ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Algebra 271 (2004) 65–107

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Polynomial interpolation in expanded groups

Erhard Aichinger [a,*,1] and Paweł M. Idziak [b,2]

[a] *Institut für Algebra, Stochastik und wissensbasierte mathematische Systeme, Johannes Kepler Universität Linz, 4040 Linz, Austria*

[b] *Computer Science Department, Jagiellonian University, Krakow, Poland*

Received 10 May 2001

Communicated by H.A. Priestley

Abstract

We call an algebra strictly 1-affine complete iff every unary congruence preserving partial function with finite domain is a restriction of a polynomial. We characterize finite strictly 1-affine complete groups with operations, and, in particular, all finite strictly 1-affine complete groups and commutative rings with unit.

1. Problem and result

Let **A** be an arbitrary algebra. By a (k-ary) polynomial of **A** we mean an expression of the form $\mathbf{t}(x_1, \ldots, x_k, a_1, \ldots, a_m)$, where **t** is a term in the language of **A** and $a_1, \ldots, a_m$ are arbitrary elements of **A**. We identify polynomials with the functions they determine. It is clear that every polynomial preserves all congruences of **A**. However, in general there are congruence preserving functions that cannot be represented by polynomials. The problem of describing algebras in which every congruence preserving function is a polynomial was posed in [10, Problem 6]. Following H. Werner [39], we call such algebras affine complete. They have received considerable attention during the last years [22,31]. Recently, K. Kaarli and R. McKenzie [21] have shown that every variety in which all algebras are affine

* Corresponding author.
E-mail addresses: erhard@algebra.uni-linz.ac.at (E. Aichinger), idziak@ii.uj.edu.pl (P.M. Idziak).

[1] The first author has been supported by a "Doktorandenstipendium" of the Austrian Academy of Sciences and by the project P-12911-INF of the Austrian Science Fund (FWF).

[2] The second author has partially been supported by a Polish KBN grant.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2003.08.008

complete must be congruence distributive. This paper also describes important steps in the study of affine complete varieties.

The situation is much more complicated if we restrict ourselves to a single algebra. For example, the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is affine complete, whereas the variety it generates is not. Results on affine complete groups and modules can be found in [18,19,28,33,34]. Difficulties also arise if we try to interpolate (congruence preserving) partial functions by polynomials. An algebra is called *strictly* affine complete if every congruence preserving partial function $T \to A$ with finite domain T contained in some power of A is a restriction of a polynomial of $\mathbf{A}$. (The precise meaning of *congruence preserving*, *k-affine complete*, and *strictly k-affine complete* is given in Definitions 4.1, 4.2, and 4.3.) J. Hagemann and C. Herrmann [13] have characterized strictly affine complete algebras. From their characterization one can infer that an algebra from a congruence permutable variety is strictly affine complete iff it is strictly 2-affine complete, i.e., all binary partial functions (here $T \subseteq A^2$) that respect congruences can be interpolated by polynomials (cf. [2]). On the other hand, polynomial interpolation for unary (partial) functions remains unsettled, even for finite algebras. Among strictly 1-affine complete algebras that are not strictly 2-affine complete we have the symmetric groups S_n with $n \geqslant 5$ [23], the groups $(\mathbb{Z}_2)^n$ with $n \geqslant 1$, and the ring $\mathbb{Z}_4$ [30]. Recent ideas concerning polynomial interpolation in groups are contained in [7,36]. From these results, one gets the impression that (strict) affine completeness imposes a restricted structure even if the concept is applied to a single algebra.

In the present paper, we develop techniques for polynomial interpolation that work for all algebras that have a group reduct; we will call those algebras *expanded groups*. In particular, our techniques work for all groups, all rings, all ring-modules, and all Ω-groups in the sense of [24]. Using these techniques, we obtain a full characterization of finite strictly 1-affine complete expanded groups; as a consequence of the extension principle for compatible functions [20], this characterization also describes all finite 1-affine complete expanded groups among those with distributive congruence lattice. (By K. Kaarli's result [20, Theorem 3], a finite algebra in a congruence permutable variety with distributive congruence lattice is strictly 1-affine complete if and only if it is 1-affine complete.)

The groups we consider will be written additively, although they need not be abelian. An ideal of an expanded group $\langle \mathbf{V}, +, -, 0, \mathbf{f}_1, \mathbf{f}_2, \ldots \rangle$ is a normal subgroup I of $\langle \mathbf{V}, +, -, 0 \rangle$ such that for all additional operations $\mathbf{f}_j$ we have

$$\mathbf{f}_j(v_1 + i_1, \ldots, v_k + i_k) - \mathbf{f}_j(v_1, \ldots, v_k) \in I$$

whenever $i_1, i_2, \ldots, i_k \in I$ and $v_1, v_2, \ldots, v_k \in V$. Similar to [14,24], we find that there is a bijective correspondence between ideals and congruences of an expanded group; however, we note that an ideal of the expanded group $\mathbf{V}$ is not necessarily a subuniverse of $\mathbf{V}$.

The lattice of the ideals of the expanded group $\mathbf{V}$ will be denoted by $\mathsf{Id}\,\mathbf{V}$, and the sum of the ideals I and J by $I \vee J$. We write $I \prec J$ if J covers I, i.e., if $I \subset J$ and there is no other ideal between I and J. If I is a strictly meet irreducible element of $\mathsf{Id}\,\mathbf{V}$ and $I \prec J$, we write I^+ for this unique J. If I is strictly join irreducible and $J \prec I$, we write I^- for this J. We abbreviate the set of all k-ary polynomials on $\mathbf{V}$ by $\mathsf{Pol}_k\,\mathbf{V}$, and the domain of a partial function f by $\mathsf{dom}\,f$.

Commutator theory usually works with congruences, but in expanded groups we rather work with ideals. For two ideals $A, B \in \mathsf{Id}\,\mathbf{V}$, the commutator $[A, B]$ is the ideal generated by the set

$$\big\{\mathbf{p}(a,b) \mid a \in A,\ b \in B,\ \mathbf{p} \in \mathsf{Pol}_2\,\mathbf{V},\ \forall x \in V\colon\ \mathbf{p}(x,0) = \mathbf{p}(0,x) = 0\big\}.$$

This is the actual definition given by S.D. Scott [36] for Ω-groups. It differs from the one previously used by P.J. Higgins [14] and A.G. Kurosh [24], but coincides with the modular commutator widely used in general algebra [8,11,12,37].

Given two ideals $I, J \in \mathsf{Id}\,\mathbf{V}$, the *centralizer* of J modulo I, written as $(I : J)$, is the largest ideal $C \in \mathsf{Id}\,\mathbf{V}$ such that $[C, J] \leqslant I$.

We need two conditions for characterizing strictly 1-affine complete expanded groups. The first one has already been isolated in [16].

Definition 1.1. An expanded group $\mathbf{V}$ satisfies the condition (SC1) if for every strictly meet irreducible ideal M of $\mathbf{V}$ we have $(M : M^+) \leqslant M^+$.

The condition (SC1) is equivalent to the following: In every subdirectly irreducible quotient of $\mathbf{V}$, the centralizer of the monolith is not strictly larger than the monolith.

The following condition requires that abelian parts of the expanded group are small:

Definition 1.2. An expanded group $\mathbf{V}$ satisfies the condition (AB2) if for all $A, B \in \mathsf{Id}\,\mathbf{V}$ with $A \prec B$ and $[B, B] \leqslant A$ the ideal B contains exactly two cosets of A.

The special role of ideals $A \prec B$ with $[B, B] \leqslant A$ and $|B/A| = 2$ has also been highlighted in [36, p. 136]. We are now ready to state our main result.

Theorem 1.3. *For a finite expanded group* $\mathbf{V}$ *the following are equivalent*:

(1) $\mathbf{V}$ *satisfies* (SC1) *and* (AB2).
(2) $\mathbf{V}$ *is strictly* 1*-affine complete.*
(3) *Every homomorphic image of* $\mathbf{V}$ *is strictly* 1*-affine complete.*
(4) *Every homomorphic image of* $\mathbf{V}$ *is* 1*-affine complete.*

The proof of Theorem 1.3 is concluded at the end of Section 10. Along the proof, we also obtain a fairly good description of unary polynomials on expanded groups with (SC1). Theorem 1.3 was initially obtained using Tame Congruence Theory [15] together with the techniques from [16]; the proof given here, however, does not use TCT.

2. Notation

Let $\mathbf{V}$ be an expanded group. Then for $v \in V$, the smallest ideal of $\mathbf{V}$ that contains v will be denoted by $\mathcal{I}_{\mathbf{V}}(v)$. We define the set $P_0(\mathbf{V})$ by

$$P_0(\mathbf{V}) := \big\{\mathbf{p} \in \mathsf{Pol}_1\,\mathbf{V} \mid \mathbf{p}(0) = 0\big\}.$$

It is known that a subset S of V is an ideal of $\mathbf{V}$ if $s_1 + s_2 \in S$ and $\mathbf{p}(s) \in S$ for all $s, s_1, s_2 \in S$ and $\mathbf{p} \in P_0(\mathbf{V})$ [29, Theorem 7.123]. We note that $x - y$ lies in the ideal $\mathcal{I}_{\mathbf{V}}(v - w)$ iff there is a $\mathbf{p} \in \mathsf{Pol}_1 \mathbf{V}$ with $\mathbf{p}(v) = x$ and $\mathbf{p}(w) = y$. This observation allows to interpolate every congruence preserving function at every 2-element subset of its domain by a polynomial.

Let $A_1,\ A_2$ be in $\mathsf{Id}\,\mathbf{V}$ such that $A_1 \leqslant A_2$. Then $I[A_1, A_2] := \{B \in \mathsf{Id}\,\mathbf{V} \mid A_1 \leqslant B \leqslant A_2\}$. We say that $I[A_1, A_2]$ projects up to $I[B_1, B_2]$ iff $A_1 = A_2 \wedge B_1$ and $B_2 = A_2 \vee B_1$ and write $I[A_1, A_2] \nearrow I[B_1, B_2]$ or $I[B_1, B_2] \searrow I[A_1, A_2]$. The smallest equivalence relation that contains $\nearrow$ will be abbreviated by $\nwarrow\!\!\searrow$. If $I[A_1, A_2] \nwarrow\!\!\searrow I[B_1, B_2]$, we say that the two intervals are *projective*.

The interval $I[A_1, A_2]$ is called *abelian* iff $[A_2, A_2] \leqslant A_1$. Obviously, this is equivalent to $(A_1 : A_2) \geqslant A_2$.

We list some important properties of the commutator operation in the following proposition:

Proposition 2.1. *Let A, B, C be ideals of the expanded group $\mathbf{V}$. Then we have*

(1) $[A \vee B, C] = [A, C] \vee [B, C]$.
(2) $[A, B] = [B, A]$.
(3) $[A, B] \leqslant A \wedge B$.
(4) *Let $A \leqslant B$. Then an element $z \in V$ lies in $(A : B)$ iff $\mathbf{s}(z, b) \in A$ for all $b \in B$ and for all $\mathbf{s} \in \mathsf{Pol}_2 \mathbf{V}$ that satisfy $\forall v \in V\colon\ \mathbf{s}(v, 0) = \mathbf{s}(0, v) = 0$.*

Although the first three properties are well known in commutator theory [8] and number (4) follows from [36, Proposition 9.5], the differences in notation justify that we state a proof.

Proof. We call a binary polynomial function $\mathbf{s}$ a *commutator polynomial* iff $\mathbf{s}(v, 0) = \mathbf{s}(0, v) = 0$ for all $v \in V$. For (1), we only show $\leqslant$. For $a \in A, b \in B, c \in C$ and a commutator polynomial $\mathbf{s}$, we have $\mathbf{s}(a+b, c) = \mathbf{s}(a+b, c) - \mathbf{s}(b, c) + \mathbf{s}(b, c)$. Considering $\mathbf{s}_1(x, y) := \mathbf{s}(x + b, y) - \mathbf{s}(b, y)$, we see $\mathbf{s}(a + b, c) - \mathbf{s}(b, c) = \mathbf{s}_1(a, c) \in [A, C]$. The second term $\mathbf{s}(b, c)$ obviously lies in $[B, C]$.

For (4), we are done if we show that the set

$$Z := \big\{z \in V \mid \mathbf{s}(z, b) \in A \text{ for all } b \in B \text{ and all commutator polynomials } \mathbf{s}\big\}$$

is an ideal of $\mathbf{V}$. We show this using [29, Theorem 7.123]. To this end, let z be in Z, and let $\mathbf{p} \in P_0(\mathbf{V})$. We want to show that $\mathbf{p}(z)$ is in Z. We fix $b \in B$ and a commutator polynomial $\mathbf{s}$, and compute $\mathbf{s}(\mathbf{p}(z), b)$. Since $z \in Z$, we know that $\mathbf{t}(z, b)$ lies in A, where $\mathbf{t}(x, y) = \mathbf{s}(\mathbf{p}(x), y)$. Thus $\mathbf{s}(\mathbf{p}(z), b) \in A$. For showing that Z is closed under addition, let $z_1, z_2 \in Z$. We write $\mathbf{s}(z_1 + z_2, b)$ as $\mathbf{s}(z_1 + z_2, b) - \mathbf{s}(z_2, b) + \mathbf{s}(z_2, b)$. Defining $\mathbf{t}(x, y) := \mathbf{s}(x + z_2, y) - \mathbf{s}(z_2, y)$, we see that $\mathbf{s}(z_1 + z_2, b) - \mathbf{s}(z_2, b)$ lies in A; since $\mathbf{s}(z_2, b)$ also lies in A, we get $\mathbf{s}(z_1 + z_2, b) \in A$. Hence Z is also closed under addition, and therefore an ideal. □

From these properties, it is easy to infer the following well-known properties of projective intervals in $\mathsf{Id}\,\mathbf{V}$, which we restate for easier reference. For two ideals A, B of $\mathbf{V}$ with $A \leqslant B$, we define the set B/A by

$$B/A := \{b + A \mid b \in B\}.$$

Proposition 2.2 (cf. [8, Remarks 4.6, p. 35]). *Let* $\mathbf{V}$ *be an expanded group and let* $A_1, A_2, B_1, B_2 \in \mathsf{Id}\,\mathbf{V}$ *such that* $I[A_1, A_2] \nsim I[B_1, B_2]$. *Then we have*:

(1) $(A_1 : A_2) = (B_1 : B_2)$.
(2) $I[A_1, A_2]$ *is abelian iff* $I[B_1, B_2]$ *is abelian.*
(3) A_2 *contains as many* A_1*-cosets as* B_2 *contains* B_1*-cosets, i.e.,* $|A_2/A_1| = |B_2/B_1|$.

Proof. The first two properties can be checked immediately. Property (3) is a consequence of the isomorphism theorem $(A_1 + B_2)/A_1 \cong B_2/A_1 \cap B_2$ for groups. □

The commutator puts the following linearity condition on polynomials:

Proposition 2.3 (cf. [8, Proposition 5.7]). *Let* $A, B \in \mathsf{Id}\,\mathbf{V}$ *and* $\mathbf{p} \in P_0(\mathbf{V})$. *Then we have* $\mathbf{p}(a) + \mathbf{p}(b) \equiv \mathbf{p}(a + b) \pmod{[A, B]}$ *for all* $a \in A$, $b \in B$.

3. Properties of expanded groups with (SC1)

As in [8, p. 77], we say that an expanded group $\mathbf{V}$ satisfies the condition (C1) iff for all ideals $A, B \in \mathsf{Id}\,\mathbf{V}$ the equality $A \wedge [B, B] = [A \wedge B, B]$ holds. In [16], a stronger version of condition (C1), as well as many other techniques applied in this paper, has been developed to describe those algebras in which every function preserving certain properties of the congruence lattice is a polynomial; this condition has been named (SC1) for "strong (C1)" there. We need the following consequences of the condition (SC1).

Proposition 3.1. *Let* $\mathbf{V}$ *be an expanded group satisfying the condition* (SC1). *Then the following holds*:

(1) *For all* $A, B \in \mathsf{Id}\,\mathbf{V}$ *with* $A \leqslant [B, B]$ *we have* $A = [A, B]$.
(2) *For all* $A, B \in \mathsf{Id}\,\mathbf{V}$ *we have* $A \wedge [B, B] = [A \wedge B, B]$.
(3) *For all* $A, B \in \mathsf{Id}\,\mathbf{V}$ *we have* $[A, B] = ([A, A] \wedge B) \vee (A \wedge [B, B])$.

Proof. For (1), suppose that in an expanded group with (SC1), we have ideals A and B such that $A \leqslant [B, B]$ and $A > [A, B]$. Since every proper ideal of $\mathbf{V}$ is the intersection of strictly meet irreducible ideals, we have a strictly meet irreducible ideal E of $\mathbf{V}$ such that $E \geqslant [A, B]$, $E \not\geqslant A$. First of all we observe that E^+ is abelian over E: Obviously, we have $E \vee A \geqslant E$. Since $E \not\geqslant A$, we have $E \vee A \geqslant E^+$. From this, we conclude

$[E^+, E^+] \leqslant [E \vee A, E \vee A] \leqslant E \vee [A, A] \leqslant E \vee [A, [B, B]] \leqslant E \vee [A, B] \leqslant E$. Now, condition (SC1) implies

$$\big(E : E^+\big) = E^+.$$

We will now show

$$\big[E^+, E \vee B\big] \leqslant E. \tag{3.1}$$

We already know that $E \vee A \geqslant E^+$. From this, we get $[E^+, E \vee B] \leqslant [E \vee A, E \vee B] \leqslant E \vee [A, B] \leqslant E$, which proves claim (3.1). Hence, by (SC1), we have $E \vee B \leqslant (E : E^+) = E^+$. Altogether, we obtain $A \leqslant [B, B] \leqslant [E \vee B, E \vee B] \leqslant [E^+, E^+] \leqslant E$, which gives $A \leqslant E$. But this is a contradiction to the choice of E. The items (2) and (3) were proved to be equivalent to (1) in [8, p. 79] and [8, Theorem 8.1]. □

Proposition 3.2. *Let* $\mathbf{V}$ *be an expanded group with* (SC1)*, and let* $A \in \mathsf{Id}\,\mathbf{V}$*. Then the commutator* $[A, A]$ *is the intersection of all subcovers* B *of* A *that satisfy* $B \geqslant [A, A]$*, and equal to* A *if no such subcover exists.*

Proof. We let A_0 be the intersection of all subcovers $B \prec A$ with $B \geqslant [A, A]$, and we set $A_0 := A$ if no such subcover exists. Then clearly $[A, A] \leqslant A_0$. Suppose that $[A, A] < A_0$. Then let E be a strictly meet irreducible ideal of $\mathbf{V}$ with $E \geqslant [A, A]$, $E \not\geqslant A_0$. Since $E \not\geqslant A_0$, we have $E \not\geqslant A$, and thus $E \vee A \geqslant E^+$. Hence we have

$$\big[E^+, E \vee A\big] \leqslant [E \vee A, E \vee A] \leqslant E \vee [A, A] \leqslant E.$$

Now condition (SC1) implies that $E \vee A = E^+$. This equality yields $I[E, E^+] \searrow I[A \wedge E, A]$. By the modularity of the lattice $\mathsf{Id}\,\mathbf{V}$, $A \wedge E \prec A$. Furthermore, since E^+ is abelian over E, Proposition 2.2 gives that A is abelian over $A \wedge E$. Therefore, $A \wedge E$ is one of the subcovers appearing in the in the intersection that forms A_0, and therefore, we have $A_0 \leqslant A \wedge E \leqslant E$. But this is a contradiction to the choice of E. □

Proposition 3.3. *For a finite expanded group* $\mathbf{V}$ *the following are equivalent*:

(1) $\mathbf{V}$ *satisfies the condition* (SC1).
(2) *There is no pair* (A, B) *of join irreducible ideals in* $\mathsf{Id}\,\mathbf{V}$ *such that* $A < B$ *and* $[A, B] \leqslant A^-$.

Proof. (1) ⇒ (2). Suppose that there are such A and B. Since $A < B$, we have $A \leqslant B^-$. By Proposition 3.2, we have $B^- \leqslant [B, B]$. Hence we have $A \leqslant [B, B]$, and therefore Proposition 3.1 implies $A = [A, B]$, which contradicts $[A, B] \leqslant A^-$.

(2) ⇒ (1). We assume that $\mathbf{V}$ does not satisfy the condition (SC1). Let M be a meet irreducible ideal of $\mathbf{V}$ such that $(M : M^+) > M^+$, and let $N := (M : M^+)$. Let B be an

ideal of $\mathbf{V}$ that is minimal with respect to the properties $B \leqslant N$, $B \not\leqslant M^+$. Obviously, B is join irreducible and $B^- \leqslant M^+$. Now we prove

$$B^- \not\leqslant M. \tag{3.2}$$

Suppose that $B^- \leqslant M$. By the choice of B, we know $M^+ \wedge B = B^-$. Hence we have $M = B^- \vee M = (M^+ \wedge B) \vee M$. By modularity of the lattice $\mathsf{Id}\,\mathbf{V}$, this is equal to $M^+ \wedge (B \vee M)$. Since M is meet irreducible, we get $B \vee M = M$. This implies $B \leqslant M$, which contradicts the choice of B and thus proves condition (3.2).

