Polynomial clones on squarefree groups

Peter Mayr*
Institut für Algebra, Johannes Kepler Universität Linz
4040 Linz, Austria
peter.mayr@jku.at

We prove that, on a set of size n, the number of clones that contain a group operation and all constant functions is finite if n is squarefree. This confirms a conjecture by Paweł Idziak from [5] where the converse implication was shown. Our result follows from the observation that the polynomial clone of an expansion of a squarefree group is uniquely determined by its binary functions. We also note that, in general, such a clone is not determined by the congruence lattice and the commutator operation of the corresponding algebra. This refutes a second conjecture from [5].

Keywords: clones of operations; polynomial functions; commutator theory.

Mathematics Subject Classification: 08A40

1. Results

A *clone* [8, 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. The clone of *polynomial functions* [8, Definition 4.4], $\mathrm{Pol}(\mathbf{A})$, on an algebra $\mathbf{A} := \langle A, F\rangle$ is the smallest clone on A that contains all fundamental operations F of $\mathbf{A}$ and all constant functions on A.

The following theorem is our main result. We will actually prove a slightly stronger statement, Theorem 25, in Section 6.

Theorem 1. *Let* $\mathbf{A}$ *be an expansion of a group of finite, squarefree order. Then* $\mathrm{Pol}(\mathbf{A})$ *is the largest clone all of whose binary functions are in* $\mathrm{Pol}_2(\mathbf{A})$.

Hence, on a set of squarefree size, every clone that contains a group operation and all constants is uniquely determined by its binary functions. Characterizing clones by an (in the best case finite) set of invariants is a means of classifying the corresponding algebras with respect to equivalence (Algebras $\mathbf{A}_1$ and $\mathbf{A}_2$ are *polynomially equivalent* if $\mathrm{Pol}(\mathbf{A}_1) = \mathrm{Pol}(\mathbf{A}_2)$). Theorem 1 yields that expansions $\mathbf{A}_1$ and $\mathbf{A}_2$ of squarefree groups are polynomially equivalent if and only if $\mathrm{Pol}_2(\mathbf{A}_1) = \mathrm{Pol}_2(\mathbf{A}_2)$.

In general there is no reason why clones that have the same k-ary functions for some $k \in \mathbb{N}$ should also have the same $(k+1)$-ary parts — even under the additional

*Supported by the Austrian Science Fund (Erwin-Schrödinger-Grant J2637-N18) and the University of Colorado at Boulder.

assumption that the clones contain a Mal'cev operation or a group operation. For a prime p there is a wellknown family of expansions of $\langle \mathbb{Z}_{p^2}, + \rangle$,

$$\mathbf{A}_k := \langle \mathbb{Z}_{p^2}, +, px_1 \dots x_k \rangle \text{ for } k \in \mathbb{N},$$

that satisfy $\mathrm{Pol}_k(\mathbf{A}_k) = \mathrm{Pol}_k(\mathbf{A}_{k+1})$ and $\mathrm{Pol}_{k+1}(\mathbf{A}_k) \subsetneq \mathrm{Pol}_{k+1}(\mathbf{A}_{k+1})$. Hence $\mathrm{Pol}(\langle \mathbb{Z}_{p^2}, + \rangle)$ has infinitely many extensions all of which have the same binary part (see also Andrei Bulatov's classification of expansions of $\langle \mathbb{Z}_{p^2}, + \rangle$ and $\langle \mathbb{Z}_p, + \rangle^2$ in [2]). In [5] Paweł Idziak observed the "only if" direction of the following.

Corollary 2. *On a finite set A the number of clones that contain a group operation and all constant functions is finite if and only if the size of A is squarefree.*

Theorem 1 yields the "if" direction of Corollary 2 since on a set A of squarefree size the pertinent clones are already determined by their binary parts and since there are only finitely many binary functions on A. For clones that contain the operations of an abelian group Corollary 2 was already conjectured to be true by Idziak [5, Conjecture 8]. It would result immediately from the following.

[5, Conjecture 9] *Let $\mathbf{A}$ be an expansion of $\langle \mathbb{Z}_n, + \rangle$ with n squarefree. Then* $\mathrm{Pol}(\mathbf{A})$ *is uniquely determined by $\langle \mathrm{Con}(\mathbf{A}), \wedge, \vee, [.,.] \rangle$, the congruence lattice of $\mathbf{A}$ expanded by the commutator operation.*

We verified this conjecture for n a product of 2 primes together with Erhard Aichinger in [1] and for n a product of 3 primes in [6]. However it is not true if n has 4 prime divisors or more. We will present a counter-example in Section 7.

2. Outline of the proof of Theorem 1

Before we give the full proof of Theorem 1 in Section 6, we briefly sketch its main elements. Any squarefree group is polynomially equivalent to an expansion of a cyclic group by Lemma 10. Hence it suffices to prove Theorem 1 for algebras $\mathbf{A}$ with cyclic group reduct. By standard induction arguments we obtain a further reduction to the case that $\mathbf{A}$ is subdirectly irreducible (see Lemma 4). Then the following description of polynomial functions into an abelian monolith, which we will show in Section 5, is the crucial result for our proof of Theorem 1.

Lemma 3. *Let $\mathbf{A}$ be a subdirectly irreducible expansion of the finite group $\langle A, + \rangle$, and let M be the monolith of $\mathbf{A}$. We assume that M is an abelian ideal of $\mathbf{A}$, that $\langle A/M, + \rangle$ is squarefree and cyclic, and that* $\gcd(|A : M|, |M|) = 1$. *Then there exist $l \in \mathbb{N}$ and subgroups $B_1, \dots, B_l$ of $\langle A, + \rangle$ that contain M such that for all $k \in \mathbb{N}$*

$$\begin{aligned} &\mathrm{Pol}_k(\mathbf{A}) \cap \{ f \in M^{A^k} \ : \ f(x + M^k) = f(x) \text{ for all } x \in A^k \} \\ &\quad = \sum_{i=1}^{l} \{ f \in M^{A^k} \ : \ f(x + B_i^k) = f(x) \text{ for all } x \in A^k \}. \end{aligned}$$

Here the sum of functions in M^{A^k} is the pointwise sum in the abelian group $\langle M,+\rangle^{A^k}$. Let $\mathbf{A}, M$ be as in the assumptions of the lemma. For $k \in \mathbb{N}$ let

$$\mathrm{W}^{(k)} := \{f \in M^{A^k} \ : \ f(x+M^k) = f(x) \text{ for all } x \in A^k\}.$$

We endow $\mathrm{W}^{(k)}$ with the structure of an $\mathbf{F}[\mathbf{G}]$-module for some finite field $\mathbf{F}$ and the group $\mathbf{G}$ of bijective affine functions on $\langle A/M,+\rangle^k$. The appropriate choice for the action of $\mathbf{F}[\mathbf{G}]$ on $\mathrm{W}^{(k)}$ guarantees that $\mathrm{Pol}_k(\mathbf{A}) \cap \mathrm{W}^{(k)}$ is an $\mathbf{F}[\mathbf{G}]$-submodule of $\mathrm{W}^{(k)}$. Applying techniques from module theory $\mathrm{W}^{(k)}$ turns out to be the sum of simple submodules. There is a natural bijection between these submodules and the subgroups of the cyclic group $\langle A/M,+\rangle$. Now $\mathrm{Pol}_k(\mathbf{A}) \cap \mathrm{W}^{(k)}$ splits into simple modules because $\mathrm{W}^{(k)}$ does. From this we obtain that there exist certain subgroups $B_1,\dots,B_l$ of $\langle A,+\rangle$ that contain M such that

$$\mathrm{Pol}_k(\mathbf{A}) \cap \mathrm{W}^{(k)} = \sum_{i=1}^{l} \{f \in M^{A^k} \ : \ f(x+B_i^k) = f(x) \text{ for all } x \in A^k\}.$$

In the final step of the proof of the lemma we show that $B_1,\dots,B_l$ can be chosen uniformly for all $k \in \mathbb{N}$.

By Lemma 3 the k-ary polynomial functions into an abelian monolith M that are constant on all cosets of M^k are uniquely determined by $\mathrm{Pol}_1(\mathbf{A})$. Using the existence of a specific idempotent polynomial function onto M and an interpolation argument, we then obtain that $\mathrm{Pol}_k(\mathbf{A}) \cap M^{A^k}$ is characterized by $\mathrm{Pol}_2(\mathbf{A})$ regardless of whether M is abelian or not.

By an induction argument we may assume that $\mathrm{Pol}_k(\mathbf{A}/M)$ is determined by $\mathrm{Pol}_2(\mathbf{A})$. Finally $\mathrm{Pol}_k(\mathbf{A})$ can be reconstructed from the polynomial functions into M together with the polynomial functions on $\mathbf{A}/M$. So $\mathrm{Pol}_2(\mathbf{A})$ determines $\mathrm{Pol}(\mathbf{A})$.

3. Notation and auxiliary results

We establish some notation and basic facts on ideals of expanded groups. We call an algebra $\mathbf{A}$ an *expanded group* if it has a binary operation symbol $+$, a unary $-$, and a constant 0 such that $\langle A,+,-,0\rangle$ is a group. A normal subgroup I of $\langle A,+\rangle$ is called an *ideal* of $\mathbf{A}$ if $f(a+i)-f(a) \in I$ for all $k \in \mathbb{N}$, all k-ary fundamental operations f of $\mathbf{A}$ and all $a \in A^k, i \in I^k$. Let $\mathrm{P}_0(\mathbf{A}) := \{p \in \mathrm{Pol}_1(\mathbf{A}) \ : \ p(0)=0\}$. We note that a subset I of A is an ideal of $\mathbf{A}$ if and only if I forms a subgroup of $\langle A,+\rangle$ and $p(I) \subseteq I$ for all $p \in \mathrm{P}_0(\mathbf{A})$ [9, Theorem 7.123].

