Algebra Univers. 65 (2011) 193–211
DOI 10.1007/s00012-011-0124-5
Published online March 25, 2011

Algebra Universalis

Mal'cev algebras with supernilpotent centralizers

Peter Mayr

Abstract. Let $\mathbf{A}$ be a finite algebra in a congruence permutable variety. We assume that for every subdirectly irreducible homomorphic image of $\mathbf{A}$ the centralizer of the monolith is n-supernilpotent. Then the clone of polynomial functions on $\mathbf{A}$ is determined by relations of arity $|A|^{n+1}$. As consequences we obtain finite implicit descriptions of the polynomial functions on finite local rings with 1 and on finite groups $\mathbf{G}$ such that in every subdirectly irreducible quotient of $\mathbf{G}$ the centralizer of the monolith is a p-group.

1. Introduction

Let $\mathbf{R} := \langle R, +, -, \cdot \rangle$ be a finite ring, and let $f\colon R^k \to R$ be a function. How can we decide whether f is polynomial over $\mathbf{R}$?

A straightforward approach is to check whether f can be interpolated by a polynomial function in arbitrarily many places. If $\mathbf{R}$ is a finite field, then every f is polynomial by Lagrange interpolation. For finite local rings with 1 we will determine a number m that is independent of the arity of f such that f is polynomial whenever it can be interpolated by some polynomial function in every set of at most m points. In particular we obtain the following.

Theorem 1.1. *Let $\mathbf{R}$ be a finite local ring with 1, and let $n \in \mathbb{N}_0$ be such that the Jacobson radical J of $\mathbf{R}$ satisfies $J^{n+1} = 0$. Then a function $f\colon R^k \to R$ is polynomial on $\mathbf{R}$ if and only if for all $S \subseteq R^k$ with $|S| \leq |R|^n$ there exists a polynomial function p on $\mathbf{R}$ such that $f|_S = p|_S$.*

Since every finite commutative ring with 1 is a direct product of local rings, we may also replace "local" with "commutative" in the assumptions of the previous result (see Corollary 6.2).

We will prove Theorem 1.1 in Section 6. In fact our techniques yield a similar finite implicit description of polynomial functions on other algebraic structures, like the finite groups all of whose Sylow subgroups are abelian

Presented by Á. Szendrei.
Received November 3, 2009; accepted in final form March 31, 2010.
2010 *Mathematics Subject Classification*: Primary: 08A40; Secondary: 13M10.
Key words and phrases: polynomial functions, interpolation, Mal'cev algebras.
The author acknowledges support from the Austrian Science Fund (Erwin-Schrödinger-Grant J2637-N18), the University of Colorado at Boulder and from the Portuguese Project ISFL-1-143 of CAUL financed by FCT and FEDER.

Birkhäuser

(Corollary 2.6) or, more generally, the Mal'cev algebras all of whose subdirectly irreducible factors have a monolith with a so-called supernilpotent centralizer (Theorem 2.1). We will define these notions and develop the necessary machinery in the next section.

2. Polynomial functions on Mal'cev algebras

The set of *polynomial functions* $\mathrm{Pol}(\mathbf{A})$ on an algebraic structure $\mathbf{A} := \langle A, F\rangle$ is formed by the fundamental operations F, the constant functions on A, the projections from A^k to A for $k \in \mathbb{N}$, and all compositions thereof (see [18, Definition 4.4]). Such a set of finitary functions is called a clone. For $A = \mathbb{Z}$ and $F = \{+, -, \cdot\}$ this defines exactly the classical polynomial functions on the ring $\langle \mathbb{Z}, +, -, \cdot\rangle$. As an example of a polynomial clone on a group, $\mathrm{Pol}(\langle \mathbb{Z}, +, -\rangle)$ is the set of affine functions on $\mathbb{Z}$ (corresponding to the ring polynomials of degree at most 1). The clone of *term functions* $\mathrm{Clo}(\mathbf{A})$ on $\mathbf{A}$ is generated by the fundamental operations F of $\mathbf{A}$ [18, Definition 4.2].

We study clones in order to classify algebras with respect to their structure and independent of their specific fundamental operations. Algebras that have the same polynomial functions, like a Boolean algebra and the corresponding Boolean ring, are said to be *polynomially equivalent* [18, Definition 4.139].

On a finite set A a clone can be described explicitly by its generating functions or implicitly by its invariant relations. For every finite algebra in a congruence permutable variety considered so far, the polynomial clone is already characterized by a finite number of finitary relations. We then say that $\mathrm{Pol}(\mathbf{A})$ is *finitely related*. A ternary function f on a set A is said to be a *Mal'cev function* if $f(x, y, y) = f(y, y, x) = x$ for all $x, y \in A$. Recall that an algebra $\mathbf{A}$ generates a congruence permutable variety if and only if it has a term function that is a Mal'cev function. In that case we call $\mathbf{A}$ a *Mal'cev algebra*. For every group $\langle G, \cdot, ^{-1}\rangle$ we have a polynomial Mal'cev function defined by $f(x, y, z) := xy^{-1}z$. If every finite Mal'cev algebra were finitely related, this would yield an affirmative answer to the following question of Idziak [10, Question 13]: Is the number of finite Mal'cev algebras up to polynomial equivalence countable?

Apart from [16], all descriptions of polynomial functions on Mal'cev algebras that we know of rely on commutator theory to some extent. In particular, algebras whose subdirectly irreducible quotients have monoliths with well-behaved centralizers were studied successfully: if every such centralizer is trivial, the algebra is affine complete (every congruence preserving function is polynomial) [9]; if every such centralizer is contained in the monolith, the algebra is weakly polynomial rich (every congruence preserving and extended type preserving function is polynomial) [11]. In this paper we will extend these kind of results by describing polynomial functions on algebras whose subdirectly irreducible quotients have monoliths with abelian (more general, supernilpotent) centralizers. For that we will need the notion of higher commutators as suggested by Bulatov in [6]. This generalizes the binary commutator for congruences on algebraic structures as developed in [8] or [18, Section 4.13]. Let $\mathbf{A}$ be an algebra, let $\operatorname{Con}(\mathbf{A})$ denote the set of congruences of $\mathbf{A}$. For $n \in \mathbb{N}$, $\alpha_1, \dots, \alpha_n \in \operatorname{Con}(\mathbf{A})$, we let $M_{\mathbf{A}}(\alpha_1, \dots, \alpha_n)$ denote the subalgebra of $\mathbf{A}^{2^{n-1} \times 2}$ that is generated by all the elements

$$\begin{pmatrix} a_1 & a_1 \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ a_1 & a_1 \\ b_1 & b_1 \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ b_1 & b_1 \end{pmatrix}, \begin{pmatrix} a_2 & a_2 \\ \vdots & \vdots \\ \vdots & \vdots \\ a_2 & a_2 \\ b_2 & b_2 \\ \vdots & \vdots \\ \vdots & \vdots \\ b_2 & b_2 \\ a_2 & a_2 \\ \vdots & \vdots \\ \vdots & \vdots \\ a_2 & a_2 \\ b_2 & b_2 \\ \vdots & \vdots \\ \vdots & \vdots \\ b_2 & b_2 \end{pmatrix}, \dots, \begin{pmatrix} a_{n-1} & a_{n-1} \\ b_{n-1} & b_{n-1} \\ a_{n-1} & a_{n-1} \\ b_{n-1} & b_{n-1} \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ a_{n-1} & a_{n-1} \\ b_{n-1} & b_{n-1} \end{pmatrix}, \begin{pmatrix} a_n & b_n \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ a_n & b_n \end{pmatrix} \in A^{2^{n-1} \times 2} \tag{2.1}$$

such that $(a_i, b_i) \in \alpha_i$ for all $i \in \{1, \dots, n\}$. The *n-ary commutator* $[\alpha_1, \dots, \alpha_n]$ is defined as the smallest $\eta \in \operatorname{Con}(\mathbf{A})$ such that for every $x \in M_{\mathbf{A}}(\alpha_1, \dots, \alpha_n)$:

$$\text{if } (x_{i1}, x_{i2}) \in \eta \text{ for all } i \in \{1, \dots, 2^{n-1} - 1\}, \text{ then } (x_{2^{n-1}1}, x_{2^{n-1}2}) \in \eta. \tag{2.2}$$

This definition is equivalent to the one given in [3, Definition 3.2] and in [6, Definition 3]. We use the notation $M_{\mathbf{A}}(\alpha_1, \dots, \alpha_n)$ as employed by Shaw in [20]. Note that $M_{\mathbf{A}}(\alpha_1) = \alpha_1$ for all $\alpha_1 \in \operatorname{Con}(\mathbf{A})$. For $n = 2$ the binary commutator defined above is precisely the term condition commutator from [8, Definition 3.2].

It is straightforward that the n-ary commutator is monotone in each argument and that it satisfies

$$[\alpha_1, \dots, \alpha_n] \leq \alpha_1 \wedge \dots \wedge \alpha_n \quad \text{and} \quad [\alpha_1, \dots, \alpha_n] \leq [\alpha_2, \dots, \alpha_n].$$

We will collect some more properties in Section 3 (see also [3]). In particular, for a group $\mathbf{G}$ with normal subgroups $N_1, \dots, N_n$ the n-ary commutator corresponds to the product of the iterated binary commutators from classical group theory (Lemma 3.6). For a ring $\mathbf{R}$ with ideals $I_1, \dots, I_n$ the n-ary commutator corresponds to the ideal generated by all products (Lemma 3.5). Explicit descriptions of the higher commutators in larger classes of expanded groups are given in [4].