Let A be minimal with $A \leqslant B^-$, $A \not\leqslant M$. We see that A is join irreducible. Furthermore, $I[M, M^+] \searrow I[A^-, A]$. Therefore, Proposition 2.2 gives $(A^- : A) = (M : M^+) \geqslant N$. This implies $(A^- : A) \geqslant B$, hence $[A, B] \leqslant A^-$. This contradicts condition (2). □

4. (SC1) and (AB2) are necessary

4.1. Necessary conditions for strictly 1*-affine complete expanded groups*

We first state the definitions of two types of affine completeness that we are going to investigate in this paper.

Definition 4.1. Let $\mathbf{A}$ be a universal algebra, let $k \in \mathbb{N}$ and let D be a subset of A^k. Then a function $f : D \to A$ is a *compatible* or *congruence preserving* function on $\mathbf{A}$ iff for all $\mathbf{a}, \mathbf{b} \in D$ we have

$$f(\mathbf{a}) \equiv f(\mathbf{b}) \left(\mathrm{mod}\ \Theta_{\mathbf{A}}(\mathbf{a}, \mathbf{b})\right),$$

where $\Theta_{\mathbf{A}}(\mathbf{a}, \mathbf{b})$ is the congruence generated by $(a_1, b_1), (a_2, b_2), \ldots, (a_k, b_k)$.

Definition 4.2. We call an algebra $\mathbf{A}$ *k-affine complete* iff every congruence preserving function from A^k to A is a polynomial function.

Definition 4.3. We call an algebra $\mathbf{A}$ *strictly k-affine complete* iff every k-ary partial congruence preserving function with finite domain is a restriction of a polynomial function.

Every finite strictly 1-affine complete expanded group satisfies (SC1):

Proposition 4.4. *Let* $\mathbf{V}$ *be a finite strictly* 1*-affine complete expanded group. Then* $\mathbf{V}$ *satisfies the condition* (SC1).

Proof. Suppose that $\mathbf{V}$ does not satisfy (SC1). Then by Proposition 3.3 there are join irreducible ideals A, B with $A < B$ and $[B, A] \leqslant A^-$. Since A and B are join irreducible ideals, they are principal. Let $a, b \in \mathbf{V}$ be such that $\mathcal{I}_{\mathbf{V}}(a) = A$ and $\mathcal{I}_{\mathbf{V}}(b) = B$. We define

a function f by $f:\{0,a,b,a+b\}\to V$, $f(0)=f(a)=f(b)=0$, $f(a+b)=a$. First we show that f is a compatible function: for this we have to show

$$a\in\mathcal{I}_{\mathbf{V}}(a+b)\wedge\mathcal{I}_{\mathbf{V}}(b)\wedge\mathcal{I}_{\mathbf{V}}(a). \tag{4.1}$$

We clearly have $a\in\mathcal{I}_{\mathbf{V}}(b)\wedge\mathcal{I}_{\mathbf{V}}(a)=B\wedge A=A$. We also have $\mathcal{I}_{\mathbf{V}}(a+b)=B$: For this, we observe that $\mathcal{I}_{\mathbf{V}}(a+b)\leqslant B$. Furthermore, b lies in $\mathcal{I}_{\mathbf{V}}(a+b)\vee\mathcal{I}_{\mathbf{V}}(a)$. From this we get

$$\mathcal{I}_{\mathbf{V}}(a+b)\vee\mathcal{I}_{\mathbf{V}}(a)=B.$$

Since B is join irreducible, this yields $\mathcal{I}_{\mathbf{V}}(a+b)=B$. Therefore (4.1) holds.

Since $\mathbf{V}$ is strictly 1-affine complete, we may assume that f is a polynomial. Now by Proposition 2.3 we get $a=f(a+b)\in[A,B]$. Hence $a\in A^-$, a contradiction to the fact that a generates A. □

Proposition 4.5. *Let* $\mathbf{V}$ *be a finite strictly* 1*-affine complete expanded group. Then* $\mathbf{V}$ *satisfies the condition* (AB2).

Proof. Seeking a contradiction, we suppose that we have $A,B\in\mathsf{Id}\,\mathbf{V}$ such that $A\prec B$, $I[A,B]$ is abelian, and B/A has more than two elements. Let B_* be minimal with the property $B_*\leqslant B$, $B_*\not\leqslant A$. Then B_* is join irreducible. Let A_* be its unique subcover. Since the intervals $I[A,B]$ and $I[A_*,B_*]$ are projective, Proposition 2.2 gives that $I[A_*,B_*]$ is abelian, and $|B_*/A_*|>2$. Now let b_1 be in B_* such that $b_1\notin A_*$, and let b_2 be in B_* such that $b_2\notin A_*, b_2\notin -b_1+A_*$. We define a function $f:\{0,b_1,b_2,b_1+b_2\}\to V$ by $f(0)=f(b_1)=f(b_2)=0$, $f(b_1+b_2)=b_1$. We want to show that this f is compatible. For this, we have to prove

$$b_1\in\mathcal{I}_{\mathbf{V}}(b_1+b_2)\wedge\mathcal{I}_{\mathbf{V}}(b_2)\wedge\mathcal{I}_{\mathbf{V}}(b_1). \tag{4.2}$$

Since every element in $B_*\setminus A_*$ generates B_*, (4.2) holds. Using that $\mathbf{V}$ is strictly 1-affine complete, we may assume that f is a polynomial. Hence Proposition 2.3 yields $f(b_1+b_2)\in[B_*,B_*]$. Thus $b_1\in A_*$, a contradiction. □

4.2. Necessary conditions for expanded groups in which each homomorphic image is 1*-affine complete*

Proposition 4.6. *Let* $\mathbf{V}$ *be an expanded group all of whose homomorphic images are* 1*-affine complete. Then* $\mathbf{V}$ *satisfies the condition* (SC1).

Proof. Suppose that condition (SC1) is not satisfied, and let M be a strictly meet irreducible element of $\mathsf{Id}\,\mathbf{V}$ such that there is an ideal $C>M^+$ with $[M^+,C]\leqslant M$.

Let π_M be the canonical epimorphism from $\mathbf{V}$ to $\mathbf{V}/M$, and let $\overline{\mathbf{V}}:=\mathbf{V}/M$, $\overline{M^+}:=\pi_M(M^+)$, $\overline{C}:=\pi_M(C)$, $\bar{0}:=\pi_M(0)$. Then $\overline{\mathbf{V}}$ is subdirectly irreducible with monolith $\overline{M^+}$.

Now, let $\overline{m}\in\overline{M^+}$ such that $\overline{m}\neq\bar{0}$, and let $c\in\overline{C}$ such that $\bar{c}\neq\bar{0},\bar{c}\neq-\overline{m}$. Then we define a mapping $f:\overline{\mathbf{V}}\to\overline{\mathbf{V}}$ by $f(\overline{m}+\bar{c})=\overline{m}$ and $f(\bar{x})=\bar{0}$ for all other $\bar{x}\in\overline{V}$. Since

f maps into the unique minimal ideal $\overline{M^+}$, it is compatible. We know that $\overline{\mathbf{V}}$ is 1-affine complete, therefore f is a polynomial. Now Proposition 2.3 yields $f(\overline{m}+\overline{c}) \in [\overline{M^+}, \overline{C}]$. But since $[M^+, C] \leqslant M$, [8, Proposition 4.4(1)] (or [26, Exercise 4.156(11)]) yields $[\overline{M^+}, \overline{C}] = \overline{0}$. So, we obtain $\overline{m} = f(\overline{m}+\overline{c}) = \overline{0}$, a contradiction. □

Proposition 4.7. *Let* $\mathbf{V}$ *be an expanded group such that every homomorphic image of* $\mathbf{V}$ *is* 1*-affine complete. Then* $\mathbf{V}$ *satisfies the condition* (AB2).

Proof. Suppose that A, B are ideals of $\mathbf{V}$ with the properties that $A \prec B$, $[B, B] \leqslant A$, and B contains more than two cosets of A. We have a strictly meet irreducible ideal M of $\mathbf{V}$ with $M \geqslant A$, $M \not\geqslant B$. We will now see that $I[A, B]$ projects up to $I[M, M^+]$. To this end, we observe that we have $M \wedge B < B$ and $M \wedge B \geqslant A$. Since $A \prec B$, we get $M \wedge B = A$. Therefore $I[A, B]$ projects up to $I[M, M \vee B]$. By modularity, we have $M \prec M \vee B$, and thus $M^+ = M \vee B$. By Proposition 2.2 the ideal M^+ contains as many cosets of M as B contains cosets of A. Therefore, there are elements $c, m \in M^+$ such that $c \notin M$, and $m \notin M$, $m \notin -c + M$. The same construction of $f : \mathbf{V}/M \to \mathbf{V}/M$ as in the proof of Proposition 4.6 yields a contradiction. □

5. Outline of the proof that (SC1) and (AB2) are sufficient

In the next sections we prove that every congruence preserving function on a finite expanded group with (SC1) and (AB2) is a polynomial. We proceed as follows: First of all, we try to find an ideal U of $\mathbf{V}$ with $U \neq 0$, $U \neq V$ that is the range of an idempotent polynomial. Not every ideal can be such a range: If $U = \mathbf{e}(V)$ with $\mathbf{e} \circ \mathbf{e} = \mathbf{e}$, $\mathbf{e} \in \mathsf{Pol}_1 \mathbf{V}$, and if A and B are join irreducible ideals of $\mathbf{V}$ with $A \leqslant U$ and $I[A^-, A] \leftrightsquigarrow I[B^-, B]$, then $B \leqslant U$. (For proving this, observe that $(\mathbf{e} - \mathbf{id})(A) = 0$, and thus $(\mathbf{e} - \mathbf{id})(A) \subseteq A^-$. One of the properties of polynomials that we shall prove in the sequel, namely Proposition 6.1, implies $(\mathbf{e} - \mathbf{id})(B) \subseteq B^-$. So for every $b \in B$ we have

$$b \overset{B^-}{\equiv} \mathbf{e}(b) \overset{U}{\equiv} 0.$$

This yields $B \leqslant B^- \vee U$. Hence $B = B \wedge (B^- \vee U)$, and, by modularity, $B = B^- \vee (B \wedge U)$. Since B is join irreducible, we obtain $B \wedge U = B$, and therefore $B \leqslant U$. A detailed account of this argument is given in [3].) We will single out certain ideals of $\mathbf{V}$ that satisfy this criterion, and call them *homogeneous ideals*. For a homogeneous ideal U of $\mathbf{V}$, we are able to describe the polynomial functions with range contained in U. Using this description, we obtain that every partial compatible function with the range contained in U is a polynomial. Once this is established, we can use induction on the height of the congruence lattice of $\mathbf{V}$ to show that $\mathbf{V}$ is strictly 1-affine complete: Let c be any partial compatible function on $\mathbf{V}$. Taking the ideal U chosen above, we first observe that, by induction, $\mathbf{V}/U$ is strictly 1-affine complete. Let $\mathbf{p}$ be the polynomial that interpolates c "modulo U". The difference $c - \mathbf{p}$ then maps V into U, it is compatible, and hence also a polynomial. This gives that $c - \mathbf{p}$ is equal to some polynomial $\mathbf{p}'$, and therefore $\mathbf{p}' + \mathbf{p}$ interpolates c.

6. Properties of polynomials

6.1. The action of polynomials on the ideals of $\mathbf{V}$

We study how polynomials act on the ideals of $\mathbf{V}$. The methods developed in this section will then be used in Propositions 7.13 and 7.14 to produce certain polynomials. First, we observe that the third property of Proposition 2.2 can be sharpened as follows.

Proposition 6.1. *Let $\mathbf{V}$ be an expanded group, let $A, B, C, D \in \mathsf{Id}\,\mathbf{V}$ with $I[A, B] \leftrightsquigarrow I[C, D]$, let $k \in \mathbb{N}$, and let $\mathbf{p} \in \mathsf{Pol}_k\,\mathbf{V}$ with $\mathbf{p}(0, \ldots, 0) = 0$. On the set B/A we define a k-ary operation $\mathbf{f}$ by*

$$\mathbf{f}(b_1 + A, \ldots, b_k + A) := \mathbf{p}(b_1, \ldots, b_k) + A.$$

On the set D/C we define a k-ary operation $\mathbf{g}$ by

$$\mathbf{g}(d_1 + C, \ldots, d_k + C) := \mathbf{p}(d_1, \ldots, d_k) + C.$$

Then the two algebras $\langle B/A, \mathbf{f}\rangle$ and $\langle D/C, \mathbf{g}\rangle$ are isomorphic.

Proof. We assume $I[A, B] \nearrow I[C, D]$. Then every element in $d \in D$ can be written as $d = b + c$ with $b \in B,\ c \in C$. The mapping $h : D/C \to B/A$, $(b + c) + C \mapsto b + A$ is an isomorphism. □

Actually, the same result holds under weaker assumptions on $\mathbf{p}$: It is enough to claim that $\mathbf{p}$ is a congruence preserving function from A^k to A with $\mathbf{p}(0, \ldots, 0) = 0$.

6.2. Near-rings of polynomials

For an expanded group $\mathbf{V}$, we will study the near-ring $\mathbf{P}_0(\mathbf{V}) := \langle P_0(\mathbf{V}), +, \circ\rangle$ of zero-preserving unary polynomials, where addition is the pointwise addition of functions and $\circ$ denotes functional composition. We will investigate how this near-ring acts on its module $\mathbf{V}$. All results that are given in this subsection are well-known in near-ring theory [27,29]. However, our notation differs significantly from these books. Therefore, in the following few paragraphs, we have summarized the concepts from near-ring theory that we will need. Other applications of the near-ring theoretic methods developed in this section can be found in [1,3].

One aim of near-ring theory is to make the concepts of ring-theory available to non-linear functions.[3] For a near-ring $\mathbf{R}$, an $\mathbf{R}$-*module* is an algebra $\langle M, +, -, 0, \langle f_r \mid r \in R\rangle\rangle$

[3] By a *near-ring*, we mean an algebra $\langle R, +, \circ\rangle$, where $\langle R, +\rangle$ is a (not necessarily abelian) group, $\langle R, \circ\rangle$ is a semigroup and the two operations are connected by the distributive law $(r_1 + r_2) \circ r_3 = r_1 \circ r_3 + r_2 \circ r_3$. Near-rings arise by studying functions on groups: Let $\mathbf{G}$ be a group. On $M_0(G) := \{f : G \to G \mid f(0) = 0\}$ we define addition pointwise and $\circ$ as functional composition. The algebra $\langle M_0(G), +, \circ\rangle$ is a near-ring. It will be important in the sequel that this near-ring is simple [27, Theorems 1.40, 1.42].

such that $\langle M, +, -, 0\rangle$ is a group and for all $a \in M$ and $r, s, t \in R$ the following equalities hold:

$$\begin{aligned} f_r\big(f_s(a)\big) &= f_t(a) \quad \text{where } r \circ s = t \text{ in } \mathbf{R}, \\ f_r(a) + f_s(a) &= f_t(a) \quad \text{where } r + s = t \text{ in } \mathbf{R}. \end{aligned} \tag{6.1}$$

In the $\mathbf{R}$-module $\mathbf{M}$, we write $r * m$ for $f_r(m)$. The laws of (6.1) then read as $r_1 * (r_2 * m) = (r_1 \circ r_2) * m$ and $(r_1 + r_2) * m = r_1 * m + r_2 * m$. We are mainly interested in the following example: we start with an expanded group $\mathbf{V}$ and take $\mathbf{R} := \mathbf{P}_0(\mathbf{V})$, $\mathbf{M} := \langle V, +, -, 0, \langle f_{\mathbf{p}} \mid \mathbf{p} \in P_0(\mathbf{V})\rangle\rangle$ with the operations $f_{\mathbf{p}}(v) := \mathbf{p}(v)$ for all $\mathbf{p} \in P_0(\mathbf{V})$, $v \in V$.

We note that the $\mathbf{R}$-modules $\mathbf{M_1}, \mathbf{M_2}$ are isomorphic if there is a group isomorphism from $\langle M_1, +\rangle$ to $\langle M_2, +\rangle$ such that $\varphi(r * m_1) = r * \varphi(m_1)$ for $r \in R, m_1 \in M_1$. A normal subgroup I of the $\mathbf{R}$-module $\mathbf{M}$ is called an *ideal* of the module $\mathbf{M}$ iff $r * (m + i) - r * m \in I$ for all $r \in N, m \in M, i \in I$. Ideals correspond to the congruences of the module $\mathbf{M}$. Every near-ring $\mathbf{R}$ has one obvious $\mathbf{R}$-module, namely $\langle R, +, -, 0, \langle f_r \mid r \in R\rangle\rangle$, where the operations f_r are defined by $f_r(r') := r \circ r'$. As in ring theory, the ideals of this module are also called left ideals of the near-ring $\mathbf{R}$: A normal subgroup L of $\langle R, +\rangle$ is a *left ideal* of the near-ring $\langle R, +, \circ\rangle$ iff $r_1 \circ (r_2 + l) - r_1 \circ r_2 \in L$ for all $r_1, r_2 \in R$, $l \in L$. Since every near-ring $\mathbf{R}$ is an expanded group, we define *ideals* of $\mathbf{R}$ as those normal subgroups I of $\langle R, +\rangle$ satisfying $r_1 \circ (r_2 + i) - r_1 \circ r_2 \in I$ and $i \circ r \in I$ for all $r, r_1, r_2 \in R$, $i \in I$. For every $\mathbf{R}$-module $\mathbf{M}$, the set $\operatorname{Ann}_{\mathbf{R}} \mathbf{M} := \{r \in R \mid \forall m \in M\colon\ r * m = 0\}$ is an ideal of $\mathbf{R}$.

We need only one result of near-ring theory; it generalizes the fact that for a finite simple ring with unit $\mathbf{R}$, all faithful simple unitary $\mathbf{R}$-modules are isomorphic (cf. [32, Proposition 2.1.15, p. 154], [5, Theorem 4.3], [29, Theorem 4.56(a)], [3, Lemma 1.3]). We will use the following version:

Proposition 6.2. *Let* $\mathbf{R}$ *be a near-ring with* $r \circ 0 = 0$ *for all* $r \in R$, *let* I *be an ideal of* $\mathbf{R}$, *and let* $\mathbf{M}$ *be an* $\mathbf{R}$*-module that satisfies* $\operatorname{Ann}_{\mathbf{R}} \mathbf{M} = I$ *and* $R * m = M$ *for all* $m \in M, m \neq 0$. *We assume that we have a left ideal* L *of* $\mathbf{R}$ *such that* $L > I$ *and there is no left ideal* L' *of* $\mathbf{R}$ *with* $L > L' > I$.

Then the $\mathbf{R}$*-module* $\mathbf{M}$ *is isomorphic to the* $\mathbf{R}$*-module with universe* $L/I = \{l + I \mid l \in L\}$ *and operations* $(l_1 + I) + (l_2 + I) := (l_1 + l_2) + I$, $r * (l + I) := (r \circ l) + I$ *for* $l_1, l_2, l \in L$, $r \in R$.

Proof. Since $L \not\leqslant \operatorname{Ann}_{\mathbf{R}} \mathbf{M}$, we have elements $l_0 \in L, m_0 \in M$ with $l_0 * m_0 \neq 0$. We define a mapping φ by

$$\varphi : L \to M, \quad l \mapsto l * m_0.$$

It is easy to see that φ is a homomorphism from the $\mathbf{R}$-module $\mathbf{L}$ into $\mathbf{M}$. Since $l_0 * m_0 \neq 0$, the assumptions on M yield $R * l_0 * m_0 = M$. Since $R * l_0 \subseteq L$, we get $L * m_0 = M$, and hence φ is surjective. We take L' to be the kernel of φ, i.e.,

$$L' = \{l \in L \mid l * m_0 = 0\}.$$

Using the definition of left ideals, one can check that L' is a left ideal of $\mathbf{R}$. Furthermore, every element of $I = \mathrm{Ann}_{\mathbf{R}}\,\mathbf{M}$ lies in L'. So we have

$$I \leqslant L' \leqslant L.$$

Since by the assumptions L covers I in the lattice of left ideals of $\mathbf{R}$, L' has to be either L or I. The element l_0 shows $L' < L$, and so $L' = I$. The homomorphism theorem yields that the module $L/L' = L/I$ is isomorphic to $\mathbf{M}$. □

We associate a $\mathbf{P}_0(\mathbf{V})$-module with every interval in the ideal lattice of $\mathbf{V}$.