By mapping each congruence of $\mathbf{A}$ to the congruence class of 0 we have a lattice isomorphism between $\mathbf{Con}(\mathbf{A})$ and the lattice of ideals of $\mathbf{A}$, $\langle \mathrm{Id}\,(\mathbf{A}),+,\cap\rangle$. We call $c \in A^{A^2}$ *absorptive* if $c(x,0)=c(0,x)=0$ for all $x \in A$. For ideals I,J of $\mathbf{A}$ we define the *commutator ideal* $[\![I,J]\!]_{\mathbf{A}}$ as the ideal of $\mathbf{A}$ that is generated by

$$\{c(i,j) \ : \ i \in I, j \in J, c \in \mathrm{Pol}_2(\mathbf{A}), c \text{ is absorptive}\}.$$

This commutator for ideals, which was introduced by Stuart Scott, corresponds to the term condition commutator for congruences in universal algebra [1, Lemma 2.9].

Let I be an ideal of $\mathbf{A}$. The *centralizer* of I in $\mathbf{A}$, denoted by $C_{\mathbf{A}}(I)$, is the maximal ideal C of $\mathbf{A}$ such that $[\![I, C]\!]_{\mathbf{A}} = 0$. If $[\![I, I]\!]_{\mathbf{A}} = 0$, then I is *abelian*.

A function $f : A^k \to A$ is *congruence preserving on* $\mathbf{A}$ if for all $\alpha \in \mathrm{Con}(\mathbf{A})$ and for all $(x_1, \dots, x_k), (y_1, \dots, y_k) \in A^k$ with $x_1 \equiv y_1 \bmod \alpha, \dots, x_k \equiv y_k \bmod \alpha$ we have $f(x_1, \dots, x_k) \equiv f(y_1, \dots, y_k) \bmod \alpha$. For a k-ary congruence preserving function f on $\mathbf{A}$ and an ideal I of $\mathbf{A}$, we define

$$f_I : (A/I)^k \to A/I,\ x + I^k \mapsto f(x) + I.$$

Lemma 4. *Let* $\mathbf{A}$ *be an expanded group with ideals* I *and* J *such that* $I \cap J = 0$. *Assume that there exists* $\pi \in \mathrm{Pol}_1(\mathbf{A})$ *such that*

$$\pi(i + j) = i \text{ for all } i \in I, j \in J.$$

Let f *be a congruence preserving function on* $\mathbf{A}$. *If* $f_I \in \mathrm{Pol}(\mathbf{A}/I)$ *and* $f_J \in \mathrm{Pol}(\mathbf{A}/J)$, *then* $f \in \mathrm{Pol}(\mathbf{A})$.

As a consequence of Lemma 4 a congruence preserving function on a squarefree expanded group is polynomial if and only if it is polynomial on all subdirectly irreducible quotients.

Proof. By $f_I \in \mathrm{Pol}(\mathbf{A}/I)$ we have $p \in \mathrm{Pol}(\mathbf{A})$ such that $f_I = p_I$. Then $g := f - p$ is congruence preserving and $g(A) \subseteq I$. By $g_J = f_J - p_J \in \mathrm{Pol}(\mathbf{A}/J)$ we have $q \in \mathrm{Pol}(\mathbf{A})$ such that $g_J = q_J$. We claim that

$$g = \pi q. \tag{3.4}$$

Assume that f is k-ary for $k \in \mathbb{N}$. For $x \in A^k$ we have $q(x) = g(x) + j$ for some $j \in J$. As $g(x) \in I$, we obtain $\pi(q(x)) = g(x)$. This proves (3.4). Thus $g \in \mathrm{Pol}(\mathbf{A})$ and consequently $f \in \mathrm{Pol}(\mathbf{A})$. □

Lemma 5. *[4] Let* $\mathbf{A}$ *be a finite subdirectly irreducible expanded group with non-abelian monolith* M, *and let* $k \in \mathbb{N}$. *Then every function from* A^k *into* M *is polynomial.*

We state a straightforward consequence of Lemma 2.4 in [1] for expanded groups.

Lemma 6. *[1, cf. Lemma 2.4] Let* $\mathbf{A}$ *be an expanded group with ideal* M, *let* $k \in \mathbb{N}$, *and let* $f \in \mathrm{Pol}_k(\mathbf{A})$. *Then*

$$f(m + x) - f(x) + f(c + x) = f(m + c + x) \text{ for all } m \in M^k, c \in C_{\mathbf{A}}(M)^k, x \in A^k.$$

Lemma 7. *[8, cf. Theorem 4.155] Let* $\mathbf{A}$ *be an expanded group with finite abelian minimal ideal* M. *Then* $\langle M, \{+\} \cup \mathrm{P}_0(\mathbf{A})|_M \rangle$ *is polynomially equivalent to a module over a full matrix ring over some finite field.*

Proof. By Lemma 6 $\mathbf{R} := \langle \mathrm{P}_0(\mathbf{A})|_M, +, \circ \rangle$ is a ring of additive functions on M. So $\langle M, \{+\} \cup \mathrm{P}_0(\mathbf{A})|_M \rangle$ is polynomially equivalent to a module over $\mathbf{R}$ (see also [8, Theorem 4.155]). Since M is a minimal ideal in $\mathbf{A}$, it is a faithful simple $\mathbf{R}$-module.

By Jacobson's density theorem [11, Theorem 2.1.6], $\mathbf{R}$ is dense in the ring of endomorphisms of M as a module over some division ring. If M is finite, this yields that $\mathbf{R}$ is isomorphic to a full matrix ring over some finite field. $\square$

Lemma 8. *Let $\mathbf{A}$ be an expanded group with finite abelian minimal ideal M. Let $f \in \mathrm{P}_0(\mathbf{A})$ be such that $f(M) \neq 0$. Then there exist $n \in \mathbb{N}$ and $p_i, q_i \in \mathrm{P}_0(\mathbf{A})$ for $i \in \{1, \ldots, n\}$ such that $(\sum_{i=1}^{n} p_i f q_i)|_M = \mathrm{id}_M$.*

Proof. Straightforward from Lemma 7 and Linear Algebra. $\square$

We will need certain polynomial functions into the monolith that are related to idempotents.

Lemma 9. *Let $\mathbf{A}$ be a finite subdirectly irreducible expanded group with monolith M, and let $C := C_{\mathbf{A}}(M)$. We assume that $M \leq C$ and that there exists $e_1 \in \mathrm{Pol}_1(\mathbf{A})$ such that $e_1(A) \subseteq M$ and $e_1|_M = \mathrm{id}_M$.*

Let $k \in \mathbb{N}$. Then there exists $e \in \mathrm{Pol}_k(\mathbf{A})$ such that $e(A^k) \subseteq M$, $e(x_1, \ldots, x_k) = x_1$ for all $x_1, \ldots, x_k \in M$, and $e(A^k \setminus C^k) = 0$.

Proof. We show that

$$\begin{aligned} \forall Z \subseteq A^k \setminus C^k \ \exists f \in \mathrm{Pol}_k(\mathbf{A}) : f(A^k) \subseteq M, f(M \times 0^{k-1}) \neq 0, \\ f(0 \times M^{k-1}) = 0, f(Z) = 0 \end{aligned} \tag{3.6}$$

by induction on the size of Z.

For the base case $Z = \emptyset$, the function $f \in \mathrm{Pol}_k(\mathbf{A})$ that is defined by $f(x_1, \ldots, x_k) := e_1(x_1)$ for all $x_1, \ldots, x_k \in A$ proves the assertion. Next we assume that $Z \neq \emptyset$. Let $z := (z_1, \ldots, z_k)$ be in Z. Then we have some $i \in \{1, \ldots, k\}$ such that $z_i \notin C$. By the induction hypothesis we have $h \in \mathrm{Pol}_k(\mathbf{A})$ and $m \in M \setminus \{0\}$ such that $h(A^k) \subseteq M$, $h(m, 0, \ldots, 0) \neq 0$, $h(0 \times M^{k-1}) = 0$, and $h(Z \setminus \{z\}) = 0$. Since the ideals of $\mathbf{A}$ that are generated by $h(m, 0, \ldots, 0)$ and by z_i, respectively, do not commute, there exists an absorptive function $c \in \mathrm{Pol}_2(\mathbf{A})$ such that $c(z_i, h(m, 0, \ldots, 0)) \neq 0$. Since $-z_i$ is contained in the ideal generated by $z_i - m$, there exists $q \in \mathrm{P}_0(\mathbf{A})$ such that $q(z_i - m) = -z_i$. For $p(x_1, \ldots, x_k) := q(x_i - m) + z_i$ we then have $p(m, \ldots, m) = z_i$ and $p(z) = 0$. We now define $f(x) := c(p(x), h(x))$ for $x \in A$. Then

$$\begin{aligned} &f(z) = c(0, h(z)) = 0, \\ &f(Z \setminus \{z\}) = c(p(Z \setminus \{z\}), 0) = 0, \\ &f(0 \times M^{k-1}) = c(p(0 \times M^{k-1}), 0) = 0, \\ &f(m, \ldots, m) = c(z_i, h(m, 0, \ldots, 0) + h(0, m, \ldots, m)) = c(z_i, h(m, 0, \ldots, 0)) \neq 0. \end{aligned}$$

For the last equation we used that, since M is abelian, $h|_{M^k}$ is additive by Lemma 6. Likewise $f|_{M^k}$ is additive. So $f(0 \times M^{k-1}) = 0$ and $f(M^k) \neq 0$ yield $f(M \times 0^{k-1}) \neq 0$. Thus (3.6) is proved.