Let $\mathbf{A}$ be an algebra in a congruence modular variety. Given $\alpha, \beta \in \mathrm{Con}(\mathbf{A})$ with $\alpha \leq \beta$, the *centralizer* $(\alpha : \beta)$ of β modulo α is the largest congruence $\sigma \in \mathrm{Con}(\mathbf{A})$ such that $[\beta, \sigma] \leq \alpha$. A congruence γ of $\mathbf{A}$ is called *abelian* if $[\gamma, \gamma] = 0_A$, the equality relation on A; it is *nilpotent of class* n [8, Definition 6.1] if

$$[\dots[[\gamma, \underbrace{\gamma], \gamma] \dots, \gamma]}_{n \text{ times}} = 0_A.$$

We say $\gamma \in \mathrm{Con}(\mathbf{A})$ is n-*supernilpotent* [3, cf. Definition 7.1] if

$$[\underbrace{\gamma, \dots, \gamma}_{n+1 \text{ times}}] = 0_A.$$

We note that an n-supernilpotent congruence is nilpotent of class n by property (HC8) in [3]. In rings and groups the converse holds as well by Lemmas 3.5 and 3.6.

Following [8, p. 60] we say that $\mathbf{A}$ satisfies the congruence identity (C1) if for all $\alpha, \beta \in \mathrm{Con}(\mathbf{A})$

$$\alpha \wedge [\beta, \beta] = [\alpha \wedge \beta, \beta].$$

This condition characterizes finitely generated residually small, congruence modular varieties [8, Theorem 10.15]. An algebra $\mathbf{A}$ in a congruence modular variety satisfies (C1) if and only if for every subdirectly irreducible homomorphic image $\mathbf{B}$ of $\mathbf{A}$ the centralizer of the monolith of $\mathbf{B}$ is abelian [7, p. 422]. In particular, finite groups with all Sylow subgroups abelian satisfy (C1) [7, p. 427].

Using higher commutators we can relax the condition (C1). An algebra $\mathbf{A}$ satisfies n-(WC1), that is, the n-th weak version of (C1), if for every subdirectly irreducible homomorphic image $\mathbf{B}$ of $\mathbf{A}$ with monolith μ the centralizer $(0_B : \mu)$ is n-supernilpotent. Note that $\mathbf{A}$ satisfies 0-(WC1) if the monolith of every subdirectly irreducible homomorphic image of $\mathbf{A}$ is non-abelian. Furthermore, 1-(WC1) is just (C1), and m-(WC1) implies n-(WC1) for $m \leq n$.

For $\alpha, \beta \in \mathrm{Con}(\mathbf{A})$ we write $\alpha \prec \beta$ if $\alpha < \beta$ and $\{\gamma \in \mathrm{Con}(\mathbf{A}) : \alpha < \gamma < \beta\}$ is empty. We are now able to state our main theorem.

Theorem 2.1. *Let $\mathbf{A}$ be a finite Mal'cev algebra that satisfies n-*(WC1) *for some $n \in \mathbb{N}_0$. For a finitary function f on $\mathbf{A}$ the following are equivalent:*

(1) *f is polynomial on $\mathbf{A}$;*

(2) *f preserves $\mathrm{Pol}_{n+1}(\mathbf{A})$;*

(3) *f preserves $\mathrm{Pol}_n(\mathbf{A})$ and $M_{\mathbf{A}}(\underbrace{\gamma, \dots, \gamma}_{n+1 \text{ times}})$ for all $\alpha, \beta \in \mathrm{Con}(\mathbf{A})$ with $\alpha \prec \beta$ and $\gamma := (\alpha : \beta)$.*

Here we consider the set of $(n+1)$-ary polynomial functions $\mathrm{Pol}_{n+1}(\mathbf{A})$ as a subalgebra of $\mathbf{A}^{A^{n+1}}$. In other words, $f \colon A^k \to A$ preserves $\mathrm{Pol}_{n+1}(\mathbf{A})$ if for all $p_1, \dots, p_k \in \mathrm{Pol}_{n+1}(\mathbf{A})$ the function

$$A^{n+1} \to A, \ x \mapsto f(p_1(x), \dots, p_k(x)),$$

is in $\mathrm{Pol}_{n+1}(\mathbf{A})$ again.

By Theorem 2.1 $\mathrm{Pol}(\mathbf{A})$ is the largest clone C on A such that the $(n+1)$-ary part of C is equal to $\mathrm{Pol}_{n+1}(\mathbf{A})$. In particular $\mathrm{Pol}(\mathbf{A})$ is determined by relations of arity $|A|^{n+1}$. The proof is given in Section 6. There we will also obtain the following result of Hagemann and Herrmann as a consequence.

Corollary 2.2 ([1, cf. Theorem 5.1], [9, cf. Theorem 3.4])**.** *Let* $\mathbf{A}$ *be a finite Mal'cev algebra all of whose subdirectly irreducible homomorphic images have non-abelian monolith. Then a finitary function* f *on* $\mathbf{A}$ *is polynomial if and only if* f *preserves all congruences of* $\mathbf{A}$*.*

Specializing Theorem 2.1 to $n = 1$ immediately yields the following result for algebras with (C1).

Corollary 2.3. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra that satisfies* (C1)*. Then a finitary function* f *on* $\mathbf{A}$ *is polynomial if and only if* f *preserves* $\mathrm{Pol}_1(\mathbf{A})$ *and* $M_{\mathbf{A}}(\gamma,\gamma)$ *for all* $\alpha,\beta \in \mathrm{Con}(\mathbf{A})$ *with* $\alpha \prec \beta$ *and* $\gamma := (\alpha : \beta)$*.*

In [11] the following stronger version of (C1) is considered. An algebra $\mathbf{A}$ satisfies (SC1) if for every subdirectly irreducible homomorphic image $\mathbf{B}$ of $\mathbf{A}$ the centralizer γ of the monolith μ is contained in μ. Hence Corollary 2.3 is an alternative to the description of polynomial functions on Mal'cev algebras with (SC1) given in [11, Theorem 31].

If the total congruence 1_A of $\mathbf{A}$ is supernilpotent, then so are all congruences of $\mathbf{A}$ by the monotonicity of the commutator. Hence Theorem 2.1 implies the following.

Corollary 2.4 ([5, cf. Proposition 5.7])**.** *Let* $\mathbf{A}$ *be a finite Mal'cev algebra such that* 1_A *is* n*-supernilpotent for some* $n \in \mathbb{N}_0$*. Then* $\mathrm{Pol}(\mathbf{A})$ *is the set of finitary functions on* $\mathbf{A}$ *that preserve* $\mathrm{Pol}_{n+1}(\mathbf{A})$*.*

Let $\mathbf{A}$ be a finite nilpotent algebra of finite type that generates a congruence modular variety and factors into a direct product of algebras of prime power size. Then 1_A is supernilpotent by [3, Lemma 7.6] (see also [13]). Hence $\mathrm{Pol}(\mathbf{A})$ is finitely related by Corollary 2.4.

Since finite p-groups are supernilpotent by Lemma 3.6, Theorem 2.1 yields the following.

Theorem 2.5. *Let* $\mathbf{G}$ *be a finite group. Assume for every subdirectly irreducible homomorphic image* $\mathbf{B}$ *of* $\mathbf{G}$ *with minimal normal subgroup* M *that the centralizer* $C_{\mathbf{B}}(M)$ *is a* p*-group of class* n*. Then a finitary function* f *on* $\mathbf{G}$ *is polynomial if and only if* f *preserves all subgroups of* $\mathbf{G}^{\max(4,|G|^n)}$ *that contain* $\{(g,\dots,g) \in G^{\max(4,|G|^n)} : g \in G\}$*.*

Theorem 2.5 will be proved in Section 6.

A finite group $\mathbf{G}$ with abelian Sylow subgroups satisfies (C1) [7, p. 427], and the term functions of $\mathbf{G}$ are exactly those that preserve all subgroups of $\mathbf{G}^3$ by [14, Theorem 2.1]. By Theorem 2.5 the polynomial functions are determined by the subgroups of $\mathbf{G}^{\max(4,|G|)}$.

Corollary 2.6. *Let $\mathbf{G}$ be a finite group with all Sylow subgroups abelian. Then a finitary function f on $\mathbf{G}$ is polynomial if and only if f preserves all subgroups of $\mathbf{G}^{\max(4,|G|)}$ that contain $\{(g,\dots,g) \in G^{\max(4,|G|)} : g \in G\}$.*

3. Some properties of the higher commutator

We collect the properties of the commutator that we will need for proving Theorem 2.1.

