mathrm{Con}(\mathbf{V}) = \{0, \beta, 1\}$: By the assumption we know that $[1, \beta] = \beta$. This implies that $\mathbf{V}$ satisfies the condition (SC1). Obviously $\mathbf{V}/\beta$ satisfies (GFp). To prove that $\mathbf{V}$ satisfies (GFp), we let $m \in \mathbb{Z}$ be such that $m \equiv 0 \pmod{q}$ and $m \equiv 1 \pmod{p}$. Applying Lemma 3.3 with $e(x) := mx$, we obtain that the $\langle 0, \beta\rangle$-minimal sets of $\mathbf{V}$ are polynomially equivalent to a one-dimensional vector space over $\mathbb{Z}_p$. Hence $\mathbf{V}$ is polynomially rich by [10, Theorem 2]. Now the proof can be concluded as it was done in the case $\mathrm{Con}(\mathbf{V}) = \{0, \alpha, \beta, 1\}$.

The case $\mathrm{Con}(\mathbf{V}) = \{0, \alpha, 1\}$ is analogous to $\mathrm{Con}(\mathbf{V}) = \{0, \beta, 1\}$. □

5. Subdirectly irreducible expanded groups with central monolith

In this section we will establish the fact that for a subdirectly irreducible expanded group $\mathbf{V}$ of order pq with central monolith every commutator preserving function is a polynomial function (see Lemma 5.5). We note that $\mathbf{V}$ certainly has an abelian group reduct by the assumption that its monolith is central.

For the proof of Lemma 5.5 we will first show that every unary function from $\mathbf{V}$ into its monolith A that is constant on all cosets of A is polynomial (Lemma 5.2) by using a result on modules over group rings (Lemma 5.1). Next we construct certain k-ary polynomial functions from $\mathbf{V}$ into A in Lemma 5.3. Then we show that every commutator preserving function from $\mathbf{V}$ into A is polynomial (Lemma 5.4). Finally we prove the general result in Lemma 5.5.

We start with some module theory (see [1] for definitions and basic results).

Lemma 5.1. *Let* $\mathbf{G} := \langle G, \circ \rangle$ *be the group of affine transformations on* $\mathbf{K} := \mathrm{GF}(p)$ *with* p *prime. Let* $\mathbf{F}$ *be a field whose characteristic is not* p*, let* M *be an* $\mathbf{F}[\mathbf{G}]$*-module with basis* $\{e_k \,|\, k \in K\}$ *such that* $g * e_k = e_{g(k)}$ *for* $g \in G, k \in K$*. Let* $s := \sum_{k \in K} e_k$*. Then* M/Fs *is a simple* $\mathbf{F}[\mathbf{G}]$*-module.*

Proof: Let $\bar{\mathbf{F}}$ denote the algebraic closure of $\mathbf{F}$, and let $\bar{M}$ be the vector space with basis $\{e_k \,|\, k \in K\}$ over $\bar{\mathbf{F}}$. Then $\bar{M}$ forms an $\bar{\mathbf{F}}[\mathbf{G}]$-module defined by the action $g * e_k = e_{g(k)}$ for $g \in G, k \in K$. We note that $\bar{M}$ also forms an $\mathbf{F}[\mathbf{G}]$-module, that M is an $\mathbf{F}[\mathbf{G}]$-submodule of $\bar{M}$ and that $\bar{F}M = \bar{M}$. First we show that

$$V := \bar{M}/\bar{F}s \text{ is a simple } \bar{\mathbf{F}}[\mathbf{G}] - \text{module.} \tag{5.1}$$

Let $H := \{g \in G \,|\, g(0) = 0\}$, and let N be the cyclic normal subgroup of order p in $\mathbf{G}$. Then $G = NH$. Since p and the characteristic of $\bar{\mathbf{F}}$ are relatively prime and since $\bar{F}$ is algebraically closed, all simple $\bar{\mathbf{F}}[\mathbf{N}]$-modules have dimension 1 over $\bar{\mathbf{F}}$. Furthermore the group $\mathbf{N}$ acts either faithfully or trivially on every simple $\bar{\mathbf{F}}[\mathbf{N}]$-module. By Maschke's theorem $\mathrm{res}^{\mathbf{G}}_{\mathbf{N}}(V)$, which is V viewed as $\bar{\mathbf{F}}[\mathbf{N}]$-module, is a sum of simple $\bar{\mathbf{F}}[\mathbf{N}]$-modules. We note that $\mathbf{N}$ acts faithfully on $\mathrm{res}^{\mathbf{G}}_{\mathbf{N}}(V)$. Hence we have a simple $\bar{\mathbf{F}}[\mathbf{N}]$-submodule L of $\mathrm{res}^{\mathbf{G}}_{\mathbf{N}}(V)$ such that $\mathbf{N}$ acts faithfully on L. For $g \in \mathbf{G}$ the conjugate modules L and $g * L$ both have dimension 1. We claim that

$$L \text{ and } g * L \text{ are isomorphic } \bar{\mathbf{F}}[\mathbf{N}] - \text{modules if and only if } g \text{ centralizes } N. \tag{5.2}$$