Definition 6.3. Let $\mathbf{V}$ be an expanded group, and let A, B be ideals of $\mathbf{V}$ with $A \leqslant B$. We define $M[A, B]$ to be the $\mathbf{P}_0(\mathbf{V})$-module

$$\langle B/A, +, -, 0, \langle f_{\mathbf{p}} \mid \mathbf{p} \in P_0(\mathbf{V})\rangle\rangle$$

with $f_{\mathbf{p}}(b + A) = \mathbf{p}(b) + A$.

The subalgebras of $M[A, B]$ correspond to the ideals of $\mathbf{V}$ from the interval $I[A, B]$.

Proposition 6.4. *Let $\mathbf{V}$ be an expanded group, and let A, B be ideals of $\mathbf{V}$ with $A \leqslant B$. Then we have*

(1) *Every submodule of $M[A, B]$ is an ideal of the module $M[A, B]$.*
(2) *The mapping μ that maps an ideal C of $\mathbf{V}$ with $A \leqslant C \leqslant B$ to $\mu(C) := C/A = \{c + A \mid c \in C\}$ is a bijection from the interval $I[A, B]$ of $\mathrm{Id}\,\mathbf{V}$ to the set of all submodules of $M[A, B]$.*

We will now give some information on the module $M[A, B]$ for a covering pair $A \prec B$ of ideals. We recall that $\mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}(M[A, B])$ is equal to $\{\mathbf{p} \in P_0(\mathbf{V}) \mid \mathbf{p}(B) \subseteq A\}$.

Proposition 6.5. *Let $\mathbf{V}$ be an expanded group, let A, B be ideals of $\mathbf{V}$ with $A \prec B$ and $[B, B] \leqslant A$, and let $I := \mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}(M[A, B])$. Then we have*

(1) *For all $\mathbf{p} \in P_0(\mathbf{V})$ the operation $f_{\mathbf{p}}$ satisfies $f_{\mathbf{p}}((b_1 + A) + (b_2 + A)) = f_{\mathbf{p}}(b_1 + A) + f_{\mathbf{p}}(b_2 + A)$ for all $b_1, b_2 \in B$.*
(2) *The near-ring $\mathbf{P}_0(\mathbf{V})/I$ is a ring; this ring is primitive on $M[A, B]$.*

Proof. Since $A \prec B$, Proposition 6.4 yields that $M[A, B]$ has no non-trivial submodules. The item (1) is a consequence of Proposition 2.3. Item (2) is a different formulation of the fact that $M[A, B]$ has no proper nonzero submodules. □

Proposition 6.6. *Let* $\mathbf{V}$ *be an expanded group, and let* A, B *be ideals of* $\mathbf{V}$ *with* $A \prec B$ *and* $[B, B] \not\leqslant A$. *We assume that* B/A *is finite. We define* $\mathbf{G} := \langle B/A, +\rangle$. *Let* $I := \mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}(M[A, B])$, *and let* φ *be the mapping defined by*

$$\varphi : P_0(\mathbf{V}) \to M_0(G),$$
$$\varphi(\mathbf{p})(b + A) := \mathbf{p}(b) + A.$$

Then the mapping φ *is a near-ring epimorphism from* $\langle P_0(\mathbf{V}), +, \circ\rangle$ *onto* $\langle M_0(G), +, \circ\rangle$ *with kernel* I.

Proof. We show that for every finite subset X of B/A with $0 + A \notin X$ and for every function $g : X \to B/A$, there is a polynomial $\mathbf{p} \in P_0(\mathbf{V})$ such that the restriction $f_{\mathbf{p}}|_X$ is equal to g. We prove this by induction on $|X|$. For $|X| = 1$, the result follows from the fact that $M[A, B]$ has no non-trivial submodules, and so $P_0(\mathbf{V}) * (b + A) = B/A$ for all $b \in B \setminus A$. Now we assume $|X| \geqslant 2$. Let $x_1,\ x_2$ be two elements of X. By the induction hypothesis there is a polynomial $\mathbf{q} \in P_0(\mathbf{V})$ with $f_{\mathbf{q}}|_{X\setminus\{x_1\}} = g$. It is then sufficient to find $\mathbf{p}$ with $f_{\mathbf{p}}|_X = g - f_{\mathbf{q}}|_X$. Such a function exists if the set S defined by

$$S := \left\{ f_{\mathbf{p}}(x_1) \mid \mathbf{p} \in P_0(\mathbf{V}), \mathbf{p}|_{X\setminus\{x_1\}} = 0 \right\}$$

is equal to B/A. To show this equality, we let $v_1,\ v_2 \in B$ be such that $v_1 + A = x_1$ and $v_2 + A = x_2$, and we define:

$$M_1 := \left\{ f_{\mathbf{p}}(x_1) \mid \mathbf{p} \in P_0(\mathbf{V}),\ f_{\mathbf{p}}|_{X\setminus\{x_1,x_2\}} = 0 \right\},$$
$$M_2 := \left\{ f_{\mathbf{p}}(x_1) \mid \mathbf{p} \in \mathsf{Pol}_1(\mathbf{V}),\ \mathbf{p}(v_2) = 0 \right\}.$$

The sets M_1 and S are universes of submodules of $M[A, B]$. By the induction hypothesis, $M_1 = B/A$. We will now show that S contains an element different from $0 + A$, which proves $S = B/A$. To this end, we observe $[B, B] \not\leqslant A$. Let b_1, b_2 be elements of B, and let $\mathbf{s}$ be a polynomial in $\mathsf{Pol}_2\,\mathbf{V}$ such that $\mathbf{s}(v, 0) = \mathbf{s}(0, v) = 0$ for all $v \in V$, and $\mathbf{s}(b_1, b_2) \notin A$. Since $b_1 + A \in M_1$, we have polynomial $\mathbf{p}_1 \in P_0(\mathbf{V})$ with

$$f_{\mathbf{p}_1}(x_1) = b_1 + A, \quad f_{\mathbf{p}_1}|_{X\setminus\{x_1,x_2\}} = 0.$$

The set M_2 is an ideal of $\mathbf{V}$. The function $\mathbf{p}$ defined by $\mathbf{p}(z) = z - v_2$ shows $M_2 \not\leqslant A$. Since $v_1, v_2 \in B$, we have $M_2 \leqslant B$, and thus $M_2 + A = B$. Hence there is a polynomial $\mathbf{p}_2 \in \mathsf{Pol}_1\,\mathbf{V}$ such that $\mathbf{p}_2(v_2) = 0$ and $\mathbf{p}_2(v_1) \in b_2 + A$. Now we consider the polynomial $\mathbf{p}_3 := \mathbf{s}(\mathbf{p}_1, \mathbf{p}_2)$. We omit the straightforward check that $\mathbf{p}_3 \in P_0(\mathbf{V})$ and $f_{\mathbf{p}_3}|_{X\setminus\{x_1\}} = 0$. So $f_{\mathbf{p}_3}(x_1)$ lies in S. Then we have

$$f_{\mathbf{p}_3}(x_1) = \mathbf{p}_3(v_1) + A = \mathbf{s}\big(\mathbf{p}_1(v_1), \mathbf{p}_2(v_1)\big) + A.$$

We have $\mathbf{p}_1(v_1)+A = f_{\mathbf{p}_1}(x_1) = b_1+A$. This yields $\mathbf{s}(\mathbf{p}_1(v_1), \mathbf{p}_2(v_1)) + A = \mathbf{s}(b_1, b_2) + A$. Since $\mathbf{s}(b_1, b_2)$ does not lie in A, we have $f_{\mathbf{p}_3}(x_1) \neq 0 + A$. Thus S contains an element different from $0 + A$. □

A similar result is [35, Theorem 8.4]. The last two propositions have the following consequence:

Corollary 6.7. *Let A, B be ideals of the expanded group $\mathbf{V}$ with $A \prec B$. We assume that B/A is finite. Then the annihilator $\mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}(M[A, B])$ is a maximal ideal of the near-ring $\mathbf{P}_0(\mathbf{V})$.*

Proof. We are done if we show that the quotient $\mathbf{R} := \mathbf{P}_0(\mathbf{V})/\mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}(M[A, B])$ is a simple near-ring. If $[B, B] \leqslant A$, then by Proposition 6.5 the near-ring $\mathbf{R}$ is a primitive ring with unit, hence isomorphic to the ring of $(n \times n)$-matrices over a field $\mathbf{F}$ and thus simple. If $[B, B] \not\leqslant A$, then Proposition 6.5 shows that $\mathbf{R}$ is isomorphic to the near-ring of all zero-preserving mappings on the finite group $\langle B/A, +\rangle$. This near-ring is simple by [27, Theorem 1.40] (cf. [29, Theorem 7.30], [4]). □

6.3. Isomorphic $\mathbf{P}_0(\mathbf{V})$-modules

Proposition 6.1 and its proof yield the following consequence:

Proposition 6.8. *Let $\mathbf{V}$ be an expanded group, let $A, B, C, D \in \mathsf{Id}\,\mathbf{V}$ with $I[A, B] \leftrightsquigarrow I[C, D]$. Then the two $\mathbf{P}_0(\mathbf{V})$-modules $M[A, B]$ and $M[C, D]$ are isomorphic.*

Some of the properties that hold if $I[A, B]$ is projective to $I[C, D]$ still hold if we assume the weaker fact that $M[A, B]$ and $M[C, D]$ are isomorphic.

Proposition 6.9. *Let $\mathbf{V}$ be an expanded group, and let $A, B, C, D \in \mathsf{Id}\,\mathbf{V}$ with $A \leqslant B$, $C \leqslant D$ such that $M[A, B]$ and $M[C, D]$ are isomorphic. Then $(A : B) = (C : D)$.*

We remark that this has been proved in [36, Theorem 12.1]. Since our notation is entirely different, we state a proof.

Proof. We show $(C : D) \leqslant (A : B)$. By Proposition 2.1(4), we know that $(A : B)$ is given by

$$\begin{aligned}\big\{z \in V \mid \mathbf{s}(z, b) \subseteq A \text{ for all } b \in B \\ \text{and } \mathbf{s} \in \mathsf{Pol}_2\,\mathbf{V} \text{ with } \forall v \in V\colon\ \mathbf{s}(v, 0) = \mathbf{s}(0, v) = 0\big\}.\end{aligned} \tag{6.2}$$

Let z be an element of $(C : D)$. We fix a binary polynomial $\mathbf{s} \in \mathsf{Pol}_2\,\mathbf{V}$ with $\mathbf{s}(v, 0) = \mathbf{s}(0, v) = 0$ for all $v \in V$, and we also fix $b \in B$. We compute $\mathbf{s}(z, b)$. Since $[(C : D), D] \leqslant C$, the polynomial $\mathbf{p}(x) := \mathbf{s}(z, x)$ has the property $\mathbf{p}(D) \subseteq C$, so the operation $f_{\mathbf{p}}$ in the module $M[C, D]$ is the zero function. Since $M[C, D]$ is isomorphic to $M[A, B]$, the operation $f_{\mathbf{p}}$ in the module $M[A, B]$ is also the zero function. So $\mathbf{p}(B) \subseteq A$. This implies $\mathbf{p}(b) \in A$, which means $\mathbf{s}(z, b) \in A$. Thus z lies in the centralizer $(A : B)$, and we have

$(C:D) \leqslant (A:B)$. Interchanging the roles of A, B with those of C, D, we obtain the required equality. □

Proposition 6.10. *Let* $\mathbf{V}$ *be an expanded group, and let* A, B, C, D *be ideals of* $\mathbf{V}$ *with* $A \prec B$, $C \prec D$ *such that the modules* $M[A, B]$ *and* $M[C, D]$ *are isomorphic. If* $I[A, B]$ *is abelian, then* $I[C, D]$ *is abelian.*

Proof. We assume $[D, D] \not\leqslant C$. Then there are $d_1, d_2 \in D$ and a binary polynomial $\mathbf{s} \in \mathsf{Pol}_2 \mathbf{V}$ with $\mathbf{s}(v, 0) = \mathbf{s}(0, v) = 0$ for all $v \in V$ and $s(d_1, d_2) \notin C$. Since $C \prec D$, $M[C, D]$ has only two subuniverses, namely $0 = C/C$ and D/C. Therefore, $P_0(\mathbf{V}) * (d_1 + C) = D/C$. Hence we have a polynomial $\mathbf{p} \in P_0(\mathbf{V})$ such that $\mathbf{p}(d_1) \in d_2 + C$. We consider the polynomial $\mathbf{t}(x) := \mathbf{s}(x, \mathbf{p}(x))$. We know that $\mathbf{t}(d_1) = \mathbf{s}(d_1, \mathbf{p}(d_1))$ is congruent to $\mathbf{s}(d_1, d_2)$ modulo C; thus we get $\mathbf{t}(d_1) \notin C$. So we have $\mathbf{t}(D) \not\subseteq C$. Since the modules $M[C, D]$ and $M[A, B]$ are isomorphic, we have $\mathbf{t}(B) \not\subseteq A$. Therefore there is an element $b \in B$ such that $\mathbf{t}(b) = \mathbf{s}(b, \mathbf{p}(b)) \notin A$. But $\mathbf{s}'(x, y) := \mathbf{s}(x, \mathbf{p}(y))$ is 0 whenever one of its arguments is 0; so $\mathbf{t}(b)$ lies in $[B, B]$. This shows $[B, B] \not\leqslant A$, and thus $I[A, B]$ is not abelian. □

The following proposition helps to find isomorphic sections in $\mathsf{Id}\,\mathbf{V}$:

Proposition 6.11 (cf. [3, Lemma 1.5]). *Let* $\mathbf{V}$ *be an expanded group and let* $A, B, C, D \in \mathsf{Id}\,\mathbf{V}$ *such that* $C \leqslant D$, $A \prec B$, *and both sets* B/A *and* D/C *are finite. We assume that each polynomial* $\mathbf{p} \in P_0(\mathbf{V})$ *with* $\mathbf{p}(D) \subseteq C$ *satisfies* $\mathbf{p}(B) \subseteq A$. *Then there are ideals* C', D' *of* $\mathbf{V}$ *with* $C \leqslant C' \prec D' \leqslant D$ *such that there is a module isomorphism from* $M[C', D']$ *onto* $M[A, B]$.

Proof. We take I to be the ideal $\mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}(M[A, B])$. Let C_1 be any ideal of $\mathbf{V}$ in $I[C, D]$. Let J_1, J_2 be the ideals of $P_0(\mathbf{V})$ defined by

$$J_1 := \mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}\big(M[C, C_1]\big), \qquad J_2 := \mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}\big(M[C_1, D]\big).$$

We show

$$J_1 \subseteq I \quad \text{or} \quad J_2 \subseteq I. \tag{6.3}$$

Seeking a contradiction, we suppose that both inclusions fail. For every polynomial $\mathbf{p} \in P_0(\mathbf{V})$, we let $\varphi(\mathbf{p})$ be the function defined by

$$\varphi(\mathbf{p}) : B/A \to B/A,$$
$$b + A \mapsto \mathbf{p}(b) + A.$$

The mapping φ is a near-ring homomorphism from $\mathbf{P}_0(\mathbf{V})$ into the near-ring of all zero-preserving mappings on B/A. The kernel of this homomorphism is I, and by Corollary 6.7, I is a maximal ideal of $\mathbf{P}_0(\mathbf{V})$.

For an ideal J of $\mathbf{P}_0(\mathbf{V})$, the image $\varphi(J)$ is an ideal of $\varphi(\mathbf{P}_0(\mathbf{V}))$. Corollary 6.7 leaves only two choices for $\varphi(J)$ in our case: $\varphi(J) = 0$ or $\varphi(J) = \varphi(\mathbf{P}_0(\mathbf{V}))$. Since J_1 and J_2 are not contained in I, we have $\varphi(J_1) = \varphi(J_2) = \varphi(\mathbf{P}_0(\mathbf{V}))$.

We choose an element $b \in B \setminus A$. The equality $\varphi(J_1) = \varphi(\mathbf{P}_0(\mathbf{V}))$ yields a polynomial $\mathbf{p}_1 \in J_1$ with

$$\varphi(\mathbf{p}_1) = \varphi(\mathbf{id}),$$

where $\mathbf{id}$ is the polynomial given by $\mathbf{id}(v) = v$ for all $v \in V$. This means that $\mathbf{p}_1(b) + A = \varphi(\mathbf{p}_1)(b + A) = \varphi(\mathbf{id})(b + A) = b + A$. In the same way, we obtain $\mathbf{p}_2 \in J_2$ with $\mathbf{p}_2(b) + A = b + A$. We consider the polynomial

$$\mathbf{p}_3 := \mathbf{p}_2 \circ \mathbf{p}_1.$$

We know $\mathbf{p}_3(D) = \mathbf{p}_2(\mathbf{p}_1(D)) \subseteq \mathbf{p}_2(C_1) \subseteq C$. Thus $\mathbf{p}_3$ lies in $\mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}(M[C, D])$, and the assumption $\mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}(M[C, D]) \subseteq \mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}(M[A, B])$ implies $\mathbf{p}_3(B) \subseteq A$. So $\mathbf{p}_3(b)$ lies in A. On the other hand, $\mathbf{p}_3(b) + A = \mathbf{p}_2(\mathbf{p}_1(b)) + A = \mathbf{p}_1(b) + A = b + A$. Since $b \in B \setminus A$, this yields the contradiction $\mathbf{p}_3(b) \notin A$. This finishes the proof of (6.3). Since there are only finitely many ideals between C and D, repeating this process allows us to obtain $C', D' \in \mathrm{Id}\,\mathbf{V}$ with $C \leqslant C' \prec D' \leqslant D$ and

$$\mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}\big(M\big[C', D'\big]\big) \leqslant I.$$

By Corollary 6.7, $\mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}(M[C', D'])$ is a maximal ideal of $\mathbf{P}_0(\mathbf{V})$, and so it is equal to I. Since $P_0(\mathbf{V})/I$ is finite, Proposition 6.2 yields that the modules $M[C', D']$ and $M[A, B]$ are isomorphic. □

7. Homogeneous ideals

7.1. Lattice theoretic properties of homogeneous ideals

In the sequel, we will work with ideals that have certain lattice-theoretic properties in the lattice $\mathrm{Id}\,\mathbf{V}$. For a lattice $\mathbf{L}$, we denote the set of its strictly join irreducible elements by $J(\mathbf{L})$. We define an equivalence relation $\sim$ on $J(\mathbf{L})$ by $\alpha \sim \beta :\Leftrightarrow I[\alpha^-, \alpha] \leftrightsquigarrow I[\beta^-, \beta]$. In this case, we say that α and β are *projective in* $\mathbf{L}$. The equivalence class of an element $\alpha \in J(\mathbf{L})$ will be denoted by $\alpha/\!\sim$.

Definition 7.1. Let $\mathbf{L}$ be a finite lattice. An element $\mu \in L$ is called *homogeneous* iff

(1) $\mu > 0$.
(2) All join irreducible elements α with $\alpha \leqslant \mu$ are projective in $\mathbf{L}$.
(3) There are no join irreducible elements $\alpha, \beta \in L$ with $\alpha \leqslant \mu, \beta \not\leqslant \mu$ such that α and β are projective in $\mathbf{L}$.

We illustrate this definition by an example. Let $\mathbf{L}_1$ be the lattice of normal subgroups of $A_5 \times \mathbb{Z}_4 \times \mathbb{Z}_2$. Then the normal subgroups $0 \times \mathbb{Z}_4 \times \mathbb{Z}_2$ and $A_5 \times 0 \times 0$ are the homogeneous elements of $\mathbf{L}_1$.

