Algebra Universalis, 17 (1983) 150–169 0002-5240/83/020150-20$01.50+0.20/0

Expanding varieties by monoids of endomorphisms

Stanley Burris* and Matthew Valeriote†

The purpose of this paper is to start a general investigation of the varieties $\mathcal{V}(\mathbf{M})$ obtained by expanding a variety $\mathcal{V}$ by a monoid of endomorphisms $\mathbf{M}$. This construction was used in [3] to manufacture the first example of a variety with a decidable theory and not of the form (discriminator)⊗(Abelian). It also plays a key role in Baur's papers [1], [2] on the first-order theory of Abelian groups with distinguished subgroups.

In the first section a few basic results are presented. In the second section we describe exactly when $\mathcal{V}(\mathbf{M})$ is a discriminator variety, generalizing the treatment of $\mathcal{BA}(\mathbf{G})$ given in [3]. The final section is devoted to Abelian varieties and the corresponding varieties of modules.

§1. Definitions and basic results

Given a variety $\mathcal{V}$ of type $\mathcal{F}$ and a monoid $\mathbf{M}=\langle M, \cdot, 1\rangle$ the variety $\mathcal{V}(\mathbf{M})$ is of type $\mathcal{F}\cup M$, where each $m\in M$ is a unary function symbol, and $\mathcal{V}(\mathbf{M})$ is axiomatized by

(i) the identities of $\mathcal{V}$

(ii) $1(x)\approx x$

(iii) $m_1(m_2(x))\approx(m_1\cdot m_2)(x)$ for $m_1, m_2\in M$

(iv) $m(f(x_1,\dots,x_k))\approx f(m(x_1),\dots,m(x_k))$ for $m\in M, f\in\mathcal{F}$.

We use the notion of *equivalent varieties* as defined in §7 of Taylor [7]. For $\mathbf{A}\in\mathcal{V}(\mathbf{M})$ let $\mathbf{A}\upharpoonright_{\mathcal{V}}$ be the reduct of $\mathbf{A}$ to the language of $\mathcal{V}$; and for $\mathcal{K}\subseteq\mathcal{V}(\mathbf{M})$ let $\mathcal{K}\upharpoonright_{\mathcal{V}}=\{\mathbf{A}\upharpoonright_{\mathcal{V}}:\mathbf{A}\in\mathcal{K}\}$.

* Research supported by NSERC Grant No. A7256

† Research supported by a Student NSERC Grant for Summer Studies

Presented by B. Jónsson. Received May 14, 1982. Accepted for publication in final form September 3, 1982.

THEOREM 1.1. *$\mathcal{V}$ is equivalent to a subvariety of $\mathcal{V}(\mathbf{M})$, and $\mathcal{V}$ is a reduct of $\mathcal{V}(\mathbf{M})$.*

Proof. Let $\mathcal{V}^*$ be the subvariety of $\mathcal{V}(\mathbf{M})$ defined by $m(x) \approx x$ for $m \in M$. Clearly $\mathcal{V}$ and $\mathcal{V}^*$ are equivalent varieties. Then $\mathcal{V} = \mathcal{V}^* \upharpoonright_{\mathcal{V}} \subseteq \mathcal{V}(\mathbf{M}) \upharpoonright_{\mathcal{V}} \subseteq \mathcal{V}$, so $\mathcal{V} = \mathcal{V}(\mathbf{M}) \upharpoonright_{\mathcal{V}}$. □

COROLLARY 1.2. *$\mathcal{V}$ and $\mathcal{V}(\mathbf{M})$ have the same Mal'cev properties.*

Proof. Certainly any Mal'cev property of $\mathcal{V}$ is also a Mal'cev property of $\mathcal{V}(\mathbf{M})$ (using the same identities); and any Mal'cev property of $\mathcal{V}(\mathbf{M})$ is one of $\mathcal{V}^*$ (as defined in the proof of Theorem 1.1), and hence it is also a Mal'cev property of $\mathcal{V}$. □

One particular construction, which we describe now, transforms an algebra in $\mathcal{V}$ into an algebra in $\mathcal{V}(\mathbf{M})$. For $\mathbf{A} \in \mathcal{V}$ let $\mathbf{A^M}$ be the algebra obtained by expanding $\mathbf{A}^M$ by defining, for $m, n \in M$ and $a \in A^M$,

$$(m(a))(n) = a(n \cdot m).$$

LEMMA 1.3. *For $\mathbf{A} \in \mathcal{V}$, $\mathbf{A^M} \in \mathcal{V}(\mathbf{M})$.*

Proof. Certainly $\mathbf{A}^M \in \mathcal{V}$, and for $a \in A^M$, $n \in M$,

$$\begin{aligned}(1(a))(n) &= a(n \cdot 1)\\ &= a(n)\end{aligned}$$

so

$$1(a) = a.$$

Next if $m_1, m_2, n \in M$ and $a \in A^M$ then

$$\begin{aligned}(m_1(m_2(a)))(n) &= (m_2(a))(n \cdot m_1)\\ &= a(n \cdot m_1 \cdot m_2)\\ &= ((m_1 \cdot m_2)(a))(n),\end{aligned}$$

so

$$m_1(m_2(a)) = (m_1 \cdot m_2)(a).$$

Now if $f \in \mathcal{F}$, $m, n \in M$, and $a_1, \ldots, a_k \in A^M$ then

$$\begin{aligned}(m(f(a_1, \ldots, a_k)))(n) &= (f(a_1, \ldots, a_k))(n \cdot m)\\ &= f(a_1(n \cdot m), \ldots, a_k(n \cdot m))\\ &= f((m(a_1))(n), \ldots, (m(a_k))(n))\\ &= (f(m(a_1), \ldots, m(a_k)))(n),\end{aligned}$$

so

$$m(f(a_1, \ldots, a_k)) = f(m(a_1), \ldots, m(a_k)). \quad \square$$

A term $p(x_1, \ldots, x_k)$ in the language of $\mathcal{V}(\mathbf{M})$ is *reduced* if $p(x_1, \ldots, x_k)$ is $p^*(m_1(x_1), \ldots, m_1(x_k), \ldots, m_l(x_1), \ldots, m_l(x_k))$, for suitable $m_1, \ldots m_l \in M$ and for $p^*(x_{11}, \ldots, x_{1k}, \ldots, x_{l1}, \ldots, x_{lk})$ a term in the language of $\mathcal{V}$.