If $g \in C_{\mathbf{G}}(N)$, then the map $L \to g * L, x \mapsto g * x$ is an $\bar{\mathbf{F}}[\mathbf{N}]$-module isomorphism. Conversely we assume that $\varphi : L \to g * L$ is an $\bar{\mathbf{F}}[\mathbf{N}]$-module isomorphism. Let $l \in L$ such that $l \neq 0$. Since l spans L, we have $r \in \bar{F}, r \neq 0$, such that $\varphi(l) = g * (rl)$. For $n \in N$ we find

$$\varphi(n * l) = n * \varphi(l) = (ng) * (rl) = r((ng) * l). \tag{5.3}$$

Let $s \in \bar{F}$ be such that $n * l = sl$. Then

$$\varphi(n * l) = \varphi(sl) = s\varphi(l) = s(g * (rl)) = r(g * (sl)) = r((gn) * l). \tag{5.4}$$

From (5.3) and (5.4) we obtain that $n^{-1}n^g$ acts trivially on L. Since N acts faithfully on L, this yields $n^g = n$. Thus g is in $C_{\mathbf{G}}(N)$ and (5.2) is proved.

By $C_{\mathbf{G}}(N) = N$ the modules $h * L$ are pairwise non-isomorphic for every $h \in H$. Hence $\sum_{h \in H} h * L$ is a direct sum and has dimension $p - 1$ over $\bar{\mathbf{F}}$. Thus

$$\sum_{h \in H} h * L = V. \tag{5.5}$$

Let U be a simple $\bar{\mathbf{F}}[\mathbf{G}]$-submodule of V, and let L' be a simple $\bar{\mathbf{F}}[\mathbf{N}]$-submodule of $\mathrm{res}^{\mathbf{G}}_{\mathbf{N}}(U)$. As an $\bar{\mathbf{F}}[\mathbf{N}]$-submodule of $\mathrm{res}^{\mathbf{G}}_{\mathbf{N}}(V)$, L' is isomorphic to $h * L$ for some

$h \in H$ by (5.5). As above it follows that U contains $i * L'$ for all $i \in H$ and that U has dimension $p-1$ over $\bar{\mathbf{F}}$. Hence $U = V$ and V is a simple $\bar{\mathbf{F}}[\mathbf{G}]$-module.

Now let W be an $\mathbf{F}[\mathbf{G}]$-module such that $Fs \leq W \leq M$. Then $\bar{F}W$ is an $\bar{\mathbf{F}}[\mathbf{G}]$-submodule of $\bar{M}$ and $\dim_{\bar{F}} \bar{F}W = \dim_F W$. By (5.1) we either have $\bar{F}W = \bar{F}s$ or $\bar{F}W = \bar{M}$. Hence $\dim_F W$ is either 1 or p. Then $W = Fs$ or $W = M$. □

Using Lemma 5.1, we can now show the existence of certain unary polynomial functions.

Lemma 5.2. *For primes p, q let $\mathbf{V}$ be an expanded group with group reduct $\langle \mathbb{Z}_p \times \mathbb{Z}_q, + \rangle$, and let $A := 0 \times \mathbb{Z}_q$. We assume that A is an ideal of $\mathbf{V}$ with $[\![V,V]\!]_{\mathbf{V}} \geq A$ and $[\![V,A]\!]_{\mathbf{V}} = 0$. Then we have*

$$(5.6) \qquad \{f \in A^V \mid f(x+a) = f(x) \textit{ for all } x \in V, a \in A\} \subseteq \mathrm{Pol}_1(\mathbf{V}).$$

Proof: Let $M := \{f \in A^V \mid f(x+a) = f(x) \text{ for all } x \in V, a \in A\}$. Since $\langle A, + \rangle$ and $\langle \mathbb{Z}_q, + \rangle$ are isomorphic, M forms a vector space for the field $\mathbf{F} := \langle \mathbb{Z}_q, +, \cdot \rangle$. For $k \in \mathbb{Z}_p$ we define $e_k \in M$ by

$$e_k((x,y)) = \begin{cases} (0,1) & \text{if } x = k, \\ (0,0) & \text{otherwise.} \end{cases}$$

Since all functions in M are constant on the cosets of A in V, we have that $\langle e_k \mid k \in \mathbb{Z}_p \rangle$ is a basis for M over $\mathbf{F}$. Let $G := \{g_{a,b} : \mathbb{Z}_p \to \mathbb{Z}_p,\ x \mapsto ax + b \mid a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p\}$. Then $\mathbf{G} := \langle G, \circ \rangle$ is the group of affine transformations on the field $\langle \mathbb{Z}_p, +, \cdot \rangle$. We define a group action of $\mathbf{G}$ on the basis of M by $g * e_k := e_{g(k)}$ for $g \in G, k \in \mathbb{Z}_p$. Now M forms a left $\mathbf{F}[\mathbf{G}]$-module of dimension p over $\mathbf{F}$. We note that for $f \in M, g \in G$ we have

$$(5.7) \qquad (g * f)((x,y)) = f((g^{-1}(x), y)) \text{ for all } x \in \mathbb{Z}_p, y \in \mathbb{Z}_q.$$

We claim that

$$(5.8) \qquad N := \mathrm{Pol}_1(\mathbf{V}) \cap M \text{ is an } \mathbf{F}[\mathbf{G}]\text{-submodule of } M.$$

Obviously N is an $\mathbf{F}$-subspace of M. We note that $G \subseteq \mathrm{Pol}_1(\langle \mathbb{Z}_p, + \rangle)$ and that the projections $(x,y) \mapsto (x,0)$ and $(x,y) \mapsto (0,y)$ are polynomial functions on $\mathbf{V}$. Then the map $V \to V, (x,y) \to (g^{-1}(x), y)$ is in $\mathrm{Pol}_1(\mathbf{V})$ for all $g \in G$. Hence, by (5.7), we have $g * f \in \mathrm{Pol}_1(\mathbf{V})$ for all $f \in N, g \in G$. This proves (5.8).