Lemma 3.1. *Let $\mathbf{A}$ be a Mal'cev algebra with congruences $\alpha_1,\dots,\alpha_n,\beta$ for $n \geq 2$, let $k \in \mathbb{N}$, and let $f\colon A^k \to A$. Assume that f preserves $M_{\mathbf{A}}(\alpha_1,\dots,\alpha_n)$ and f preserves $M_{\mathbf{A}}(\alpha_1,\dots,\alpha_{i-1},\beta,\alpha_{i+1},\dots,\alpha_n)$ for $i \in \{1,\dots,n\}$. Then f preserves $M_{\mathbf{A}}(\alpha_1,\dots,\alpha_{i-1},\alpha_i \vee \beta,\alpha_{i+1},\dots,\alpha_n)$.*

Proof. For any $g \in S_n$ the elements of $M_{\mathbf{A}}(\alpha_{g(1)},\dots,\alpha_{g(n)})$ can be obtained from those of $M_{\mathbf{A}}(\alpha_1,\dots,\alpha_n)$ by permuting the coordinates. Hence it suffices to prove the assertion for $i = 1$.

We claim that

$$\begin{aligned} &M_{\mathbf{A}}(\alpha_1 \vee \beta,\alpha_2,\dots,\alpha_n) \\ &\quad = \Big\{ \begin{pmatrix} X \\ Y \end{pmatrix} \in A^{2^{n-1}\times 2} : \exists Z \in A^{2^{n-2}\times 2} \begin{pmatrix} X \\ Z \end{pmatrix} \in M_{\mathbf{A}}(\alpha_1,\alpha_2,\dots,\alpha_n), \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \begin{pmatrix} Z \\ Y \end{pmatrix} \in M_{\mathbf{A}}(\beta,\alpha_2,\dots,\alpha_n) \Big\}. \end{aligned} \tag{3.1}$$

For proving $\subseteq$, let $s \in M_{\mathbf{A}}(\alpha_1 \vee \beta,\alpha_2,\dots,\alpha_n)$. Then s can be written as a term in generators as given in (2.1). In particular we have $o,p \in \mathbb{N}_0$, $t \in \mathrm{Clo}_{o+p}(\mathbf{A})$, $(a_1,b_1),\dots,(a_o,b_o) \in \alpha_1 \vee \beta$ with

$$A := \begin{pmatrix} a_1 & \cdots & a_o \\ \vdots & & \vdots \\ a_1 & \cdots & a_o \end{pmatrix}, \quad B := \begin{pmatrix} b_1 & \cdots & b_o \\ \vdots & & \vdots \\ b_1 & \cdots & b_o \end{pmatrix} \quad \text{in } A^{2^{n-2}\times o}$$

and $L, R \in A^{2^{n-2}\times p}$ such that

$$s = \begin{pmatrix} t(A,L) & t(A,R) \\ t(B,L) & t(B,R) \end{pmatrix}.$$

Here we abuse notation for the sake of readability. The function t of arity $o+p$ is applied to a block matrix in $A^{2^{n-2}\times(o+p)}$ by applying it to each row of that matrix. The result is then a vector in $A^{2^{n-2}}$. We identify the quadruple of four such vectors with an element in $A^{2^{n-1}\times 2}$.

Further we have $c_1,\dots,c_o \in A$ such that $(a_l,c_l) \in \alpha$ and $(c_l,b_l) \in \beta$ for all $l \in \{1,\dots,o\}$. Let

$$C := \begin{pmatrix} c_1 & \cdots & c_o \\ \vdots & & \vdots \\ c_1 & \cdots & c_o \end{pmatrix} \text{ be in } A^{2^{n-2}\times o}.$$

Then we have

$$\begin{pmatrix} t(A,L) & t(A,R) \\ t(C,L) & t(C,R) \end{pmatrix} \in M_{\mathbf{A}}(\alpha_1, \alpha_2, \ldots, \alpha_n),$$
$$\begin{pmatrix} t(C,L) & t(C,R) \\ t(B,L) & t(B,R) \end{pmatrix} \in M_{\mathbf{A}}(\beta, \alpha_2, \ldots, \alpha_n).$$

Hence s is contained in the set on the right hand side of (3.1).

For the converse inclusion in (3.1) let $m \in \mathrm{Pol}_3(\mathbf{A})$ be a Mal'cev function, and let $\binom{X}{Z} \in M_{\mathbf{A}}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\binom{Z}{Y} \in M_{\mathbf{A}}(\beta, \alpha_2, \ldots, \alpha_n)$. Then $\binom{X}{Z}, \binom{Z}{Z}$, and $\binom{Z}{Y}$ are all in $M_{\mathbf{A}}(\alpha_1 \vee \beta, \alpha_2, \ldots, \alpha_n)$. Hence $m(\binom{X}{Z}, \binom{Z}{Z}, \binom{Z}{Y}) = \binom{X}{Y}$ is in $M_{\mathbf{A}}(\alpha_1 \vee \beta, \alpha_2, \ldots, \alpha_n)$. This proves (3.1). The assertion of the lemma is now straightforward. □

Lemma 3.2. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra, let* $n, k \in \mathbb{N}$*, and let* $f \colon A^k \to A$*. Assume that* f *preserves* $\mathrm{Pol}_n(\mathbf{A})$*. Then* f *preserves* $M_{\mathbf{A}}(\alpha_1, \ldots, \alpha_n)$ *for all* $\alpha_1, \ldots, \alpha_n \in \mathrm{Con}(\mathbf{A})$*.*

Proof. First assume that $\alpha_1, \ldots, \alpha_n$ are principal congruences of $\mathbf{A}$ that are generated by pairs $(a_1, b_1), \ldots, (a_n, b_n) \in A^2$, respectively. We recall that in a Mal'cev algebra

$$\alpha_i = \{(p(a_i), p(b_i)) : p \in \mathrm{Pol}_1(\mathbf{A})\}$$

for all $i \in \{1, \ldots, n\}$ [18, Theorem 4.70 (ii)]. Then each generator of the subalgebra $M_{\mathbf{A}}(\alpha_1, \ldots, \alpha_n)$ from (2.1) can be rewritten as the image of some matrix in a_i and b_i under some unary polynomial function. Moreover every element in $M_{\mathbf{A}}(\alpha_1, \ldots, \alpha_n)$ is of the form

$$p\left(\begin{pmatrix} a_1 & a_1 \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ a_1 & a_1 \\ b_1 & b_1 \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ b_1 & b_1 \end{pmatrix}, \begin{pmatrix} a_2 & a_2 \\ \vdots & \vdots \\ \vdots & \vdots \\ a_2 & a_2 \\ b_2 & b_2 \\ \vdots & \vdots \\ \vdots & \vdots \\ b_2 & b_2 \\ a_2 & a_2 \\ \vdots & \vdots \\ \vdots & \vdots \\ a_2 & a_2 \\ b_2 & b_2 \\ \vdots & \vdots \\ \vdots & \vdots \\ b_2 & b_2 \end{pmatrix}, \ldots, \begin{pmatrix} a_{n-1} & a_{n-1} \\ b_{n-1} & b_{n-1} \\ a_{n-1} & a_{n-1} \\ b_{n-1} & b_{n-1} \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ a_{n-1} & a_{n-1} \\ b_{n-1} & b_{n-1} \end{pmatrix}, \begin{pmatrix} a_n & b_n \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ a_n & b_n \end{pmatrix}\right)$$

for some $p \in \mathrm{Pol}_n(\mathbf{A})$. Now f preserves $M_{\mathbf{A}}(\alpha_1, \dots, \alpha_n)$ since by assumption the function

$$A^n \to A, \; x \mapsto f(p_1(x), \dots, p_k(x)),$$

is in $\mathrm{Pol}_n(\mathbf{A})$ for all $p_1, \dots, p_k \in \mathrm{Pol}_n(\mathbf{A})$. Finally Lemma 3.1 implies the assertion for arbitrary congruences. □

As a consequence the n-ary commutators are determined by the n-ary polynomial functions.

Corollary 3.3 ([3, cf. Corollary 6.10]). *Let* $\mathbf{A}_1 := \langle A, F_1 \rangle$, $\mathbf{A}_2 := \langle A, F_2 \rangle$ *be finite Mal'cev algebras such that* $\mathrm{Pol}_n(\mathbf{A}_1) = \mathrm{Pol}_n(\mathbf{A}_2)$ *for some* $n \in \mathbb{N}$. *Then* $\mathrm{Con}(\mathbf{A}_1) = \mathrm{Con}(\mathbf{A}_2)$ *and, for all* $\alpha_1, \dots, \alpha_n \in \mathrm{Con}(\mathbf{A}_1)$,

$$M_{\mathbf{A}_1}(\alpha_1, \dots, \alpha_n) = M_{\mathbf{A}_2}(\alpha_1, \dots, \alpha_n),$$

and $[\alpha_1, \dots, \alpha_n]$ *is the same in* $\mathbf{A}_1$ *and* $\mathbf{A}_2$.

Proof. Since the congruences are determined by unary polynomial functions, we have $\mathrm{Con}(\mathbf{A}_1) = \mathrm{Con}(\mathbf{A}_2)$. Let $\alpha_1, \dots, \alpha_n \in \mathrm{Con}(\mathbf{A}_1)$. The functions in F_2 preserve $\mathrm{Pol}_n(\mathbf{A}_1)$ and hence $M_{\mathbf{A}_1}(\alpha_1, \dots, \alpha_n)$ by Lemma 3.2. Then $M_{\mathbf{A}_2}(\alpha_1, \dots, \alpha_n) \subseteq M_{\mathbf{A}_1}(\alpha_1, \dots, \alpha_n)$. The converse inclusion follows similarly. □

For algebras that have a group reduct $\langle A, +, -, 0 \rangle$ Aichinger and Mudrinski give an explicit description of commutators by 0-absorbing polynomial functions in [3]. Note that every congruence on such an algebra is already determined by a single congruence class. For $0 \in A$ a function $f \colon A^n \to A$ is 0-*absorbing* if $f(a_1, \dots, a_n) = 0$ whenever one of the arguments $a_1, \dots, a_n \in A$ is 0. We restate the result of Aichinger and Mudrinski for easier reference.