LEMMA 1.4. *For every term $p(x_1, \ldots, x_k)$ in the language of $\mathcal{V}(\mathbf{M})$ there is a reduced term $p_*(x_1, \ldots, x_k)$ such that*

$$\mathcal{V}(\mathbf{M}) \models p(x_1, \ldots, x_k) \approx p_*(x_1, \ldots, x_k).$$

Proof. After replacing $x_1, \ldots, x_k$ by $1(x_1), \ldots, 1(x_k)$ one just repeatedly uses properties (iii) and (iv) of the definition of $\mathcal{V}(\mathbf{M})$ to push the m's occurring in $p(x_1, \ldots, x_k)$ down to the variables. $\square$

For $X \subseteq A, \mathbf{A} \in \mathcal{V}(\mathbf{M})$, let $M(X) = \{m(x) : m \in M, x \in X\}$; and $Sg_{\mathbf{A}}(X)$ is the *subuniverse* of $\mathbf{A}$ generated by X. Let $T_{\mathcal{V}}$ be the set of *terms* in the language of $\mathcal{V}$.

LEMMA 1.5. *For $\mathbf{A} \in \mathcal{V}(\mathbf{M})$ and $X \subseteq A$,*

$$Sg_{\mathbf{A}}(X) = Sg_{\mathbf{A}\restriction_{\mathcal{V}}}(M(X)).$$

Proof. We have

$$\begin{aligned}Sg_{\mathbf{A}}(X) &= \{p(a_1, \ldots, a_k) : p \in T_{\mathcal{V}(\mathbf{M})}, a_1, \ldots, a_k \in X\}\\ &= \{p^*(m_1(a_1), \ldots, m_l(a_k)) : p^* \in T_{\mathcal{V}},\\ &\quad m_1, \ldots, m_l \in M, a_1, \ldots, a_k \in X\}\\ &= Sg_{\mathbf{A}\restriction_{\mathcal{V}}}(M(x)). \quad \square\end{aligned}$$

If a variety $\mathcal{V}$ is trivial then of course so is $\mathcal{V}(\mathbf{M})$. This gives a degenerate case in many of the following results.

THEOREM 1.6. *If $\mathcal{V}$ is a nontrivial variety then $\mathcal{V}(\mathbf{M})$ is locally finite iff $\mathcal{V}$ is locally finite and $\mathbf{M}$ is finite.*

Proof. Suppose $\mathcal{V}(\mathbf{M})$ is locally finite. As $\mathcal{V}$ is a reduct of $\mathcal{V}(\mathbf{M})$ it follows that $\mathcal{V}$ is locally finite. Let $\mathbf{A}\in\mathcal{V}$ be an algebra with $|A|\geq|M|$, and choose a one-to-one function $a\in A^M$. Then for $m_1, m_2\in M$, we have the following holding in $\mathbf{A}^{\mathbf{M}}$:

$$\begin{aligned} m_1(a)=m_2(a) &\Rightarrow (m_1(a))(1)=(m_2(a))(1)\\ &\Rightarrow a(m_1)=a(m_2)\\ &\Rightarrow m_1=m_2. \end{aligned}$$

This says that $|Sg_{\mathbf{A}^{\mathbf{M}}}(\{a\})|\geq|M|$. As $\mathcal{V}(\mathbf{M})$, and hence $\mathbf{A}^{\mathbf{M}}$, is locally finite, $\mathbf{M}$ must be a finite monoid.

For the converse suppose $\mathcal{V}$ is locally finite and $\mathbf{M}$ is finite. Then for $\mathbf{A}\in\mathcal{V}(\mathbf{M})$ and X a finite subset of A, the set $M(X)$ is finite, so by Lemma 1.5 $Sg_{\mathbf{A}}(X)$ is finite. Thus $\mathcal{V}(\mathbf{M})$ is locally finite. □

LEMMA 1.7. *Suppose $\mathcal{V}$ is a nontrivial variety and $\mathbf{M}$ is a monoid. If $m_1, m_2\in M$ then*

$$\mathcal{V}(\mathbf{M})\models m_1(x)\approx m_2(x) \quad \text{iff} \quad m_1=m_2.$$

Proof. (The proof of this is contained in the first paragraph of the proof of Theorem 1.6.) □

A variety generated by finitely many finite algebras, or equivalently by a single finite algebra, is *finitely generated.*

THEOREM 1.8. *Suppose $\mathcal{V}$ is a nontrivial variety. If $\mathcal{V}(M)$ is finitely generated then $\mathbf{M}$ is finite and $\mathcal{V}$ is finitely generated.*

Proof. Let $\mathbf{A}$ be a finite member of $\mathcal{V}(\mathbf{M})$ such that $\mathcal{V}(\mathbf{M})=\mathrm{HSP}(\mathbf{A})$. Then $\mathcal{V}=\mathrm{HSP}(\mathbf{A})\restriction_{\mathcal{V}}\subseteq\mathrm{HSP}(\mathbf{A}\restriction_{\mathcal{V}})\subseteq\mathcal{V}$, so $\mathcal{V}=\mathrm{HSP}(\mathbf{A}\restriction_{\mathcal{V}})$, and hence $\mathcal{V}$ is finitely generated. Next, since the free algebra $\mathbf{F}_{\mathcal{V}(\mathbf{M})}(\bar{x})$ is finite (as $\mathcal{V}(\mathbf{M})$ is locally finite), the set $M(\{\bar{x}\})$ must be finite, and then by Lemma 1.7 $\mathbf{M}$ is a finite monoid. □

When we are working with elements a, b in a direct product $\prod_{i\in I}A_i$ we use the notation

$$[\![a=b]\!]=\{i\in I: a(i)=b(i)\}$$

$$[\![a\neq b]\!]=\{i\in I: a(i)\neq b(i)\}.$$

LEMMA 1.9. *Suppose* $\mathbf{A}\in\mathcal{V}$.