Proposition 7.2. *Let* $\mathbf{L}$ *be a finite lattice, let* μ *be a homogeneous element of* $\mathbf{L}$*, and let* α *be a join irreducible element of* $\mathbf{L}$ *with* $\alpha \leqslant \mu$*. Then the element* μ *is the join of all elements in* $\alpha/\sim$*.*

Proof. We have to show

$$\mu = \bigvee_{\beta \in \alpha/\sim} \beta. \tag{7.1}$$

For $\geqslant$, suppose $\mu \not\geqslant \bigvee_{\beta\in\alpha/\sim}\beta$. Then there is $\beta' \in \alpha/\sim$ such that $\beta' \not\leqslant \mu$, which contradicts (3) of Definition 7.1. For showing equality in (7.1), suppose $\mu > \bigvee_{\beta\in\alpha/\sim}\beta$. Since every element of a finite lattice is the join of the join irreducibles below it, there is a join irreducible element $\gamma \in L$ with $\gamma \leqslant \mu$ and $\gamma \notin \alpha/\sim$. This contradicts (2) of Definition 7.1. □

Proposition 7.3. *Let* $\mathbf{L}$ *be a finite lattice, let* μ *be a homogeneous element of* $\mathbf{L}$*, let* α *be a join irreducible element of* $\mathbf{L}$ *with* $\alpha \leqslant \mu$*, and let* γ *and* δ *be elements in* $\mathbf{L}$ *with* $\gamma \prec \delta \leqslant \mu$*. Then the interval* $I[\gamma, \delta]$ *is projective to* $I[\alpha^-, \alpha]$*.*

Proof. We take β minimal with $\beta \leqslant \delta$, $\beta \not\leqslant \gamma$. Then the interval $I[\gamma, \delta]$ is projective to $I[\beta^-, \beta]$, and so by (2) of Definition 7.1 projective to $I[\alpha^-, \alpha]$. □

Proposition 7.4. *Let* $\mathbf{L}$ *be a finite modular lattice, and let* $\alpha, \beta, \gamma \in L$*. If at least one of the elements* α, β, γ *is a homogeneous element of* $\mathbf{L}$*, then the following two equalities hold*:

$$\alpha \vee (\beta \wedge \gamma) = (\alpha \vee \beta) \wedge (\alpha \vee \gamma),$$
$$\alpha \wedge (\beta \vee \gamma) = (\alpha \wedge \beta) \vee (\alpha \wedge \gamma).$$

Proof (cf. [26, p. 96, Claim 2]). Let μ be a homogeneous element of $\mathbf{L}$, and let α, β be any elements of $\mathbf{L}$. We first show

$$(\alpha \vee \mu) \wedge (\alpha \vee \beta) = \alpha \vee (\mu \wedge \beta). \tag{7.2}$$

We suppose $(\alpha \vee \mu) \wedge (\alpha \vee \beta) > \alpha \vee (\mu \wedge \beta)$. We let $\alpha' \in L$ be such that

$$\alpha \vee (\mu \wedge \beta) \leqslant \alpha' \prec (\alpha \vee \mu) \wedge (\alpha \vee \beta).$$

Then we have

$$(\alpha \vee \mu) \wedge (\alpha \vee \beta) = \big(\alpha' \vee \mu\big) \wedge \big(\alpha' \vee \beta\big). \tag{7.3}$$

From $\alpha \leqslant \alpha'$ we obtain $\leqslant$ of (7.3). For proving $\geqslant$, we observe that the assumption $\alpha' \geqslant \alpha \vee (\mu \wedge \beta)$ implies

$$\big(\alpha' \vee \mu\big) \wedge \big(\alpha' \vee \beta\big) \geqslant \big(\alpha \vee (\beta \wedge \mu) \vee \mu\big) \wedge \big(\alpha \vee (\beta \wedge \mu) \vee \beta\big) = (\alpha \vee \mu) \wedge (\alpha \vee \beta).$$

This proves (7.3). We will now show that the interval $I[\alpha', (\alpha' \vee \mu) \wedge (\alpha' \vee \beta)]$ projects down to a section lying under μ. In every modular lattice L, the interval $I[a, (a \vee b) \wedge (a \vee c)]$ projects down to the interval $I[a \wedge c, (a \vee b) \wedge c]$ for all $a, b, c \in L$. In our case, this implies

$$I\big[\alpha', \big(\alpha' \vee \mu\big) \wedge \big(\alpha' \vee \beta\big)\big] \searrow I\big[\alpha' \wedge \mu, \big(\alpha' \vee \beta\big) \wedge \mu\big] \tag{7.4}$$

and

$$I\big[\alpha', \big(\alpha' \vee \mu\big) \wedge \big(\alpha' \vee \beta\big)\big] \searrow I\big[\alpha' \wedge \beta, \big(\alpha' \vee \mu\big) \wedge \beta\big]. \tag{7.5}$$

Let η be minimal in $\mathbf{L}$ with respect to $\eta \leqslant (\alpha' \vee \mu) \wedge \beta$, $\eta \nleqslant \alpha' \wedge \beta$. We obtain $I[\eta^-, \eta] \nearrow I[\alpha' \wedge \beta, (\alpha' \vee \mu) \wedge \beta]$, and thus by (7.4) and (7.5), the interval $I[\eta^-, \eta]$ is projective to $I[\alpha' \wedge \mu, (\alpha' \vee \beta) \wedge \mu]$.

We now show

$$\eta \nleqslant \mu. \tag{7.6}$$

Suppose $\eta \leqslant \mu$. Then $\eta \leqslant \mu \wedge ((\alpha' \vee \mu) \wedge \beta) = \mu \wedge \beta$. By the choice of α', we have $\mu \wedge \beta \leqslant \alpha'$, and thus $\eta \leqslant \alpha'$. But then $\eta \leqslant \alpha' \wedge ((\alpha' \vee \mu) \wedge \beta) = \alpha' \wedge \beta$, which is in contradiction to the choice of η. This proves (7.6).

Since $I[\eta^-, \eta]$ is projective to $I[\alpha' \wedge \mu, (\alpha' \vee \beta) \wedge \mu]$, Proposition 7.3 tells that $I[\eta^-, \eta]$ is projective to $I[0, \rho]$ for every atom ρ below μ. Thus ρ and η contradict the 3rd condition in Definition 7.1. This completes the proof of (7.2).

Property (7.2) yields that a homogeneous element of the lattice $\mathbf{L}$ is a *dually standard* (in the sense of [9, Definition III.2.1]) element of $\mathbf{L}$. By [9, Corollary III.2.8 and Theorem III.2.5], all equalities stated in Proposition 7.4 hold. □

The fact that a homogeneous element μ of the modular lattice $\mathbf{L}$ satisfies $\mu \wedge (\alpha \vee \beta) = (\mu \wedge \alpha) \vee (\mu \wedge \beta)$ allows us to find a pseudocomplement μ^* of μ, i.e., the largest μ^* with $\mu \wedge \mu^* = 0$.

Definition 7.5. Let $\mathbf{L}$ be a finite lattice, and let μ be a homogeneous element of $\mathbf{L}$. We define μ^* as the join of all elements $\gamma \in L$ with $\gamma \wedge \mu = 0$.

If $\mathbf{L}$ is a finite modular lattice and μ is a homogeneous element of $\mathbf{L}$, then the remark preceding this definition yields $\mu \wedge \mu^* = 0$.

Definition 7.6. Let $\mathbf{L}$ be a finite lattice, and let α be any element of $\mathbf{L}$. We define $\Phi(\alpha)$ as the intersection of all subcovers of α; furthermore $\Phi(0) := 0$.

7.2. Homogeneous ideals and commutators

We switch from abstract lattices to the ideal lattice of a finite expanded group $\mathbf{V}$. We define *homogeneous ideals* of $\mathbf{V}$ as those that are homogeneous elements of the lattice $\mathsf{Id}\,\mathbf{V}$. For each homogeneous ideal U, the ideal U^* is the largest ideal such that $U \wedge U^* = 0$, and for each ideal A of $\mathbf{V}$ with $A > 0$, the ideal $\Phi(A)$ is the intersection of all subcovers of A.

Before giving more information on U and U^*, we state the following fact on projective join irreducible elements of $\mathsf{Id}\,\mathbf{V}$.

Proposition 7.7. *Let* $\mathbf{V}$ *be an expanded group, and let* $A, B \in J(\mathsf{Id}\,\mathbf{V})$ *with* $[A, A] = A$ *and* $B \sim A$. *Then* $B = A$.

Proof. Suppose that $A \neq B$. Then either $B \not\leqslant A$ or $A \not\leqslant B$.

Case $B \not\leqslant A$. We have $B \wedge A \prec B$. Since B is join irreducible, this implies $B \wedge A \leqslant B^-$, and hence we have $[B, A] \leqslant B^-$. Therefore we have $A \leqslant (B^- : B)$. By Proposition 2.2, this implies $A \leqslant (A^- : A)$, from which we get $[A, A] \leqslant A^-$, which is a contradiction.

Case $A \not\leqslant B$. We first observe that Proposition 2.2 gives $[B, B] = B$. In the same way as in the previous case we obtain $B \leqslant (A^- : A) = (B^- : B)$, a contradiction to $[B, B] = B$. □

This shows that every non-abelian minimal ideal of a finite expanded group is homogeneous.

Proposition 7.8. *Let* $\mathbf{V}$ *be a finite expanded group, and let* U *be a homogeneous ideal of* $\mathbf{V}$. *Let* A, B *be ideals of* $\mathbf{V}$ *with* $A \prec B \leqslant U$. *Then* $(A : B) = (\Phi(U) : U)$.

Proof. Let S be a subcover of U. By Proposition 7.3, the interval $I[A, B]$ is projective to $I[S, U]$ in $\mathsf{Id}\,\mathbf{V}$; hence Proposition 2.2 yields $(A : B) = (S : U)$. We will now prove

$$(S : U) = \big(\Phi(U) : U\big). \tag{7.7}$$

Since $S \geqslant \Phi(U)$, we have the inclusion $\geqslant$ of (7.7). For proving $\leqslant$, let S' be a subcover of U. Propositions 2.2 and 7.3 give $(S : U) = (S' : U)$, and hence $[(S : U), U] \leqslant S'$ for all subcovers S' of U. So we have $[(S : U), U] \leqslant \Phi(U)$, and therefore $(S : U) \leqslant (\Phi(U) : U)$, which proves (7.7). □

Proposition 7.9. *Let* $\mathbf{V}$ *be a finite expanded group, and let* U *be a homogeneous ideal of* $\mathbf{V}$. *Then one of the following two alternatives holds*:

(1) $[U, U] < U$ *and* $(\Phi(U) : U) \geqslant U \vee U^*$.
(2) $[U, U] = U$, U *is an atom of* $\mathsf{Id}\,\mathbf{V}$, *and* $(\Phi(U) : U) = U^*$.

Proof. If $[U,U] \prec U$, there is a subcover S of U in $\mathsf{Id}\,\mathbf{V}$ with $[U,U] \leqslant S \prec U$. Proposition 7.8 yields $(S:U) = (\Phi(U):U)$. Since $U \leqslant (S:U)$, we get

$$U \leqslant \big(\Phi(U):U\big).$$

Since U and U^* have zero intersection, we also have $(\Phi(U):U) \geqslant U^*$. Altogether, we have $(\Phi(U):U) \geqslant U \vee U^*$.

We now treat the case $[U,U] = U$. Let S be a subcover of U in $\mathsf{Id}\,\mathbf{V}$. We have $(S:U) \geqslant S$. We assume that S' is another subcover of U. We know $(S':U) \geqslant S'$. Propositions 7.3 and 2.2 yield $(S':U) = (S:U)$. So we get $(S:U) \geqslant S \vee S' = U$, which leads to the contradiction $[U,U] \leqslant S$. So U has only one subcover and is thus join irreducible. Let A be an atom of $\mathsf{Id}\,\mathbf{V}$ with $A \leqslant U$. By Proposition 7.3, A and U are projective join irreducible elements of $\mathsf{Id}\,\mathbf{V}$. Proposition 7.7 gives $A = U$. What remains to show is $(\Phi(U):U) = U^*$. To prove this, it is sufficient to show that for every $A \in \mathsf{Id}\,\mathbf{V}$, $[U,A] = 0$ iff $U \wedge A = 0$. The "if"-part follows from $[U,A] \leqslant U \wedge A = 0$. For the "only if"-part, we assume that $[U,A] = 0$ but $U \wedge A \neq 0$. Since U is an atom of $\mathsf{Id}\,\mathbf{V}$, we have $A \geqslant U$, and so $[U,A] = 0$ implies $[U,U] = 0$, which is not the case. □

Proposition 7.10. *Let* $\mathbf{V}$ *be a finite expanded group, let* U *be a homogeneous ideal of* $\mathbf{V}$, *and let* $A, B \in \mathsf{Id}\,\mathbf{V}$ *with* $A \leqslant U$ *and* $B \not\leqslant (\Phi(U):U)$. *Then we have* $[A,B] = A$.

Proof. Suppose $[A,B] \prec A$. Then there is an ideal $A' \prec A$ with $[A,B] \leqslant A'$. This implies $B \leqslant (A':A)$. Proposition 7.8 now yields $B \leqslant (\Phi(U):U)$. □

Proposition 7.11. *Let* $\mathbf{V}$ *be a finite expanded group, and let* U *be a homogeneous ideal of* $\mathbf{V}$. *Then for each ideal* B *of* $\mathbf{V}$ *we have* $B \leqslant (\Phi(U):U)$ *or* $B \geqslant U$.

Proof. We assume that $B \not\geqslant U$. This implies $B \wedge U \prec U$ and thus $[U,B] \prec U$. So there is a subcover S of U in $\mathsf{Id}\,\mathbf{V}$ with $[U,B] \leqslant S \prec U$. This yields $B \leqslant (S:U)$. By Proposition 7.8, we get $B \leqslant (\Phi(U):U)$. □

7.3. Homogeneous ideals and polynomials

Since all prime intervals in the ideal lattice that are below a homogeneous ideal are projective, Proposition 6.1 puts the following restrictions on polynomials.

Proposition 7.12. *Let* $\mathbf{V}$ *be a finite expanded group, and let* U *be a homogeneous ideal of* $\mathbf{V}$. *Let* A *and* B *be ideals of* $\mathbf{V}$ *with* $A \prec B \leqslant U$, *and let* $\mathbf{q} \in P_0(\mathbf{V})$ *be such that* $\mathbf{q}(B) \subseteq A$. *Then for every* $D \in \mathsf{Id}\,\mathbf{V}$ *with* $D \leqslant U$ *we have* $\mathbf{q}(D) \subseteq \Phi(D)$.

Proof. Let C be a subcover of D in the lattice $\mathsf{Id}\,\mathbf{V}$. By Proposition 7.3, the intervals $I[C,D]$ and $I[A,B]$ are projective in $\mathsf{Id}\,\mathbf{V}$. We apply Proposition 6.1 to the polynomial $\mathbf{q}$ and the sets D/C and B/A and obtain that $\mathbf{q}$ induces the zero function on D/C, and hence we have $\mathbf{q}(D) \subseteq C$. Therefore $\mathbf{q}(D)$ is contained in every subcover of D, which implies $\mathbf{q}(D) \subseteq \Phi(D)$. □

The following proposition is fundamental for constructing polynomials on $\mathbf{V}$.

Proposition 7.13. *Let $\mathbf{V}$ be a finite expanded group, and let U be a homogeneous ideal of $\mathbf{V}$. Then there are polynomials $\mathbf{e}_1, \mathbf{e}_2$ in $P_0(\mathbf{V})$ with the properties*

$$\mathbf{e}_1\big(u+u^*\big) = u \quad \text{for all } u \in U,\ u^* \in U^*,$$
$$\mathbf{e}_2\big(u+u^*\big) = u^* \quad \text{for all } u \in U,\ u^* \in U^*.$$

Proof. Let T be a subcover of U, and let I and A be the ideals of $\mathbf{P}_0(\mathbf{V})$ defined by

$$I := \mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}\big(M[T,U]\big),$$
$$A := \mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}\big(M\big[0,U^*\big]\big).$$

By Corollary 6.7, I is a maximal ideal of $\mathbf{P}_0(\mathbf{V})$. We show

$$A \not\subseteq I. \tag{7.8}$$

We suppose $A \subseteq I$. Then Proposition 6.11 gives ideals $B, S \in \mathsf{Id}\,\mathbf{V}$ with $0 \leqslant S \prec B \leqslant U^*$ such that $M[S,B]$ and $M[T,U]$ are isomorphic. Let α be the $\mathbf{P}_0(\mathbf{V})$-isomorphism. We take α' to be a mapping from B to U such that $\alpha'(b)+T = \alpha(b+S)$ for all $b \in B$. We have

$$\mathbf{p}\big(\alpha'(b)\big) \equiv \alpha'\big(\mathbf{p}(b)\big) \pmod{T} \quad \text{for all } \mathbf{p} \in P_0(\mathbf{V}),\ b \in B$$

and also

$$\alpha'(b_1+b_2) \equiv \alpha'(b_1)+\alpha'(b_2) \pmod{T} \quad \text{for all } b_1, b_2 \in B.$$

We define a subset K of V by

$$K := \big\{b+\alpha'(b)+s+t \mid b \in B,\ s \in S,\ t \in T\big\}.$$

We check that for $k_1, k_2 \in K$ and $\mathbf{p} \in P_0(\mathbf{V})$ we have $k_1+k_2 \in K$ and $\mathbf{p}(k_1) \in K$. Therefore K is an ideal of $\mathbf{V}$. We compute $K \wedge U$. Let $k = b+\alpha'(b)+s+t$ ($b \in B,\ s \in S,\ t \in T$) be an element of $K \wedge U$. Since $\alpha'(b)$ and t lie in U, we have $b+s \in U$. Since b and s are elements of U^*, we have $b+s \in U^* \wedge U$, and thus $b+s = 0$. Therefore $b \in S$. This implies $\alpha'(b) \in T$. So all four summands $b, \alpha'(b), s$, and t lie in $S \vee T$. We conclude

$$K \wedge U \leqslant S \vee T.$$

Now we compute $K \wedge U^*$: Suppose $b+\alpha'(b)+s+t \in U^*$. Then $\alpha'(b)+t \in U^*$. So $\alpha'(b)+t = 0$. This implies $\alpha'(b) \in T$, hence $b \in S$. Again, all summands are in $S \vee T$, so we have

$$K \wedge U^* \leqslant S \vee T.$$

We know $K = K \wedge (U \vee U^*) = (K \wedge U) \vee (K \wedge U^*)$. So we have

$$K \leqslant S \vee T.$$

We will infer the contradiction $B \subseteq S$ from this fact. We fix $b \in B$. The element $b + \alpha'(b)$ lies in K and hence in $S \vee T$. Since $\alpha'(b)$ lies in U, we have $b \in S \vee T \vee U = S \vee U$. But b also lies in B, thus we have

$$b \in (S \vee U) \wedge B = (S \wedge B) \vee (U \wedge B) = S \vee 0 = S,$$

so $B \subseteq S$, a contradiction. This yields (7.8).

Since $A \not\leqslant I$, and since I is a maximal ideal of $\mathbf{P}_0(\mathbf{V})$, we have $A + I = P_0(\mathbf{V})$. So there are polynomials $\mathbf{a} \in A, \mathbf{i} \in I$ such that

$$\mathbf{a} + \mathbf{i} = \mathbf{id}.$$

From this equation, we see that $\mathbf{i}$ satisfies $\mathbf{i}(u^*) = u^*$ for all $u^* \in U^*$ and $\mathbf{i}(U) \subseteq T$. By Proposition 7.12, we have $\mathbf{i}(U) \subseteq \Phi(U)$. Again by Proposition 7.12 we have $\mathbf{i}(\Phi(U)) \subseteq \Phi(\Phi(U))$, and thus $\mathbf{i}^2(U) \subseteq \Phi(\Phi(U)) =: \Phi^{(2)}(U)$. In the same way, we obtain

$$\mathbf{i}^n(U) \subseteq \Phi^{(n)}(U).$$

Since for every ideal $D > 0$ the ideal $\Phi(D)$ is strictly below D, there is a natural number k with $\mathbf{i}^k(U) = 0$. Now $\mathbf{e}_2 := \mathbf{i}^k$ and $\mathbf{e}_1 := \mathbf{id} - \mathbf{e}_2$ are the required polynomials. □

Proposition 7.14. *Let* $\mathbf{V}$ *be a finite expanded group, and let* U *be a homogeneous ideal of* $\mathbf{V}$. *Then there is a polynomial* $\mathbf{e}_3 \in P_0(\mathbf{V})$ *with the properties*

$$\mathbf{e}_3(u) = u \quad \text{for all } u \in U,$$
$$\mathbf{e}_3(V) \subseteq \big(\Phi(U) : U\big) \vee U.$$

Proof. It is a consequence of Proposition 7.9 that $[U, U] < U$ implies $(\Phi(U) : U) \vee U = (\Phi(U) : U)$, whereas $[U, U] = U$ implies $(\Phi(U) : U) \vee U = U^* \vee U$.

Let T be a subcover of U in $\mathsf{Id}\,\mathbf{V}$. Let A and I be the ideals of $\mathbf{P}_0(\mathbf{V})$ defined by

$$I := \mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}\big(M[T, U]\big),$$
$$A := \mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}\big(M\big[\big(\Phi(U) : U\big) \vee U, V\big]\big).$$

We show

$$A \not\subseteq I. \tag{7.9}$$

We suppose $A \subseteq I$. Then Proposition 6.11 yields that there are ideals $C, D \in \mathsf{Id}\,\mathbf{V}$ with $(\Phi(U) : U) \vee U \leqslant C \prec D \leqslant V$ such that the modules $M[C, D]$ and $M[T, U]$ are isomorphic. Then Propositions 6.9 and 7.8 yield $(C : D) = (T : U) = (\Phi(U) : U)$.

If $[U,U] \leqslant T$, Proposition 6.10 yields that $I[C,D]$ is abelian, and so $[D,D] \leqslant C$. Hence we have $D \leqslant (C:D)$, and therefore $D \leqslant (\Phi(U):U)$, a contradiction. This proves (7.9) for the case $[U,U] \leqslant T$.

If $[U,U] \not\leqslant T$, we have $(T:U) \not\geqslant U$, and so by Proposition 7.8, we have $(\Phi(U):U) \not\geqslant U$. This implies

$$\big(\Phi(U):U\big) \vee U > \big(\Phi(U):U\big) = (C:D) \geqslant C,$$

which is again a contradiction. This completes the proof of (7.9).