Lemma 3.4 ([3, Corollary 6.11]). *Let* $\mathbf{A}$ *be an algebra that has a group reduct* $\langle A, +, -, 0 \rangle$, *let* $n \in \mathbb{N}$, *and let* $\alpha_1, \dots, \alpha_n \in \mathrm{Con}(\mathbf{A})$. *Then* $0/[\alpha_1, \dots, \alpha_n]$ *is equal to the subgroup of* $\langle A, +, -, 0 \rangle$ *that is generated by*

$$\bigcup \{ p(0/\alpha_1, \dots, 0/\alpha_n) : p \in \mathrm{Pol}_n(\mathbf{A}) \textit{ and } p \textit{ is } 0\textit{-absorbing} \}.$$

We give a further specialization of the commutator to rings and groups in terms of ideals and normal subgroups, respectively.

Lemma 3.5. *Let* $\mathbf{R} := \langle R, +, -, 0, \cdot \rangle$ *be a ring with congruences* $\alpha_1, \dots, \alpha_n$ *modulo ideals* $I_1, \dots, I_n$, *respectively. Then* $[\alpha_1, \dots, \alpha_n]$ *is the congruence modulo the ideal generated by*

$$C := \bigcup_{f \in S_n} I_{f(1)} I_{f(2)} \cdots I_{f(n)}.$$

Proof. For a polynomial $p \in \mathbf{R}[x_1, \dots, x_n]$, we denote the induced polynomial function by $\bar{p} \colon R^n \to R$. For proving $C \subseteq 0/[\alpha_1, \dots, \alpha_n]$ we let $f \in S_n$. The polynomial $t := x_{f(1)} x_{f(2)} \cdots x_{f(n)}$ induces a 0-absorbing function $\bar{t}$ on R. Hence $\bar{t}(I_1, \dots, I_n) = I_{f(1)} I_{f(2)} \cdots I_{f(n)}$ is contained in the class of 0 modulo $[\alpha_1, \dots, \alpha_n]$ by Lemma 3.4. Thus $C \subseteq 0/[\alpha_1, \dots, \alpha_n]$.

Next we show that every element in $0/[\alpha_1,\dots,\alpha_n]$ is in the subgroup of $\langle R,+,-,0\rangle$ that is generated by C. Let p be a polynomial in $\mathbf{R}[x_1,\dots,x_n]$ that induces a 0-absorbing function $\bar{p}$. There exist $l\in\mathbb{N}$ and monomials $m_1,\dots,m_l\in\mathbf{R}[x_1,\dots,x_n]$ such that $\bar{p}=\sum_{i=1}^{l}\bar{m_i}$. Since

$$\sum_{i=1}^{l}\bar{m_i}(0,r_2,\dots,r_n)=0$$

for all $r_2,\dots,r_n\in R$, we may assume that x_1 is a factor in every $m_1,\dots,m_l$. Likewise every $x_2,\dots,x_n$ occurs as factor (at least once) in every $m_1,\dots,m_l$. Hence, for $i\in\{1,\dots,l\}$, we have $\bar{m_i}(I_1,\dots,I_n)\subseteq I_{f(1)}I_{f(2)}\cdots I_{f(n)}$ for some $f\in S_n$. Thus $\bar{p}(I_1,\dots,I_n)$ is in the subgroup generated by C. The result follows from Lemma 3.4. □

Lemma 3.6. *Let* $\mathbf{G}:=\langle G,\cdot,^{-1},1\rangle$ *be a group with congruences* $\alpha_1,\dots,\alpha_n$ *modulo normal subgroups* $N_1,\dots,N_n$*, respectively. Then* $[\alpha_1,\dots,\alpha_n]$ *is the congruence modulo*

$$C:=\prod_{f\in S_n}[\dots[[N_{f(1)},N_{f(2)}],N_{f(3)}],\dots,N_{f(n)}].$$

Here $[A,B]:=\langle a^{-1}b^{-1}ab : a\in A,\ b\in B\rangle$ *denotes the classical commutator of normal subgroups* A,B *of* $\mathbf{G}$ *from group theory.*

Proof. See [15, Chapter 1] for a definition of polynomials over arbitrary algebraic structures. For a polynomial p in $X:=\{x_1,\dots,x_n\}$ over $\mathbf{G}$, we denote the induced polynomial function by $\bar{p}\colon G^n\to G$.

For proving $C\subseteq 1/[\alpha_1,\dots,\alpha_n]$ we let $f\in S_n$. The term

$$t:=[\dots[[x_{f(1)},x_{f(2)}],x_{f(3)}],\dots,x_{f(n)}]$$

induces a 1-absorbing function $\bar{t}$ on G. Hence

$$\bar{t}(N_1,\dots,N_n)=[\dots[[N_{f(1)},N_{f(2)}],N_{f(3)}],\dots,N_{f(n)}]$$

is contained in the class of 1 modulo $[\alpha_1,\dots,\alpha_n]$ by Lemma 3.4. Thus $C\subseteq 1/[\alpha_1,\dots,\alpha_n]$.

Next we show the converse inclusion. As for rings, we want some appropriate representation of polynomials. We use the approach developed in [2]. As in Definition 6.1 of [2], we let $C(G,X)$ denote the smallest set of expressions such that $G\cup X\cup\{x_1^{-1},\dots,x_n^{-1}\}\subseteq C(G,X)$ and $[u,v]\in C(G,X)$ for all $u,v\in C(G,X)$. For $c\in C(G,X)$ we define the set of arguments, $\operatorname{Arg}(c)$, recursively:

- If $c\in G$, then $\operatorname{Arg}(c):=\emptyset$.
- If $c=x_i$ or $c=x_i^{-1}$ for some $i\in\{1,\dots,n\}$, then $\operatorname{Arg}(c):=\{i\}$.
- If $c=[u,v]$ for some $u,v\in C(G,X)$, then $\operatorname{Arg}(c):=\operatorname{Arg}(u)\cup\operatorname{Arg}(v)$.

Let $p\in\operatorname{Pol}_n(\mathbf{G})$ be 1-absorbing but not constant. We claim that there exist $m\in\mathbb{N}$ and $q_1,\dots,q_m\in C(G,X)$ with $\operatorname{Arg}(q_1)=\dots=\operatorname{Arg}(q_m)=\{1,\dots,n\}$ such that

$$p \text{ is induced by } q_1\cdots q_m. \tag{3.2}$$

Let $\leq$ be a linear order on the power set of $\{1, \dots, n\}$ which refines $\subseteq$, the subset relation. By the appropriate version of commutator collection [2, Lemma 6.5 (2)] we find $k, m_1, \dots, m_k \in \mathbb{N}$ and $f_{1,1}, \dots, f_{k,m_k} \in C(G, X)$ such that p is induced by the polynomial

$$\prod_{i=1}^{k} (f_{i,1} \cdots f_{i,m_i})$$

and

$$\begin{aligned}\operatorname{Arg}(f_{1,1}) = \cdots = \operatorname{Arg}(f_{1,m_1}) < \operatorname{Arg}(f_{2,1}) = \cdots = \operatorname{Arg}(f_{2,m_2}) < \cdots \\ \cdots < \operatorname{Arg}(f_{k,1}) = \cdots = \operatorname{Arg}(f_{k,m_k}).\end{aligned}$$

That is, p can be represented by a product of commutator polynomials whose sets of arguments are ordered with respect to $\leq$.

Let $A := \operatorname{Arg}(f_{1,1}) = \cdots = \operatorname{Arg}(f_{1,m_1})$ and suppose $A \neq \{1, \dots, n\}$. For $(g_1, \dots, g_n) \in G^n$ with $g_i = 1$ whenever $i \notin A$, we have

$$1 = p(g_1, \dots, g_n) = \bar{f}_{1,1}(g_1, \dots, g_n) \cdots \bar{f}_{1,m_1}(g_1, \dots, g_n).$$

Since $f_{1,1}, \dots, f_{1,m_1}$ do not depend on arguments with index outside of A, we obtain

$$\bar{f}_{1,1}(g) \cdots \bar{f}_{1,m_1}(g) = 1 \quad \text{for all } g \in G^n.$$

Now p is induced by

$$\prod_{i=2}^{k} (f_{i,1} \cdots f_{i,m_i}).$$

By repeated use of this argument we finally obtain (3.2).

For normal subgroups $H_1, \dots, H_m$ of $\mathbf{G}$ we write

$$l(H_1, \dots, H_m) := [\dots[[H_1, H_2], H_3], \dots, H_m].$$

We will show that for all $q \in C(G, X)$ with $\operatorname{Arg}(q) = \{1, \dots, n\}$ and for all $N_1, \dots, N_n \trianglelefteq \mathbf{G}$

$$\bar{q}(N_1, \dots, N_n) \subseteq \prod_{f \in S_n} l(N_{f(1)}, \dots, N_{f(n)}) \tag{3.3}$$

by induction on the weight of q. As in Definition 6.1 of [2], we define the weight of some $c \in C(G, X)$, $\operatorname{wt}(c)$, recursively:

- If $c \in G$, then $\operatorname{wt}(c) := 1$.
- If $c = x_i$ or $c = x_i^{-1}$ for some $i \in \{1, \dots, n\}$, then $\operatorname{wt}(c) := 1$.
- If $c = [u, v]$ for some $u, v \in C(G, X)$, then $\operatorname{wt}(c) := \operatorname{wt}(u) + \operatorname{wt}(v)$.