(a) *If* $\mathbf{A}^{\mathbf{M}}$ *is a simple algebra then either* $\mathbf{A}$ *is a trivial algebra or one can conclude that* $\mathbf{M}$ *is a finite group and* $\mathbf{A}$ *is a simple algebra.*

(b) *Suppose* $\mathbf{S}$ *is a simple algebra,* $\mathbf{G}$ *is a finite group. If the variety generated by* $\mathbf{S}$ *is distributive then* $\mathbf{S}^{\mathbf{G}}$ *is a simple algebra.*

Proof. (a) If $\mathbf{A}$ is a trivial algebra then this part is obvious, so suppose $\mathbf{A}$ is nontrivial. Let U_r be the set of elements in M with a right inverse, i.e.,

$$U_r=\{m\in M: m\cdot m^*=1 \quad \text{for some} \quad m^*\in M\},$$

and let the binary relation θ be defined on A^M by

$$\theta=\{\langle a,b\rangle\in A^M\times A^M: [\![a\neq b]\!]\subseteq U_r\}.$$

Then θ is an equivalence relation since, for $a,b,c\in A^M$,

$$[\![a\neq a]\!]\subseteq U_r,$$

$$[\![a\neq b]\!]\subseteq U_r \Rightarrow [\![b\neq a]\!]\subseteq U_r,$$

and

$$[\![a\neq b]\!]\subseteq U_r, [\![b\neq c]\!]\subseteq U_r \Rightarrow [\![a\neq c]\!]\subseteq U_r$$

as

$$[\![a\neq c]\!]\subseteq [\![a\neq b]\!]\cup[\![b\neq c]\!].$$

Next θ is compatible with all fundamental operations f of $\mathbf{A}^M$ since if $\langle a_1,b_1\rangle,\ldots,\langle a_k,b_k\rangle\in\theta$ then

$$[\![f(a_1,\ldots,a_k)\neq f(b_1,\ldots,b_k)]\!]\subseteq[\![a_1\neq b_1]\!]\cup\cdots\cup[\![a_k\neq b_k]\!]\subseteq U_r.$$

Now if $m \in M$ and $\langle a, b\rangle \in \theta$ then for $n \in [\![m(a) \neq m(b)]\!]$ we have

$$(m(a))(n) \neq (m(b))(n),$$

i.e.,

$$a(n \cdot m) \neq b(n \cdot m).$$

This leads to $n \cdot m \in [\![a \neq b]\!] \subseteq U_r$, so $n \in U_r$. Thus $[\![m(a) \neq m(b)]\!] \subseteq U_r$, so $\langle m(a), m(b)\rangle \in \theta$. Thus we have proved θ is a congruence on $\mathbf{A}^{\mathbf{M}}$. Now $\Delta < \theta$ as $\emptyset \neq U_r$, and as $\mathbf{A}^{\mathbf{M}}$ is a simple algebra we must have $\theta = \nabla$; hence $U_r = M$. This guarantees that $\mathbf{M}$ is a group.

Now define a binary relation $\hat{\theta}$ on A^M by

$$\hat{\theta} = \{\langle a, b\rangle \in A^M \times A^M : [\![a \neq b]\!] \text{ is finite}\}.$$

Then $\hat{\theta}$ is a well-known congruence on $\mathbf{A}^M$, and $\Delta < \hat{\theta}$. For $m \in M$ and $\langle a, b\rangle \in \hat{\theta}$,

$$\begin{aligned}[\![m(a) \neq m(b)]\!] &= \{n \in M : (m(a))(n) \neq (m(b))(n)\} \\ &= \{n \in M : a(n \cdot m) \neq b(n \cdot m)\} \\ &= \{n \in M : n \cdot m \in [\![a \neq b]\!]\} \\ &= \alpha_m^{-1}([\![a \neq b]\!]),\end{aligned}$$

where $\alpha_m : M \to M$ is defined by $\alpha_m(n) = n \cdot m$. As α_m is a bijection ($\mathbf{M}$ is a group), it follows that $[\![m(a) \neq m(b)]\!]$ is finite, so $\langle a, b\rangle \in \hat{\theta}$ implies $\langle m(a), m(b)\rangle \in \hat{\theta}$. Thus $\hat{\theta}$ is also a congruence on $\mathbf{A}^{\mathbf{M}}$, and as $\mathbf{A}^{\mathbf{M}}$ is a simple algebra we must have $\hat{\theta} = \nabla$. But this can happen only if M is finite.

Next if ϕ is a congruence on $\mathbf{A}$ let ϕ^* be the binary relation on A^M defined by

$$\phi^* = \{\langle a, b\rangle \in A^M \times A^M : \langle a(n), b(n)\rangle \in \phi \quad \text{for} \quad n \in M\}.$$

Again ϕ^* is a well-known congruence on $\mathbf{A}^M$. Now for $m, n \in M$ and $\langle a, b\rangle \in \phi^*$ we have

$$\langle (m(a))(n), (m(b))(n)\rangle = \langle a(n \cdot m), b(n \cdot m)\rangle \in \phi;$$

hence $\langle m(a), m(b)\rangle \in \phi^*$. Consequently ϕ^* is a congruence on $\mathbf{A}^{\mathbf{M}}$. As $\mathbf{A}^{\mathbf{M}}$ is simple this forces ϕ to be $\Delta_{\mathbf{A}}$ or ∇_A; hence $\mathbf{A}$ is a simple algebra.

(b) Again the interesting case is when $\mathbf{S}$ is nontrivial. From the congruence-distributive assumption and the finiteness of $\mathbf{G}$ we know (see IV §11.10 of [5]) that all congruences on $\mathbf{S}^G$ are of the form, for $J \subseteq G$,

$$\theta_J = \{\langle a, b\rangle \in S^G : [\![a \neq b]\!] \subseteq J\}.$$

Now if θ is a congruence on $\mathbf{S}^{\mathbf{G}}$ and $\theta \neq \Delta$ then there must exist $\langle a, b\rangle \in \theta$ and $g \in G$ such that $a(g) \neq b(g)$. Then, for $h \in G$,

$$a(h \cdot h^{-1} \cdot g) \neq b(h \cdot h^{-1} \cdot g),$$

so

$$((h^{-1} \cdot g)(a))(h) \neq ((h^{-1} \cdot g)(b))(h).$$

As

$$\langle (h^{-1} \cdot g)(a), (h^{-1} \cdot g)(b)\rangle \in \theta$$

and

$$h \in [\![(h^{-1} \cdot g)(a) \neq (h^{-1} \cdot g)(b)]\!]$$

it follows that the $J \subseteq G$ for which $\theta = \theta_J$ must be $J = G$. Thus $\theta = \nabla$, so $\mathbf{S}^{\mathbf{G}}$ is indeed simple. □