The ideal $I := \mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}(M[T,U])$ is a maximal ideal of $\mathbf{P}_0(\mathbf{V})$. By Proposition 7.12, we have $I = \mathrm{Ann}_{\mathbf{P}_0(\mathbf{V})}(M[\Phi(U),U])$. Since $A \nsubseteq I$, we have $I + A = P_0(\mathbf{V})$. Hence there are polynomials $\mathbf{i} \in I$, $\mathbf{a} \in A$ with $\mathbf{i} + \mathbf{a} = \mathbf{id}$. This yields that $\mathbf{i}$ satisfies $\mathbf{i}(U) \subseteq \Phi(U)$ and $\mathbf{i}(v) \in v + ((\Phi(U):U) \vee U)$ for all $v \in V$. Using Proposition 7.12, we obtain that for some power $\mathbf{i}^k$ we have $\mathbf{i}^k(U) = 0$ and $\mathbf{i}^k(v) \in v + ((\Phi(U):U) \vee U)$ for all $v \in V$. Then $\mathbf{e}_3 := \mathbf{id} - \mathbf{i}^k$ satisfies the required properties. □

Propositions 7.13 and 7.14 have the following consequence.

Proposition 7.15. *Let* $\mathbf{V}$ *be a finite expanded group with the homogeneous ideal* U. *If* $(\Phi(U):U) \leqslant U \vee U^*$, *then there exists a polynomial* $\mathbf{e}$ *with* $\mathbf{e}(V) \subseteq U$ *and* $\mathbf{e}(u) = u$ *for all* $u \in U$.

Proof. We use Proposition 7.14 to construct $\mathbf{e}_3$ and Proposition 7.13 to construct $\mathbf{e}_1$. Then $\mathbf{e} := \mathbf{e}_1 \circ \mathbf{e}_3$ satisfies the required properties. □

The following proposition is an extension of [7, Theorem 3.2].

Proposition 7.16. *Let* $\mathbf{V}$ *be a finite expanded group, and let* U *be a homogeneous ideal of* $\mathbf{V}$ *with* $(\Phi(U):U) \leqslant U \vee U^*$. *Let* f *be a partial function on* V *with domain* $T \subseteq V$. *We assume* $f(T) \subseteq U$. *Then the following are equivalent.*

(1) *There is a polynomial* $\mathbf{p} \in \mathsf{Pol}_1\mathbf{V}$ *with* $\mathbf{p}(V) \subseteq U$ *and* $\mathbf{p}(t) = f(t)$ *for all* $t \in T$.
(2) *For each coset* $C := v + (\Phi(U):U)$ *with* $v \in V$ *there is a polynomial* $\mathbf{p}_C \in \mathsf{Pol}_1\mathbf{V}$ *such that* $\mathbf{p}_C(t) = f(t)$ *for all* $t \in T \cap C$.

Proof. (1) ⇒ (2) is obvious; therefore we just prove (2) ⇒ (1). Let $T = \{t_1, t_2, \ldots, t_n\}$. We proceed by induction on n.

Case $n = 1$. The constant polynomial $\mathbf{p}(x) := f(t_1)$ fulfills the required properties.

Case $n = 2$. If $t_1 \equiv t_2 \pmod{(\Phi(U):U)}$, then there exists a polynomial $\mathbf{p}$ with $\mathbf{p}|_T = f$. Let $\mathbf{e}_U$ be the idempotent polynomial constructed in Proposition 7.15. The function $\mathbf{q}(t) := \mathbf{e}_U(\mathbf{p}(t))$ satisfies the required properties.

If $t_1 \not\equiv t_2 \pmod{(\Phi(U):U)}$, Proposition 7.11 gives $\mathcal{I}_{\mathbf{V}}(t_1 - t_2) \geqslant U$. Since $f(t_1) - f(t_2) \in U$, there is a polynomial $\mathbf{p} \in \mathsf{Pol}_1\mathbf{V}$ with $\mathbf{p}(t_1) = f(t_1)$, $\mathbf{p}(t_2) = f(t_2)$. The function $\mathbf{q}(t) := \mathbf{e}_U(\mathbf{p}(t))$ satisfies the required properties.

Case $n \geqslant 3$. If all elements of T are contained in one coset $v + (\Phi(U) : U)$, we know by assumption that there is a polynomial $\mathbf{p} \in \mathsf{Pol}_1 \mathbf{V}$ with $\mathbf{p}(z) = f(z)$ for all z such that $z \in T$. Now $\mathbf{q}(x) := \mathbf{e}_U(\mathbf{p}(x))$ interpolates f on T and has range contained in U.

We shall now assume that $t_1 - t_2 \notin (\Phi(U) : U)$. By induction hypothesis, we find a polynomial $\mathbf{q}_1 \in \mathsf{Pol}_1 \mathbf{V}$ with $\mathbf{q}_1(V) \subseteq U$ that agrees with f on $\{t_2, t_3, \ldots, t_n\}$. Subtracting $\mathbf{q}_1$ from f, we are left with a function f_1 which satisfies $f_1(t_2) = f_1(t_3) = \cdots = f_1(t_n) = 0$, $f_1(T) \subseteq U$, and still f_1 can be interpolated at each intersection of its domain with a coset of $(\Phi(U) : U)$ by a polynomial. For interpolating f_1 at T, we define two subsets S and B of V as follows:

$$S := \big\{\mathbf{p}(t_1) \mid \mathbf{p} \in \mathsf{Pol}_1 \mathbf{V},\ \mathbf{p}(V) \subseteq U,\ \mathbf{p}(t_2) = \mathbf{p}(t_3) = \mathbf{p}(t_4) = \cdots = \mathbf{p}(t_n) = 0\big\},$$
$$B := \big\{\mathbf{p}(t_1) \mid \mathbf{p} \in \mathsf{Pol}_1 \mathbf{V},\ \mathbf{p}(V) \subseteq U,\ \mathbf{p}(t_3) = \mathbf{p}(t_4) = \cdots = \mathbf{p}(t_n) = 0\big\}.$$

It is obvious that both S and B are ideals of $\mathbf{V}$ and that $S \subseteq B$. By induction hypothesis, we know $f_1(t_1) \in B$, and in order to find the polynomial that interpolates f at T, we prove $f_1(t_1) \in S$. For this, we show

$$S = B. \tag{7.10}$$

Let $D := \mathcal{I}_{\mathbf{V}}(t_1 - t_2)$. We know that $D \not\leqslant (\Phi(U) : U)$ and $B \leqslant U$, hence Proposition 7.10 yields $[B, D] = B$. We will now show

$$[B, D] \leqslant S. \tag{7.11}$$

For that purpose, we show that all generators of $[B, D]$ of the form $\mathbf{s}(b, d)$ with $\mathbf{s} \in \mathsf{Pol}_2 \mathbf{V}$, $\mathbf{s}(0, x) = \mathbf{s}(x, 0) = 0$, $b \in B, d \in D$ are in S. This can be seen as follows. Since $b \in B$, there is a function $\mathbf{q}_1 \in \mathsf{Pol}_1 \mathbf{V}$ such that

$$\mathbf{q}_1(t_1) = b, \qquad \mathbf{q}_1(t_3) = \mathbf{q}_1(t_4) = \cdots = \mathbf{q}_1(t_n) = 0,$$

and $\mathbf{q}_1(V) \subseteq U$. Since $d \in D = \mathcal{I}_{\mathbf{V}}(t_1 - t_2)$, there is a function $\mathbf{q}_2 \in \mathsf{Pol}_1 \mathbf{V}$ such that

$$\mathbf{q}_2(t_1) = d, \qquad \mathbf{q}_2(t_2) = 0.$$

Then $\mathbf{q}(x) := \mathbf{s}(\mathbf{q}_1(x), \mathbf{q}_2(x))$ is zero on $t_2, t_3, \ldots, t_n$ and the range of $\mathbf{q}$ is contained in U. This implies $\mathbf{q}(t_1) \in S$, which means $\mathbf{s}(b, d) \in S$. Thus we have proved (7.11), and therefore Eq. (7.10). Hence there is a polynomial whose range is contained in U that interpolates f_1 at T. This completes the proof of Proposition 7.16. □

This result yields a complete description of partial compatible functions whose domain is contained in a non-abelian minimal ideal. Corresponding results for groups were proved in [7, Theorem 2.1], [27, Theorem 10.24].

Proposition 7.17. *Let* $\mathbf{V}$ *be a finite expanded group, let* $T \subseteq V$*, and let* A *be a minimal ideal of* $\mathbf{V}$*. We assume* $[A, A] = A$*. Then for a function* $c : T \to A$*, the following are equivalent*:

(1) *The function c is a partial compatible function on* $\mathbf{V}$.
(2) *For all $x, y \in T$ with $x - y \in (0:A)$ we have $c(x) = c(y)$.*
(3) *There is a polynomial $\mathbf{p} \in \mathsf{Pol}_1 \mathbf{V}$ with $\mathbf{p}|_T = c$ and $\mathbf{p}(V) \subseteq A$.*
(4) *There is a polynomial $\mathbf{p} \in \mathsf{Pol}_1 \mathbf{V}$ with $\mathbf{p}|_T = c$.*

Proof. For (1) $\Rightarrow$ (2), we take $x, y \in T$ such that $x - y \in (0:A)$. By Proposition 7.7, every non-abelian minimal ideal of $\mathbf{V}$ is homogeneous. So Proposition 7.9 yields $(0:A) = A^*$. Since c is compatible, we have $c(x) - c(y) \in A^*$. Since $c(x) - c(y)$ also lies in A, we have $c(x) = c(y)$. For (2) $\Rightarrow$ (3), we observe that c is constant on each A^*-coset, and so Proposition 7.16 implies that c is the restriction of a polynomial $\mathbf{p}$ with $\mathbf{p}(V) \subseteq A$. The implication (3) $\Rightarrow$ (4) is obvious. For (4) $\Rightarrow$ (1), we observe that every polynomial is congruence preserving. □

If we include the case that the homogeneous ideal U satisfies $[U, U] < U$, we can describe polynomials with range in homogeneous ideal U as follows:

Proposition 7.18. *Let $\mathbf{V}$ be a finite expanded group, and let U be a homogeneous ideal of $\mathbf{V}$ with $(\Phi(U):U) \leqslant U \vee U^*$. Let $R := \{\mathbf{p}|_U \mid \mathbf{p} \in \mathsf{Pol}_1 \mathbf{V},\ \mathbf{p}(U) \subseteq U\}$, and let $\{v_0, v_1, v_2, \ldots, v_{s-1}\}$ be a transversal through the cosets of $U \vee U^*$. We define a mapping*

$$\Gamma : R^s \to \big\{\mathbf{p} \in \mathsf{Pol}_1 \mathbf{V} \mid \mathbf{p}(V) \subseteq U\big\},$$

where the function $\mathbf{q} = \Gamma(\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_{s-1})$ is defined by

$$\mathbf{q}\big(v_i + u + u^*\big) = \mathbf{r}_i(u) \quad \text{for all } i \in \{0, 1, \ldots, s-1\},\ u \in U,\ u^* \in U^*.$$

Then Γ is a bijection.

Proof. First, we show that $\mathbf{q}$ is really a polynomial. By Proposition 7.16 this is the case if the restriction of $\mathbf{q}$ to every $(\Phi(U):U)$-coset is the restriction of a polynomial. In the case $[U, U] = U$, we have $(\Phi(U):U) = U^*$. The restriction of $\mathbf{q}$ to a U^*-coset is constant, and therefore a polynomial. In the case $[U, U] < U$, we know $(\Phi(U):U) = U \vee U^*$, and so we have to show that the restriction of $\mathbf{q}$ to every $U \vee U^*$-coset is a polynomial. We take $\mathbf{e}$ to be the idempotent polynomial with range U constructed in Proposition 7.15. Defining $\mathbf{t}_i(x) := \mathbf{e}(\mathbf{r}_i(-v_i + x))$, we obtain $\mathbf{q}(v_i + u + u^*) = \mathbf{r}_i(u) = \mathbf{e}(\mathbf{r}_i(u)) = \mathbf{t}_i(v_i + u)$. By the fact that $\mathbf{t}_i$ has range contained in U, and by $U \wedge U^* = 0$, we have $\mathbf{t}_i(v_i + u) = \mathbf{t}_i(v_i + u + u^*)$. So $\mathbf{t}_i$ interpolates $\mathbf{q}$ at $v_i + (U \vee U^*)$.

For showing that Γ is surjective, we fix a polynomial $\mathbf{q}$ with range contained in U, and define $\mathbf{r}_i(x) := \mathbf{q}(v_i + x)$. Since $\mathbf{q}$ has range contained in U, we get $\mathbf{q}(v_i + u + u^*) = \mathbf{q}(v_i + u)$, and so the required equality $\mathbf{r}_i(u) = \mathbf{q}(v_i + u + u^*)$ for $u \in U, u^* \in U^*$ holds.

The mapping Γ is injective because $\mathbf{r}_i(u) \neq \mathbf{r}_i(u')$ implies $\mathbf{q}(v_i + u) \neq \mathbf{q}(v_i + u')$. □

8. Restrictions of polynomials to homogeneous ideals

Proposition 7.18 allows to reduce the problem of describing polynomials on certain finite expanded groups $\mathbf{V}$ to describing the restrictions of polynomials to a homogeneous ideal. We define the set

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

In the case that the homogeneous ideal U satisfies $[U,U] = U$, we know that U is an atom of $\mathsf{Id}\,\mathbf{V}$. So Proposition 6.6 (or Proposition 7.16) implies that every mapping $m : U \to U$ is a polynomial.

In describing polynomials for the case $[U,U] < U$, we restrict ourselves to the case $\Phi(U) = 0$. By Proposition 7.9, we then have $[U,U] = 0$. For a field $\mathbf{D}$, let $\mathbf{M}_n(\mathbf{D})$ be the ring of $(n \times n)$-matrices over $\mathbf{D}$, and let $\mathbf{D}^{(n\times m)}$ denote the $\mathbf{M}_n(\mathbf{D})$-module of all $(n \times m)$-matrices with entries from $\mathbf{D}$.

Proposition 8.1. *Let U be a homogeneous ideal of the finite expanded group $\mathbf{V}$. We assume that we have $\Phi(U) = 0$ and $[U,U] = 0$. We take $\mathbf{R}$ to be the ring with the universe*

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

and the operations given by pointwise addition of functions and their composition. We take $\mathbf{U}$ to be the $\mathbf{R}$-module

$$\langle U, +, -, 0, \langle f_{\mathbf{r}} \mid \mathbf{r} \in R\rangle\rangle,$$

where the operation $f_{\mathbf{r}}$ is defined by $f_{\mathbf{r}}(u) := \mathbf{r}(u)$.

Then there are: a field $\mathbf{D}$, natural numbers m, n, a ring isomorphism $\varepsilon_R : \mathbf{R} \to \mathbf{M}_n(\mathbf{D})$, and a group isomorphism $\varepsilon_U : \langle U, +\rangle \to \langle \mathbf{D}^{(n\times m)}, +\rangle$ such that for $r \in R$ and $u \in U$ we have

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

This proposition makes it possible to identify the elements of U with $(n \times m)$-matrices, and the restrictions of polynomials with $(n \times n)$-matrices.

Proof. Since $[U,U] = 0$, Proposition 2.3 gives that $\mathbf{R}$ is a ring and $\mathbf{U}$ is an $\mathbf{R}$-module. We observe that the universes of $\mathbf{R}$-submodules of $\mathbf{U}$ are the ideals of $\mathbf{V}$ below U.

Since $\Phi(U) = 0$, [26, Lemma 4.83] yields that $I[0,U]$ is a complemented lattice and thus, again by [26, Lemma 4.83], U is the join of atoms of $\mathsf{Id}\,\mathbf{V}$. By Proposition 7.3, all these atoms are projective in $\mathsf{Id}\,\mathbf{V}$. Proposition 6.1 yields that these atoms are isomorphic as $\mathbf{R}$-modules. Let A be one of these atoms. We see that the ring $\mathbf{R}$ is faithful on A. To this end, we fix $\mathbf{r} \in R$ with $\mathbf{r}(A) = 0$. We show $\mathbf{r}(U) = 0$. We fix $u \in U$. Since U is the join of

atoms that are projective to A, we have elements $b_1, b_2, \ldots, b_n$ with $u = b_1 + b_2 + \cdots + b_n$ such that each b_i lies in some atom projective to A. So we have

$$\mathbf{r}\left(\sum_{i=1}^{n} b_i\right) = \sum_{i=1}^{n} \mathbf{r}(b_i).$$

But since $\mathbf{r}(A) = 0$, Proposition 6.1 yields $\mathbf{r}(B) = 0$ for every atom B that is projective to A. So each summand $\mathbf{r}(b_i)$ is 0, which implies $\mathbf{r}(u) = 0$.

Hence $\mathbf{R}$ is primitive on A; thus by Jacobson's Density Theorem [17, p. 28] $\mathbf{R}$ is isomorphic to the matrix ring $\mathbf{M}_n(\mathbf{D})$, where $\mathbf{D}$ is the field of all $\mathbf{R}$-endomorphisms of A, and n is the dimension of A over $\mathbf{D}$.

We observe that the $\mathbf{R}$-module $\mathbf{U}$ is the sum of finitely many simple $\mathbf{R}$-modules that are $\mathbf{R}$-isomorphic to A, and therefore $\mathbf{U}$ is isomorphic to A^m for some $m \in \mathbb{N}$. Since the module A is isomorphic to $\mathbf{D}^{(n\times 1)}$, we obtain that $\mathbf{U}$ is isomorphic to $(\mathbf{D}^{(n\times 1)})^m = \mathbf{D}^{(n\times m)}$. □

We will now examine compatible functions on the module $\mathbf{D}^{(n\times m)}$.

Proposition 8.2. *Every vector space over* $\mathbf{GF}(2)$ *is strictly* 1*-affine complete.*

Proof. Let $\mathbf{V}$ be a vector space over $\mathbf{GF}(2)$, and let $c : T \subseteq V \to V$ be a compatible function. We fix two elements $t_1, t_2 \in T$ with $t_1 \neq t_2$. Since c is a compatible function, it can be interpolated at $\{t_1, t_2\}$ by a polynomial $\mathbf{p}$. Let $c_1 := c - \mathbf{p}$. We show $c_1(T) = 0$, and to this end, we fix $t_3 \in T$. Since the intersection of the subspace generated $t_3 - t_1$ with the subspace generated by $t_3 - t_2$ is zero, we get $c_1(t_3) = 0$. Hence $\mathbf{p}$ is the polynomial that interpolates c. □

Proposition 4.5 shows that a finite module over a finite simple ring with unit can only be strictly 1-affine complete if every minimal submodule has precisely two elements, and hence the ring has to be the two element field. But as the 2-dimensional vector space over $\mathbf{GF}(3)$ shows, there are modules that are 1-affine complete, but not strictly 1-affine complete. More examples of affine complete modules are given in the following result due to [33], which we will not need for characterizing strictly 1-affine complete expanded groups, but which will help us to characterize all 1-affine complete expanded groups with (SC1).

Proposition 8.3. *Let* $\mathbf{R}$ *be a finite simple ring with unit, and let* $\mathbf{N}$ *be a faithful simple unitary* $\mathbf{R}$*-module. If* $|N| = 2$ *or* $m \geqslant 2$*, then the module* $\mathbf{N}^m$ *is* 1*-affine complete.*

Proof. If N has two elements, then $\mathbf{N}$ is obviously 1-affine complete. If $m \geqslant 2$, then it follows from [33] that $\mathbf{N}$ is even k-affine complete for all natural numbers k. □

9. Polynomials on expanded groups with (SC1)

We will now show that a finite expanded group with (SC1) has a homogeneous ideal U, and that the centralizer $(\Phi(U):U)$ is less or equal to $U \vee U^*$. We recall that $J(\mathsf{Id}\,\mathbf{V})$ is the set of all strictly join irreducible elements of $\mathsf{Id}\,\mathbf{V}$ and for $A, B \in J(\mathsf{Id}\,\mathbf{V})$ we have $A \sim B$ if $I[A^-, A] \nleftrightarrow I[B^-, B]$.

If A is abelian over A^-, we have the following possibility to compute the centralizer $(A^-:A)$.