By (3.6) we have $f \in \mathrm{Pol}_k(\mathbf{A})$ such that $f(A^k) \subseteq M$, $f(M \times 0^{k-1}) \neq 0$, $f(0 \times M^{k-1}) = 0$, and $f(A^k \setminus C^k) = 0$. Since M is abelian, by Lemma 7 there exist endomorphisms $l_1, \ldots, l_k$ of $\langle M, +\rangle$ such that $f(x_1, \ldots, x_k) = \sum_{i=1}^{k} l_i(x_i)$ for all $x_1, \ldots, x_k \in M$. Now $f(0 \times M^{k-1}) = 0$ yields $l_2(M) = \cdots = l_k(M) = 0$ and hence $f(x_1, \ldots, x_k) = l_1(x_1)$ for all $x_1, \ldots, x_k \in M$. Since $l_1(M) \neq 0$, by Lemma 8 we have $n \in \mathbb{N}$ and $p_i, q_i \in \mathrm{P}_0(\mathbf{A})$ for $i \in \{1, \ldots, n\}$ such that $(\sum_{i=1}^{n} p_i l_1 q_i)|_M = \mathrm{id}_M$.

Hence $e : A^k \to A$, $(x_1, \ldots, x_k) \mapsto \sum_{i=1}^{n} p_i(f(q_i(x_1), x_2, \ldots, x_k))$, is a polynomial function on $\mathbf{A}$ that satisfies $e(A^k) \subseteq M$, $e(x_1, \ldots, x_k) = x_1$ for all $x_1, \ldots, x_k \in M$, and $e(A^k \setminus C^k) = 0$. $\square$

Finally we show that every group with cyclic Sylow subgroups is polynomially equivalent to an expansion of a cyclic group.

Lemma 10. *Let $\mathbf{G} := \langle G, \cdot\rangle$ be a finite group with cyclic Sylow subgroups. Then there exists a function $+$ in $\mathrm{Pol}_2(\mathbf{G})$ such that $\langle G, +\rangle$ is a cyclic group.*

Proof. By [10, 10.1.10] there exist a cyclic normal subgroup N and a cyclic subgroup H of $\mathbf{G}$ such that $G = HN$ and $\gcd(|N|, |H|) = 1$. We define

$$(h_1 n_1) + (h_2 n_2) := h_1 h_2 n_1 n_2 \text{ for all } h_1, h_2 \in H, n_1, n_2 \in N.$$

Obviously $\langle G, +\rangle$ is a cyclic group. To show that $+$ is in $\mathrm{Pol}_2(\mathbf{G})$ we consider the function $f : G \to G$ such that $f(hn) = n$ for all $h \in H, n \in N$. We show

$$f \in \mathrm{Pol}_1(\mathbf{G}) \tag{3.9}$$

by induction on $|G|$. Let P be a non-trivial Sylow subgroup of $\langle N, \cdot\rangle$. Then P is a normal Sylow subgroup of $\mathbf{G}$. By [10, 10.1.8] we have a characteristic complement K for P in its centralizer $C_{\mathbf{G}}(P)$. In particular K is normal in $\mathbf{G}$. First we consider the case that K is non-trivial. Then $f_P \in \mathrm{Pol}_1(\mathbf{G}/P)$ and $f_K \in \mathrm{Pol}_1(\mathbf{G}/K)$ by the induction hypothesis. Since P and K commute and their orders are relatively prime, there obviously exists $\pi \in \mathrm{Pol}_1(\mathbf{G})$ such that $\pi(pk) = p$ for all $p \in P, k \in K$. Hence $f \in \mathrm{Pol}_1(\mathbf{G})$ by Lemma 4.

Next we assume that $K = 1$. Then, by [7, Lemma 3.1(1)], $\mathbf{G}$ is a Frobenius group with Frobenius complement H and kernel $N = P$. Let $l \in \mathbb{Z}$ be such that $l \equiv 1 \bmod |N|$ and $l \equiv 0 \bmod |H|$. Let $h \in H, h \neq 1$, and let $n \in N$. We consider

$$(hn)^l = h^l n^{h^{l-1}} \cdots n^h n.$$

Since h acts as a fixed-point-free automorphism on N and since the order of h divides l, [10, 10.5.1(iv)] yields $n^{h^{l-1}} \cdots n^h n = 1$. Hence we have

$$(hn)^l = 1 \text{ and } n^l = n.$$

Thus $f(x) = \prod_{t \in H} (t^{-1}x)^l$ for all $x \in G$, and (3.9) is proved. Since $x + y = xf(x)^{-1} y f(y)^{-1} f(x) f(y)$ for all $x, y \in G$, we obtain that $+$ is in $\mathrm{Pol}_2(\mathbf{G})$. $\square$

4. Modules

We establish some results in module theory (see [3] for definitions and basic facts) that we will need for our proof of Theorem 1. Let $\mathbf{G}$ be a group of permutations on a set Ω, and let $\mathbf{F}$ be a field. Then $F[\Omega]$ forms a vector space over $\mathbf{F}$ with basis Ω. Furthermore $F[\Omega]$ is an $\mathbf{F}[\mathbf{G}]$-module by the action $g * \omega := g(\omega)$ for $g \in G, \omega \in \Omega$.

We say that $\mathbf{G}$ is *sharply* 2*-transitive* on Ω if for all $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \Omega$ with $\alpha_1 \neq \alpha_2, \beta_1 \neq \beta_2$ there exists a unique element $g \in G$ such that $g(\alpha_1) = \beta_1, g(\alpha_2) = \beta_2$.

Lemma 11. *Let $\mathbf{G}$ be a sharply 2-transitive permutation group on a finite set Ω, let $\alpha \in \Omega$, and let $\mathbf{F}$ be a field whose characteristic does not divide $|\Omega|$.*

(1) Then $F[\Omega]$ is the direct sum of the simple $\mathbf{F}[\mathbf{G}]$-submodules $W_0 := \operatorname{span}_F(\sum_{\omega \in \Omega} \omega)$ and $W_1 := \operatorname{span}_F(\alpha - \omega \ : \ \omega \in \Omega, \omega \neq \alpha)$.
(2) $\operatorname{End}_{\mathbf{F}[\mathbf{G}]}(W_0) \cong \mathbf{F}$ and $\operatorname{End}_{\mathbf{F}[\mathbf{G}]}(W_1) \cong \mathbf{F}$.

Proof. By straightforward calculations W_0 and W_1 are $\mathbf{F}[\mathbf{G}]$-submodules of $F[\Omega]$ of dimension 1 and $|\Omega| - 1$ over $\mathbf{F}$, respectively. Since $|\Omega| \neq 0$ in $\mathbf{F}$, we have the direct decomposition $F[\Omega] = W_0 \dot{+} W_1$. As 1-dimensional vector space W_0 is simple. To show that W_1 is a simple $\mathbf{F}[\mathbf{G}]$-module we let U be a non-trivial submodule of W_1, and let $\beta \in \Omega \setminus \{\alpha\}$. We will prove that

$$\alpha - \beta \in U. \tag{4.1}$$

Since $\mathbf{G}$ is transitive on Ω, we have $u := \sum_{\omega \in \Omega} f_\omega \omega$ in U with $f_\omega \in F$ for $\omega \in \Omega$ and $f_\alpha \neq 0$. Let $G_\alpha := \{g \in G \ : \ g(\alpha) = \alpha\}$ be the stabilizer of α in G. Since $\mathbf{G}$ is sharply 2-transitive on Ω, G_α is transitive on $\Omega \setminus \{\alpha\}$. Furthermore the identity is the only element in G_α that fixes any $\omega \in \Omega \setminus \{\alpha\}$. Let $v := \sum_{g \in G_\alpha} g * u$. We obtain

$$v = |G_\alpha| f_\alpha \alpha + \sum_{\varphi \in \Omega \setminus \{\alpha\}} (f_\varphi \sum_{\omega \in \Omega \setminus \{\alpha\}} \omega).$$

As $u \in W_1$, we have $f_\alpha + \sum_{\varphi \in \Omega \setminus \{\alpha\}} f_\varphi = 0$. So

$$v = |G_\alpha| f_\alpha \alpha - f_\alpha \sum_{\omega \in \Omega \setminus \{\alpha\}} \omega.$$

Now let $h \in G$ be such that $h(\alpha) = \beta, h(\beta) = \alpha$. Then

$$v - h * v = (|G_\alpha| + 1) f_\alpha (\alpha - \beta).$$

Since $|G_\alpha| + 1 = |\Omega|$ and $f_\alpha \neq 0$, we have $(|G_\alpha| + 1) f_\alpha \neq 0$ in $\mathbf{F}$. So $v - h * v \in U$ yields (4.1). Thus $U = W_1$ and W_1 is simple. (1) is proved.