§2. Discriminator varieties

Most of the background information on discriminator varieties can be found in IV §9 of [5] or in §9 of [6]. Given a variety $\mathcal{V}$ let $\mathcal{V}_S$ be the class of simple algebras in $\mathcal{V}$, and let $\mathcal{V}_{DI}$ be the class of directly indecomposable members of $\mathcal{V}$. The notation $\mathbf{A} \leq_{bp} \prod_{x \in X} \mathbf{A}_x$ means $\mathbf{A}$ is a Boolean product of the indexed family of algebras $(\mathbf{A}_x)_{x \in X}$, i.e., (i) $\mathbf{A}$ is a subdirect product of the family $(\mathbf{A}_x)_{x \in X}$, and X can be endowed with a Boolean space topology such that (ii) $[\![a = b]\!]$ is clopen for all $a, b \in A$, and (iii) for $a, b \in A$ and N a clopen subset of X, $a\restriction_N \cup b\restriction_{X-N} \in A$. $\Gamma^a(\mathcal{K})$ denotes the class of all Boolean products of members of $\mathcal{K}$. A variety $\mathcal{V}$ is a *discriminator variety* if $\mathcal{V}$ is generated by $\mathcal{V}_S$ and there is a discriminator term

$t(x, y, z)$ for $\mathcal{V}_S$, i.e., $\mathcal{V}_S$ satisfies

$$[x \approx y \to t(x, y, z) \approx z] \,\&\, [x \not\approx y \to t(x, y, z) \approx x].$$

We summarize the basic results on discriminator varieties that we will need in the following theorem.

THEOREM 2.1. *Let $\mathcal{V}$ be a discriminator variety, and let $t(x, y, z)$ be a discriminator term for $\mathcal{V}_S$.*

(a) $\mathcal{V}_{DI} = \mathcal{V}_S$
(b) $\mathcal{V} = I\Gamma^a(\mathcal{V}_S)$
(c) *For $\mathbf{S} \in \mathcal{V}_S$, the factor congruences on $\mathbf{S}^I$ are of the form, for $J \subseteq I$, $\theta_J = \{\langle a, b\rangle \in S^I \times S^I : [\![a \neq b]\!] \subseteq J\}$.*
(d) *Every $\mathbf{A} \in \mathcal{V}$ is isomorphic to a Boolean product $\mathbf{A}^*$ of simple algebras, i.e., $\mathbf{A} \leq_{bp} \prod_{x \in X} \mathbf{S}_x$, $\mathbf{S}_x \in \mathcal{V}$ for $x \in X$, such that at most one $\mathbf{S}_x$ is a trivial algebra. For $\mathbf{A}$ a nontrivial algebra we can furthermore require that x be a nonisolated point of X if $\mathbf{S}_x$ is indeed trivial.*

Let $\mathbf{A} \leq_{bp} \prod_{x \in X} \mathbf{S}_x$, $\mathbf{S}_x$ simple, in (e)–(h).

(e) *For $a, b, c, d \in A$,*

$$[\![a \neq b]\!] \subseteq [\![c \neq d]\!] \quad \text{iff} \quad t(c, d, a) = t(c, d, b),$$

and

$$[\![a \neq b]\!] \cup [\![c \neq d]\!] = [\![t(a, b, c) \neq t(b, a, d)]\!].$$

(f) *Every congruence θ on $\mathbf{A}$ is of the form*

$$\theta_U = \{\langle a, b\rangle \in A^2 : \ [\![a \neq b]\!] \subseteq U\},$$

for U an open subset of X. The factor congruences on $\mathbf{A}$ are precisely those of the form θ_N for N a clopen subset of X.
(g) *All finitely generated congruences on $\mathbf{A}$ are principal, and indeed for $a, b \in A$ we have $\theta(a, b) = \theta_{[\![a \neq b]\!]}$. A clopen subset N of X is of the form $[\![a \neq b]\!]$ iff $\mathbf{S}_x$ is nontrivial for $x \in N$.*
(h) *The set of principal congruences on $\mathbf{A}$ forms a sublattice of the congruence lattice of $\mathbf{A}$ which embeds into the lattice of clopen subsets of X under the mapping $\theta(a, b) \to [\![a \neq b]\!]$; this is a Boolean lattice if no $\mathbf{S}_x$ is trivial.*

Now we are ready to prove our main result in this section.

THEOREM 2.2. *For $\mathscr{V}$ a nontrivial variety and* $\mathbf{M}$ *a monoid,* $\mathscr{V}(\mathbf{M})$ *is a discriminator variety iff* $\mathscr{V}$ *is a discriminator variety and* $\mathbf{M}$ *is a finite group.*

Proof. ($\Rightarrow$) Since $\mathscr{V}$ is equivalent to a subvariety of the discriminator variety $\mathscr{V}(\mathbf{M})$ by Theorem 1.1, it follows that $\mathscr{V}$ must be a discriminator variety. Next let $\mathbf{S}$ be a nontrivial simple algebra in $\mathscr{V}$. We claim that $\mathbf{S}^{\mathbf{M}}$ is a directly indecomposable algebra. To see this we note that factor congruences on $\mathbf{S}^{\mathbf{M}}$ must be of the form

$$\theta_J = \{\langle a, b\rangle \in S^M \times S^M : [\![a \neq b]\!] \subseteq J\},$$

for $J \subseteq M$, by 2.1(c). So suppose θ_J, θ_{M-J} is a pair of factor congruences on $\mathbf{S}^{\mathbf{M}}$. We can assume $1 \in J$. If $J \neq M$ choose an element $m \in M - J$, and then choose $a, b \in S^M$ with $[\![a \neq b]\!] = \{m\}$. Then

$$[\![a \neq b]\!] \subseteq M - J,$$

so,

$$\langle a, b\rangle \in \theta_{M-J}.$$

This implies

$$\langle m(a), m(b)\rangle \in \theta_{M-J},$$

so

$$[\![m(a) \neq m(b)]\!] \subseteq M - J,$$

i.e.,

$$J \subseteq [\![m(a) = m(b)]\!].$$

But this is impossible as $1 \in J$ and $m(a)(1) \neq m(b)(1)$ (since $a(m) \neq b(m)$). Thus $J = M$, and hence $\mathbf{S}^{\mathbf{M}}$ is directly indecomposable. This forces $\mathbf{S}^{\mathbf{M}}$ to be simple by 2.1(a), so by Lemma 1.9(a) it follows that $\mathbf{M}$ is a finite group.