Proposition 9.1. *Let* $\mathbf{V}$ *be an expanded group with* (SC1)*, and let* $A \in J(\mathsf{Id}\,\mathbf{V})$ *satisfy* $[A, A] \leqslant A^-$*. Then for every strictly meet irreducible ideal* E *with the properties* $E \geqslant A^-$*,* $E \not\geqslant A$ *we have* $(A^-:A) = E \vee A$*.*

Proof. We have $I[A^-, A] \nearrow I[E, E \vee A]$ (and therefore $E \vee A = E^+$). Hence, Proposition 2.2 gives $(E : E \vee A) \geqslant E \vee A$. Since E is meet irreducible, the condition (SC1) implies that $(E : E \vee A) = E \vee A$. Proposition 2.2 now yields $(A^-:A) = E \vee A$. □

Each equivalence class $A/\!\sim$ is an antichain:

Proposition 9.2. *Let* $\mathbf{V}$ *be an expanded group with* (SC1)*, and let* $A, B \in J(\mathsf{Id}\,\mathbf{V})$ *such that* $A \sim B$ *and* $A \leqslant B$*. Then* $A = B$*.*

Proof. If $[A, A] = A$, the result follows from Proposition 7.7. Hence, we assume $[A, A] \leqslant A^-$. Suppose that $A < B$. Then let E be a strictly meet irreducible element of $\mathsf{Id}\,\mathbf{V}$ with $E \geqslant A^-$, $E \not\geqslant A$. By Proposition 9.1, we have $(A^-:A) = E \vee A$. Since $B \geqslant A$, the modular law yields $(B \wedge E) \vee A = B \wedge (E \vee A)$. By Proposition 2.2, we have $E \vee A = (A^-:A) = (B^-:B) \geqslant B$. Hence we get $(B \wedge E) \vee A \geqslant B$. On the other hand, both $B \wedge E$ and A are $\leqslant B$. Altogether, we get $(B \wedge E) \vee A = B$. Since B is join irreducible and $A < B$, we have $B \wedge E = B$, which implies $B \leqslant E$. Therefore, we also have $A \leqslant E$, which contradicts the choice of E. □

Proposition 9.3. *Let* $\mathbf{V}$ *be an expanded group with* (SC1)*, and let* $A, B, C \in J(\mathsf{Id}\,\mathbf{V})$*. If* $A \sim B$ *and* $B < C$*, then* $A < C$*.*

Proof. We first show $A \leqslant C$: Suppose that $A \not\leqslant C$. The commutator $[A, C]$ fulfills $[A, C] \leqslant A$. Since A is join irreducible, this means that either $[A, C] = A$ or $[A, C] \leqslant A^-$. If $[A, C] = A$, we have $A \wedge C \geqslant [A, C] = A$, and hence $A \leqslant C$. If $[A, C] \leqslant A^-$, we have $(A^-:A) \geqslant C$. Proposition 2.2 yields $(B^-:B) \geqslant C$, from which we get $[B, C] \leqslant B^-$. Since both B and C are join irreducible, Proposition 3.3 yields that $\mathbf{V}$ does not satisfy (SC1). Hence we must have $A \leqslant C$. Now suppose that $A = C$. Then we have $A \sim B$ and $B < A$, which contradicts Proposition 9.2. □

These properties allow us to define an order relation $\leqslant$ on $J(\mathsf{Id}\,\mathbf{V})/\!\sim$:

Definition 9.4. Let $\mathbf{V}$ be an expanded group with (SC1), and let $A, B \in J(\mathsf{Id}\,\mathbf{V})$. We define

$$A/{\sim} \leqslant B/{\sim} \quad \text{iff} \quad \exists A' \in A/{\sim}\, \exists B' \in B/{\sim}\colon\ A' \leqslant B'.$$

Proposition 9.5. *Let* $\mathbf{V}$ *be an expanded group with* (SC1). *Then we have*:

(1) $\leqslant$ *is a partial order on* $J(\mathsf{Id}\,\mathbf{V})/{\sim}$.
(2) $A/{\sim} \leqslant B/{\sim}$ *iff* $\forall A' \in A/{\sim}\, \exists B' \in B/{\sim}\colon\ A' \leqslant B'$.

Proof. For (1), we observe that the relation $\leqslant$ is obviously reflexive. Let us now prove that it is transitive. Let $A, B, C \in J(\mathsf{Id}\,\mathbf{V})$ such that $A/{\sim} \leqslant B/{\sim}$ and $B/{\sim} \leqslant C/{\sim}$. By definition, there are ideals $A' \in A/{\sim}$, $B', B'' \in B/{\sim}$, and $C' \in C/{\sim}$ such that $A' \leqslant B'$ and $B'' \leqslant C'$. If $B'' = C'$, we have $B/{\sim} = C/{\sim}$ and thus $A/{\sim} \leqslant C/{\sim}$. If $B'' < C'$, then Proposition 9.3 yields $B' \leqslant C'$. Hence we have $A' \leqslant C'$ and therefore $A/{\sim} \leqslant C/{\sim}$. Now we show that $\leqslant$ is antisymmetric: let $A, B \in J(\mathsf{Id}\,\mathbf{V})$ such that $A/{\sim} \leqslant B/{\sim}$ and $B/{\sim} \leqslant A/{\sim}$. Hence there are $A', A'' \in A/{\sim}$ and $B', B'' \in B/{\sim}$ with $A' \leqslant B'$ and $B'' \leqslant A''$. If $B'' = A''$, we have $A/{\sim} = B/{\sim}$. If $B'' < A''$, Proposition 9.3 yields $B' \leqslant A''$. Hence we get $A' \leqslant A''$. Now Proposition 9.2 yields $A' = A''$. In the same way, we obtain $B' = B''$. From this, we get $A' \leqslant B' \leqslant A'$, which implies $A' = B'$ and hence also $A/{\sim} = B/{\sim}$.

The "if"-direction of (2) is obvious. For "only if", let $A, B \in J(\mathsf{Id}\,\mathbf{V})$ such that $A/{\sim} \leqslant B/{\sim}$. Now let A' be an arbitrary element of $A/{\sim}$. We know that there are A'', B'' with $A'' \in A/{\sim}$, $B'' \in B/{\sim}$ such that $A'' \leqslant B''$. If $A'' = B''$, then $A' \in B/{\sim}$, hence $B' := A'$ is an element in $B/{\sim}$ with $A' \leqslant B'$. If $A'' < B''$, Proposition 9.3 gives $A' \leqslant B''$, hence B'' is an element in $B/{\sim}$ with $A' \leqslant B'$. □

Proposition 9.6. *Let* $\mathbf{V}$ *be a finite expanded group with* (SC1), *and let* $A/{\sim}$ *be a minimal element of* $(J(\mathsf{Id}\,\mathbf{V})/{\sim}, \leqslant)$. *Then every ideal* $A' \in A/{\sim}$ *is a minimal ideal of* $\mathbf{V}$.

Proof. Let B be a minimal ideal of $\mathbf{V}$ with $B \leqslant A'$. As a minimal ideal, B is join irreducible. By the definition of $\leqslant$, we get $B/{\sim} \leqslant A'/{\sim}$. Since $A'/{\sim}$ is minimal with respect to $\leqslant$, we get $B \in A'/{\sim}$. But now we have $B \sim A'$ and $B \leqslant A'$; so Proposition 9.2 yields $B = A'$, and thus A' is minimal. □

We are now ready to construct a homogeneous ideal U:

Proposition 9.7. *Let* $\mathbf{V}$ *be a finite expanded group with* (SC1), *and let* $A \in \mathsf{Id}\,\mathbf{V}$ *be such that* $A/{\sim}$ *is a minimal element of* $J(\mathsf{Id}\,\mathbf{V})/{\sim}$. *Then the ideal* U *defined by*

$$U := \bigvee_{B \in A/{\sim}} B \tag{9.1}$$

is a homogeneous ideal of $\mathbf{V}$.

Proof. We first show that every join irreducible ideal C with $C \leqslant U$ satisfies $C \sim A$. By Proposition 9.6, every element in $A/{\sim}$ is an atom of $\mathsf{Id}\,\mathbf{V}$. Therefore, U is the join of

all atoms in $I[0,U]$. [26, Lemma 4.83] implies that $I[0,U]$ is relatively complemented. So C has a complement in $I[C^-,U]$, which gives $S \in \mathsf{Id}\,\mathbf{V}$ such that $S \vee C = U$ and $S \wedge C = C^-$. Thus $I[C^-,C]$ projects up to $I[S,U]$. Since U is the join of elements in $A/\!\sim$, we find an ideal $B \in \mathsf{Id}\,\mathbf{V}$ with $B \sim A$ such that $B \not\leqslant S$. So we have $S \vee B > S$, and since by modularity we have $U \succ S$, we get $S \vee B = U$. We also obtain $S \wedge B \leqslant B^-$, and, using again modularity, $S \wedge B = B^-$ and thus $I[B^-,B] \nearrow I[S,U]$. But since $I[S,U]$ projects down to $I[C^-,C]$, we obtain $C \sim B$, and thus $C \sim A$.

For property (3) in Definition 7.1, suppose that there are join irreducible ideals B, D in $\mathsf{Id}\,\mathbf{V}$ such that $B \leqslant U$, $D \not\leqslant U$, and B and D are projective. By the fact that all join irreducibles below U are projective, B is projective to A. Therefore D appears in the join by which U is defined, and so we have $D \leqslant U$, a contradiction. □

More information on the interval $I[0,U]$ can be obtained from Proposition 8.1.

So every expanded group with (SC1) has at least one homogeneous ideal. And in expanded groups with (SC1), all homogeneous ideals have special properties. The most important one is $(\Phi(U):U) \leqslant U \vee U^*$, which allows to use Proposition 7.15.

Proposition 9.8. *Let* $\mathbf{V}$ *be a finite expanded group with* (SC1)*, and let* U *be a homogeneous ideal of* $\mathbf{V}$*. Then we have*:

(1) $\Phi(U) = 0$.
(2) *If* $[U,U] < U$*, then* $[U,U] = 0$ *and* $(0:U) = U \vee U^*$.
(3) *If* $[U,U] = U$*, then* U *is an atom of* $\mathsf{Id}\,\mathbf{V}$ *and* $(0:U) = U^*$.

Proof. If $[U,U] = U$, then Proposition 7.7 yields that U is an atom of $\mathsf{Id}\,\mathbf{V}$, and so (1) is immediate.

Let us now consider the case $[U,U] < U$. We first show that U is the join of all atoms A of $\mathsf{Id}\,\mathbf{V}$ with $A \leqslant U$. Suppose it were not. Since U is the join of all join irreducible elements of $\mathsf{Id}\,\mathbf{V}$ that are $\leqslant U$, there must be a join irreducible ideal $B \in \mathsf{Id}\,\mathbf{V}$ such that B is not an atom. Let A be an atom of $\mathsf{Id}\,\mathbf{V}$ with $A \leqslant B$. By the definition of homogeneous ideals, we know $I[0,A] \leftrightsquigarrow I[B^-,B]$, which contradicts Proposition 9.2.

Now we show that every atom $A \leqslant U$ satisfies $[A,A] = 0$; for this purpose, we look at $(0:A)$. From Proposition 7.8, we obtain $(0:A) = (\Phi(U):U)$. By Proposition 7.9 and $[U,U] < U$, we have $(\Phi(U):U) \geqslant U$. Hence $(0:A) \geqslant U$, and thus $[A,A] \leqslant [U,A] = 0$.

From the fact that U is the join of atoms A that satisfy $[A,A] = 0$, we obtain, using Proposition 2.1, $[U,U] = 0$. By Proposition 3.2, 0 is therefore the intersection of all subcovers of U, which implies $\Phi(U) = 0$. This finishes the proof of (1).

For the proof of (2), we observe that $[U,U] = 0$ and $U \wedge U^* = 0$ imply $(0:U) \geqslant U \vee U^*$. We now show $(0:U) \leqslant U \vee U^*$. By Proposition 3.1 we have

$$\begin{aligned} 0 &= \big[(0:U),U\big] \\ &= \big(\big[(0:U),(0:U)\big] \wedge U\big) \vee \big((0:U) \wedge [U,U]\big) \\ &= \big[(0:U),(0:U)\big] \wedge U. \end{aligned}$$

The definition of U^* thus yields $[(0:U),(0:U)] \leqslant U^*$. Since $\mathbf{V}/U^*$, as a quotient of an expanded group with (SC1), satisfies the condition (SC1), Proposition 3.2 gives that the coatoms of the lattice $I[U^*/U^*, (0:U)/U^*]$ (as a sublattice of $\mathsf{Id}\,\mathbf{V}/U^*$) intersect to $0 = U^*/U^*$. (Here we write A/U^* for the image of A under the canonical epimorphism from $\mathbf{V}$ onto $\mathbf{V}/U^*$.) By [26, Lemma 4.83], we know that the lattice $I[U^*/U^*, (0:U)/U^*]$ is complemented. Hence also the isomorphic lattice $I[U^*, (0:U)]$ is complemented. Let K be a complement of $U^* \vee U$ in $I[U^*, (0:U)]$. Then we have $U^* = K \wedge (U^* \vee U)$. By congruence modularity, this is equal to $(K \wedge U) \vee U^*$. This implies $K \wedge U \leqslant U^*$. Therefore, we also have $K \wedge U \leqslant U^* \wedge U$, thus

$$K \wedge U = 0.$$

This implies $K \leqslant U^*$. Hence we get $(0:U) = (U^* \vee U) \vee K \leqslant U^* \vee U$, which finishes the proof of (2).

For item (3), we observe that if $[U,U] = U$ then $[A,U] = 0$ iff $A \wedge U = 0$. This shows $(0:U) = U^*$. □

10. Interpolation of compatible functions

Proposition 10.1. *Let* $\mathbf{V}$ *be a finite expanded group, and let* U *be a homogeneous ideal of* U *with* $[U,U] = 0$, $(0:U) = U \vee U^*$ *and* $\Phi(U) = 0$. *We assume that every atom* A *of* $\mathsf{Id}\,\mathbf{V}$ *with* $A \leqslant U$ *has precisely two elements. Let* c *be a unary partial compatible function on* $\mathbf{V}$ *such that the domain* T *of* c *is contained in* $(0:U)$ *and* $c(T) \subseteq U$. *Then* c *can be interpolated by a polynomial on* T.

Proof. For getting started, we will not interpolate c, but a function c_1, which is a partial function from U to U defined as follows.

$$c_1 : U \to U,$$
$$u \mapsto \begin{cases} c(u+u^*), & \text{if there is a } u^* \in U^* \text{ with } u+u^* \in T, \\ \text{undefined}, & \text{else.} \end{cases}$$

The function c_1 is well defined. To show this, let u be in U, and let a^* and b^* be in U^* such that $u+a^*$ and $u+b^*$ lie in the domain of c. We then have $c(u+a^*) \equiv c(u+b^*) \pmod{U^*}$ because c is a compatible function. Since the range of c is contained in U, we have $c(u+a^*) \equiv c(u+b^*) \pmod{U \wedge U^*}$, which implies $c(u+a^*) = c(u+b^*)$. This last equality makes $c_1(u)$ well defined.

Now we show that c_1 is a compatible partial function on $\mathbf{V}$. For that purpose, let $u_1, u_2 \in \mathsf{dom}\, c_1$. We have to show

$$c_1(u_1) \equiv c_1(u_2) \pmod{I}, \tag{10.1}$$

where I is given by $I := \mathcal{I}_{\mathbf{V}}(u_1 - u_2)$. First of all we notice that $c_1(u_1) = c(u_1 + u_1^*)$ for some $u_1^* \in U^*$. In the same way we find u_2^* such that $c_1(u_2) = c(u_2 + u_2^*)$ for some

$u_2^* \in U^*$. We immediately see that $u_1 + u_1^* \equiv u_2 + u_2^* \pmod{I \vee U^*}$. The function c is compatible. Therefore we have $c(u_1 + {u_1}^*) \equiv c(u_2 + {u_2}^*) \pmod{I \vee U^*}$, and, since the range of c is contained in U, we get $c(u_1 + u_1^*) \equiv c(u_2 + u_2^*) \pmod{(I \vee U^*) \wedge U}$. But by congruence modularity and $I \leqslant U$, we get $(I \vee U^*) \wedge U = I \vee (U^* \wedge U) = I \vee 0 = I$. This implies (10.1).

Proposition 8.1 tells how to see U as a vector space over $\mathbf{GF}(2)$, and so there is a natural number m such that we can view c as a partial compatible function on the vector space $\mathbf{GF}(2)^m$. By Proposition 8.2, we have a polynomial $\mathbf{p} \in \mathsf{Pol}_1 \mathbf{V}$ that interpolates c_1. Since U is the range of an idempotent polynomial function (Proposition 7.15), we may assume that the range of $\mathbf{p}$ is contained in U. Now we show that $\mathbf{p}$ agrees with c on T. To this end, let $t \in T$. Since $U \vee U^* = (0:U)$, we know that $t = u + u^*$ for some $u \in U,\ u^* \in U^*$. Now we have $c(t) = c(u + u^*)$. By the definition of c_1, $c(u + u^*)$ is equal to $c_1(u) = \mathbf{p}(u)$. Since $\mathbf{p}(u + u^*)$ is congruent to $\mathbf{p}(u)$ modulo U^*, and since the range of $\mathbf{p}$ is contained in U, the fact that $U \wedge U^* = 0$ yields $\mathbf{p}(u) = \mathbf{p}(u + u^*)$. Altogether, we get $\mathbf{p}(t) = c(t)$. □

Proposition 10.2. *Let* $\mathbf{V}$ *be a finite expanded group, and let* U *be a homogeneous ideal of* U *with* $[U, U] = 0$, $(0:U) = U \vee U^*$ *and* $\Phi(U) = 0$. *We assume that every atom* A *of* $\mathsf{Id}\,\mathbf{V}$ *with* $A \leqslant U$ *has precisely two elements. Let* c *be a unary partial compatible function on* $\mathbf{V}$ *with domain* T *such that* $c(T) \subseteq U$. *Then* c *can be interpolated by a polynomial on* T.

Proof. By Proposition 7.16, it is sufficient to interpolate c on each coset of $(0:U)$ separately. But the interpolating polynomial on every single coset exists by Proposition 10.1. □

Now we glue all our pieces together to give a proof of Theorem 1.3.

Proposition 10.3. *Let* $\mathbf{V}$ *be a finite expanded group. If* $\mathbf{V}$ *satisfies* (SC1) *and* (AB2), *then* $\mathbf{V}$ *is strictly* 1*-affine complete.*

Proof. We induct on the size of $\mathbf{V}$. The statement is obvious for one-element algebras. For the induction step, we use Proposition 9.7 to construct a homogeneous ideal U. By Proposition 9.8, we have $\Phi(U) = 0$ and $(\Phi(U):U) \leqslant U \vee U^*$. Since both properties (SC1) and (AB2) carry over to homomorphic images of $\mathbf{V}$, we know by the induction hypothesis that $\mathbf{V}/U$ is strictly 1-affine complete. Let c be a partial compatible function on $\mathbf{V}$ with finite domain T. By the strict affine completeness of $\mathbf{V}/U$, we first interpolate c modulo U after which we are left with a compatible function c_1 whose range is contained in U. If $[U, U] = U$, then by Proposition 7.9, U is a minimal ideal of $\mathbf{V}$, and so Proposition 7.17 tells that c_1 is a polynomial.

If $[U, U] < U$, then by Proposition 9.8, we have $[U, U] = 0$. The condition (AB2) implies that every atom A of $\mathsf{Id}\,\mathbf{V}$ with $A \leqslant U$ has precisely two elements. From Proposition 10.2 we obtain that c_1 is a polynomial. □

We have now concluded the proof of our main result stated in Theorem 1.3: Proposition 10.3 proves (1) ⇒ (2), Propositions 4.4 and 4.5 prove (2) ⇒ (1). Propositions 4.6 and 4.7 prove (3) ⇒ (1). For (1) ⇒ (4), we observe that both conditions (SC1) and (AB2)

carry over to homomorphic images. Therefore, by Proposition 10.3, every homomorphic image of a finite expanded group with (SC1) and (AB2) is strictly 1-affine complete. The implication (4) $\Rightarrow$ (3) obviously holds for finite algebras.

11. Strictly 1-affine complete groups and rings

In this section we characterize those finite groups and commutative rings with unit that satisfy (SC1) and (AB2). A group G is called *perfect* iff it coincides with its derived subgroup.

Proposition 11.1. *For a finite group* $\mathbf{G}$*, the following are equivalent.*

(1) $\mathbf{G}$ *satisfies* (SC1) *and* (AB2).
(2) $\mathbf{G}$ *has a normal subgroup* H *such that every normal subgroup* I *of* $\mathbf{G}$ *with* $I \leqslant H$ *is perfect and* $\mathbf{G}/H$ *is isomorphic to* $(\mathbb{Z}_2)^n$ *for some* $n \in \mathbb{N}_0$.