To show (2) we note that

$$\operatorname{End}_{\mathbf{F}[\mathbf{G}]}(F[\Omega]) \cong \operatorname{End}_{\mathbf{F}[\mathbf{G}]}(W_0) \times \operatorname{End}_{\mathbf{F}[\mathbf{G}]}(W_1) \tag{4.5}$$

by (1). Let $r \in \operatorname{End}_{\mathbf{F}[\mathbf{G}]}(F[\Omega])$. Since $\mathbf{G}$ is transitive on the basis Ω of $F[\Omega]$, r is uniquely determined by $r(\alpha)$. We have $f_\omega \in F$ for $\omega \in \Omega$ such that

$$r(\alpha) = \sum_{\omega \in \Omega} f_\omega \omega.$$

Let $h \in G_\alpha$. Then

$$r(\alpha) = \sum_{\omega \in \Omega} f_\omega h(\omega).$$

By comparing coordinates we obtain that $f_{h^{-1}(\omega)} = f_\omega$ for all $\omega \in \Omega$. Since G_α is transitive on $\Omega \setminus \{\alpha\}$, there exists $f \in F$ such that $f_\omega = f$ for all $\omega \in \Omega \setminus \{\alpha\}$. Hence

$$r(\alpha) = f_\alpha \alpha + f \sum_{\omega \in \Omega \setminus \{\alpha\}} \omega$$

and consequently $\mathrm{End}_{\mathbf{F}[\mathbf{G}]}(F[\Omega])$ has dimension at most 2 over $\mathbf{F}$. Together with (4.5) this yields $\mathbf{F} \cong \mathrm{End}_{\mathbf{F}[\mathbf{G}]}(W_0) \cong \mathrm{End}_{\mathbf{F}[\mathbf{G}]}(W_1)$. □

We state some facts about modules for direct products of groups.

Lemma 12. *Let $\mathbf{F}$ be a field, let $\mathbf{G}, \mathbf{H}$ be groups, let M be an $\mathbf{F}[\mathbf{G}]$-module, let N be an $\mathbf{F}[\mathbf{H}]$-module.*

(1) Then $M \otimes_F N$ is an $\mathbf{F}[\mathbf{G} \times \mathbf{H}]$-module defined by

$$(g, h) * (m \otimes n) := (g *_M m) \otimes (h *_N n)$$

for all $g \in G, h \in H, m \in M, n \in N$.

(2) Assume that M_1, M_2 are $\mathbf{F}[\mathbf{G}]$-submodules for M such that $M = M_1 \dot{+} M_2$ is a direct sum and that N_1, N_2 are $\mathbf{F}[\mathbf{H}]$-submodules for N such that $N = N_1 \dot{+} N_2$. Then

$$M \otimes_F N = M_1 \otimes_F N_1 \dot{+} M_1 \otimes_F N_2 \dot{+} M_2 \otimes_F N_1 \dot{+} M_2 \otimes_F N_2.$$

(3) If M is a simple $\mathbf{F}[\mathbf{G}]$-module and N is a simple $\mathbf{F}[\mathbf{H}]$-module and $\mathrm{End}_{\mathbf{F}[\mathbf{G}]}(M) \otimes_F \mathrm{End}_{\mathbf{F}[\mathbf{H}]}(N)$ is a division algebra, then $M \otimes_F N$ is a simple $\mathbf{F}[\mathbf{G} \times \mathbf{H}]$-module.

Proof. Item (1) is immediate, (2) follows from [3, (2.17)] and (3) from [3, Theorem 10.38 (i)]. □

Let $\mathbf{K}$ be a field, let $k \in \mathbb{N}$, and let $\mathrm{AGL}(k, K)$ denote the group of bijective $\mathbf{K}$-affine functions on the $\mathbf{K}$-vector space K^k.

Lemma 13. *Let $k, m \in \mathbb{N}$, let $\mathbf{K}_1, \dots, \mathbf{K}_m$ be finite fields, and let $\mathbf{F}$ be a field whose characteristic is distinct from the characteristic of $\mathbf{K}_i$ for all $i \in \{1, \dots, m\}$.*

(1) Then $W := F[K_1^k] \otimes_F \cdots \otimes_F F[K_m^k]$ is an $\mathbf{F}[\mathrm{AGL}(k, K_1) \times \cdots \times \mathrm{AGL}(k, K_m)]$-module defined by

$$(g_1, \dots, g_m) * (x_1 \otimes \cdots \otimes x_m) := g_1(x_1) \otimes \cdots \otimes g_m(x_m)$$

for $g_i \in \mathrm{AGL}(k, K_i), x_i \in K_i^k$ for all $i \in \{1, \dots, m\}$.

(2) *Furthermore W is the sum of simple* $\mathbf{F}[\mathrm{AGL}(k,K_1)\times\cdots\times\mathrm{AGL}(k,K_m)]$*-submodules* $U_1\otimes_F\cdots\otimes_F U_m$ *with*

$$U_i\in\{\mathrm{span}_F(\sum_{x\in K_i^k}x),\ \mathrm{span}_F(0-x\ :\ x\in K_i^k, x\neq 0)\}$$

for all $i\in\{1,\dots,m\}$.

Proof. Item (1) is immediate from Lemma 12. For (2) we let $\mathbf{K}$ be a finite field. Then $W_0 := \mathrm{span}_F(\sum_{x\in K^k}x)$ and $W_1 := \mathrm{span}_F(0-x\ :\ x\in K^k, x\neq 0)$ are obviously $\mathbf{F}[\mathrm{AGL}(k,K)]$-submodules of $F[K^k]$. For the field extension $\mathbf{E}$ of $\mathbf{K}$ of degree k, there is a natural embedding $\alpha : \mathrm{AGL}(1,E)\to\mathrm{AGL}(k,K)$ with $\alpha(\mathrm{AGL}(1,E))$ acting sharply 2-transitively on K^k. Then W_0 and W_1 are simple $\mathbf{F}[\alpha(\mathrm{AGL}(1,E))]$-modules by Lemma 11. Hence they are simple $\mathbf{F}[\mathrm{AGL}(k,K)]$-modules with $\mathrm{End}_{\mathbf{F}[\mathrm{AGL}(k,K)]}(W_0)\cong\mathbf{F}$ and $\mathrm{End}_{\mathbf{F}[\mathrm{AGL}(k,K)]}(W_1)\cong\mathbf{F}$. Now (2) follows from Lemma 12. $\square$

5. Piecewise constant functions into the monolith

This section consists only of the proof of Lemma 3. We use the following conventions and notation. Let $\mathbf{A}$ be a subdirectly irreducible expanded group, and let M be the monolith of $\mathbf{A}$. We assume that M is an abelian ideal of $\mathbf{A}$, that $\langle A/M,+\rangle$ is squarefree and cyclic, and that $\gcd(|A:M|,|M|)=1$. For $k\in\mathbb{N}$ let

$$\mathrm{W}^{(k)} := \{f\in M^{A^k}\ :\ f(x+M^k)=f(x)\text{ for all }x\in A^k\}$$

and

$$\mathrm{U}^{(k)} := \mathrm{Pol}_k(\mathbf{A})\cap\mathrm{W}^{(k)}.$$

First we will endow $\mathrm{W}^{(k)}$ with the structure of a module with submodule $\mathrm{U}^{(k)}$. Then we apply Lemma 13 to obtain a precise description of the k-ary polynomial functions into M that are constant on the cosets of M^k. Finally we show that this description does not depend on the arity k. This will conclude the proof of Lemma 3.

Claim 14. *$|M|$ is a prime power.*

Proof. Follows from Lemma 7 since M is an abelian minimal ideal of $\mathbf{A}$. $\square$

Claim 15. *Let* $\mathbf{F}:=\mathrm{GF}(|M|)$*, let* $m\in\mathbb{N}$*, let* $q_1,\dots,q_m$ *be the prime divisors of* $|A:M|$*, and let* $\mathbf{G}:=\mathrm{AGL}(k,\mathbb{Z}_{q_1})\times\cdots\times\mathrm{AGL}(k,\mathbb{Z}_{q_m})$*. Then* $\mathrm{W}^{(k)}$ *forms an* $\mathbf{F}[\mathbf{G}]$*-module with submodule* $\mathrm{U}^{(k)}$*.*

Proof. Since $\langle M,+\rangle$ is an abelian group, $\langle\mathrm{W}^{(k)},+\rangle$ is an abelian group with respect to pointwise addition of functions and $\mathrm{U}^{(k)}$ is a subgroup of $\langle\mathrm{W}^{(k)},+\rangle$. We let $\mathbf{F}$ and $\mathbf{G}$ act on $\langle\mathrm{W}^{(k)},+\rangle$ by composition with polynomial functions. By Lemma 7 we have an embedding φ of $\mathbf{F}$ into $\langle \mathrm{P}_0(\mathbf{A})|_M, +, \circ\rangle$. Then $\mathrm{W}^{(k)}$ forms a vector space over $\mathbf{F}$ by

$$af := \varphi(a)f \text{ for } a \in F \text{ and } f \in \mathrm{W}^{(k)}. \tag{5.3}$$

Also $F\mathrm{U}^{(k)} \subseteq \mathrm{U}^{(k)}$ which makes $\mathrm{U}^{(k)}$ an $\mathbf{F}$-subspace of $\mathrm{W}^{(k)}$.