($\Leftarrow$) Let $\mathscr{V}$ be a nontrivial discriminator variety and let $\mathbf{G}$ be a finite group. Let $\mathbf{A}$ be a nontrivial directly indecomposable member of $\mathscr{V}(\mathbf{G})$. As every algebra in a discriminator variety can be represented as a Boolean product of simple algebras by 2.1(b), we can assume

$$\mathbf{A}\restriction_{\mathcal{V}} \leq_{bp} \prod_{x\in X} \mathbf{S}_x, \mathbf{S}_x \in \mathcal{V}_S.$$

Furthermore by 2.1(d) we can assume that at most one $\mathbf{S}_x$ is trivial, and if there is a trivial $\mathbf{S}_x$ then x is not an isolated point of the Boolean space X.

For $a, b, c, d \in A$ we have

$$[\![a \neq b]\!] \subseteq [\![c \neq d]\!] \quad \text{iff} \quad t(c, d, a) = t(c, d, b),$$

where $t(x, y, z)$ is a discriminator term for $\mathcal{V}_S$ (by 2.1(e)). Consequently, for $g \in G$ we have

$$[\![a \neq b]\!] \subseteq [\![c \neq d]\!] \quad \text{iff} \quad [\![g(a) \neq g(b)]\!] \subseteq [\![g(c) \neq g(d)]\!].$$

Thus each g induces an automorphism $\bar{g}$ on the lattice $\mathbf{L}$ of all clopen subsets of X of the form $[\![a \neq b]\!]$, namely

$$\bar{g} : [\![a \neq b]\!] \mapsto [\![g(a) \neq g(b)]\!].$$

For U an open subset of X, θ_U is a congruence on $\mathbf{A}\restriction_{\mathcal{V}}$ by 2.1(f); hence θ_U is a congruence on $\mathbf{A}$ iff $[\![a \neq b]\!] \subseteq U$ implies $[\![g(a) \neq g(b)]\!] \subseteq U$, for $a, b \in A$, $g \in G$.

Suppose now that N is a clopen subset of X such that θ_N is a congruence of $\mathbf{A}$. For $a, b \in A$, if

$$N \cap [\![a \neq b]\!] = \varnothing \quad \text{but} \quad N \cap [\![g(a) \neq g(b)]\!] \neq \varnothing$$

for some $g \in G$, then for some $c, d \in A$,

$$[\![c \neq d]\!] = N \cap [\![g(a) \neq g(b)]\!]$$

by 2.1(g). But then

$$\varnothing \neq [\![g^{-1}(c) \neq g^{-1}(d)]\!] \subseteq [\![a \neq b]\!],$$

and

$$[\![g^{-1}(c) \neq g^{-1}(d)]\!] \subseteq N$$

(as θ_N is a congruence on $\mathbf{A}$), contradicting the fact that $N \cap [\![a \neq b]\!] = \varnothing$. Thus θ_{X-N} is also a congruence on $\mathbf{A}$. As $\mathbf{A}$ is directly indecomposable this says $N = \varnothing$ or $N = X$ are the only possibilities.

Now if N is a clopen subset of X of the form $[\![a \neq b]\!]$ then

$$\bar{G}(N) = \bigcup_{g \in G} \bar{g}(N)$$

is also a clopen subset of X as $\mathbf{G}$ is a finite group; and furthermore if $[\![c \neq d]\!] \subseteq \bar{G}(N)$ then

$$\begin{aligned}\bar{g}([\![c \neq d]\!]) &\subseteq \bar{g}\bar{G}(N)\\ &= \bar{g}\Big(\bigcup_{h \in G} \bar{h}(N)\Big)\\ &= \bigcup_{h \in G} \bar{g}\bar{h}(N)\\ &= \bigcup_{h \in G} \bar{h}(N) = \bar{G}(N),\end{aligned}$$

so $\theta_{\bar{G}(N)}$ is a congruence on $\mathbf{A}$. Thus

$$a \neq b \quad \text{implies} \quad \bar{G}([\![a \neq b]\!]) = X.$$

Consequently there are no trivial algebras $\mathbf{S}_x$, for $x \in X$. Thus the clopen subsets of the form $[\![a \neq b]\!]$ form a subfield $\mathbf{B}$ of the Boolean algebra of all subsets of X by 2.1(g), and furthermore the $\bar{g}$'s are automorphisms of $\mathbf{B}$, for $g \in G$, with the property that $\bar{G}(N) = \bigcup_{g \in G} \bar{g}(N)$ is X for $N \neq \varnothing$. Such Boolean algebras with a group of automorphisms were studied in [3], and for $\mathbf{G}$ finite we proved that the above condition involving $\bar{G}$ forces $|B| \leq 2^{|G|}$. Thus X must be a finite discrete space (indeed $|X| \leq |G|$). Consequently $\mathbf{A}$ is a simple algebra as all congruences on $\mathbf{A}$ are of the form θ_U with U open, and now we know that all open subsets of X are actually clopen sets N (we've already proved that if θ_N is a congruence then $N = \varnothing$ or X). At this point we know that $\mathcal{V}(\mathbf{G})$ is a semisimple variety as $\mathcal{V}(\mathbf{G})_{DI} \subseteq \mathcal{V}(\mathbf{G})_S$.