If $\operatorname{wt}(q) = 1$, then $n = 1$ and the assertion is immediate. So assume that $q = [u, v]$ for some $u, v \in C(G, X)$. Let $\operatorname{Arg}(u) = \{a_1, \dots, a_s\}$, $\operatorname{Arg}(v) = \{b_1, \dots, b_t\}$. By the induction hypothesis and the distributivity of the commutator we have

$$\bar{q}(N_1, \dots, N_n) \subseteq \prod_{g \in S_s} \prod_{h \in S_t} [l(N_{a_{g(1)}}, \dots, N_{a_{g(s)}}), l(N_{b_{h(1)}}, \dots, N_{b_{h(t)}})]. \tag{3.4}$$

We now use a second induction on t. If $t = 1$, then (3.3) is immediate from (3.4). So assume $t > 1$. For fixed $g \in S_s$, $h \in S_t$ we write $H := l(N_{a_{g(1)}}, \dots, N_{a_{g(s)}})$, $K := l(N_{b_{h(1)}}, \dots, N_{b_{h(t-1)}})$, and $L := N_{b_{h(t)}}$. By the Three-Subgroup-Lemma [19, 5.1.10] we have

$$[H,[K,L]] \leq [[H,L],K] \cdot [[H,K],L].$$

By the assumption of the second induction both $[[H,L],K]$ and $[[H,K],L]$ are contained in $\prod_{f \in S_n} l(N_{f(1)}, \dots, N_{f(n)})$. Consequently

$$[H,[K,L]] \leq \prod_{f \in S_n} l(N_{f(1)}, \dots, N_{f(n)})$$

and (3.3) follows from (3.4). Together with (3.2) and Lemma 3.4 this completes the proof of the lemma. □

4. Adding and multiplying by using the commutator

In our proof of Theorem 2.1 we will adapt the idea of Lagrange interpolation from fields to Mal'cev algebras. In this section we show how to emulate addition and multiplication of functions.

Let $\mathbf{A}$ be a Mal'cev algebra with Mal'cev function $m \in \mathrm{Pol}_3(\mathbf{A})$. For $o, x, y \in A$ we write

$$x +_o y := m(x,o,y) \quad \text{and} \quad x -_o y := m(x,y,o). \tag{4.1}$$

The following easy observation that these operations allow us to mimic addition and subtraction of a group will often be useful.

Lemma 4.1. *Let $\mathbf{A}$ be an algebra with congruences α, γ such that $[\alpha,\gamma] = 0_A$. Let m be a Mal'cev polynomial on $\mathbf{A}$, and let $x, y, z \in A$ be such that $x \equiv_\alpha y \equiv_\gamma z$. Then*

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

Proof. For $u, v \in A$ we define a binary polynomial function by

$$f(u,v) := m(m(x,u,v),v,u).$$

As $\begin{pmatrix} x & x \\ y & y \end{pmatrix}, \begin{pmatrix} y & z \\ y & z \end{pmatrix} \in M_{\mathbf{A}}(\alpha,\gamma)$, we obtain $\begin{pmatrix} f(x,y) & f(x,z) \\ f(y,y) & f(y,z) \end{pmatrix} \in M_{\mathbf{A}}(\alpha,\gamma)$. Since $f(x,y) = x = f(x,z)$ and $[\alpha,\gamma] = 0_A$, the term condition (2.2) for $n = 2$ implies that $f(y,y) = f(y,z)$. Now the assertion follows from $f(y,y) = x$ and $f(y,z) = m(m(x,y,z),z,y)$. □

Next we state a well-known local description of polynomial functions on a single class of an abelian congruence.

Lemma 4.2. *Let $\mathbf{A}$ be a finite Mal'cev algebra with abelian minimal congruence α, and let $o \in A$. Then*

$$\mathbf{V} := \langle o/\alpha, \{+_o, -_o, o\} \cup \{f|_{o/\alpha} : f \in \mathrm{Pol}_1(\mathbf{A}),\ f(o) = o\}\rangle$$

is a module over a full matrix ring over some field $\mathbf{F}$.

Proof. Since α is abelian, $\mathbf{V}$ is a faithful ring module by [18, Theorem 4.155]. Since α is a minimal congruence, $\mathbf{V}$ is simple. Hence, by Jacobson's density theorem and by finiteness, $\mathbf{V}$ is a module over some matrix ring $\mathbf{F}_n^n$ for a field $\mathbf{F}$. □

The following lemma guarantees the existence of a binary polynomial function t that locally plays the role of a ring multiplication.

Lemma 4.3. *Let $\mathbf{A}$ be a finite Mal'cev algebra with abelian, minimal congruence α, let $\gamma := (0_A : \alpha)$ with $\gamma \neq 1_A$, let $o \in A$, and let $c, d \in A$ such that $(c,d) \notin \gamma$. Then we have $t \in \mathrm{Pol}_2(\mathbf{A})$ such that $t(o,y) = t(y,c) = o$ for all $y \in A$ and $t(x,d) = x$ for all $x \in o/\alpha$.*

Proof. First we show that

$$\forall b \in o/\alpha \; \exists w_b \in \mathrm{Pol}_2(\mathbf{A}) \; \forall y \in A: \; w_b(o,y) = w_b(y,c) = o, \; w_b(b,d) = b. \quad (4.2)$$

Let $b \in o/\alpha,\ b \neq o$. Since the congruence $\beta := \mathrm{Cg}_{\mathbf{A}}(c,d)$ that is generated by (c,d) is not below γ, we have $[\alpha,\beta] \neq 0_A$. In a Mal'cev algebra $\mathbf{A}$ the principal congruence generated by $(i,j) \in A^2$ is given as

$$\mathrm{Cg}_{\mathbf{A}}(i,j) = \{(p(i),p(j)) : p \in \mathrm{Pol}_1(\mathbf{A})\}$$

[18, Theorem 4.70 (ii)]. Since $\alpha = \mathrm{Cg}_{\mathbf{A}}(o,b)$, we then obtain

$$M_{\mathbf{A}}(\alpha,\beta) = \Big\{ \begin{pmatrix} s(o,c) & s(o,d) \\ s(b,c) & s(b,d) \end{pmatrix} : s \in \mathrm{Pol}_2(\mathbf{A}) \Big\}.$$

By the term condition (2.2) and by $[\alpha,\beta] \neq 0_A$, we have $s \in \mathrm{Pol}_2(\mathbf{A})$ such that

$$s(o,c) = s(o,d) \quad \text{and} \quad s(b,c) \neq s(b,d).$$

We define

$$u(x,y) := m(m(s(x,y), s(o,y), s(o,c)), s(x,c), s(b,c)).$$

Then

$$\begin{aligned} u(o,y) &= s(b,c) \quad \text{for all } y \in A, \\ u(x,c) &= s(b,c) \quad \text{for all } x \in A, \\ u(b,d) &= m(s(b,d), s(o,d), s(o,c)) = s(b,d). \end{aligned}$$

Note that $(s(b,c), s(b,d)) \in [\alpha,\beta]$ and $[\alpha,\beta] = \alpha$ since α is a minimal congruence. So $\mathrm{Cg}_{\mathbf{A}}(s(b,c), s(b,d)) = \alpha$. In particular there exists $v \in \mathrm{Pol}_1(\mathbf{A})$ such that $v(s(b,c)) = o$ and $v(s(b,d)) = b$. Thus $w_b(x,y) := v(u(x,y))$ satisfies the assertions of (4.2).

By Lemma 4.2 o/α forms a vector space $\mathbf{V}$ over some field $\mathbf{F}$. Let B be a basis for $\mathbf{V}$. For $b \in B$ we have $e_b \in \mathrm{Pol}_1(\mathbf{A})$ such that $e_b(o) = o, e_b(b) = b$ and $e(B \setminus \{b\}) = o$. Let w_b as in (4.2). We claim that

$$t(x,y) := \sum_{b \in B} e_b(w_b(x,y))$$

satisfies the assertions of the lemma. Certainly $t(o,y) = t(y,c) = o$ for all $y \in A$. Since $x \mapsto t(x,d)$ is an $\mathbf{F}$-linear function on $\mathbf{V}$ that acts as identity on a basis B, we obtain $t(x,d) = x$ for all $x \in o/\alpha$. □

5. Functions on centralizer classes

In this section we characterize polynomial functions on an algebra $\mathbf{A}$ by their behaviour on quotients and on certain congruence classes. This will allow us to reduce the study of $\mathrm{Pol}(\mathbf{A})$ to the study of polynomial functions on smaller algebras.

A function $f\colon A^k \to A$ *preserves* a congruence α of $\mathbf{A}$ if $f(x_1,\dots,x_k) \equiv_\alpha f(y_1,\dots,y_k)$ for all $x_1,\dots,x_k,y_1,\dots,y_k \in A$ with $x_1 \equiv_\alpha y_1,\dots,x_k \equiv_\alpha y_k$. Then f induces the function

$$f_\alpha\colon (A/\alpha)^k \to A/\alpha,\ (x_1/\alpha,\dots,x_k/\alpha) \mapsto f(x_1,\dots,x_k)/\alpha,$$

on the quotient A/α.