By the assumption of the lemma the group reduct of $\mathbf{A}/M$ is isomorphic to $\mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_m}$. So we have a group isomorphism

$$\alpha : \mathbb{Z}_{q_1}^k \times \cdots \times \mathbb{Z}_{q_m}^k \to (A/M)^k.$$

Let $m_1 \in M, m_1 \neq 0$. For $r \in \mathbb{Z}_{q_1}^k \times \cdots \times \mathbb{Z}_{q_m}^k$ we define

$$e_r : A^k \to M,\ (x_1, \ldots, x_k) \mapsto \begin{cases} m_1 \text{ if } (x_1 + M, \ldots, x_k + M) = \alpha(r), \\ 0 \ \text{ else.} \end{cases}$$

The functions $(e_r \ : \ r \in \mathbb{Z}_{q_1}^k \times \cdots \times \mathbb{Z}_{q_m}^k)$ are a basis for $\mathrm{W}^{(k)}$ over $\mathbf{F}$. We let $\mathbf{G}$ act on this basis by $(g_1, \ldots, g_m) * e_{(r_1,\ldots,r_m)} := e_{(g_1(r_1),\ldots,g_m(r_m))}$ for $(g_1, \ldots, g_m) \in G$ and $(r_1, \ldots, r_m) \in \mathbb{Z}_{q_1}^k \times \cdots \times \mathbb{Z}_{q_m}^k$. Then $\mathrm{W}^{(k)}$ forms an $\mathbf{F}[\mathbf{G}]$-module. We note that for all $f \in \mathrm{W}^{(k)}, g \in G$, and $x \in (A/M)^k$

$$(g * f)(x) = f\alpha g^{-1}\alpha^{-1}(x).$$

Hence, for showing that $\mathrm{U}^{(k)}$ is closed under the action of $\mathbf{G}$, it suffices to prove

$$\alpha G \alpha^{-1} \subseteq (\mathrm{Pol}_k(\mathbf{A}/M))^k. \tag{5.7}$$

By the definition of $\mathbf{G}$, $\alpha G\alpha^{-1}$ forms the group of bijective affine functions on $\langle A/M, +\rangle^k$. Let $g \in \alpha G\alpha^{-1}$. Since $\langle A/M, +\rangle$ is cyclic, there exist $a_{ij} \in \mathbb{Z}$ for $i, j \in \{1, \ldots, k\}$ and $b \in (A/M)^k$ such that for all $x_1, \ldots, x_k \in A/M$

$$g(x_1, \ldots, x_k) = (\sum_{j=1}^{k} a_{1j}x_j, \ldots, \sum_{j=1}^{k} a_{kj}x_j) + b.$$

Hence we have $g \in (\mathrm{Pol}_k(\langle A/M, +\rangle))^k$ and consequently (5.7). Thus $G*\mathrm{U}^{(k)} \subseteq \mathrm{U}^{(k)}$, and $\mathrm{U}^{(k)}$ is an $\mathbf{F}[\mathbf{G}]$-submodule of $\mathrm{W}^{(k)}$. □

Claim 16. *The* $\mathbf{F}$*-linear function* $\beta : F[\mathbb{Z}_{q_1}^k] \otimes_F \cdots \otimes_F F[\mathbb{Z}_{q_m}^k] \to \mathrm{W}^{(k)}$ *that is defined by*

$$\beta(r_1 \otimes \cdots \otimes r_m) := e_{(r_1,\ldots,r_m)} \textit{ for } r_1 \in \mathbb{Z}_{q_1}^k, \ldots, r_m \in \mathbb{Z}_{q_m}^k$$

is an $\mathbf{F}[\mathbf{G}]$*-isomorphism.*

Proof. Immediate from the definitions. □

For $I \subseteq \{1, \ldots, m\}$ we define

$$W_I := \beta(U_1 \otimes_F \cdots \otimes_F U_m) \text{ with } U_i := \begin{cases} \mathrm{span}_F(0 - x \ : \ x \in \mathbb{Z}_{q_i}^k, x \neq 0) & \text{if } i \in I, \\ \mathrm{span}_F(\sum_{x \in \mathbb{Z}_{q_i}^k} x) & \text{else.} \end{cases}$$

By Claim 16 and Lemma 13 we can thus index the simple summands of $\mathrm{W}^{(k)}$ by the subsets of $\{1,\ldots,m\}$ and obtain the following.

Claim 17. *There exist $l \in \mathbb{N}$ and subsets $I_1,\ldots,I_l$ of $\{1,\ldots,m\}$ such that $\mathrm{U}^{(k)} = W_{I_1} + \cdots + W_{I_l}$.*

Claim 18. *Let $i \in \{1,\ldots,m\}$. Assume that $W_{\{1,\ldots,i\}} \leq \mathrm{U}^{(k)}$. Then $W_{\{1,\ldots,i-1\}} \leq \mathrm{U}^{(k)}$.*

Proof. For $j \in \{1,\ldots,i\}$, let $r_j \in \mathbb{Z}_{q_j}^k, r_j \neq 0$, and let

$$f := \beta(0 - r_1 \otimes \cdots \otimes 0 - r_i \otimes \sum_{x_{i+1}\in\mathbb{Z}_{q_{i+1}}^k} x_{i+1} \otimes \cdots \otimes \sum_{x_m\in\mathbb{Z}_{q_m}^k} x_m).$$

Then f is in $\mathrm{U}^{(k)}$. To determine f explicitly we use the multilinearity of the tensor product and obtain

$$\begin{aligned}
f = \beta([&0 \otimes \cdots \otimes 0 \\
&-(r_1 \otimes 0 \otimes \cdots \otimes 0 + \cdots + 0 \otimes \cdots \otimes 0 \otimes r_i) \\
&+\cdots \\
&+(-1)^i\, r_1 \otimes \cdots \otimes r_i] \otimes [\sum_{x_{i+1}\in\mathbb{Z}_{q_{i+1}}^k,\ldots,x_m\in\mathbb{Z}_{q_m}^k} x_{i+1} \otimes \cdots \otimes x_m]) \\
= \sum_{x_{i+1}\in\mathbb{Z}_{q_{i+1}}^k,\ldots,x_m\in\mathbb{Z}_{q_m}^k} &[e_{(0,\ldots,0,x_{i+1},\ldots,x_m)} \\
&-(e_{(r_1,0,\ldots,0,x_{i+1},\ldots,x_m)} + \cdots + e_{(0,\ldots,0,r_i,x_{i+1},\ldots,x_m)}) \\
&+\cdots \\
&+(-1)^i\, e_{(r_1,\ldots,r_i,x_{i+1},\ldots,x_m)}].
\end{aligned}$$

Let $t \in \mathbb{N}$ be such that $t \equiv 0 \bmod q_i$ and $t \equiv 1 \bmod q_j$ for all $j \in \{1,\ldots,m\}, j \neq i$. Let $(s_1,\ldots,s_m) \in \mathbb{Z}_{q_1}^k \times \cdots \times \mathbb{Z}_{q_m}^k$, and let $x \in A^k$. If $s_i \neq 0$, then

$$e_{(s_1,\ldots,s_m)}(tx) = 0.$$

If $s_i = 0$, then

$$e_{(s_1,\ldots,s_m)}(tx) = \begin{cases} m_1 \text{ if } x \in \alpha(s_1,\ldots,s_{i-1},\mathbb{Z}_{q_i}^k,s_{i+1},\ldots,s_m), \\ 0 \quad \text{else.} \end{cases}$$

Hence

$$e_{(s_1,\ldots,s_{i-1},0,s_{i+1},\ldots s_m)}(tx) = \sum_{y_i\in\mathbb{Z}_{q_i}^k} e_{(s_1,\ldots,s_{i-1},y_i,s_{i+1},\ldots s_m)}(x).$$

Consequently the function $g : A^k \to A,\ x \mapsto f(tx)$, satisfies

$$\begin{aligned} g = & \sum_{x_i \in \mathbb{Z}_{q_i}^k, x_{i+1} \in \mathbb{Z}_{q_{i+1}}^k, \dots, x_m \in \mathbb{Z}_{q_m}^k} [e_{(0,\dots,x_i,x_{i+1},\dots,x_m)} \\ & -(e_{(r_1,0,\dots,0,x_i,x_{i+1},\dots,x_m)} + \cdots + e_{(0,\dots,0,r_{i-1},x_i,x_{i+1},\dots,x_m)}) \\ & + \cdots \\ & +(-1)^{i-1} e_{(r_1,\dots,r_{i-1},x_i,x_{i+1},\dots,x_m)}] \\ = & \beta(0 - r_1 \otimes \cdots \otimes 0 - r_{i-1} \otimes \sum_{x_i \in \mathbb{Z}_{q_i}^k} x_i \otimes \cdots \otimes \sum_{x_m \in \mathbb{Z}_{q_m}^k} x_m). \end{aligned}$$

Thus g is in $W_{\{1,\dots,i-1\}}$. Since g is a polynomial function by its definition, we have $g \in \mathrm{U}^{(k)}$. Hence

$$\beta(0 - r_1 \otimes \cdots \otimes 0 - r_{i-1} \otimes \sum_{x_i \in \mathbb{Z}_{q_i}^k} x_i \otimes \cdots \otimes \sum_{x_m \in \mathbb{Z}_{q_m}^k} x_m) \in \mathrm{U}^{(k)}$$

for all $r_1 \in \mathbb{Z}_{q_1}^k, \dots, r_{i-1} \in \mathbb{Z}_{q_{i-1}}^k$. Thus $\mathrm{U}^{(k)}$ contains a basis for $W_{\{1,\dots,i-1\}}$ and $W_{\{1,\dots,i-1\}} \leq \mathrm{U}^{(k)}$. □

Since the proof of Claim 18 does not depend on the chosen ordering of the primes $q_1, \dots, q_m$, we actually have the following result.