Before continuing let us note that the *switching term*

$$s(x, y, u, v) = t(t(x, y, u), t(x, y, v), v)$$

is such that $\mathcal{V}_S$ satisfies

$$[x \approx y \to s(x, y, u, v) \approx u] \mathbin{\&} [x \not\approx y \to s(x, y, u, v) \approx v].$$

By repeatedly applying the identity

$$[\![a \neq b]\!] \cup [\![c \neq d]\!] = [\![t(a, b, c) \neq t(b, a, d)]\!]$$

we can find terms $p(x_1, \ldots, x_n, y_1, \ldots, y_n)$, $q(x_1, \ldots, x_n, y_1, \ldots, y_n)$ where $G = \{g_1, \ldots, g_n\}$, such that for $a, b \in A$ (and using the notation $p(\vec{g}(a), \vec{g}(b))$ for $p(g_1(a), \ldots, g_n(a), g_1(b), \ldots, g_n(b))$, etc.) we have

$$\begin{aligned} \bar{G}([\![a \neq b]\!]) &= \bigcup_{g \in G} [\![g(a) \neq g(b)]\!] \\ &= [\![p(\vec{g}(a), \vec{g}(b)) \neq q(\vec{g}(a), \vec{g}(b))]\!]. \end{aligned}$$

Then let

$$t^*(x, y, z) = s(p(\vec{g}(x), \vec{g}(y)), q(\vec{g}(x), \vec{g}(y)), z, x).$$

We see that for $a, b, c \in A$ ($\mathbf{A}$ as above),

$$[\![p(\vec{g}(a), \vec{g}(b)) \neq q(\vec{g}(a), \vec{g}(b))]\!] = \begin{cases} \varnothing & \text{if} \quad a = b \\ X & \text{if} \quad a \neq b \end{cases}$$

as $\bar{G}([\![a \neq b]\!])$ takes these values. Consequently

$$t^*(a, b, c) = \begin{cases} c & \text{if} \quad a = b \\ a & \text{if} \quad a \neq b, \end{cases}$$

so $t^*(x, y, z)$ is a discriminator term for $\mathcal{V}(\mathbf{G})_S$. Thus $\mathcal{V}(\mathbf{G})$ is indeed a discriminator variety. □

§3. Abelian varieties

A variety $\mathcal{V}$ is Abelian if it satisfies, for all terms t,

$$\forall x \forall y \forall \vec{u} \forall \vec{v} [t(x, \vec{u}) \approx t(x, \vec{v}) \leftrightarrow t(y, \vec{u}) \approx t(y, \vec{v})]. \tag{1}$$

The background for this section can be found in [4].

THEOREM 3.1. *$\mathcal{V}(\mathbf{M})$ is Abelian iff $\mathcal{V}$ is Abelian.*

Proof. ($\Rightarrow$) If $\mathcal{V}(\mathbf{M})$ is Abelian then so is every subvariety of $\mathcal{V}(\mathbf{M})$. But then by Theorem 1.1 $\mathcal{V}$ is Abelian.

($\Leftarrow$) Given a term $t(x, y_1, \ldots, y_n)$ in the language of $\mathcal{V}(\mathbf{M})$ let $t^*(m_1(x), \ldots, m_1(y_n), \ldots, m_l(x), \ldots, m_l(y_n))$ be an equivalent reduced term (as guaranteed by Lemma 1.4). Then for $a, b, c_1, \ldots, c_n, d_1, \ldots, d_n \in A$, where $\mathbf{A} \in \mathcal{V}(\mathbf{M})$, we have, by repeated use of the property (1), which holds for $\mathcal{V}$, using the abbreviations $m_1(\vec{c})$ for $m_1(c_1), \ldots, m_1(c_n)$, etc.,

$$t(a, \vec{c}) = t(a, \vec{d})$$

$$\Leftrightarrow t^*(m_1(a), m_1(\vec{c}), m_2(a), m_2(\vec{c}), \ldots, m_l(a), m_l(\vec{c})) \\ = t^*(m_1(a), m_1(\vec{d}), m_2(a), m_2(\vec{d}), \ldots, m_l(a), m_l(\vec{d}))$$

$$\Leftrightarrow t^*(m_1(b), m_1(\vec{c}), m_2(a), m_2(\vec{c}), \ldots, m_l(a), m_l(\vec{c})) \\ = t^*(m_1(b), m_1(\vec{d}), m_2(a), m_2(\vec{d}), \ldots, m_l(a), m_l(\vec{d}))$$

$$\Leftrightarrow t^*(m_1(b), m_1(\vec{c}), m_2(b), m_2(\vec{c}), \ldots, m_l(a), m_l(\vec{c})) \\ = t^*(m_1(b), m_1(\vec{d}), m_2(b), m_2(\vec{d}), \ldots, m_l(a), m_l(\vec{d}))$$

$$\vdots$$

$$\Leftrightarrow t^*(m_1(b), m_1(\vec{c}), m_2(b), m_2(\vec{c}), \ldots, m_l(b), m_l(\vec{c})) \\ = t^*(m_1(b), m_1(\vec{d}), m_2(b), m_2(\vec{d}), \ldots, m_l(b), m_l(\vec{d})).$$

$$\Leftrightarrow t(b, \vec{c}) = t(b, \vec{d}).$$

Thus (1) holds for $\mathcal{V}(\mathbf{M})$, so $\mathcal{V}(\mathbf{M})$ is Abelian. $\square$

Associated with each congruence-modular Abelian variety is a variety of modules ${}_{\mathbf{R}(\mathscr{A})}\mathbf{M}$, where $\mathbf{R}(\mathscr{A})$ is a ring with unit. Indeed the varieties $\mathscr{A}$ and ${}_{\mathbf{R}(\mathscr{A})}\mathbf{M}$ are in many respects equivalent. Our main result in this section is to establish a simple connection between $\mathbf{R}(\mathscr{A})$ and $\mathbf{R}(\mathscr{A}(\mathbf{M}))$. First let us sketch the details of the basic results on modular Abelian varieties.