Proof. (1) $\Rightarrow$ (2). Let H be the intersection of all normal subgroups of index 2 in $\mathbf{G}$. Then $\mathbf{G}/H$ is a group of exponent 2. Seeking a contradiction, we suppose that B is a normal subgroup of $\mathbf{G}$ with $B \leqslant H$ that is not perfect. By [26, Exercise 4.156(11)], the derived subgroup B' is equal to the commutator $[B, B]$, taken in $\mathbf{G}$. Thus there is a normal subgroup A of $\mathbf{G}$ such that $A \prec B$ in $\mathsf{Id}\,\mathbf{G}$, and the interval $I[A, B]$ is abelian. We choose C to be maximal among the normal subgroups of $\mathbf{G}$ with $C \geqslant A$, $C \not\geqslant B$. We observe that C is meet irreducible and that $I[A, B]$ projects up to $I[C, C^+]$, and thus Proposition 2.2 and (AB2) imply that C^+ contains precisely two cosets of C. Passing to $\mathbf{G}/C$ and using the fact that every normal subgroup with two elements lies in the center, we obtain $(C : C^+) = G$. Hence, condition (SC1) implies $G = C^+$. So C is a normal subgroup of $\mathbf{G}$ with index 2, and thus $C \geqslant H \geqslant B$, a contradiction to the choice of C.

(2) $\Rightarrow$ (1). Suppose that (AB2) fails. Then there are normal subgroups $A \prec B$ of $\mathbf{G}$ with $[B, B] \leqslant A$ and $|B/A| > 2$, and hence $\mathbf{G}$ has a principal series in which one of the factors is abelian and of size greater than 2. But by the assumptions, $\mathbf{G}$ has another principal series in which the only abelian factors are of size 2, contradicting the fact that all principal series have isomorphic factors.

For proving (SC1), suppose that there is a meet irreducible normal subgroup M of $\mathbf{G}$ such that $(M : M^+) > M^+$. If $M \geqslant H$, then since all meet irreducible normal subgroups of $\mathbb{Z}_2^n$ are maximal, $M^+ = G$, which contradicts the fact that $(M : M^+)$ is strictly greater than M^+. If $M \not\geqslant H$, the interval $I[M, M^+]$ projects down to $I[M \wedge H, M^+ \wedge H]$. This interval forms an abelian section below H, thus $M^+ \wedge H$ is not perfect. □

Altogether, we have established the following characterization of affine complete groups:

Corollary 11.2. *For a finite group* $\mathbf{G}$*, the following are equivalent*:

(1) $\mathbf{G}$ *has a normal subgroup* H *such that every normal subgroup* I *of* $\mathbf{G}$ *with* $I \leqslant H$ *is perfect, and* $G = H$ *or* $\mathbf{G}/H$ *is of exponent* 2.
(2) $\mathbf{G}$ *is strictly* 1*-affine complete.*
(3) *Every homomorphic image of* $\mathbf{G}$ *is* 1*-affine complete.*

However, we note that (1) ⇒ (2) and (1) ⇒ (3) of Corollary 11.2 can also be proved from [25, Chapter 1, Proposition 12.5] or from Proposition 7.17.

Now we switch to finite commutative rings with unit. First we characterize subdirectly irreducible such rings that satisfy (AB2) and (SC1).

Proposition 11.3. *For a finite commutative ring* $\mathbf{R}$ *with unit, the following are equivalent*:

(1) $\mathbf{R}$ *is subdirectly irreducible and satisfies* (AB2) *and* (SC1).
(2) $\mathbf{R}$ *is either* $\mathbb{Z}_4$*, the matrix ring* $\left\{\left(\begin{smallmatrix} x & 0 \\ y & x \end{smallmatrix}\right) \mid x, y \in \mathrm{GF}(2)\right\}$*, or a finite field.*

Proof. The implication (2) ⇒ (1) is obvious. For (1) ⇒ (2), let $\mathbf{R}$ be a ring satisfying the conditions in (1). If the Jacobson radical $J(\mathbf{R})$ is zero, the ring $\mathbf{R}$ is semisimple and therefore a direct product of fields. But since $\mathbf{R}$ is subdirectly irreducible, it follows that $\mathbf{R}$ is a field. So we assume that $J(\mathbf{R})$ is not zero. Let us recall that for commutative rings the commutator operation is just ideal multiplication. We know that $J(\mathbf{R})$ is a nilpotent ideal of $\mathbf{R}$, in other words, the sequence $J^{(n+1)}(\mathbf{R}) := [J^{(n)}(\mathbf{R}), J(\mathbf{R})]$, $J^{(1)}(\mathbf{R}) := J(\mathbf{R})$ eventually reaches 0. Since Proposition 3.1(1) implies $[A, A] = [[A, A], A]$ for all ideals A of a ring with (SC1), we get $[J(\mathbf{R}), J(\mathbf{R})] = 0$.

Now let M be the unique minimal ideal of $\mathbf{R}$. Then $M \leqslant J(\mathbf{R})$. Since $[M, J(\mathbf{R})] \leqslant [J(\mathbf{R}), J(\mathbf{R})] = 0$, condition (SC1) gives $M = J(\mathbf{R})$. Furthermore $[M, M] = 0$, and so condition (AB2) gives that $|M| = 2$. Let m be the nonzero element of M. The ring $\mathbf{R}/M$ is semisimple and therefore isomorphic to a direct product $\mathbf{F}_1 \times \mathbf{F}_2 \times \cdots \times \mathbf{F}_k$ of fields. We will now show $k = 1$, i.e., $\mathbf{R}/M$ is a field: Suppose that $k > 1$. Then $\mathbf{R}/M$ has an idempotent element different from $0 + M$ and $1 + M$. Hence $\mathbf{R}$ contains an element $a \notin \{0, 1, m, 1 + m\}$ that satisfies $a^2 = a$ or $a^2 = a + m$.

Case $a^2 = a$. Since M is the unique minimal ideal of $\mathbf{R}$, there is an $r \in \mathbf{R}$ such that $m = ra$. We know that $m^2 = 0$, hence we have

$$0 = m^2 = r^2a^2 = r^2a = rm.$$

From this, we get $[\mathcal{I}_{\mathbf{R}}(r), M] = 0$, and hence condition (SC1) implies $r \in M$. Thus we have $r = m$ and therefore $m = ma$, which implies $m(a - 1) = 0$. This implies $[\mathcal{I}_{\mathbf{R}}(a - 1), M] = 0$, and hence by (SC1) we have $a - 1 \in M$.

Case $a^2 = a + m$. Then for $a' := a + m$ we have $a'^2 = (a + m)^2 = a^2 + 2am + m^2 = a + m + 0 + 0 = a'$. As in the case $a^2 = a$, we obtain $a' - 1 \in M$. Hence in both cases we get that a lies in $\{0, 1, m, 1 + m\}$, a contradiction.

Consequently $\mathbf{R}/M$ is isomorphic to a field $\mathbf{F}$. Suppose that this field has f elements. Since the ring $\mathbf{R}$ is local, every element not in M is invertible, hence $\mathbf{R}$ contains $2f-2$ invertible and 2 noninvertible elements. We consider the mapping $\varphi: R \to R,\ r \mapsto r+1$. If r is invertible, we get $rm = m$. From this it follows that $(r+1)m = 0$. Hence $(r+1)$ is a zero divisor and therefore not invertible. Since the mapping φ is injective, we get $2f-2 \leqslant 2$. But this implies $f = 2$, and thus $\mathbf{F}$ is a field with 2 elements.

By inspection of all rings with four elements, we find $\mathbb{Z}_4$ and the matrix ring $\left\{\left(\begin{smallmatrix} x & 0 \\ y & x \end{smallmatrix}\right) \mid x, y \in \mathrm{GF}(2)\right\}$ as the only subdirectly irreducible commutative rings with unit and two element radical. □

Altogether, we have established the following characterization of affine complete commutative rings with unit:

Corollary 11.4. *For a finite commutative ring* $\mathbf{R}$ *with unit, the following are equivalent*:

(1) *Every subdirectly irreducible homomorphic image of* $\mathbf{R}$ *is either a field, the ring* $\mathbb{Z}_4$, *or the matrix ring* $\left\{\left(\begin{smallmatrix} x & 0 \\ y & x \end{smallmatrix}\right) \mid x, y \in \mathrm{GF}(2)\right\}$.
(2) $\mathbf{R}$ *is strictly* 1*-affine complete.*
(3) *Every homomorphic image of* $\mathbf{R}$ *is* 1*-affine complete.*

Proof. We observe that any finite expanded group $\mathbf{V}$ satisfies (SC1) and (AB2) if every subdirectly irreducible quotient of $\mathbf{V}$ satisfies (SC1) and (AB2). For (SC1), this follows from the definition. Suppose that (AB2) fails in $\mathbf{V}$ and that A and B produce this failure, which means $A \prec B$, $[B, B] \leqslant A$, and that B contains more than two cosets of A. As in the proof of Proposition 4.7, we project $I[A, B]$ up to an interval $I[M, M^+]$ with meet irreducible M. (AB2) then fails in the subdirectly irreducible quotient $\mathbf{V}/M$. So we see that by Proposition 11.3, (1) is equivalent to the fact that $\mathbf{R}$ satisfies (SC1) and (AB2). Now the result follows from Theorem 1.3. □

12. 1-affine complete expanded groups with (SC1)

In the previous sections, we have given a complete description of those finite expanded groups in which every unary partial compatible function is a polynomial. We are now going to examine those expanded groups in which every unary *total* compatible function is a polynomial. Such algebras are called 1-affine complete. For finite groups, 1-affine complete groups have been characterized for the class of abelian groups [28] and Hamiltonian groups [34]. Furthermore, all finite strictly 1-affine complete groups are obviously also 1-affine complete, and, as the group $\mathbb{Z}_3 \times \mathbb{Z}_3$ shows, the converse is not true. This example already shows that in contrast to the situation for strictly 1-affine complete groups, 1-affine completeness is not preserved under the formation of homomorphic images.

In this section we characterize the 1-affine complete expanded groups among the expanded groups with (SC1) by a condition on the ideals of $\mathbf{V}$. To this end, we look at

the meet irreducible ideals of $\mathbf{V}$, and we collect those in the set $M(\mathsf{Id}\,\mathbf{V})$. We define an equivalence relation $\approx$ on $M(\mathsf{Id}\,\mathbf{V})$ by $M \approx N :\Leftrightarrow I[M, M^+] \nsim I[N, N^+]$. In this case, we say that M and N are *projective* meet irreducible ideals of $\mathbf{V}$. We need the following condition (AM):

Definition 12.1. A finite expanded group $\mathbf{V}$ satisfies the condition (AM) if for all meet irreducible ideals M in $\mathsf{Id}\,\mathbf{V}$ at least one of the following conditions holds:

(1) The interval $I[M, M^+]$ is not abelian.
(2) M^+ contains precisely two cosets of M.
(3) There is a meet irreducible ideal $N \in M(\mathsf{Id}\,\mathbf{V})$ with $N \neq M$ and $N \approx M$.

We observe that if every meet irreducible ideal fulfills one of the first two conditions then $\mathbf{V}$ satisfies the condition (AB2). The condition (AM) is weaker than (AB2) because it also allows that for an abelian interval $I[M, M^+]$ (M meet irreducible) the ideal M^+ contains more than two cosets modulo M as long as there is another meet irreducible ideal projective to M.

Theorem 12.2. *A finite expanded group with* (SC1) *is* 1*-affine complete if and only if it satisfies* (AM).

In the remainder of this section, we prove Theorem 12.2. To this end, we relate the third condition of Definition 12.1 to the join irreducible ideals of $\mathbf{V}$. We recall that $J(\mathsf{Id}\,\mathbf{V})$ is the set of all strictly join irreducible elements of $\mathsf{Id}\,\mathbf{V}$ and for $A, B \in J(\mathsf{Id}\,\mathbf{V})$ we have $A \sim B$ if $I[A^-, A] \nsim I[B^-, B]$.

Proposition 12.3. *Let* $\mathbf{V}$ *be a finite expanded group with* (SC1)*, let* A *be a join irreducible ideal of* $\mathbf{V}$*, and let* M *be a meet irreducible ideal of* $\mathbf{V}$ *such that the intervals* $I[A^-, A]$ *and* $I[M, M^+]$ *are projective. Then the following are equivalent*:

(1) *There is a meet irreducible ideal* $N \in M(\mathsf{Id}\,\mathbf{V})$ *with* $N \neq M$ *and* $N \approx M$.
(2) *There is a join irreducible ideal* $B \in J(\mathsf{Id}\,\mathbf{V})$ *with* $B \neq A$ *and* $B \sim A$.

Proof. (2) $\Rightarrow$ (1). Let A and B be given as in condition (2). By Proposition 9.2, A and B are incomparable. In particular, $A \not\geqslant B$, so that we can pick a maximal ideal E with $E \geqslant A$ and $E \not\geqslant B$. We will now show

$$E \geqslant B^-. \tag{12.1}$$

Suppose $E \not\geqslant B^-$. Then we have $E \vee B^- > E$. Since E was chosen to be maximal with $E \geqslant A$, $E \not\geqslant B$, we must have

$$E \vee B^- \geqslant B. \tag{12.2}$$

Since $E \not\geqslant B$, we have $E \wedge B < B$. But B is join irreducible, and therefore we have

$$E \wedge B \leqslant B^-. \tag{12.3}$$

From (12.2), we obtain $B = B \wedge (E \vee B^-)$. By modularity of $\mathsf{Id}\,\mathbf{V}$, this is equal to $(B \wedge E) \vee B^-$. But by (12.3), this is equal to B^-, and hence we have $B = B^-$, which is a contradiction. This completes the proof of (12.1). By its choice, E is a meet irreducible ideal of $\mathbf{V}$. We have

$$E \approx M. \tag{12.4}$$

To prove this, we observe that the interval $I[B^-, B]$ projects up to $I[E, E \vee B]$. So by modularity, $E \vee B$ is a cover of E, and therefore $E \vee B$ is equal to E^+. This yields $I[E, E^+] \searrow I[B^-, B] \leftrightsquigarrow I[A^-, A] \leftrightsquigarrow I[M, M^+]$, which proves (12.4).

Now we choose F in $\mathsf{Id}\,\mathbf{V}$ such that F is maximal with the property $F \geqslant A^-$, $F \not\geqslant A$. We obtain that F is meet irreducible and $I[F, F^+] \searrow I[A^-, A]$. Hence we have $F \approx M$.

Since $E \geqslant A$ and $F \not\geqslant A$, we have $E \neq F$. Hence the class $M/\!\approx$ contains at least two elements: E and F.

(1) $\Rightarrow$ (2). Let M and N be given as in condition (1). If $(M : M^+) = M$, then Proposition 2.2 yields $M = (M : M^+) = (N : N^+) = N$. Therefore, we have $(M : M^+) = M^+$, and, again by Proposition 2.2, $M^+ = N^+$. Hence M and N are incomparable. Now switching joins and meets we may repeat the proof of (2) $\Rightarrow$ (1) to obtain that the class $A/\!\sim$ contains at least two elements. □

We will now see that the condition (AM) is preserved under forming certain homomorphic images. To this end, we first need the following lattice theoretic result.

Proposition 12.4. *Let* $\mathbf{L}$ *be a finite modular lattice, let* μ *be a homogeneous element of* $\mathbf{L}$*, and let* α, β *be two meet irreducible elements of* $\mathbf{L}$ *with* $I[\alpha, \alpha^+] \leftrightsquigarrow I[\beta, \beta^+]$*. We assume* $\alpha \geqslant \mu$*. Then we have*:

(1) $\beta \geqslant \mu$.
(2) *The intervals* $I[\alpha, \alpha^+]$ *and* $I[\beta, \beta^+]$ *are projective in the sublattice* $\mathbf{L}_\mu$ *of* $\mathbf{L}$ *with universe* $L_\mu := I[\mu, 1]$.

Proof. For proving (1), we suppose $\beta \not\geqslant \mu$. We choose γ minimal in $\mathbf{L}$ with $\gamma \leqslant \mu$, $\gamma \not\leqslant \beta$, and obtain $I[\gamma^-, \gamma] \nearrow I[\beta, \beta^+]$. We choose δ minimal in $\mathbf{L}$ such that $\delta \leqslant \alpha^+$, $\delta \not\leqslant \alpha$, and obtain $I[\delta^-, \delta] \nearrow I[\alpha, \alpha^+]$. Since $\delta \not\leqslant \alpha$, we have $\delta \not\leqslant \mu$. Altogether, we have $I[\gamma^-, \gamma] \leftrightsquigarrow I[\delta^-, \delta]$, $\gamma \leqslant \mu$ and $\delta \not\leqslant \mu$, which contradicts the assumption that μ is homogeneous.

Now we prove (2). Since $I[\alpha, \alpha^+] \leftrightsquigarrow I[\beta, \beta^+]$, there is a natural number n, and there are $\gamma_1, \gamma_2, \ldots, \gamma_{2n-1}, \delta_1, \delta_2, \ldots, \delta_{2n-1} \in L$ such that

$$\begin{aligned} I\big[\alpha, \alpha^+\big] &\searrow I[\gamma_1, \delta_1] \nearrow I[\gamma_2, \delta_2] \searrow \\ &\cdots \nearrow I[\gamma_{2n-2}, \delta_{2n-2}] \searrow I[\gamma_{2n-1}, \delta_{2n-1}] \nearrow I\big[\beta, \beta^+\big]. \end{aligned} \tag{12.5}$$

We notice that for $\rho_1, \rho_2, \ldots, \rho_6$ in a modular lattice with $\rho_1 \prec \rho_2$, the conditions $I[\rho_1, \rho_2] \nearrow I[\rho_3, \rho_4]$ and $I[\rho_3, \rho_4] \nearrow I[\rho_5, \rho_6]$ imply $I[\rho_1, \rho_2] \nearrow I[\rho_5, \rho_6]$. Now for each γ_{2k}, δ_{2k} in (12.5) we pick an element $\eta_{2k} \in L$ which is maximal with $\eta_{2k} \geqslant \gamma_{2k}$, $\eta_{2k} \not\geqslant \delta_{2k}$. Then η_{2k} is a meet irreducible element of $\mathbf{L}$ and we have

$$I\big[\alpha, \alpha^+\big] \searrow I[\gamma_1, \delta_1] \nearrow I\big[\eta_2, \eta_2^+\big] \searrow \cdots \nearrow I\big[\eta_{2n-2}, \eta_{2n-2}^+\big] \searrow I[\gamma_{2n-1}, \delta_{2n-1}] \nearrow I\big[\beta, \beta^+\big].$$

By property (1) shown above we know that for each η_{2k} we have $\eta_{2k} \geqslant \mu$. Now we show that we even have

$$I\big[\alpha, \alpha^+\big] \searrow I[\gamma_1 \vee \mu, \delta_1 \vee \mu] \nearrow I\big[\eta_2, \eta_2^+\big] \searrow \cdots \nearrow I\big[\eta_{2n-2}, \eta_{2n-2}^+\big] \searrow I[\gamma_{2n-1} \vee \mu, \delta_{2n-1} \vee \mu] \nearrow I\big[\beta, \beta^+\big]. \tag{12.6}$$

To this end, let γ, δ be any elements of $\mathbf{L}$, and let η be a meet irreducible element of $\mathbf{L}$ with $\eta \geqslant \mu$. We assume $I[\gamma, \delta] \nearrow I[\eta, \eta^+]$. Then we also have

$$I[\gamma \vee \mu, \delta \vee \mu] \nearrow I\big[\eta, \eta^+\big]. \tag{12.7}$$

To prove (12.7), we compute $(\delta \vee \mu) \vee \eta = \mu \vee (\delta \vee \eta) = \mu \vee \eta^+ = \eta^+$ and $(\delta \vee \mu) \wedge \eta$, which by modularity of $\mathbf{L}$ is equal to $\mu \vee (\delta \wedge \eta) = \mu \vee \gamma$. So we have shown all relations stated in (12.6), and thus $I[\alpha, \alpha^+]$ and $I[\beta, \beta^+]$ are projective even inside the interval $I[\mu, 1]$. □

Proposition 12.5. *Let* $\mathbf{V}$ *be a finite expanded group that satisfies* (AM)*, and let* U *be a homogeneous ideal of* $\mathbf{V}$*. Then* $\mathbf{V}/U$ *satisfies* (AM) *as well.*

Proof. To prove that $\mathbf{V}/U$ satisfies (AM), we fix a meet irreducible ideal E of $\mathbf{V}$ with $E \geqslant U$ and the properties that the interval $I[E, E^+]$ is abelian and E^+ contains more than two cosets of E. We show that then there is a meet irreducible ideal F in $\mathsf{Id}\, V$ such that $F \neq E$ and $I[F, F^+]$ is projective to $I[E, E^+]$ inside the interval $I[U, V]$ of $\mathsf{Id}\, \mathbf{V}$. Since $\mathbf{V}$ satisfies (AM), we have a meet irreducible ideal G of $\mathbf{V}$ such that $G \neq E$ and $I[G, G^+]$ is projective to $I[E, E^+]$ in $\mathsf{Id}\, \mathbf{V}$. By Proposition 12.4, we obtain that $G \geqslant U$, and also that $I[G, G^+]$ is projective to $I[E, E^+]$ even in $I[U, V]$. □

12.1. (AM) *is necessary for* 1*-affine completeness*

We are now going to show that every 1-affine complete expanded group with (SC1) satisfies (AM).

First of all, we need the concept of lifting a function from a quotient to the whole algebra.