Let $s := \sum_{k \in \mathbb{Z}_p} e_k$. Then Fs is an $\mathbf{F}[\mathbf{G}]$-submodule of N. By Lemma 5.1 M/Fs is a simple $\mathbf{F}[\mathbf{G}]$-module. To obtain $N = M$, it then suffices to show that

$$(5.9) \qquad N \not\leq Fs.$$

To this end we let $c \in \mathrm{Pol}_2(\mathbf{V})$ be such that $c(x,0) = c(0,x) = 0$ for all $x \in V$, and we let $a, b \in V$ be such that $p \cdot c(a,b) \neq 0$. Such c, a, b exist by the assumption that $[\![V,V]\!]_{\mathbf{V}} \geq A$. The function $f : V \to V,\ x \mapsto p \cdot c(x,b)$, is in $\mathrm{Pol}_1(\mathbf{V})$ and satisfies $f(V \setminus A) \neq \{0\}$ and $f(A) = \{0\}$ because of $[\![V,A]\!]_{\mathbf{V}} = 0$. Hence we have $f \in N \setminus Fs$. This proves (5.9). Thus $N = M$ by Lemma 5.1 and $M \subseteq \mathrm{Pol}_1(\mathbf{V})$. □

In the following we construct k-ary polynomial functions.

Lemma 5.3. *For primes p, q let $\mathbf{V}$ be an expanded group with group reduct $\langle \mathbb{Z}_p \times \mathbb{Z}_q, + \rangle$, and let $A := 0 \times \mathbb{Z}_q$. Let $k \in \mathbb{N}, k > 1$. We assume that there exists $f \in \mathrm{Pol}_{k-1}(\mathbf{V})$ such that $f(x) = (0,1)$ for all $x \in A^{k-1}$ and $f(x) = (0,0)$ for all $x \in V^{k-1} \setminus A^{k-1}$.*

Then there exists a polynomial function $g \in \mathrm{Pol}_k(\mathbf{V})$ such that $g(x) = (0,p)$ for all $x \in A^k$ and $g(x) = (0,0)$ for all $x \in V^k \setminus A^k$.

Proof: We define $g : V^k \to V$ by

$$\begin{aligned} g(x_1, \ldots, x_k) := \ & \textstyle\sum_{i=1}^{p-1} f(x_1, \ldots, x_{k-2}, x_k - i x_{k-1}) \\ & - \textstyle\sum_{i=1}^{p-1} f(x_1, \ldots, x_{k-2}, x_k - (i,0)) + f(x_1, \ldots, x_{k-2}, x_{k-1}). \end{aligned}$$

Then g is in $\mathrm{Pol}_k(\mathbf{V})$.

First we assume that $x_1, \ldots, x_k \in A$. By the definition of f we obtain $g(x_1, \ldots, x_k) = (p-1)(0,1) - (p-1)(0,0) + (0,1) = (0,p)$. Obviously we have $g(x_1, \ldots, x_k) = (0,0)$ if $(x_1, \ldots, x_{k-2}) \notin A^{k-2}$. So for all of the following we assume that $x_1, \ldots, x_{k-2} \in A$. We consider the case that $x_{k-1} \in A, x_k \in V \setminus A$. Then there is no $i \in \{1, \ldots, p-1\}$ such that $x_k - i x_{k-1} \in A$. Since we have a unique element $i \in \{1, \ldots, p-1\}$ such that $x_k - (i,0) \in A$, we find $g(x_1, \ldots, x_k) = (0,0) - (0,1) + (0,1) = (0,0)$.

Next we consider $x_{k-1} \in V \setminus A, x_k \in A$. Then neither $x_k - i x_{k-1}$ nor $x_k - (i,0)$ are contained in A for any $i \in \{1, \ldots, p-1\}$. Consequently $g(x_1, \ldots, x_k) = (0,0)$.

Finally we let $x_{k-1}, x_k \in V \setminus A$. Then we have uniquely determined elements $i, j \in \{1, \ldots, p-1\}$ such that $x_k - i x_{k-1} \in A$ and $x_k - (j,0) \in A$. Hence $g(x_1, \ldots, x_k) = (0,1) - (0,1) + (0,0) = (0,0)$. Thus g satisfies the assertions of the lemma. □

Lemma 5.4. *Let p, q be distinct primes, let $\mathbf{V}$ be an expanded group with cyclic group reduct of order pq, and let $A = pV$. We assume that A is an ideal of $\mathbf{V}$ and that $[\![V, V]\!]_{\mathbf{V}} \geq A$ and $[\![V, A]\!]_{\mathbf{V}} = 0$.*

Then we have

(5.10)

$$\{f \in A^{V^k} \mid f(x+a) = f(x) - f(0) + f(a) \text{ for all } x \in V^k, a \in A^k\} \subseteq \mathrm{Pol}_k(\mathbf{V})$$

for all $k \in \mathbb{N}$.