The next three reduction results from [12] will be needed for the proof of Theorem 2.1 in the next section. First we observe when a function that induces polynomials on proper quotients is in fact polynomial.

Lemma 5.1 ([12, Theorem 1]). *Let $\mathbf{A}$ be a finite Mal'cev algebra, and let $\alpha,\beta \in \mathrm{Con}(\mathbf{A})$ be such that $\alpha \wedge \beta = 0_A$ and that $\gamma = (\gamma \wedge \alpha) \vee (\gamma \wedge \beta)$ for all $\gamma \in \mathrm{Con}(\mathbf{A})$ with $\gamma \leq \alpha \vee \beta$. Let f be a function on A that preserves α and β. Then $f \in \mathrm{Pol}(\mathbf{A})$ if and only if $f_\alpha \in \mathrm{Pol}(\mathbf{A}/\alpha)$ and $f_\beta \in \mathrm{Pol}(\mathbf{A}/\beta)$.*

The next one characterizes polynomial functions by their behaviour on a quotient modulo some congruence α and by the polynomial functions into single α-classes.

Lemma 5.2 ([12, Lemma 6]). *Let $\mathbf{A}$ be a finite Mal'cev algebra, let $\alpha \in \mathrm{Con}(\mathbf{A})$, and let $\mathcal{R}$ be a set of relations on A which are invariant under $\mathrm{Pol}(\mathbf{A})$. Let $k \in \mathbb{N}$, and let $f\colon A^k \to A$. We assume that, for all $o \in f(A^k)$, all k-ary $\mathcal{R}$-preserving functions into o/α are polynomial. We assume that f is $\mathcal{R}$-preserving, that f preserves α, and that $f_\alpha \in \mathrm{Pol}_k(\mathbf{A}/\alpha)$. Then $f \in \mathrm{Pol}_k(\mathbf{A})$.*

For algebras with non-abelian minimal congruence we have an easy reduction.

Lemma 5.3 ([12, Corollary 14]). *Let $\mathbf{A}$ be a finite Mal'cev algebra with non-abelian minimal congruence α. Let f be a congruence preserving function on $\mathbf{A}$ such that $f_\alpha \in \mathrm{Pol}(\mathbf{A}/\alpha)$. Then $f \in \mathrm{Pol}(\mathbf{A})$.*

It remains to investigate algebras with abelian minimal congruences.

Lemma 5.4. *Let $\mathbf{A}$ be a finite Mal'cev algebra with abelian minimal congruence α, let $\gamma := (0_A : \alpha)$, and let $o \in A$. Let $k \in \mathbb{N}$, and let $f\colon A^k \to o/\alpha$. We assume that for every $a \in A^k$ there exists $g \in \mathrm{Pol}_k(\mathbf{A})$ such that $f|_{a/\gamma} = g|_{a/\gamma}$. Then $f \in \mathrm{Pol}_k(\mathbf{A})$.*

Proof. Let $a \in A^k$, and let $p \in \operatorname{Pol}_k(\mathbf{A})$ be such that $p(a/\gamma) \subseteq o/\alpha$. First we show that

$$\forall Z \subseteq A^k \setminus (a/\gamma)\ \exists h \in \operatorname{Pol}_k(\mathbf{A}):\ h|_{a/\gamma} = p|_{a/\gamma} \text{ and } h(Z) \subseteq \{o\}. \tag{5.1}$$

To this end, we will adapt the idea of Lagrange interpolation from rings and use induction on the size of Z. The base case for $Z = \emptyset$ holds by choosing $h := p$. For the following we assume that we have $z \in Z$. Then we have some $i \in \{1, \dots, k\}$ such that $z_i \notin a_i/\gamma$. By Lemma 4.3 we have $t \in \operatorname{Pol}_2(\mathbf{A})$ such that $t(o, y) = t(y, z_i) = o$ for all $y \in A$ and $t(x, a_i) = x$ for all $x \in o/\alpha$. By the induction hypothesis we have $l \in \operatorname{Pol}_k(\mathbf{A})$ such that $l|_{a/\gamma} = p|_{a/\gamma}$ and $l(Z \setminus \{z\}) \subseteq \{o\}$. We define

$$h(x_1, \dots, x_k) := t(l(x_1, \dots, x_k), x_i).$$

Then $h(z) = t(l(z), z_i) = o$ and $h(y) = t(o, y_i) = o$ for all $y \in Z \setminus \{z\}$. Let $x \in a/\gamma$. Then $t(o, x_i) = o = t(o, a_i)$ yields $t(l(x), x_i) \equiv t(l(x), a_i) \mod [\alpha, \gamma]$ by (2.2) since $l(x) \in o/\alpha$. Hence $t(l(x), x_i) = t(l(x), a_i) = l(x) = p(x)$. This proves (5.1). The result follows by adding functions that interpolate on every class of γ using Lemma 4.2. □

Lemma 5.4 together with Lemma 5.2 immediately yields the following.

Lemma 5.5. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra with abelian minimal congruence* α *and* $\gamma := (0_A : \alpha)$. *Let* $k \in \mathbb{N}$, *and let* $f\colon A^k \to A$. *We assume that* f *preserves* α, *that* $f_\alpha \in \operatorname{Pol}_k(\mathbf{A}/\alpha)$, *and that for every* $a \in A^k$ *there exists* $g \in \operatorname{Pol}_k(\mathbf{A})$ *such that* $f|_{a/\gamma} = g|_{a/\gamma}$. *Then* $f \in \operatorname{Pol}_k(\mathbf{A})$.

Proof. Consider the graphs of k-ary functions whose restriction to every γ-class is polynomial,

$$C := \left\{h \in A^{A^k} : \forall a \in A^k\ \exists g \in \operatorname{Pol}_k(\mathbf{A})\ h|_{a/\gamma} = g|_{a/\gamma}\right\}.$$

Note that $p\colon A^k \to A$ preserves C if and only if p is in C. Clearly every polynomial function on $\mathbf{A}$ preserves C.

For every $o \in A$, every function $p\colon A^k \to o/\gamma$ that preserves C is polynomial by Lemma 5.4. Hence by Lemma 5.2 every $f\colon A^k \to A$ that preserves C and α and that satisfies $f_\alpha \in \operatorname{Pol}_k(\mathbf{A}/\alpha)$ is polynomial. □

6. Algebras satisfying (WC1)

For proving the main result of this article, Theorem 2.1, we need one more lemma.

Lemma 6.1. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra with abelian minimal congruence* α. *We assume that* $\gamma := (0_A : \alpha)$ *is* n*-supernilpotent for some* $n \in \mathbb{N}$. *Let* $k \in \mathbb{N}$, *let* $o \in A$, *and let* $f\colon A^k \to o/\alpha$ *be such that* f *preserves* $\operatorname{Pol}_n(\mathbf{A})$ *and* $C := M_{\mathbf{A}}(\underbrace{\gamma, \dots, \gamma}_{n+1 \text{ times}})$. *Then* $f \in \operatorname{Pol}_k(\mathbf{A})$.

Proof. We will show the assertion by induction on the arity k of f. For $k \leq n$ the assumption that f preserves the set of all graphs of n-ary polynomial functions yields $f \in \mathrm{Pol}_k(\mathbf{A})$. We assume $k > n$ in the following. Since f preserves C, we have that C is a subalgebra of the expansion $\mathbf{A} + f := \langle A, \mathrm{Pol}(\mathbf{A}) \cup \{f\}\rangle$. Hence γ is n-supernilpotent in $\mathbf{A} + f$ as well. Since C has a natural embedding into $M_{\mathbf{A}}(\underbrace{\gamma, \ldots, \gamma}_{k+1 \text{ times}})$ by repeating coordinates, it is straightforward from the definition of the higher commutator that

$$\gamma \text{ is } k\text{-supernilpotent in } \mathbf{A} + f \tag{6.1}$$

(cf. property (HC3) in [3]). Let $a_1, \ldots, a_k \in A$. For $S \subseteq \{1, \ldots, k\}$ we define $f[x_S \to a_S] \colon A^k \to A$ by $f[x_S \to a_S](x_1, \ldots, x_k) = f(u_1, \ldots, u_k)$ where $u_i = a_i$ if $i \in S$ and $u_i = x_i$ else. Clearly $f[x_S \to a_S]$ preserves $\mathrm{Pol}_n(\mathbf{A})$ and $M_{\mathbf{A}}(\underbrace{\gamma, \ldots, \gamma}_{n+1 \text{ times}})$. Hence, if $S \neq \emptyset$, then $f[x_S \to a_S]$ depends on less than k arguments and is polynomial by the induction assumption.