Claim 19. *Let $I \subseteq \{1, \dots, m\}$. If $W_I \leq \mathrm{U}^{(k)}$, then $\sum_{J \subseteq I} W_J \leq \mathrm{U}^{(k)}$.*

For a subgroup B of $\langle A, + \rangle$ that contains M we define

$$\mathrm{Fix}_{B^k}(\mathrm{W}^{(k)}) := \{f \in \mathrm{W}^{(k)} \ : \ f(x + B^k) = f(x) \text{ for all } x \in A^k\}.$$

Claim 20. *Let $I \subseteq \{1, \dots, m\}$, let $d := \prod_{i \in I} q_i$, and let B be the unique subgroup of index d in $\langle A, + \rangle$. Then $\sum_{J \subseteq I} W_J = \mathrm{Fix}_{B^k}(\mathrm{W}^{(k)})$.*

Proof. We note that the basis vectors of W_J for $J \subseteq I$ are fixed under translations by all elements in $\alpha^{-1}((B/M)^k)$. Hence

$$\sum_{J \subseteq I} W_J \leq \mathrm{Fix}_{B^k}(\mathrm{W}^{(k)}). \tag{5.17}$$

Further

$$\begin{aligned} \dim_{\mathbf{F}} \sum_{J \subseteq I} W_J &= \sum_{J \subseteq I} \dim_{\mathbf{F}} W_J \\ &= \sum_{J \subseteq I} \prod_{j \in J} (q_j^k - 1) \\ &= \sum_{J \subseteq I} |\{x \in \mathbb{Z}_d^k \ : \ \mathrm{ord} x = \prod_{j \in J} q_j\}| \\ &= |\mathbb{Z}_d^k| \\ &= \dim_{\mathbf{F}} \mathrm{Fix}_{B^k}(\mathrm{W}^{(k)}). \end{aligned}$$

Hence we have equality in (5.17). □

Claim 21. *There exist $l \in \mathbb{N}$ and subgroups $B_1, \ldots, B_l$ of $\langle A, +\rangle$ that contain M such that*

$$\mathrm{U}^{(k)} = \mathrm{Fix}_{B_1^k}(\mathrm{W}^{(k)}) + \cdots + \mathrm{Fix}_{B_l^k}(\mathrm{W}^{(k)}).$$

Proof. Follows from Claims 17, 19, and 20. □

Claim 22. *Let $l \in \mathbb{N}$, and let $B, B_1, \ldots, B_l$ be subgroups of $\langle A, +\rangle$ that contain M. Assume that $\mathrm{Fix}_{B^k}(\mathrm{W}^{(k)}) \leq \mathrm{Fix}_{B_1^k}(\mathrm{W}^{(k)}) + \cdots + \mathrm{Fix}_{B_l^k}(\mathrm{W}^{(k)})$. Then $B_i \leq B$ for some $i \in \{1, \ldots, l\}$.*

Proof. Let $I \subseteq \{1, \ldots, m\}$ be such that $|A : B| = \prod_{i \in I} q_i$. Then W_I is a submodule of $\mathrm{Fix}_{B^k}(\mathrm{W}^{(k)})$ and hence of $\mathrm{Fix}_{B_1^k}(\mathrm{W}^{(k)}) + \cdots + \mathrm{Fix}_{B_l^k}(\mathrm{W}^{(k)})$. Since W_I is simple and not isomorphic to any other submodule of $\mathrm{W}^{(k)}$, there exists $i \in \{1, \ldots, l\}$ such that $W_I \leq \mathrm{Fix}_{B_i^k}(\mathrm{W}^{(k)})$. Then $\mathrm{Fix}_{B^k}(\mathrm{W}^{(k)}) \leq \mathrm{Fix}_{B_i^k}(\mathrm{W}^{(k)})$ by Claim 20. Thus $B_i \leq B$. □

Claim 23. *Let B be a subgroup of $\langle A, +\rangle$ that contains M. Then the following are equivalent:*

(1) $\mathrm{Fix}_B(W^{(1)}) \subseteq \mathrm{Pol}_1(\mathbf{A})$.
(2) $\mathrm{Fix}_{B^k}(\mathrm{W}^{(k)}) \subseteq \mathrm{Pol}_k(\mathbf{A})$.

Proof. Let $i : A \to A^k,\ x \mapsto (x, 0, \ldots, 0)$. The mapping

$$\rho : \mathrm{W}^{(k)} \to W^{(1)}, f \to fi,$$

is onto and satisfies $\rho(\mathrm{U}^{(k)}) = U^{(1)}$ and $\rho(\mathrm{Fix}_{B^k}(\mathrm{W}^{(k)})) = \mathrm{Fix}_B(W^{(1)})$.

(2)⇒(1): If $\mathrm{Fix}_{B^k}(\mathrm{W}^{(k)}) \subseteq \mathrm{Pol}_k(\mathbf{A})$, then $\mathrm{Fix}_B(W^{(1)}) = \rho(\mathrm{Fix}_{B^k}(\mathrm{W}^{(k)})) \subseteq \mathrm{Pol}_1(\mathbf{A})$.

(1)⇒(2): We assume $\mathrm{Fix}_B(W^{(1)}) \subseteq \mathrm{Pol}_1(\mathbf{A})$. By Claim 21 we have $l \in \mathbb{N}$ and subgroups $B_1, \ldots, B_l$ of $\langle A, +\rangle$ that contain M such that

$$\mathrm{Fix}_{B_1^k}(\mathrm{W}^{(k)}) + \cdots + \mathrm{Fix}_{B_l^k}(\mathrm{W}^{(k)}) = \mathrm{U}^{(k)}.$$

For $f \in \mathrm{Fix}_B(W^{(1)})$ the function

$$f' : A^k \to M, (x_1, \ldots, x_k) \mapsto f(x_1),$$

is in $\mathrm{U}^{(k)}$. Now $f' \in \mathrm{Fix}_{B_1^k}(\mathrm{W}^{(k)}) + \cdots + \mathrm{Fix}_{B_l^k}(\mathrm{W}^{(k)})$ yields that

$$f = \rho(f') \in \rho(\mathrm{Fix}_{B_1^k}(\mathrm{W}^{(k)}) + \cdots + \mathrm{Fix}_{B_l^k}(\mathrm{W}^{(k)})) = \mathrm{Fix}_{B_1}(W^{(1)}) + \cdots + \mathrm{Fix}_{B_l}(W^{(1)}).$$

Hence $\mathrm{Fix}_B(W^{(1)}) \leq \mathrm{Fix}_{B_1}(W^{(1)}) + \cdots + \mathrm{Fix}_{B_l}(W^{(1)})$. By Claim 22 there exist $i \in \{1, \ldots, l\}$ such that $B_i \leq B$. Then $\mathrm{Fix}_{B^k}(\mathrm{W}^{(k)}) \leq \mathrm{Fix}_{B_i^k}(\mathrm{W}^{(k)}) \leq \mathrm{U}^{(k)}$. □

Proof of Lemma 3. By Claim 21 we have $l \in \mathbb{N}$ and subgroups $B_1, \dots, B_l$ of $\langle A, +\rangle$ that contain M such that

$$\mathrm{Pol}_1(\mathbf{A}) \cap W^{(1)} = \mathrm{Fix}_{B_1}(W^{(1)}) + \cdots + \mathrm{Fix}_{B_l}(W^{(1)}). \tag{5.23}$$

Claim 23, (1)⇒(2), yields

$$\mathrm{Pol}_k(\mathbf{A}) \cap W^{(k)} \geq \mathrm{Fix}_{B_1^k}(W^{(k)}) + \cdots + \mathrm{Fix}_{B_l^k}(W^{(k)}). \tag{5.24}$$

Seeking a contradiction we suppose that the inequality in (5.24) is strict. By Claims 21 and 22 there exists a subgroup B of $\langle A, +\rangle$ such that $M \leq B$, $B_i \not\leq B$ for any $i \in \{1, \dots, l\}$ and $\mathrm{Fix}_{B^k}(W^{(k)}) \leq \mathrm{Pol}_k(\mathbf{A}) \cap W^{(k)}$. Then $\mathrm{Fix}_B(W^{(1)}) \leq \mathrm{Pol}_1(\mathbf{A}) \cap W^{(1)}$ by Claim 23, (2)⇒(1). But by Claim 22 $\mathrm{Fix}_B(W^{(1)}) \not\leq \mathrm{Fix}_{B_1}(W^{(1)}) + \cdots + \mathrm{Fix}_{B_l}(W^{(1)})$ because $B_i \not\leq B$ for any $i \in \{1, \dots, l\}$. This contradicts (5.23). Hence we have equality in (5.24). □

6. The proof of Theorem 1

For an algebra $\mathbf{A} := \langle A, F\rangle$ and $k, r \in \mathbb{N}$ let

$$\mathrm{Comp}_k(A, \mathrm{Pol}_r(\mathbf{A})) := \{f \in A^{A^k} : f(g_1, \dots, g_k) \in \mathrm{Pol}_r(\mathbf{A}) \text{ for all } g_1, \dots, g_k \in \mathrm{Pol}_r(\mathbf{A})\}$$

and

$$\mathrm{Comp}(A, \mathrm{Pol}_r(\mathbf{A})) := \bigcup_{k \in \mathbb{N}} \mathrm{Comp}_k(A, \mathrm{Pol}_r(\mathbf{A})).$$

So $\mathrm{Comp}(A, \mathrm{Pol}_r(\mathbf{A}))$ is the set of finitary functions that preserve (the graphs of) the r-ary polynomial functions on $\mathbf{A}$.

Lemma 24. *Let $\mathbf{A}$ be an algebra, let $k, r \in \mathbb{N}$, and let $\bar{\mathbf{A}} := \langle A, \mathrm{Comp}(A, \mathrm{Pol}_r(\mathbf{A}))\rangle$. Then we have:*

(1) $\mathrm{Comp}(A, \mathrm{Pol}_r(\mathbf{A}))$ *is the largest clone C on A such that the set of r-ary functions in C is equal to* $\mathrm{Pol}_r(\mathbf{A})$.
(2) $\mathrm{Pol}(\bar{\mathbf{A}}) = \mathrm{Comp}(A, \mathrm{Pol}_r(\mathbf{A}))$.
(3) $\mathrm{Con}(\bar{\mathbf{A}}) = \mathrm{Con}(\mathbf{A})$.