Proof: First we show that

$$\{f \in A^{V^k} \mid f(x+a) = f(x) \text{ for all } x \in V^k, a \in A^k\} \subseteq \mathrm{Pol}_k(\mathbf{V}) \tag{5.11}$$

by induction on k. For $k = 1$ we have (5.11) by Lemma 5.2. We now assume that $k > 1$. By the induction hypothesis the assumptions of Lemma 5.3 are satisfied.

Hence we have $g \in \mathrm{Pol}_k(\mathbf{V})$ such that $g(x) = (0, p)$ for $x \in A^k$ and $g(x) = (0, 0)$ else. Since $p \neq q$, we find that all functions from V^k to A that are constant on A^k and map $V^k \setminus A^k$ to 0 are polynomial functions. Hence all functions from V^k to A that are constant on one coset of A^k and 0 elsewhere are in $\mathrm{Pol}_k(\mathbf{V})$. This yields (5.11).

We now let $f \in A^{V^k}$ such that $f(x+a) = f(x) - f(0) + f(a)$ for all $x \in V^k, a \in A^k$. Then the restriction of f to A^k is affine, that is, we have $c_1, \ldots, c_k \in \mathbb{Z}$ such that $f((a_1, \ldots, a_k)) = \sum_{i=1}^{k} c_i a_i + f(0)$ for all $a_1, \ldots, a_k \in A$. Since $p \neq q$, we have some $r \in \mathbb{Z}$ such that $r \equiv 0 \pmod{p}$ and $r \equiv 1 \pmod{q}$. We consider

$$h : V^k \to A,\ (x_1, \ldots, x_k) \mapsto r \cdot (\sum_{i=1}^{k} c_i x_i + f(0)).$$

Then we have $f(a) = h(a)$ for all $a \in A^k$. Further h is an affine function on $\langle V^k, + \rangle$. For $x \in V^k, a \in A^k$ we obtain

$$\begin{aligned} (f-h)(x+a) &= f(x+a) - h(x+a) \\ &= f(x) - f(0) + f(a) - (h(x) - h(0) + h(a)) \\ &= (f-h)(x). \end{aligned}$$

Thus $f - h$ is in $\mathrm{Pol}_k(\mathbf{V})$ by (5.11). Since h is polynomial, we have $f \in \mathrm{Pol}_k(\mathbf{V})$. □

Now we can prove the main result of this section.

Lemma 5.5. *Let p, q be primes with $p \neq q$, and let $\mathbf{V}$ be an expanded group with $|V| = pq$. We assume that $\mathbf{Con}(\mathbf{V})$ is isomorphic to a three element chain and that the monolith μ of $\mathbf{V}$ is central. Then every commutator preserving function of $\mathbf{V}$ is a polynomial function of $\mathbf{V}$.*

Proof: We note that $\mathbf{V}$ has a cyclic group reduct by the assumptions. Let $f : V^k \to V$ be a commutator preserving function of $\mathbf{V}$. Then we may define $f_\mu : (V/\mu)^k \to V/\mu,\ \bar{x}/\mu \mapsto f(\bar{x})/\mu$. Since $\mathbf{V}/\mu$ is simple and has a cyclic group reduct, f_μ is in $\mathrm{Pol}_k(\mathbf{V}/\mu)$. Hence we have $g \in \mathrm{Pol}_k(\mathbf{V})$ such that $f_\mu = g_\mu$ on V/μ. Let $A := \gamma^{-1}(\mu)$. Then $f - g : V^k \to V, x \mapsto f(x) - g(x)$, satisfies $(f-g)(V^k) \subseteq A$. Since $f - g$ is commutator preserving, it preserves $\rho(1, \mu, 0, m)$ with $m(x, y, z) = x - y + z$ by Lemma 2.6. Hence $(f-g)(x) - (f-g)(0) + (f-g)(a) = (f-g)(x - 0 + a)$ for all $x \in V^k, a \in A^k$. By Lemma 5.4 we have $f - g \in \mathrm{Pol}_k(\mathbf{V})$. Since $g \in \mathrm{Pol}_k(\mathbf{V})$, we obtain $f \in \mathrm{Pol}_k(\mathbf{V})$. □

6. Clones of commutator preserving operations

By Lemmas 4.1 and 5.5 we have proved that each clone extending $\mathrm{Pol}(\langle \mathbb{Z}_{pq}, + \rangle)$ is the clone of commutator preserving operations of some expansion of the group $\langle \mathbb{Z}_{pq}, + \rangle$. In this section we determine the inclusions among these clones. Let $\mathbf{A}$

be an algebra, and let m be a Mal'cev polynomial of $\mathbf{A}$. We abbreviate the set of *commutator preserving operations on* $\mathbf{A}$ by $\mathrm{CP}(\mathbf{A})$. Then Lemma 2.6 tells that we have $\mathrm{CP}(\mathbf{A}) = \mathrm{Comp}(A, \mathrm{Con}(\mathbf{A}) \cup \mathrm{Cen}(\mathbf{A}, m))$.