Since the image of f is contained in a module by Lemma 4.2, we may define

$$g := \sum_{S \subseteq \{1,\ldots,k\}} (-1)^{|S|} f[x_S \to a_S].$$

Here addition and subtraction are as in (4.1). Note that g is polynomial on $\mathbf{A} + f$. Since $f = f[x_\emptyset \to a_\emptyset]$, we have

$$f = g - \sum_{S \subseteq \{1,\ldots,k\}, S \neq \emptyset} (-1)^{|S|} f[x_S \to a_S]. \tag{6.2}$$

Note that $g(x_1, \ldots, x_k) = o$ whenever $x_i = a_i$ for some index $i \in \{1, \ldots, k\}$. We claim that

$$g(a_1/\gamma, \ldots, a_n/\gamma) = o. \tag{6.3}$$

Let $b_i \in a_i/\gamma$ for $i \in \{1, \ldots, k\}$. Then

$$g(x_1, \ldots, x_k) = o \quad \text{for all } (x_1, \ldots, x_k) \in (\textstyle\prod_{i=1}^k \{a_i, b_i\}) \setminus \{(b_1, \ldots, b_k)\}.$$

Together with (6.1) and the term condition (2.2) this yields $g(b_1, \ldots, b_k) = o$. Hence (6.3) is proved. In particular, by (6.2), there exists $p \in \mathrm{Pol}_k(\mathbf{A})$ such that $f|_{a/\gamma} = p|_{a/\gamma}$. Now Lemma 5.4 yields $f \in \mathrm{Pol}_k(\mathbf{A})$. □

Proof of Theorem 2.1. The implication (1) ⇒ (2) is immediate and (2) ⇒ (3) follows from Lemma 3.2. It only remains to show (3) ⇒ (1). Assume that $\mathbf{A}$ is a finite Mal'cev algebra that satisfies n-(WC1), and let f be a finitary function on A such that f preserves $\mathrm{Pol}_n(\mathbf{A})$ and $M_{\mathbf{A}}(\underbrace{\gamma, \ldots, \gamma}_{n+1 \text{ times}})$ for all $\rho, \sigma \in \mathrm{Con}(\mathbf{A})$ with $\rho \prec \sigma$ and $\gamma := (\rho : \sigma)$. First we claim that

$$f \text{ preserves all congruences of } \mathbf{A}. \tag{6.4}$$

If $n \geq 1$, this follows from the fact that f preserves $\mathrm{Pol}_1(\mathbf{A})$. Assume $n = 0$. Let $\rho, \sigma \in \mathrm{Con}(\mathbf{A})$ such that ρ is meet irreducible and σ is the unique cover of ρ. Then $(\rho : \sigma) = \rho$ by 0-(WC1). By assumption f preserves $M_{\mathbf{A}}(\rho)$, which is equal to ρ. Hence f preserves all meet irreducible congruences of $\mathbf{A}$. Since every congruence of $\mathbf{A}$ is the intersection of meet irreducibles, (6.4) follows.

Now we are ready to prove that f is polynomial by induction on $|A|$. Let α be a minimal congruence of $\mathbf{A}$. Clearly $\mathbf{A}/\alpha$ satisfies n-(WC1), and f_α preserves $\mathrm{Pol}_n(\mathbf{A}/\alpha)$ and $M_{\mathbf{A}/\alpha}(\underbrace{\gamma,\dots,\gamma}_{n+1 \text{ times}})$ for all centralizers γ of prime intervals in $\mathrm{Con}(\mathbf{A}/\alpha)$. Hence

$$f_\alpha \in \mathrm{Pol}(\mathbf{A}/\alpha) \tag{6.5}$$

by the induction assumption. If α is non-abelian, this suffices for $f \in \mathrm{Pol}(\mathbf{A})$ by Lemma 5.3. In the following we assume that α is abelian. Suppose there exists another minimal congruence α' of $\mathbf{A}$ such that $0_A, \alpha, \alpha', \alpha \vee \alpha'$ are the only congruences of $\mathbf{A}$ that are contained in $\alpha \vee \alpha'$. By Lemma 5.1 $f_\alpha \in \mathrm{Pol}(\mathbf{A}/\alpha)$ and $f_{\alpha'} \in \mathrm{Pol}(\mathbf{A}/\alpha')$ implies $f \in \mathrm{Pol}(\mathbf{A})$. Hence we may assume that for every minimal congruence α' of $\mathbf{A}$ with $\alpha' \neq \alpha$ there exists $\alpha'' \in \mathrm{Con}(\mathbf{A})$ with $\alpha \wedge \alpha'' = \alpha' \wedge \alpha'' = 0_A$ and $\alpha \vee \alpha'' = \alpha' \vee \alpha'' = \alpha \vee \alpha'$. So the intervals $I[0_A, \alpha]$ and $I[0_A, \alpha']$ are projective (see [18, Definition 2.26]). Then the centralizers $\gamma := (0_A : \alpha)$ and $(0_A : \alpha')$ are equal by [8, Chapter 9, Exercise 4].

Let $\delta \in \mathrm{Con}(\mathbf{A})$ be maximal such that $\alpha \wedge \delta = 0_A$. Then $\mathbf{B} := \mathbf{A}/\delta$ is subdirectly irreducible with monolith $(\alpha \vee \delta)/\delta$. Since the intervals $I[0_A, \alpha]$ and $I[\delta, \alpha \vee \delta]$ are projective, we have $\gamma = (\delta : \alpha \vee \delta)$ again. Clearly $\delta \leq \gamma$. By the assumption γ/δ is n-supernilpotent in $\mathbf{B}$. Hence $\epsilon := [\underbrace{\gamma,\dots,\gamma}_{n+1 \text{ times}}]$ is contained in δ. In particular $\epsilon \wedge \alpha = 0_A$. Since γ and hence ϵ are independent of the choice of the minimal congruence α, we obtain that ϵ intersects every minimal congruence of $\mathbf{A}$ trivially. Thus $\epsilon = 0_A$ and γ is n-supernilpotent in $\mathbf{A}$.

Then every function into a single class modulo α that preserves $\mathrm{Pol}_n(\mathbf{A})$ and $M_{\mathbf{A}}(\underbrace{\gamma,\dots,\gamma}_{n+1 \text{ times}})$ is polynomial by Lemma 6.1. Hence f is in $\mathrm{Pol}(\mathbf{A})$ by Lemma 5.2. □

Proof of Corollary 2.2. The statement is straightforward from Theorem 2.1 (1) $\Leftrightarrow$ (3). Because of its shortness we give a direct proof using only Lemma 5.3 in the following.

Let $\mathbf{A}$ be a finite Mal'cev algebra that satisfies 0-(WC1). Certainly every polynomial function is congruence preserving. We will prove the converse by induction on $|A|$. Let f be a congruence preserving function on $\mathbf{A}$, let $\alpha \in \mathrm{Con}(\mathbf{A})$ be minimal, and let $\delta \in \mathrm{Con}(\mathbf{A})$ be maximal such that $\alpha \wedge \delta = 0_A$. Then $\mathbf{A}/\delta$ is subdirectly irreducible with monolith $(\alpha \vee \delta)/\delta$. By 0-(WC1) we have $(\delta : \alpha \vee \delta) = \delta$. Then also $(0_A : \alpha) = \delta$ by the projectivity of the intervals $I[0_A, \alpha]$ and $I[\delta, \alpha \vee \delta]$. In particular α is not abelian. Since the induced function f_α is in $\mathrm{Pol}(\mathbf{A}/\alpha)$ by the induction assumption, Lemma 5.3 yields $f \in \mathrm{Pol}(\mathbf{A})$. □

We will now prove the specialization of Theorem 2.1 to groups.

Proof of Theorem 2.5. Let $\mathbf{G}$ be a finite group. Assume that every subdirectly irreducible homomorphic image $\mathbf{B}$ of $\mathbf{G}$ has a minimal normal subgroup M whose centralizer $C_{\mathbf{B}}(M)$ is some p-group of class $n \in \mathbb{N}_0$. Let $m := \max(4, |G|^n)$.

Clearly every polynomial function of $\mathbf{G}$ preserves all subgroups of $\mathbf{G}^m$ that contain $D := \{(g, \dots, g) \in G^m : g \in G\}$. For the converse we observe that the congruence $\equiv_{C_{\mathbf{B}}(M)}$ is the centralizer of $\equiv_M$, and $\equiv_{C_{\mathbf{B}}(M)}$ is n-supernilpotent by Lemma 3.6. Thus $\mathbf{G}$ satisfies n-(WC1). By Theorem 2.1 a finitary function f is polynomial on $\mathbf{G}$ if f preserves $\mathrm{Pol}_n(\mathbf{G})$ and $M_{\mathbf{G}}(\underbrace{\gamma, \dots, \gamma}_{n+1 \text{ times}})$ for all congruences γ of $\mathbf{G}$. We will encode these groups as subgroups of $\mathbf{G}^m$ that contain D. Let $v_1, \dots, v_{|G|^n}$ be the elements of G^n, and let

$$P := \{(p(v_1), \dots, p(v_{|G|^n}), \underbrace{p(v_{|G|^n}), \dots, p(v_{|G|^n})}_{m-|G|^n \text{ times}}) \in G^m : p \in \mathrm{Pol}_n(\mathbf{G})\}.$$

Then P is a subgroup of $\mathbf{G}^m$ that contains D. Clearly f preserves $\mathrm{Pol}_n(\mathbf{G})$ if and only if f preserves P.