A modular Abelian variety $\mathscr{A}$ is congruence-permutable, so there is a Mal'cev term $p(x, y, z)$ for $\mathcal{A}$. Let $R = \{r(\bar{u}, \bar{v}) \in F_{\mathcal{A}}(\bar{u}, \bar{v}) : \mathcal{A} \models r(v, v) \approx v\}$. Then define the operations $+, \cdot, -, 0, 1$ on R by

$$r(\bar{u}, \bar{v}) + s(\bar{u}, \bar{v}) = p(r(\bar{u}, \bar{v}), \bar{v}, s(\bar{u}, \bar{v}))$$

$$r(\bar{u}, \bar{v}) \cdot s(\bar{u}, \bar{v}) = r(s(\bar{u}, \bar{v}), \bar{v})$$

$$-r(\bar{u}, \bar{v}) = p(\bar{v}, r(\bar{u}, \bar{v}), \bar{v})$$

$$0 = \bar{v}$$

$$1 = \bar{u}.$$

This gives us the ring $\mathbf{R}$ associated with $\mathcal{A}$, i.e., $\mathbf{R}(\mathcal{A})$. Terms $r(u, v)$ such that $\mathcal{V} \models r(v, v) \approx v$ are called *binary idempotent terms.*

In the following, when working with the function associated with a term $p(x_1, \ldots, x_n)$ on an algebra $\mathbf{A}$ we will write $p^{\mathbf{A}}(x_1, \ldots, x_n)$ with the exception of $\mathbf{A} = \mathbf{F}_{\mathcal{A}(\mathbf{M})}(\bar{u}, \bar{v})$, in which case we omit the superscript. Also we will write $\mathbf{F}$ for $\mathbf{F}_{\mathcal{A}}(\bar{u}, \bar{v})$.

Next, given $\mathbf{A} \in \mathcal{A}$ and $\alpha \in A$ we can construct on the set A a left $\mathbf{R}(\mathcal{A})$-module $\mathbf{M}(\mathbf{A}, \alpha) = \langle A, +, -, \alpha, (r)_{r \in \mathbf{R}(\mathcal{A})} \rangle$ by defining, for $a, b \in A$,

$$a + b = p^{\mathbf{A}}(a, \alpha, b)$$

$$-a = p^{\mathbf{A}}(\alpha, a, \alpha)$$

$$0 = \alpha$$

$$r \cdot a = r^{\mathbf{A}}(a, \alpha).$$

Furthermore, for each term $p(x_1, \ldots, x_n)$ in the language of $\mathcal{A}$ one can find a term $p_M(x_1, \ldots, x_n) = \sum_{1 \le i \le n} r_i \cdot x_i$ in the language of $R(\mathcal{A})$-modules such that for $\mathbf{A} \in \mathcal{A}$ and $\alpha \in A$,

$$p^{\mathbf{A}}(x_1, \ldots, x_n) = p_M^{\mathbf{M}(\mathbf{A}, \alpha)}(x_1, \ldots, x_n) + p^{\mathbf{A}}(\alpha, \ldots, \alpha).$$

i.e., for $a_1, \ldots, a_n \in A$ we have

$$p^{\mathbf{A}}(a_1, \ldots, a_n) = \sum_{1 \le i \le n} r_i \cdot a_i + p^{\mathbf{A}}(\alpha, \ldots, \alpha),$$

where the module operations on the right are those of $\mathbf{M}(\mathbf{A}, \alpha)$. This also can be written as

$$p^{\mathbf{A}}(a_1, \ldots, a_n) = \sum_{1 \le i \le n} r_i^{\mathbf{A}}(a_i, \alpha) + p^{\mathbf{A}}(\alpha, \ldots, \alpha).$$

Given a monoid $\mathbf{M}$ and a ring $\mathbf{R}$ we define $R[M]$ to be the set of all functions $\vec{r} \in R^M$ such that $r_m = 0$ for all but finitely many $m \in M$(r_m being the value of $\vec{r}$ at m). Then we define the *monoid-ring* $\mathbf{R}[\mathbf{M}]$ with universe $R[M]$ by

$$\vec{0}(m) = 0$$

$$\vec{1}(1) = 1, \vec{1}(m) = 0 \quad \text{if} \quad m \ne 1$$

$$(\vec{r} + \vec{s})(m) = r_m + s_m$$

$$(\vec{r} \cdot \vec{s})(m) = \sum_{m_1 \cdot m_2 = m} r_{m_1} \cdot s_{m_2}.$$

If $\mathscr{A}$ is an Abelian variety then we can use the same Mal'cev term for $\mathscr{A}$ and $\mathscr{A}(\mathbf{M})$. Then we can easily see that we have a natural embedding $\phi : \mathbf{R}(\mathscr{A}) \to \mathbf{R}(\mathscr{A}(\mathbf{M}))$ defined by $\phi(r^{\mathbf{F}}(\bar{u}, \bar{v})) = r(\bar{u}, \bar{v})$, where $r(u, v)$ is a binary idempotent term in the language of $\mathbf{A}$. The image of $\mathbf{R}(\mathscr{A})$ under ϕ will be called $\mathbf{R}^*$; thus $\mathbf{R}^*$ is the subring of $\mathbf{R}(\mathscr{A}(\mathbf{M}))$ whose universe consists of all $r(\bar{u}, \bar{v})$ where $r(u, v)$ is a binary idempotent term in the language of $\mathbf{A}$.

We would like to know what new binary idempotent terms we have in the language of $\mathscr{A}(\mathbf{M})$. The most obvious candidates are of the form $m(u) - m(v)$, properly expressed in the language of $\mathscr{A}(\mathbf{M})$. As it turns out these, along with the original binary idempotent terms of $\mathscr{A}$, generate $\mathbf{R}(\mathscr{A}(\mathbf{M}))$ in a simple fashion. We give this fundamental decomposition in the next lemma.

LEMMA 3.2. *Given an idempotent term $r(u, v)$ in the language of $\mathscr{A}(\mathbf{M})$ there is a unique $\vec{r} \in R^*[M]$ such that*

$$r(\bar{u}, \bar{v}) = \sum r_m(\bar{u}, \bar{v}) \cdot (m(\bar{u}) - m(\bar{v}))$$

where the module operations on the right side are those of $\mathbf{M}(\mathbf{F}_{\mathscr{A}(\mathbf{M})}(\bar{u}, \bar{v}), \bar{v})$. (The sum is $\bar{v}$ if each $r_m(\bar{u}, \bar{v}) = \bar{v}$; otherwise it is defined to be the finite sum over all m for which $r_m(\bar{u}, \bar{v}) \ne \bar{v}$.) The mapping $r(\bar{u}, \bar{v}) \mapsto \vec{r}$ described above is a bijection from $R(\mathscr{A})$ to $R^*[M]$.