Lemma 6.1. *Let* $\mathbf{A}$ *be an algebra that has a Mal'cev polynomial, and let* $\mathbf{A}^*$ *be the algebra* $\langle A, \mathrm{CP}(\mathbf{A})\rangle$. *Then* $\mathbf{Con}^*(\mathbf{A}^*) = \mathbf{Con}^*(\mathbf{A})$.

Proof: Every fundamental operation of $\mathbf{A}$ is in $\mathrm{CP}(\mathbf{A})$ and is therefore a fundamental operation of $\mathbf{A}^*$. Hence $\mathbf{A}^*$ is an expansion of $\mathbf{A}$ and $\mathrm{Con}(\mathbf{A}^*) \subseteq \mathrm{Con}(\mathbf{A})$. In order to show $\mathrm{Con}(\mathbf{A}) \subseteq \mathrm{Con}(\mathbf{A}^*)$, we let α be a congruence of $\mathbf{A}$. By the definition of $\mathbf{A}^*$ every fundamental operation of $\mathbf{A}^*$ preserves α. Therefore $\alpha \in \mathrm{Con}(\mathbf{A}^*)$. Thus $\mathrm{Con}(\mathbf{A}^*) = \mathrm{Con}(\mathbf{A})$. Now we show that the commutators are the same. To this end we show that for all $\alpha, \beta, \eta \in \mathrm{Con}(\mathbf{A})$, α centralizes β modulo η in $\mathbf{A}$ if and only if α centralizes β modulo η in $\mathbf{A}^*$. The "if"-direction follows immediately from the fact that $\mathbf{A}$ is a reduct of $\mathbf{A}^*$. For the "only if"-direction we let m be a Mal'cev polynomial of $\mathbf{A}$. We assume that α centralizes β modulo η in $\mathbf{A}$. Then $\rho(\alpha, \beta, \eta, m)$ is in $\mathrm{Cen}(\mathbf{A}, m)$. Since every fundamental operation (and therefore every polynomial operation) of $\mathbf{A}^*$ preserves the relations in $\mathrm{Cen}(\mathbf{A}, m)$, Lemma 2.4 yields that α centralizes β modulo η in $\mathbf{A}^*$. □

Lemma 6.2. *Let* $\mathbf{A}$ *be an algebra, and let* m *be a Mal'cev polynomial on* A. *Let* $\mathbf{A}_1$ *and* $\mathbf{A}_2$ *be two expansions of* $\mathbf{A}$. *Then the following are equivalent:*

(1) $\mathrm{CP}(\mathbf{A}_1) \subseteq \mathrm{CP}(\mathbf{A}_2)$;
(2) $\mathrm{Con}(\mathbf{A}_2) \subseteq \mathrm{Con}(\mathbf{A}_1)$ *and* $[\alpha, \beta]_{\mathbf{A}_2} \geq [\alpha, \beta]_{\mathbf{A}_1}$ *for all* $\alpha, \beta \in \mathrm{Con}(\mathbf{A}_2)$;
(3) $\mathrm{Con}(\mathbf{A}_2) \subseteq \mathrm{Con}(\mathbf{A}_1)$ *and* $\mathrm{Cen}(\mathbf{A}_2, m) \subseteq \mathrm{Cen}(\mathbf{A}_1, m)$.

Proof: (1)⇒(2): For $i \in \{1, 2\}$ let $\mathbf{B}_i := \langle A, \mathrm{CP}(\mathbf{A}_i)\rangle$. By Lemma 6.1 we have

$$\mathbf{Con}^*(\mathbf{B}_i) = \mathbf{Con}^*(\mathbf{A}_i) \text{ for } i = 1, 2. \tag{6.1}$$

Since $\mathbf{B}_2$ is an expansion of $\mathbf{B}_1$, we have $\mathrm{Con}(\mathbf{B}_2) \subseteq \mathrm{Con}(\mathbf{B}_1)$. Next we fix $\alpha, \beta \in \mathrm{Con}(\mathbf{A}_2)$ and show

$$[\alpha, \beta]_{\mathbf{B}_2} \geq [\alpha, \beta]_{\mathbf{B}_1}.$$

We know that α centralizes β modulo $[\alpha, \beta]_{\mathbf{B}_2}$ in $\mathbf{B}_2$. Since $\mathbf{B}_1$ is a reduct of $\mathbf{B}_2$, α centralizes β modulo $[\alpha, \beta]_{\mathbf{B}_2}$ in $\mathbf{B}_1$. Hence we have $[\alpha, \beta]_{\mathbf{B}_1} \leq [\alpha, \beta]_{\mathbf{B}_2}$.

(2)⇒(3): Let ρ be in $\mathrm{Cen}(\mathbf{A}_2, m)$. Then there are $\alpha, \beta, \eta \in \mathrm{Con}(\mathbf{A}_2)$ such that α centralizes β modulo η in $\mathbf{A}_2$ and $\rho = \rho(\alpha, \beta, \eta, m)$. We have $[\alpha, \beta]_{\mathbf{A}_2} \leq \eta$ and therefore $[\alpha, \beta]_{\mathbf{A}_1} \leq \eta$. By Proposition 2.3 we obtain that α centralizes β modulo η in $\mathbf{A}_1$ and therefore $\rho \in \mathrm{Cen}(\mathbf{A}_1, m)$.