Next let $\alpha_1, \dots, \alpha_{n+1} \in \mathrm{Con}(\mathbf{G})$. Then $M_{\mathbf{G}}(\alpha_1, \dots, \alpha_{n+1})$ is a subgroup of $\mathbf{G}^{2^{n+1}}$ that contains $\{(g, \dots, g) \in G^{2^{n+1}} : g \in G\}$. Note that $2^{n+1} \leq |G|^n$ except if $n = 0$ or if $n = 1$ and $|G| \leq 3$. In any case $2^{n+1} \leq m$. We define

$$\begin{aligned} &M(\alpha_1, \dots, \alpha_{n+1}) \\ &\qquad := \{(v_1, \dots, v_{2^{n+1}}, \underbrace{v_{2^{n+1}}, \dots, v_{2^{n+1}}}_{m-2^{n+1} \text{ times}}) \in G^m : v \in M_{\mathbf{G}}(\alpha_1, \dots, \alpha_{n+1})\}. \end{aligned}$$

Then $M(\alpha_1, \dots, \alpha_{n+1})$ is a subgroup of $\mathbf{G}^m$ that contains D. Moreover f preserves $M_{\mathbf{G}}(\alpha_1, \dots, \alpha_{n+1})$ if and only if f preserves $M(\alpha_1, \dots, \alpha_{n+1})$. Thus $\mathrm{Pol}(\mathbf{G})$ is determined by subgroups of $\mathbf{G}^m$ that contain D. □

Finally we obtain some consequences of Theorem 2.1 for rings.

Proof of Theorem 1.1. Let $\mathbf{R}$ be a finite local ring with 1, and let $n \in \mathbb{N}_0$ be such that the Jacobson radical J of $\mathbf{R}$ satisfies $J^{n+1} = 0$. If $n = 0$ or $|R| \leq 3$, then $J = 0$ and $\mathbf{R}$ is a simple ring with 1. Since $R^2 = R$, Lemma 3.5 implies that 1_R is non-abelian. Hence every finitary function on $\mathbf{R}$ is polynomial by Lemma 5.3. Then the assertion is trivially true. We assume $n \geq 1$ and $|R| \geq 4$ in the following.

Clearly every polynomial function on $\mathbf{R}$ can be interpolated by a polynomial in every $|R|^n$ places. For the converse, we first show that $\mathbf{R}$ satisfies n-(WC1). Let $\mathbf{B}$ be a subdirectly irreducible homomorphic image of $\mathbf{R}$. Then $\mathbf{B}$ is local with greatest ideal $\bar{J}$, the image of J, and a smallest ideal M. Let C be the maximal ideal in $\mathbf{B}$ such that $C \cdot M = 0$ and $M \cdot C = 0$. By Lemma 3.5 the induced congruence $\equiv_C$ is the centralizer of the monolith $\equiv_M$ of $\mathbf{B}$. Since $\mathbf{B}$ contains an identity, we have $C \subsetneq \bar{J}$. By assumption $C^{n+1} \subseteq \bar{J}^{n+1} = \bar{0}$. Hence C is nilpotent and $\equiv_C$ is an n-supernilpotent congruence of $\mathbf{B}$ by Lemma 3.5.

Thus $\mathbf{R}$ satisfies n-(WC1). By Theorem 2.1 the polynomial functions on $\mathbf{R}$ are determined by subrings of $\mathbf{R}^{|R|^n}$ and $\mathbf{R}^{2^{n+1}}$. Since $n \geq 1$ and $|R| \geq 4$, we have that $m := |R|^n$ is greater than 2^{n+1}. As in the proof of Theorem 2.5 we obtain that a finitary function f is polynomial over $\mathbf{R}$ if f preserves all subrings of $\mathbf{R}^m$ that contain $D := \{(r, \dots, r) \in R^m : r \in R\}$.

Let $f\colon R^k \to R$ be such that for all $S \subseteq R^k$ with $|S| \leq m$ there exists a polynomial function p on $\mathbf{R}$ such that $f|_S = p|_S$. Let U be a subring of $\mathbf{R}^m$ that contains D. We claim that f preserves U. Let $\begin{pmatrix} u_{11} \\ \vdots \\ u_{1m} \end{pmatrix}, \dots, \begin{pmatrix} u_{k1} \\ \vdots \\ u_{km} \end{pmatrix} \in U$.

Then

$$f(\begin{pmatrix} u_{11} \\ \vdots \\ u_{1m} \end{pmatrix}, \dots, \begin{pmatrix} u_{k1} \\ \vdots \\ u_{km} \end{pmatrix}) = \begin{pmatrix} f(u_{11}, \dots, u_{k1}) \\ \vdots \\ f(u_{1m}, \dots, u_{km}) \end{pmatrix}.$$

By assumption we have $p \in \operatorname{Pol}_k(\mathbf{R})$ such that

$$\begin{pmatrix} f(u_{11}, \dots, u_{k1}) \\ \vdots \\ f(u_{1m}, \dots, u_{km}) \end{pmatrix} = \begin{pmatrix} p(u_{11}, \dots, u_{k1}) \\ \vdots \\ p(u_{1m}, \dots, u_{km}) \end{pmatrix} = p(\begin{pmatrix} u_{11} \\ \vdots \\ u_{1m} \end{pmatrix}, \dots, \begin{pmatrix} u_{k1} \\ \vdots \\ u_{km} \end{pmatrix}).$$

The last element is in U because every polynomial function preserves U. Hence f preserves U, and f is polynomial. □

Corollary 6.2. *Let $\mathbf{R}$ be a finite commutative ring with 1, and let $n \in \mathbb{N}_0$ be such that the Jacobson radical J of $\mathbf{R}$ satisfies $J^{n+1} = 0$. Then a congruence preserving function $f\colon R^k \to R$ is polynomial on $\mathbf{R}$ if and only if for all $S \subseteq R^k$ with $|S| \leq |R|^n$ there exists a polynomial function p on $\mathbf{R}$ such that $f|_S = p|_S$.*

Proof. By [17, Theorem VI.2] every finite commutative ring $\mathbf{R}$ with 1 is a direct product of some local rings $\mathbf{R}_1, \dots, \mathbf{R}_m$. Note that a congruence preserving function f on $\mathbf{R}_1 \times \cdots \times \mathbf{R}_m$ is polynomial if and only if f induces polynomial functions on every factor $\mathbf{R}_1, \dots, \mathbf{R}_m$. Hence the result follows from Theorem 1.1. □

Acknowledgement. The author is grateful to Erhard Aichinger, Nebojša Mudrinski, and Jason Shaw for helpful discussions.

References

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

[2] Aichinger, E., Ecker, J.: Every $(k+1)$-affine complete nilpotent group of class k is affine complete. Internat. J. Algebra Comput. **16**, 259–274 (2006)

[3] Aichinger, E., Mudrinski, N.: Some applications of higher commutators in Mal'cev algebras. Algebra Universalis **63**, 367–403 (2010)

[4] Aichinger, E., Mudrinski, N.: On determining the higher commutator operation in classes of expanded groups (2009, submitted)

[5] Aichinger, E., Mudrinski, N.: Polynomial clones of Malcev algebras with small congruence lattices. Acta Math. Hungar. **126**, 315–333 (2010)

[6] Bulatov, A.: On the number of finite Mal'tsev algebras. In: Contributions to General Algebra, vol. 13 (Velké Karlovice, 1999/Dresden, 2000), pp. 41–54. Heyn, Klagenfurt (2001)

[7] Freese, R., McKenzie, R.: Residually small varieties with modular congruence lattices. Trans. Amer. Math. Soc. **264**, 419–430 (1981)

[8] Freese, R., McKenzie, R.N.: Commutator Theory for Congruence Modular Varieties. London Math. Soc. Lecture Note Ser., vol. 125. Cambridge University Press (1987)

[9] Hagemann, J., Herrmann, C.: Arithmetical locally equational classes and representation of partial functions. In: Universal Algebra (Esztergom, 1977). Colloq. Math. Soc. János Bolyai, vol. 29, pp. 345–360. North-Holland, Amsterdam (1982)

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

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

[12] Kaarli, K., Mayr, P.: Polynomial functions on subdirect products. Monatsh. Math. **159**, 341–359 (2010)

[13] Kearnes, K.A.: Congruence modular varieties with small free spectra. Algebra Universalis **42**, 165–181 (1999)

[14] Kearnes, K.A., Szendrei, Á.: Clones of finite groups. Algebra Universalis **54**, 23–52 (2005)

[15] Lausch, H., Nöbauer, W.: Algebra of Polynomials. North-Holland, Amsterdam; Elsevier, New York (1973)

[16] Mayr, P.: Polynomial clones on squarefree groups. Internat. J. Algebra Comput. **18**, 759–777 (2008)

[17] McDonald, B.R.: Finite Rings with Identity. Pure and Applied Mathematics, vol. 28. Marcel Dekker, New York (1974)

[18] McKenzie, R.N., McNulty, G.F., Taylor, W.F.: Algebras, Lattices, Varieties, vol. I. Wadsworth & Brooks/Cole, Monterey (1987)

[19] Robinson, D.J.S.: A Course in the Theory of Groups, 2nd edn. Graduate Texts in Mathematics, vol. 80. Springer, New York (1996)

[20] Shaw, J.: Commutator Relations and the Clone of Finite Groups. PhD thesis, University of Colorado, Boulder (2008)

Peter Mayr
CAUL, Av. Prof. Gama Pinto 2, 1649-003 Lisboa, Portugal, and
Institut für Algebra, JKU Linz, Altenberger Str. 69, 4040 Linz, Austria
e-mail: stein@cii.fc.ul.pt