Definition 12.6. Let β be a congruence of the algebra $\mathbf{A}$, and let f be a function from A/β to A/β. A function $g : A \to A$ is called a *lifting* of f iff we have $g(x)/\beta = f(x/\beta)$ for all $x \in A$.

Proposition 12.7. *Let* $\mathbf{A}$ *be an algebra, let* f *be a compatible function on* A/β*, and let* g *be a lifting of* f*. Then for every* $x, y \in A$*, the function* g *satisfies*

$$g(x) \equiv g(y) \quad \big(\mathrm{mod}\ \Theta_{\mathbf{A}}(x, y) \vee \beta\big).$$

Proof. Since f is compatible, we know $(f(x/\beta), f(y/\beta)) \in \Theta_{\mathbf{A}/\beta}(x/\beta, y/\beta)$. Since $g(x)/\beta = f(x/\beta)$, this is equivalent to

$$\big(g(x)/\beta, g(y)/\beta\big) \in \Theta_{\mathbf{A}/\beta}(x/\beta, y/\beta).$$

By [26, Theorem 4.15], we have

$$\Theta_{\mathbf{A}/\beta}(x/\beta, y/\beta) = \big\{(z/\beta, u/\beta) \mid (z, u) \in \beta \vee \Theta_{\mathbf{A}}(x, y)\big\}.$$

Hence there are z' and u' in A such that $(g(x), z') \in \beta$, $(z', u') \in \beta \vee \Theta_{\mathbf{A}}(x, y)$ and $(u', g(y)) \in \beta$. □

The next propositions aim at finding a lifting of a compatible function that is again compatible. The following lemma gives a test whether a lifting is compatible.

Proposition 12.8. *Let* $\mathbf{V}$ *be a finite expanded group, let* U *be a homogeneous ideal of* $\mathbf{V}$*, and* f *be a unary compatible function on* $\mathbf{V}/U$*. Then a lifting* g *of* f *is compatible iff*

$$g(x) \equiv g(y) \quad \big(\mathrm{mod}\ \mathcal{I}_{\mathbf{V}}(x - y)\big)$$

for all $x, y \in V$ *with* $x - y \in (\Phi(U) : U)$*.*

Proof. The "only if"-part is immediate. For the "if"-part we assume that g is a lifting of f which is compatible on each coset of $(\Phi(U) : U)$. We have to show the compatibility condition

$$g(x) \equiv g(y) \quad \big(\mathrm{mod}\ \mathcal{I}_{\mathbf{V}}(x - y)\big) \quad \text{for all } x, y \in V. \tag{12.8}$$

If $x - y \in (\Phi(U) : U)$, then (12.8) holds by the assumption on g. If $x - y \notin (\Phi(U) : U)$, then we have $\mathcal{I}_{\mathbf{V}}(x - y) \not\leqslant (\Phi(U) : U)$. Now Proposition 7.11 gives $\mathcal{I}_{\mathbf{V}}(x - y) \geqslant U$. By Proposition 12.7, we know that $g(x)$ is congruent to $g(y)$ modulo $\mathcal{I}_{\mathbf{V}}(x - y) \vee U$. But this ideal is just $\mathcal{I}_{\mathbf{V}}(x - y)$, which proves (12.8). □

Proposition 12.9. *Let* $\mathbf{V}$ *be a finite expanded group, and let* U *be a homogeneous ideal of* $\mathbf{V}$ *with* $(\Phi(U) : U) \leqslant U \vee U^*$*. Then for every unary compatible function* f *on* $\mathbf{V}/U$ *there is a lifting* g *which is a compatible function on* $\mathbf{V}$*.*

Proof. We define T to be a transversal through the cosets of $(\Phi(U) : U) \vee U$, i.e., we let T be such that $|T \cap (v + (\Phi(U) : U) \vee U)| = 1$ for each $v \in V$. By the assumptions, we

have $(\Phi(U):U)\vee U\leqslant U^*\vee U$, and thus we can find functions s_T, s_U and s_{U^*} on V such that for all v in V we have

$$v=s_T(v)+s_U(v)+s_{U^*}(v),$$

and furthermore $s_T(v)\in T$, $s_U(v)\in U$, and $s_{U^*}(v)\in U^*$. Let L_f be any lifting of f. The function L_f might not be compatible, but the function g we produce out of it will be. We define $g:V\to V$ by

$$g(v):=s_T\big(L_f(v)\big)+s_{U^*}\big(L_f(v)\big).$$

Since $g(v)$ differs from $L_f(v)$ only by $s_U(L_f(v))$, the function g is also a lifting of f. We prove that it is compatible. To this end, let x, y be in V. By Proposition 12.8, we may assume that x and y are congruent modulo $(\Phi(U):U)$. Proposition 12.7 tells that $L_f(x)$ is congruent to $L_f(y)$ modulo $\mathcal{I}_{\mathbf{V}}(x-y)\vee U$. Since both ideals stay below $(\Phi(U):U)\vee U$, we have $L_f(x)\equiv L_f(y)\pmod{(\Phi(U):U)\vee U}$, which implies

$$s_T\big(L_f(x)\big)=s_T\big(L_f(y)\big).$$

Since g is a lifting of f, by Proposition 12.7, $g(x)-g(y)$ lies in $\mathcal{I}_{\mathbf{V}}(x-y)\vee U$. We will now see that $g(x)-g(y)$ lies in U^* as well. We have

$$\begin{aligned}g(x)&=s_T\big(L_f(x)\big)+s_{U^*}\big(L_f(x)\big)=s_T\big(L_f(y)\big)+s_{U^*}\big(L_f(x)\big)\\&\overset{U^*}{\equiv}s_T\big(L_f(y)\big)+s_{U^*}\big(L_f(y)\big)=g(y).\end{aligned}$$

Altogether, we get

$$g(x)\equiv g(y)\quad\big(\mathrm{mod}\,\big(\mathcal{I}_{\mathbf{V}}(x-y)\vee U\big)\wedge U^*\big).$$

By Proposition 7.4, we have $(\mathcal{I}_{\mathbf{V}}(x-y)\vee U)\wedge U^*=(\mathcal{I}_{\mathbf{V}}(x-y)\wedge U^*)\vee(U\wedge U^*)=\mathcal{I}_{\mathbf{V}}(x-y)\wedge U^*\leqslant\mathcal{I}_{\mathbf{V}}(x-y)$. This proves (12.8). Hence g is the required compatible lifting of f. □

Corollary 12.10. *Let* $\mathbf{V}$ *be a finite* 1*-affine complete expanded group, and let* U *be homogeneous ideal of* $\mathbf{V}$ *with* $(\Phi(U):U)\leqslant U\vee U^*$. *Then* $\mathbf{V}/U$ *is also* 1*-affine complete.*

Proof. Let c be a unary compatible function on $\mathbf{V}/U$. Then we use Proposition 12.9 to produce a compatible lifting of c. Since $\mathbf{V}$ is 1-affine complete, this lifting, say $\mathbf{p}$, is in $\mathsf{Pol}_1\mathbf{V}$. Now the function

$$\begin{aligned}\mathbf{q}:V/U&\to V/U,\\x+U&\mapsto\mathbf{p}(x)+U\end{aligned}$$

is a polynomial of $\mathbf{V}/U$ and equal to c. □

We are now ready to prove that every finite 1-affine complete expanded group with (SC1) satisfies (AM).

Proof (*"only if"-part of Theorem* 12.2). Let $\mathbf{V}$ be a minimal failure, that is, let $\mathbf{V}$ be a minimal (with respect to cardinality) 1-affine complete expanded group with (SC1) in which (AM) fails. Proposition 9.7 supplies us a nonzero homogeneous ideal U of $\mathbf{V}$. By Proposition 9.8 and Corollary 12.10, $\mathbf{V}/U$ is 1-affine complete. By the minimality of $\mathbf{V}$, $\mathbf{V}/U$ therefore satisfies (AM). Since (AM) fails in $\mathbf{V}$, there must be a meet irreducible ideal of $\mathbf{V}$ such that $I[M, M^+]$ is abelian, M^+ contains at least three cosets modulo M and M is alone in its $\approx$-class. We have $M \not\geqslant U$, because if $M \geqslant U$, then M causes a failure of (AM) in $\mathbf{V}/U$. Now let B be minimal in $\mathsf{Id}\,\mathbf{V}$ with $B \leqslant U$, $B \not\leqslant M$. Obviously B is join irreducible and $I[B^-, B]$ projects up to $I[M, M^+]$. By the implication (2) $\Rightarrow$ (1) of Proposition 12.3, B is alone in its $\sim$-class. Hence Proposition 7.2 implies $B = U$, and so U is a minimal ideal of $\mathbf{V}$, and we have $[U, U] = 0$, and $|U| \geqslant 3$.

We choose an element $a \in U$ with $a \neq 0$ and define a function $f : U \to U$ by $f(x) = 0$ for $x \in U \setminus \{a\}$ and $f(a) = a$. Proposition 9.8 yields $(0 : U) = U \vee U^*$, and thus Proposition 7.15 supplies an idempotent polynomial function $\mathbf{e} \in \mathsf{Pol}_1\,\mathbf{V}$ with range U. We form the function g as

$$\begin{aligned} g : V &\to V, \\ v &\mapsto f\big(\mathbf{e}(v)\big). \end{aligned}$$

The function g is compatible: To show this, let x, y be in V. If $\mathcal{I}_{\mathbf{V}}(x - y) \geqslant U$, then $g(x) - g(y)$ lies in $\mathcal{I}_{\mathbf{V}}(x - y)$ because the range of g is contained in U. If $\mathcal{I}_{\mathbf{V}}(x - y) \not\geqslant U$, then by the fact that U is a minimal ideal we have $U \wedge \mathcal{I}_{\mathbf{V}}(x - y) = 0$. Since $\mathbf{e}(x) - \mathbf{e}(y)$ lies in both U and $\mathcal{I}_{\mathbf{V}}(x - y)$, we have $\mathbf{e}(x) = \mathbf{e}(y)$. This implies $g(x) = g(y)$. Now we show that g cannot be a polynomial. Suppose it were. Then take $b \in U$ such that $b \neq 0, b \neq a$; by the fact that U contains at least three elements, such a b exists. If g is a polynomial, then Proposition 2.3 gives

$$g(a - b) + g(b) \equiv g(a) \quad \big(\mathrm{mod}\,[U, U]\big).$$

But $g(a - b) = g(b) = 0$, and $g(a) = f(a) = a$. This implies $a \in [U, U]$, and hence $a = 0$, a contradiction to the choice of a. Altogether, g is a compatible function which cannot be a polynomial; therefore $\mathbf{V}$ is not 1-affine complete, contradicting the assumptions. This finishes the proof of the "only if"-part of Theorem 12.2. □

12.2. (AM) *is sufficient for* 1*-affine completeness*

We are now going to show that every finite expanded group with (SC1) and (AM) is 1-affine complete.

Proof (*"if"-part of Theorem* 12.2). We induct on the cardinality of $\mathbf{V}$. The result is obvious if $|V| = 1$. For $|V| \geqslant 1$, Proposition 9.7 supplies us a homogeneous ideal U of $\mathbf{V}$. Since

$\mathbf{V}/U$ is 1-affine complete by induction hypothesis, it is sufficient to show that every compatible function $c: V \to U$ is a polynomial.

If $[U,U] = U$, then by Proposition 9.8, U is a minimal ideal of $\mathbf{V}$, and therefore Proposition 7.17 yields the interpolating polynomial.

If $[U,U] < U$, then by Proposition 9.8 we have $[U,U] = 0$. By Proposition 7.16, we only need to show that $c|_K$ is a polynomial for every single coset K modulo $(0:U)$. We choose a coset $K = v + (0:U)$ and define a compatible function $c_1(x) := c(v+x) - c(v)$. In order to interpolate c at K, we interpolate c_1 on $(0:U)$. By the fact that $(0:U) = U \vee U^*$ and $U \wedge U^* = 0$, a polynomial $\mathbf{p} \in \mathsf{Pol}_1 \mathbf{V}$ with $\mathbf{p}((0:U)) \subseteq U$ and $\mathbf{p}|_U = c_1|_U$ agrees with c_1 on $(0:U)$. As in Proposition 8.1, we form the ring $\mathbf{R}$ of all zero-preserving polynomials on U, that is, we let $\mathbf{R}$ be the ring with universe $R := \{\mathbf{p}|_U \mid \mathbf{p} \in P_0(\mathbf{V})\}$. By Proposition 8.1, we know that $\mathbf{R}$ is the full matrix ring over a field, and that the $\mathbf{R}$-module U is isomorphic to the direct product of m copies of the primitive $\mathbf{R}$-module A, where A is a minimal ideal of $\mathbf{V}$ with $A \leqslant U$. Since every sub-$\mathbf{R}$-module of U is an ideal of $\mathbf{V}$, the function $c_1|_U$ is also a compatible function on the $\mathbf{R}$-module U. If $m = 1$, then $A = U$, and so A is alone in its $\sim$-class. Let E be an ideal of $\mathbf{V}$ that is maximal with $E \geqslant A^-$, $E \not\geqslant A$. Then the implication (1) $\Rightarrow$ (2) of Proposition 12.3 yields that E is not projective to any other meet irreducible ideal. By condition (AM), we know that E^+ contains precisely two cosets of E, and thus by Proposition 2.2(3), U has precisely two elements. Thus for both cases $m = 1$ and $m > 1$, Proposition 8.3 yields that the $\mathbf{R}$-module U is 1-affine complete. Hence the function $c_1|_U$ lies in R. Therefore we have a polynomial function $\mathbf{q}$ with $\mathbf{q}|_U = c_1|_U$. The function $\mathbf{p} := \mathbf{e}_U \circ \mathbf{q}$, where $\mathbf{e}_U$ is the idempotent polynomial with range U constructed in Proposition 7.15, satisfies $\mathbf{p}|_U = c_1|_U$ and $\mathbf{p}(V) \subseteq U$. Hence $c|_K$ is a polynomial, which finishes the proof of the "if"-part of Theorem 12.2. □

Using Theorem 12.2, we find the following examples of 1-affine complete algebras:

(1) Let p be an odd prime, let $n \geqslant 2$, and let $\mathbf{B}$ be the elementary abelian group with p^n elements. Then the generalized dihedral group determined by $\mathbf{B}$ (see [38, p. 10]) is 1-affine complete (cf. [6]).
(2) Let $\mathbf{F}$ be a finite field, let $n \geqslant 2$, and let $\mathbf{R}$ be the (commutative) polynomial ring $\mathbf{F}[x_1, x_2, \ldots, x_n]$. We take I to be the ideal generated by all quadratic monomials, i.e., by $\{x_i x_j \mid i, j \in \{1,2,\ldots,n\}, i \neq j\} \cup \{x_i^2 \mid i \in \{1,2,\ldots,n\}\}$. Then the ring $\mathbf{R}/I$ is 1-affine complete.

References

[1] E. Aichinger, On maximal ideals of tame near-rings, Riv. Mat. Univ. Parma (6) 2* (1999) 215–233.
[2] E. Aichinger, On Hagemann's and Herrmann's characterization of strictly affine complete algebras, Algebra Universalis 44 (2000) 105–121.
[3] E. Aichinger, On near-ring idempotents and polynomials on direct products of Ω-groups, Proc. Edinburgh Math. Soc. (2) 44 (2001) 379–388.
[4] S. Berman, R.J. Silverman, Simplicity of near-rings of transformations, Proc. Amer. Math. Soc. 10 (1959) 456–459.
[5] G. Betsch, Some structure theorems on 2-primitive near-rings, Colloq. Math. Soc. János Bolyai 6 (1973) 73–102.
[6] J. Ecker, Functions on groups. Compatibility vs. polynomiality, PhD thesis, Johannes Kepler University, Linz, 2001. Available at www.algebra.uni-linz.ac.at/~juergen.

[7] Y. Fong, K. Kaarli, Unary polynomials on a class of groups, Acta Sci. Math. (Szeged) 61 (1–4) (1995) 139–154.
[8] R. Freese, R.N. McKenzie, Commutator Theory for Congruence Modular Varieties, in: London Math. Soc. Lecture Note Ser., Vol. 125, Cambridge University Press, Cambridge, 1987.
[9] G. Grätzer, General Lattice Theory, Birkhäuser Verlag, Basel–Stuttgart, 1978.
[10] G. Grätzer, Universal Algebra, 2nd Edition, Springer-Verlag, Berlin, 1979.
[11] H.P. Gumm, Geometrical Methods in Congruence Modular Algebras, in: Mem. Amer. Math. Soc., Vol. 45, American Mathematical Society, Providence, RI, 1983.
[12] H.P. Gumm, A. Ursini, Ideals in universal algebras, Algebra Universalis 19 (1984) 45–54.
[13] J. Hagemann, C. Herrmann, Arithmetical locally equational classes and representation of partial functions, in: Universal Algebra, Esztergom (Hungary), in: Colloq. Math. Soc. János Bolyai, Vol. 29, 1982, pp. 345–360.
[14] P.J. Higgins, Groups with multiple operators, Proc. London Math. Soc. (3) 6 (1956) 366–416.
[15] D. Hobby, R. McKenzie, The Structure of Finite Algebras, in: Contemp. Math., Vol. 76, American Mathematical Society, Providence, RI, 1988.
[16] P.M. Idziak, K. Słomczyńska, Polynomially rich algebras, J. Pure Appl. Algebra 156 (1) (2001) 33–68.
[17] N. Jacobson, Structure of Rings, 2nd Edition, in: Amer. Math. Soc. Colloq. Publ., Vol. 37, American Mathematical Society, Providence, RI, 1964.
[18] K. Kaarli, On Near-Rings Generated by the Endomorphisms of Some Groups, in: Tartu Riikl. Ül. Toimetised, Vol. 464, University of Tartu, Estonia, 1978.
[19] K. Kaarli, Affine complete abelian groups, Math. Nachr. 107 (1982) 235–239.
[20] K. Kaarli, Compatible function extension property, Algebra Universalis 17 (1983) 200–207.
[21] K. Kaarli, R.N. McKenzie, Affine complete varieties are congruence distributive, Algebra Universalis 38 (3) (1997) 329–354.
[22] K. Kaarli, A.F. Pixley, Affine complete varieties, Algebra Universalis 24 (1987) 74–90.
[23] H.K. Kaiser, Über kompatible Funktionen in universalen Algebren, Acta Math. Acad. Sci. Hungar. 30 (1–2) (1977) 105–111.
[24] A.G. Kurosh, Lectures on General Algebra, Chelsea, New York, 1965.
[25] H. Lausch, W. Nöbauer, Algebra of Polynomials, North-Holland, Amsterdam, London, American Elsevier Publishing Company, New York, 1973.
[26] R.N. McKenzie, G.F. McNulty, W.F. Taylor, Algebras, Lattices, Varieties, Vol. I, Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, CA, 1987.
[27] J.D.P. Meldrum, Near-Rings and Their Links With Groups, Pitman (Advanced Publishing Program), Boston, MA, 1985.
[28] W. Nöbauer, Über die affin vollständigen, endlich erzeugbaren Moduln, Monatsh. Math. 82 (1976) 187–198.
[29] G.F. Pilz, Near-Rings, 2nd Edition, North-Holland Publishing Company, Amsterdam, New York, Oxford, 1983.
[30] G.F. Pilz, Y.S. So, Near-rings of polynomials and polynomial functions, J. Austr. Math. Soc. Ser. A 29 (1) (1980) 61–70.
[31] A.F. Pixley, Functional and affine completeness and arithmetical varieties, in: Proceedings of the NATO Advanced Study Institute and Seminaire de Mathematiques Superieures, Montreal, Canada, 1991, in: NATO ASI Ser. C Math. Phys. Sci., Vol. 389, Kluwer Acad. Publ., 1993, pp. 317–357.
[32] L.H. Rowen, Ring Theory, Vol. I, Academic Press, Inc., San Diego, CA, 1988.
[33] A. Saks, Affine Completeness of Modules, in: Tartu Riikl. Ül. Toimetised, Vol. 700, University of Tartu, Estonia, 1985.
[34] M. Saks, Polünomiaalsed funktsioonid rühmadel (Polynomial functions on groups), Diploma work, University of Tartu, Estonia, 1983.
[35] S.D. Scott, Tame near-rings and N-groups, Proc. Edinburgh Math. Soc. (2) 23 (3) (1980) 275–296.
[36] S.D. Scott, The structure of Ω-groups, in: Nearrings, Nearfields and K-Loops (Hamburg, 1995), Kluwer Acad. Publ., Dordrecht, 1997, pp. 47–137.
[37] J.D.H. Smith, Mal'cev Varieties, in: Lecture Notes in Math., Vol. 554, Springer Verlag, Berlin, 1976.
[38] M. Weinstein, Examples of Groups, Polygonal Publishing House, Passaic, NJ, 1977.
[39] H. Werner, Produkte von Kongruenzklassengeometrien universeller Algebren, Math. Z. 121 (1971) 111–140.