The implication (3)⇒(1) is immediate. □

7. Proofs for the results of section 1

We will now prove the main result of the present paper.

Proof of Theorem 1.1: The implication (1)$\Rightarrow$(2) is obvious.

(2)$\Rightarrow$(3): It is known that the congruences of every algebra are determined by its unary polynomial functions [17, Theorem 4.19]. By Lemma 2.9 the commutator operation on every expanded group is determined by its binary polynomial functions. Thus we have $\mathbf{Con}^*(\mathbf{V}_1) = \mathbf{Con}^*(\mathbf{V}_2)$.

(3)$\Rightarrow$(1): Let $m(x, y, z) := x - y + z$ for all $x, y, z \in V$. By Lemma 4.1 and Lemma 5.5 we have

$$\mathrm{Pol}(\mathbf{V}_i) = \mathrm{CP}(\mathbf{V}_i) \text{ for } i = 1, 2.$$

Now (2)$\Rightarrow$(1) of Lemma 6.2 yields $\mathrm{CP}(\mathbf{V}_1) = \mathrm{CP}(\mathbf{V}_2)$. □

We will now show that for all primes p, q with $p \neq q$ there are precisely 17 clones extending $\mathrm{Pol}(\langle \mathbb{Z}_{pq}, +\rangle)$. From Theorem 1.1 we know that each such clone $\mathcal{C}$ is determined by $\mathbf{Con}^*(\langle \mathbb{Z}_{pq}, \mathcal{C}\rangle)$. Some easy checking shows that Figure 1 actually exhibits all sublattices of $\mathbf{Con}(\langle \mathbb{Z}_{pq}, +\rangle)$ with all conceivable commutator operations. We notice that the commutator operation must be monotonous in each argument, commutative, distributive with respect to joins, and that the commutator of two congruences is always contained in their meet. Since the clones of polynomial functions are exactly those of the commutator preserving functions, we see from Lemma 6.2 that the inclusions are those indicated in Figure 1. What we still need to prove is that for each lattice with commutator operation $\mathbf{L}$ drawn in Figure 1 there really is a clone $\mathcal{C}$ that contains the addition such that $\mathbf{Con}^*(\langle \mathbb{Z}_{pq}, \mathcal{C}\rangle) = \mathbf{L}$. We will produce generators for each of these clones. The following lemma will help in building new clones from existing ones.

Lemma 7.1. *Let* $\mathbf{A}$ *be an algebra with a Mal'cev polynomial* m*, let* $\mathbf{A}_1 = \langle A, F_1\rangle$ *and* $\mathbf{A}_2 = \langle A, F_2\rangle$ *be expansions of* $\mathbf{A}$*, and let* $\mathbf{A}_1 + \mathbf{A}_2$ *be the algebra* $\langle A, F_1 \cup F_2\rangle$*. Then we have:*

(1) $\mathrm{Con}(\mathbf{A}_1 + \mathbf{A}_2) = \mathrm{Con}(\mathbf{A}_1) \cap \mathrm{Con}(\mathbf{A}_2)$.
(2) *For all* $\alpha, \beta \in \mathrm{Con}(\mathbf{A}_1 + \mathbf{A}_2)$ *we have*

$$[\alpha, \beta]_{\mathbf{A}_1+\mathbf{A}_2} = \inf \{\eta \in \mathrm{Con}(\mathbf{A}_1 + \mathbf{A}_2) \mid [\alpha, \beta]_{\mathbf{A}_1} \subseteq \eta \text{ and } [\alpha, \beta]_{\mathbf{A}_2} \subseteq \eta\}. \tag{7.1}$$

Proof: Item (1) is obvious. For proving (2), we fix $\alpha, \beta \in \mathrm{Con}(\mathbf{A}_1) \cap \mathrm{Con}(\mathbf{A}_2)$. From the fact that $\mathbf{A}_1 + \mathbf{A}_2$ is an expansion of $\mathbf{A}_1$ we obtain $[\alpha, \beta]_{\mathbf{A}_1} \leq [\alpha, \beta]_{\mathbf{A}_1+\mathbf{A}_2}$, and similarly $[\alpha, \beta]_{\mathbf{A}_2} \leq [\alpha, \beta]_{\mathbf{A}_1+\mathbf{A}_2}$. Hence we have $\inf \{\eta \in \mathrm{Con}(\mathbf{A}_1 + \mathbf{A}_2) \mid [\alpha, \beta]_{\mathbf{A}_1} \leq \eta \text{ and } [\alpha, \beta]_{\mathbf{A}_2} \leq \eta\} \leq [\alpha, \beta]_{\mathbf{A}_1+\mathbf{A}_2}$. For proving the converse inclusion, let $\eta \in \mathrm{Con}(\mathbf{A}_1) \cap \mathrm{Con}(\mathbf{A}_2)$ be such that $[\alpha, \beta]_{\mathbf{A}_1} \leq \eta$ and $[\alpha, \beta]_{\mathbf{A}_2} \leq \eta$. Then every function $f \in \mathrm{Pol}(\mathbf{A}_1 + \mathbf{A}_2)$ preserves the relation $\rho(\alpha, \beta, \eta, m)$. Therefore we have $[\alpha, \beta]_{\mathbf{A}_1+\mathbf{A}_2} \leq \eta$ by Lemma 2.4. This establishes $\leq$ of equation (7.1). □

Proof of Corollary 1.2: Let $\mathbf{V} := \langle \mathbb{Z}_p \times \mathbb{Z}_q, +\rangle$, let α be the kernel of the first projection mapping $\pi_1 : \mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{Z}_p, \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \mapsto x$, let β be the kernel of the second projection mapping, and let $m(x, y, z) := x - y + z$. We will now produce generators for clones $\mathcal{C}$ on V that have the following congruence lattices and commutators.