Proof. Items (1) and (2) are immediate from the definitions. Since $\mathrm{Pol}_1(\mathbf{A}) = \mathrm{Pol}_1(\bar{\mathbf{A}})$ and since the unary polynomial functions determine the congruences of an algebra [8, Theorem 4.18], we have (3). □

We are now ready to prove the following stronger version of Theorem 1.

Theorem 25. *Let $\mathbf{A}$ be an expansion of a group of squarefree order n.*

(1) If n is odd, then $\mathrm{Pol}(\mathbf{A}) = \mathrm{Comp}(A, \mathrm{Pol}_1(\mathbf{A}))$.
(2) If n is even, then $\mathrm{Pol}(\mathbf{A}) = \mathrm{Comp}(A, \mathrm{Pol}_2(\mathbf{A}))$.

Proof. By Lemma 10 there exists a binary polynomial function $+$ on the group reduct of $\mathbf{A}$ such that $\langle A, +\rangle$ is a cyclic group. Since $\mathrm{Pol}(\mathbf{A}) = \mathrm{Pol}(\langle A, \mathrm{Pol}(\mathbf{A})\rangle)$, we may assume that $\mathbf{A}$ is an expansion of $\langle A, +\rangle$.

Let $r := 1$ if n is odd and $r := 2$ if n is even. Let $\bar{\mathbf{A}} := \langle A, \mathrm{Comp}(A, \mathrm{Pol}_r(\mathbf{A}))\rangle$, and let $k \in \mathbb{N}$. By Lemma 24 we only need to show that

$$\mathrm{Pol}_k(\bar{\mathbf{A}}) \subseteq \mathrm{Pol}_k(\mathbf{A}). \tag{6.3}$$

We use induction on $|A|$. First we assume that there exist non-trivial ideals $I, J \in \mathrm{Id}\,(\mathbf{A})$ such that $I \cap J = 0$. Let $f \in \mathrm{Pol}_k(\bar{\mathbf{A}})$. Since f is congruence preserving on $\mathbf{A}$ by Lemma 24 (3), we may consider f_I and f_J on the quotients A/I and A/J, respectively. Now $f_I \in \mathrm{Pol}_k(\bar{\mathbf{A}}/I)$, $f_J \in \mathrm{Pol}_k(\bar{\mathbf{A}}/J)$ yield $f_I \in \mathrm{Pol}_k(\mathbf{A}/I)$, $f_J \in \mathrm{Pol}_k(\mathbf{A}/J)$ by the induction assumption. Since the orders of I and J are relatively prime, there exists $\pi \in \mathrm{Pol}_1(\langle A, +\rangle)$ such that $\pi(i + j) = i$ for all $i \in I, j \in J$. So, by Lemma 4, we obtain $f \in \mathrm{Pol}_k(\mathbf{A})$.

For the following we assume that $\mathbf{A}$ is subdirectly irreducible with monolith M. By Lemma 24 (3) the same is true for $\bar{\mathbf{A}}$. We claim that

$$\mathrm{Pol}_k(\bar{\mathbf{A}}) \cap M^{A^k} \subseteq \mathrm{Pol}_k(\mathbf{A}) \cap M^{A^k}. \tag{6.4}$$

If M is non-abelian in $\mathbf{A}$, then $M^{A^k} \subseteq \mathrm{Pol}_k(\mathbf{A})$ by Lemma 5 and (6.4) follows trivially. We assume that M is an abelian ideal in $\mathbf{A}$. Then $\langle M, \mathrm{Pol}(\mathbf{A})|_M\rangle$ is polynomially equivalent to a vector space by Lemma 7. If $|M| > 2$, this yields $M^A \not\subseteq \mathrm{Pol}_1(\mathbf{A})$. If $|M| = 2$, we still obtain $M^{A^2} \not\subseteq \mathrm{Pol}_2(\mathbf{A})$. Since $\mathrm{Pol}_r(\mathbf{A}) = \mathrm{Pol}_r(\bar{\mathbf{A}})$ by Lemma 24, Lemma 5 implies that M is abelian in $\bar{\mathbf{A}}$ in both cases. Let

$$C := \min\{H \leq \langle A, +\rangle \;:\; \exists e \in \mathrm{Pol}_1(\mathbf{A}) \text{ with } e(A) \subseteq M, e|_M = \mathrm{id}_M, e(A \setminus H) = 0\}.$$

Then C is the centralizer of M in $\mathbf{A}$ and in $\bar{\mathbf{A}}$ by Lemmas 6 and 9. Let T be a transversal for the cosets of C in A, and let $f \in \mathrm{Pol}_k(\bar{\mathbf{A}}) \cap M^{A^k}$. Then

$$f(m + c + t) = f(m + t) - f(t) + f(c + t) \text{ for all } m \in M^k, c \in C^k, t \in T^k$$

by Lemma 6. Since M is abelian and n is squarefree, $\langle M, \mathrm{Pol}(\bar{\mathbf{A}})|_M\rangle$ is polynomially equivalent to a vector space over $\mathbf{F} := \mathrm{GF}(|M|)$ by Lemma 7. Let $s \in T^k$ be fixed. The function $g \in M^{M^k}$ that is defined by $g(m) := f(m + s) - f(s)$ for $m \in M^k$ is $\mathbf{F}$-linear. Since M has prime order, there exist $c_{s,1}, \ldots, c_{s,k} \in \mathbb{Z}$ such that

$$f((m_1, \ldots, m_k) + s) = \sum_{i=1}^{k} c_{s,i} m_i + f(s) \text{ for all } m_1, \ldots, m_k \in M.$$

Since $|M|$ and $|A : M|$ are relatively prime, there exists an idempotent polynomial function on $\langle A, +\rangle$ that maps A onto M. By Lemma 9 we have functions $e_i \in \mathrm{Pol}_k(\mathbf{A})$ for $i \in \{1, \ldots, k\}$ such that $e_i(A^k) \subseteq M$, $e_i(x_1, \ldots, x_k) = x_i$ for all $x_1, \ldots, x_k \in M$, and $e_i(A^k \setminus C^k) = 0$. We consider

$$h_s : A^k \to M,\ x \mapsto \sum_{i=1}^{k} c_{s,i} e_i(x - s) + f(s).$$

By its definition h_s is in $\mathrm{Pol}_k(\mathbf{A})$. We have $h_s(x) = f(x)$ for all $x \in M^k + s$ and $h_s(x) = f(s)$ for all $x \in A^k \setminus (C^k + s)$. As a polynomial function h_s satisfies $h_s(m+c+x) = h_s(m+x) - h_s(x) + h_s(c+x)$ for all $m \in M^k$, $c \in C^k$, $x \in A^k$ by Lemma 6. For $m \in M^k$ and $c \in C^k$ we then obtain

$$\begin{aligned}(f - \sum_{t\in T^k} h_t)(m+c+s) &= f(m+c+s) - h_s(m+c+s) - \sum_{t\in T^k\setminus\{s\}} f(t)\\ &= f(m+s) - f(s) + f(c+s)\\ &\quad -(h_s(m+s) - h_s(s) + h_s(c+s)) - \sum_{t\in T^k\setminus\{s\}} f(t)\\ &= f(c+s) - h_s(c+s) - \sum_{t\in T^k\setminus\{s\}} f(t).\end{aligned}$$

Thus $f - \sum_{t\in T^k} h_t$ is constant on all cosets of M^k in A^k.

Since the functions into M that are constant on the cosets of M in A are the same in $\mathrm{Pol}_1(\bar{\mathbf{A}})$ and in $\mathrm{Pol}_1(\mathbf{A})$, Lemma 3 yields that every k-ary polynomial function on $\bar{\mathbf{A}}$ that maps into M and is constant on all cosets of M^k in A^k is in $\mathrm{Pol}_k(\mathbf{A})$. In particular $f - \sum_{t\in T^k} h_t \in \mathrm{Pol}_k(\mathbf{A})$. As $\sum_{t\in T^k} h_t \in \mathrm{Pol}_k(\mathbf{A})$, we finally obtain $f \in \mathrm{Pol}_k(\mathbf{A})$. Thus (6.4) is proved.

We are now ready to show (6.3). By the Homomorphism Theorem for subalgebras of $\mathbf{A}^{A^k}$ and $\bar{\mathbf{A}}^{A^k}$, respectively, we have

$$\begin{aligned}|\mathrm{Pol}_k(\mathbf{A})| &= |\mathrm{Pol}_k(\mathbf{A}/M)| \cdot |\mathrm{Pol}_k(\mathbf{A}) \cap M^{A^k}|,\\ |\mathrm{Pol}_k(\bar{\mathbf{A}})| &= |\mathrm{Pol}_k(\bar{\mathbf{A}}/M)| \cdot |\mathrm{Pol}_k(\bar{\mathbf{A}}) \cap M^{A^k}|.\end{aligned}$$

By the induction hypothesis, $\mathrm{Pol}(\bar{\mathbf{A}}/M) \subseteq \mathrm{Pol}(\mathbf{A}/M)$, and by (6.4) we obtain

$$|\mathrm{Pol}_k(\bar{\mathbf{A}})| \leq |\mathrm{Pol}_k(\mathbf{A})|.$$

Since $\mathrm{Pol}_k(\bar{\mathbf{A}}) \supseteq \mathrm{Pol}_k(\mathbf{A})$ by Lemma 24, this yields (6.3). □

In the proof of Theorem 25 knowledge about $\mathrm{Pol}_2(\mathbf{A})$ is required only for proving (6.4) for the case of an abelian 2-element section in $\mathrm{Con}(\mathbf{A})$. If there are no such sections in $\mathrm{Con}(\mathbf{A})$ (in particular, if $|\mathbf{A}|$ is odd), then $\mathrm{Pol}_1(\mathbf{A})$ determines $\mathrm{Pol}(\mathbf{A})$. However not all polynomial clones of squarefree expanded groups are determined by their unary functions. Consider $\mathrm{Pol}_1(\langle \mathbb{Z}_2, +\rangle) = \mathrm{Pol}_1(\langle \mathbb{Z}_2, +, \cdot\rangle)$ but $\mathrm{Pol}_2(\langle \mathbb{Z}_2, +\rangle) \neq \mathrm{Pol}_2(\langle \mathbb{Z}_2, +, \cdot\rangle)$.