(1) $\operatorname{Con}(\langle V, \mathcal{C}\rangle) = \{0, \alpha, \beta, 1\}$, $[1, 1] = 0$: We take $\mathcal{C} := \operatorname{Pol}(\langle V, +\rangle)$.

(2) $\operatorname{Con}(\langle V, \mathcal{C}\rangle) = \{0, \alpha, 1\}$, $[1, 1] = \alpha$, $[1, \alpha] = 0$: Let f be the function on $\mathbb{Z}_p \times \mathbb{Z}_q$ defined by

$$f(\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)) = \begin{cases} \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) & \text{if } x = 0, \\ \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right) & \text{else.} \end{cases}$$

We claim that $\mathcal{C} := \operatorname{Pol}(\langle V, +, f\rangle)$ has the required properties The function f preserves α because it maps V into one coset of α. Since $(\left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)) \in \beta$ and $(\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)) \notin \beta$, the function f does not preserve β. From the fact that f maps V into one coset of α, we see that f preserves $\rho(1, 1, \alpha, m)$, hence $[1, 1] \leq \alpha$. Brief calculations show that f preserves $\rho(1, \alpha, 0, m)$, hence $[1, \alpha] = 0$. By Lemma 3.1 the equation $[1, 1] = 0$ would lead to the contradiction $\beta \in \operatorname{Con}(\langle V, +, f\rangle)$. Hence $[1, 1] = \alpha$.

(3) $\operatorname{Con}(\langle V, \mathcal{C}\rangle) = \{0, \alpha, \beta, 1\}$, $[\alpha, \alpha] = 0$, $[\beta, \beta] = \beta$: This lattice and its commutators is realized by the direct product of the field of size p and the zero-ring of size q. For $p > 2$ we may also use the function $f : \mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{Z}_p \times \mathbb{Z}_q, \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} x^2 \\ 0 \end{smallmatrix}\right)$ and obtain that $\operatorname{Pol}(\langle V, +, f\rangle)$ has the required properties.

(4) $\operatorname{Con}(\langle V, \mathcal{C}\rangle) = \{0, \alpha, \beta, 1\}$, $[\alpha, \alpha] = \alpha$, $[\beta, \beta] = 0$: This case is symmetric to case (3).

(5) $\operatorname{Con}(\langle V, \mathcal{C}\rangle) = \{0, \beta, 1\}$, $[1, 1] = \beta$, $[1, \beta] = 0$: This case is symmetric to case (2).

(6) $\operatorname{Con}(\langle V, \mathcal{C}\rangle) = \{0, \alpha, 1\}$, $[1, 1] = \alpha$, $[1, \alpha] = \alpha$, $[\alpha, \alpha] = 0$: Let f be the function on $\mathbb{Z}_p \times \mathbb{Z}_q$ defined by

$$f(\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)) = \begin{cases} \left(\begin{smallmatrix} 0 \\ y \end{smallmatrix}\right) & \text{if } x = 0, \\ \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right) & \text{else.} \end{cases}$$

We consider $\langle V, +, f\rangle$. The function f preserves α because it maps V into one coset of α. Since $(\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)) \in \beta$ and $(\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)) \notin \beta$, the function f does not preserve β. From the fact that f maps V into one coset of α, we see that f preserves $\rho(1, 1, \alpha, m)$, hence $[1, 1] \leq \alpha$. Now we show $[1, \alpha] \neq 0$. To this end we show that f does not preserve $\rho(1, \alpha, 0, m)$. We have $(\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)) \in \rho(1, \alpha, 0, m)$ but $(\left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)) \notin \rho(1, \alpha, 0, m)$. For proving $[\alpha, \alpha] = 0$, one can check that f preserves $\rho(\alpha, \alpha, 0, m)$. Thus $\mathcal{C} := \operatorname{Pol}(\langle V, +, f\rangle)$ realizes this congruence lattice.

(7) $\operatorname{Con}(\langle V, \mathcal{C}\rangle) = \{0, \beta, 1\}$, $[1, 1] = \beta$, $[1, \beta] = \beta$, $[\beta, \beta] = 0$: This case is symmetric to case (6).

All other lattices and commutator operations drawn in Figure 1 can be obtained from the listed clones using Lemma 7.1. □

Since for $p > 2$, $q > 2$ the 17 indicated clones differ in their unary parts, we obtain the following corollary.

Corollary 7.2. *Let p, q be odd primes with $p \neq q$, let $\mathrm{M}_{\mathrm{aff}}(\mathbb{Z}_{pq}) := \mathrm{Pol}_1(\langle \mathbb{Z}_{pq}, + \rangle)$, and let $\mathrm{M}(\mathbb{Z}_{pq}) := \{f \,|\, f : \mathbb{Z}_{pq} \to \mathbb{Z}_{pq}\}$. Then there are exactly 17 subnear-rings of $\langle \mathrm{M}(\mathbb{Z}_{pq}), +, \circ \rangle$ that contain $\mathrm{M}_{\mathrm{aff}}(\mathbb{Z}_{pq})$.*

Proof: We map each clone $\mathcal{C}$ that extends $\mathrm{Pol}(\langle \mathbb{Z}_{pq}, + \rangle)$ to the set $\mathcal{C}_1$ of all unary functions in $\mathcal{C}$. By [8, Lemma 1 (3)] this mapping is a surjection onto the near-rings between $\mathrm{M}_{\mathrm{aff}}(\mathbb{Z}_{pq})$ and $\mathrm{M}(\mathbb{Z}_{pq})$. Now we have to show that all 17 clones produce different near-rings. Suppose that $\mathcal{C}$ and $\mathcal{D}$ are two clones extending $\mathrm{Pol}(\langle \mathbb{Z}_{pq}, + \rangle)$ that have the same set of unary operations. From the construction of the 17 clones given in the proof of Corollary 1.2, we see that for $p \geq 3$, $q \geq 3$ each of the 17 clones is generated by $+$ and its set of unary functions. Hence $\mathcal{C} = \mathcal{D}$. □

Using [6, Proposition 5.3], one obtains from this result that for odd primes p, q with $p \neq q$ there are exactly 17 nonisomorphic zerosymmetric near-rings N with identity that have $\langle \mathbb{Z}_{pq}, + \rangle$ as a compatible and faithful N-group.

The proof of our final Corollary 1.3 is immediate from Theorem 1.1.

Proof of Corollary 1.3: There are only finitely many group operations on a set with pq elements. By Theorem 1.1 each of those is contained in only finitely many constantive clones. □

References

[1] W. A. Adkins and S. H. Weintraub. *Algebra. An approach via module theory.* Springer-Verlag, New York, 1992.

[2] 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*, pages 21–25, North-Holland, Amsterdam, 1986.

[3] E. Aichinger. On Hagemann's and Herrmann's characterization of strictly affine complete algebras. *Algebra Universalis*, 44:105–121, 2000.

[4] E. Aichinger. On near-ring idempotents and polynomials on direct products of Ω-groups. *Proc. Edinburgh Math. Soc. (2)*, 44:379–388, 2001.

[5] E. Aichinger. On the maximal ideals of non-zero-symmetric near-rings and of composition algebras of polynomial functions on Ω-groups. *Quaest. Math.*, 24(4):453–480, 2001.

[6] E. Aichinger. A bound on the number of unary polynomial functions and a decidability result for near-rings. *International Journal of Algebra and Computation*, 15(2):279–289, 2005.

[7] E. Aichinger and P. M. Idziak. Polynomial interpolation in expanded groups. *J. Algebra*, 271(1):65–107, 2004.

[8] E. Aichinger, D. Mašulović, R. Pöschel, and J. S. Wilson. Completeness for concrete near-rings. *J. Algebra*, 279(1):61–78, 2004.

[9] A. 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(2):193–221, 2002. Multiple-valued logic in Eastern Europe.

[10] A. A. Bulatov and P. M. Idziak. Counting Mal'tsev clones on small sets. *Discrete Math.*, 268(1-3):59–80, 2003.

[11] R. Freese and R. N. McKenzie. *Commutator Theory for Congruence Modular varieties*, volume 125 of *London Math. Soc. Lecture Note Ser.* Cambridge University Press, 1987.

[12] J. Hagemann and C. Herrmann. Arithmetical locally equational classes and representation of partial functions. In *Universal Algebra, Esztergom (Hungary)*, volume 29, pages 345–360, Colloq. Math. Soc. János Bolyai, 1982.

[13] D. Hobby and R. McKenzie. *The structure of finite algebras*, volume 76 of *Contemporary mathematics*. American Mathematical Society, 1988.

[14] P. M. Idziak. Clones containing Mal'tsev operations. *Internat. J. Algebra Comput.*, 9(2):213–226, 1999.

[15] P. M. Idziak and K. Słomczyńska. Polynomially rich algebras. *J. Pure Appl. Algebra*, 156(1):33–68, 2001.

[16] E. W. Kiss. Three remarks on the modular commutator. *Algebra Universalis*, 29(4):455–476, 1992.

[17] R. N. McKenzie, G. F. McNulty, and W. F. Taylor. *Algebras, lattices, varieties, Volume I.* Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, California, 1987.

[18] G. F. Pilz. *Near-rings.* North-Holland Publishing Company – Amsterdam, New York, Oxford, 2nd edition, 1983.

[19] S. D. Scott. The structure of Ω-groups. In *Nearrings, nearfields and K-loops (Hamburg, 1995)*, pages 47–137, Kluwer Acad. Publ., Dordrecht, 1997.

Institut für Algebra
Johannes Kepler Universität Linz
4040 Linz, Austria
E-mail: erhard@algebra.uni-linz.ac.at
E-mail: peter.mayr@algebra.uni-linz.ac.at