Theorem 1 follows immediately from Lemma 24 and Theorem 25. We also obtain the equivalence of (1) and (2) of Theorem 1.1 in [1] but not that (3) implies (1).

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

(1) $\mathrm{Pol}(\mathbf{A}_1) = \mathrm{Pol}(\mathbf{A}_2)$.
(2) $\mathrm{Pol}_2(\mathbf{A}_1) = \mathrm{Pol}_2(\mathbf{A}_2)$.
(3) $\langle \mathrm{Con}(\mathbf{A}_1), \wedge, \vee, [.,.]\rangle = \langle \mathrm{Con}(\mathbf{A}_2), \wedge, \vee, [.,.]\rangle$.

7. Congruences and commutators do not determine polynomial functions

In [1] and [6] we verified Idziak's conjecture [5, Conjecture 9] for expanded groups whose order is the product of at most 3 distinct primes by showing that every function on such an algebra that preserves congruences and binary commutators is polynomial. In this section we show that this is not true for expansions of groups whose order is the product of more than 3 primes.

To simplify notation we present 2 concrete expansions of $\langle \mathbb{Z}_{210}, + \rangle$ with the same congruences and commutator relations but distinct clones. These examples can be easily generalized to the case of $\mathbb{Z}_n$ with n the product of at least 4 primes.

Let $V := \mathbb{Z}_{210}$. For $X \subseteq V^2$ we define $g_X : V^2 \to V$ by

$$g_X(x) := \begin{cases} 30 \text{ if } x \in X, \\ 0 \ \text{ otherwise.} \end{cases}$$

Let $A := 6V, B := 10V, C := 15V, M := 30V$. We define

$$\mathbf{V}_1 := \langle V, +, g_{A^2}, g_{B^2}, g_{C^2} \rangle \text{ and } \mathbf{V}_2 := \langle V, +, g_{M^2} \rangle.$$

Claim 26. $\mathrm{Pol}(\mathbf{V}_1) \subseteq \mathrm{Pol}(\mathbf{V}_2)$.

Proof. Obvious since M is a subgroup of A, B, and C. $\square$

Claim 27. *Let $i \in \{1, 2\}$. Then $\mathbf{V}_i$ is subdirectly irreducible with monolith M, and $\mathbf{V}_i/M$ is term equivalent to the cyclic group of order 30. In particular* $\mathrm{Id}\,(\mathbf{V}_1) = \mathrm{Id}\,(\mathbf{V}_2)$.

Proof. Let $u \in V, u \neq 0$. We show that the ideal U of $\mathbf{V}_i$ that is generated by u contains M. If $u \in A \cap B \cap C$, then $u \in M \setminus 0$ and $U = M$. Assume $u \notin A$. Since g_{A^2} is in $\mathrm{Pol}(\mathbf{V}_i)$, U contains $g_{A^2}(0,0) - g_{A^2}(u,0) = 30$ and consequently $M \subseteq U$. The cases $u \notin B$ and $u \notin C$, respectively, are dealt with in the same way. $\square$

Claim 28. *Let $i \in \{1, 2\}$. Then $[\![V, M]\!]_{\mathbf{V}_i} = 0$ and $[\![X, Y]\!]_{\mathbf{V}_i} = M$ for all $X, Y \in \{A, B, C\}$.*

Proof. Since $g_{A^2}, g_{B^2}, g_{C^2}, g_{M^2}$ are constant on the cosets of M^2 in V^2, we have

$$f(x) - f(x+m) + f(z) = f(-m+z) \text{ for all } x, z \in V^2, m \in M^2, f \in \{g_{A^2}, g_{B^2}, g_{C^2}, g_{M^2}\}.$$

Hence $[\![V, M]\!]_{\mathbf{V}_i} = 0$ by [1, Lemma 2.4]. Since $g_{(6,10)+C^2} \in \mathrm{Pol}_2(\mathbf{V}_i)$ is absorptive and $g_{(6,10)+C^2}(A \times B) = \{0, 30\}$, we obtain $M \subseteq [\![A, B]\!]_{\mathbf{V}_i}$. By $[\![A, B]\!]_{\mathbf{V}_i} \subseteq A \cap B = M$, we have $[\![A, B]\!]_{\mathbf{V}_i} = M$. Similarly $[\![B, C]\!]_{\mathbf{V}_i} = [\![A, C]\!]_{\mathbf{V}_i} = M$.

Since $\mathbf{V}_i/M$ is term equivalent to an abelian group, we have $[\![A, A]\!]_{\mathbf{V}_i} \subseteq M$. From $g_{(6,6)+C^2}(A, A) = \{0, 30\}$ we obtain $M \subseteq [\![A, A]\!]_{\mathbf{V}_i}$. Thus $[\![A, A]\!]_{\mathbf{V}_i} = M$, and similarly $[\![B, B]\!]_{\mathbf{V}_i} = [\![C, C]\!]_{\mathbf{V}_i} = M$. $\square$

By the previous claim the commutator operations on $\mathbf{V}_1$ and $\mathbf{V}_2$ are equal on all pairs of join irreducible ideals. Thus we have the following.

Claim 29. $[\![X,Y]\!]_{\mathbf{V}_1} = [\![X,Y]\!]_{\mathbf{V}_2}$ *for all ideals* X, Y *of* $\mathbf{V}_1$.

A straighforward application of our description of polynomial functions in Section 5 yields that $\mathrm{Pol}(\mathbf{V}_1) \neq \mathrm{Pol}(\mathbf{V}_2)$. Instead we will show this inequality directly by presenting an 8-ary relation that is preserved by the fundamental operations of $\mathbf{V}_1$ but not by those of $\mathbf{V}_2$. Let

$$\begin{aligned} S := \{(x_1,\dots,x_8) \in V^8 \ : \ & \{x_2-x_1, x_5-x_3, x_7-x_4, x_8-x_6\} \subseteq A, \\ & \{x_3-x_1, x_5-x_2, x_6-x_4, x_8-x_7\} \subseteq B, \\ & \{x_4-x_1, x_6-x_3, x_7-x_2, x_8-x_5\} \subseteq C, \\ & x_1-(x_2+x_3+x_4)+x_5+x_6+x_7 = x_8\}. \end{aligned}$$

Claim 30. S *is a subalgebra of* ${\mathbf{V}_1}^8$.

Proof. Clearly S forms a subgroup of $\langle V,+\rangle^8$. Let $x, y \in S$, $g := g_{A^2}$. We show that $(g(x_1,y_1),\dots,g(x_8,y_8)) \in S$. Since g preserves the congruences induced by A, B, C, it suffices to show

$$g(x_1,y_1)-(g(x_2,y_2)+g(x_3,y_3)+g(x_4,y_4))+g(x_5,y_5)+g(x_6,y_6)+g(x_7,y_7) = g(x_8,y_8). \quad (7.4)$$

Since g is constant on the cosets of A^2 in V^2, we have $g(x_1,y_1) = g(x_2,y_2)$, $g(x_3,y_3) = g(x_5,y_5), g(x_4,y_4) = g(x_7,y_7), g(x_6,y_6) = g(x_8,y_8)$, which proves (7.4). Similarly g_{B^2} and g_{C^2} preserve S. □

Claim 31. g_{M^2} *does not preserve* S.

Proof. Note that $x := (0,6,10,15,6+10,10+15,6+15,6+10+15)$ is in S but $g_{M^2}(x,x) = (30,0,\dots,0)$ is not in S. □

Hence $g_{M^2} \notin \mathrm{Pol}(\mathbf{V}_1)$ which yields our final result. We recall that the clone of *term functions* [8, Definition 4.2], $\mathrm{Clo}(\mathbf{A})$, on an algebra $\mathbf{A} := \langle A, F\rangle$ is the smallest clone on A that contains all fundamental operations F of $\mathbf{A}$.

Claim 32. $\mathrm{Clo}(\mathbf{V}_1) \neq \mathrm{Clo}(\mathbf{V}_2)$ *and* $\mathrm{Pol}(\mathbf{V}_1) \neq \mathrm{Pol}(\mathbf{V}_2)$.

Acknowledgements

The author thanks Erhard Aichinger and Ágnes Szendrei for helpful discussions on the material in this paper.

References

[1] E. Aichinger and P. Mayr. Polynomial clones on groups of order pq. *Acta Math. Hungar.*, 114(3):267–285, 2007.

[2] 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.

[3] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I.* John Wiley & Sons Inc., New York, 1981. With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication.

[4] 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.

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

[6] P. Mayr. Polynomial clones on groups of order pqr. *Johannes Kepler Universität Linz - Berichte der mathematischen Institute*, number 563, 2007.

[7] P. Mayr. The polynomial functions on Frobenius complements. *Acta Sci. Math. (Szeged)*, 72(1-2):37–50, 2006.

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

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

[10] D. J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1996.

[11] L. H. Rowen. *Ring Theory, Volume I.* Academic Press, Inc., San Diego, California, 1988.