Proof. First we find a reduced term (by Lemma 1.4) $r^*(m_1(u), m_1(v), \ldots, m_n(u), m_n(v))$ which is equivalent to $r(u, v)$. We assume the m_i's are distinct. As $\mathscr{A}(\mathbf{M}) \models \mathrm{r}(\mathrm{v}, \mathrm{v}) \approx \mathrm{v}$ we have

$$\mathscr{A}(\mathbf{M}) \models r^*(m_1(v), m_1(v), \ldots, m_n(v), m_n(v)) \approx v. \tag{2}$$

Since $r^*(x_1, y_1, \ldots, x_n, y_n)$ is in the language of $\mathscr{A}$ we can find idempotent terms $r_i(u, v)$, $s_i(u, v)$ in the language of $\mathscr{A}$, $1 \le i \le n$, such that for $\mathbf{A} \in \mathscr{A}$ and $\alpha \in A$ (with module operations in $\mathbf{M}(\mathbf{A}, \alpha)$)

$$r^{*\mathbf{A}}(x_1, y_1, \ldots, x_n, y_n) = \sum_{1 \le i \le n} r_i^{\mathbf{A}}(x_i, \alpha) + \sum_{1 \le i \le n} s_i^{\mathbf{A}}(y_i, \alpha) + r^{*\mathbf{A}}(\alpha, \ldots, \alpha). \tag{3}$$

This equation will also hold for $\mathbf{A} \in \mathscr{A}(\mathbf{M})$ since the addition operation of $\mathbf{M}(\mathbf{A}, \alpha)$ is the same as that of $\mathbf{M}(\mathbf{A} \restriction_{\mathscr{A}}, \alpha)$.

From (2) we have

$$\mathscr{A}(\mathbf{M}) \models r^*(v, v, \ldots, v) \approx v;$$

thus from (3)

$$r^{\mathbf{A}}(u, v) = \sum_{1 \le i \le n} r_i^{\mathbf{A}}(m_i^{\mathbf{A}}(u), \alpha) + \sum_{1 \le i \le n} s_i^{\mathbf{A}}(m_i^{\mathbf{A}}(v), \alpha). \tag{4}$$

Now let $\mathbf{A} = \mathbf{F}^{\mathbf{M}}$. Then for $a, \alpha \in A$ we have from (4)

$$a = r^{\mathbf{A}}(a, a) = \sum_{1 \le i \le n} r_i^{\mathbf{A}}(m_i^{\mathbf{A}}(a), \alpha) + \sum_{1 \le i \le n} s_i^{\mathbf{A}}(m_i^{\mathbf{A}}(a), \alpha).$$

With module operations in $\mathbf{M}(\mathbf{F}, \alpha(1))$ we have, by evaluating at 1,

$$a(1) = \sum_{1 \le i \le n} r_i^{\mathbf{F}}(a(m_i), \alpha(1)) + \sum_{1 \le i \le n} s_i^{\mathbf{F}}(a(m_i), \alpha(1)).$$

For a fixed j, if $m_j \ne 1$ let us choose a such that $a(m) = \bar{u}$ for $m = m_j$, $a(m) = \bar{v}$

otherwise; and let $\alpha(m)=\bar{v}$ for all m. Then

$$\bar{v}=r_j^{\mathbf{F}}(\bar{u},\bar{v})+s_j^{\mathbf{F}}(\bar{u},\bar{v}).$$

But then

$$\bar{v}=r_j(\bar{u},\bar{v})+s_j(\bar{u},\bar{v}),$$

i.e.,

$$s_j(\bar{u},\bar{v})=-r_j(\bar{u},\bar{v}) \quad \text{if} \quad m_j\neq 1.$$

Thus, noting that $1(\bar{u})-1(\bar{v})=\bar{u}$, we have from (4)

$$\begin{aligned} r(\bar{u},\bar{v}) &= \sum_{1\le i\le n} r_i(\bar{u},\bar{v})\cdot m_i(\bar{u})+\sum_{1\le i\le n} s_i(\bar{u},\bar{v})\cdot m_i(\bar{v}) \\ &= \sum_{1\le i\le n} r_i(\bar{u},\bar{v})\cdot (m_i(\bar{u})-m_i(\bar{v})). \end{aligned}$$

To show that this representation is unique suppose $\vec{r},\vec{s}\in R^*[M]$ and

$$\sum r_m(\bar{u},\bar{v})\cdot(m(\bar{u})-m(\bar{v}))=\sum s_m(\bar{u},\bar{v})\cdot(m(\bar{u})-m(\bar{v})).$$

Then

$$\sum r_m(m(\bar{u})-m(\bar{v}),\bar{v})=\sum s_m(m(\bar{u})-m(\bar{v}),\bar{v}).$$

Now given any $\mathbf{A}\in\mathcal{A}(\mathbf{M})$ and $a,b\in A$ the homomorphism $\lambda:\mathbf{F}_{\mathcal{A}(\mathbf{M})}(\bar{u},\bar{v})\to\mathbf{A}$ defined by $\lambda(\bar{u})=a$, $\lambda(\bar{v})=b$, is also a homomorphism from $\mathbf{M}(\mathbf{F}_{\mathcal{A}(\mathbf{M})}(\bar{u},\bar{v}),\bar{v})\to$ $\mathbf{M}(\mathbf{A},b)$; hence for $\mathbf{A}\in\mathcal{A}(\mathbf{M})$ and $a,b\in A$

$$\mathbf{A}\models\sum r_m^{\mathbf{A}}(m^{\mathbf{A}}(a)-m^{\mathbf{A}}(b),b)=\sum s_m^{\mathbf{A}}(m^{\mathbf{A}}(a)-m^{\mathbf{A}}(b),b).$$

Now let $\mathbf{A}=\mathbf{F}^{\mathbf{M}}$, and evaluate both sides at 1 to obtain

$$\sum r_m^{\mathbf{F}}(a(m)-b(m),b(1))=\sum s_m^{\mathbf{F}}(a(m)-b(m),b(1)).$$

Letting $b(m)=v$ for all m we have

$$\sum r_m^{\mathbf{F}}(a(m),\bar{v})=\sum s_m^{\mathbf{F}}(a(m),\bar{v}).$$

For $n\in M$ let $a(n)=\bar{u}$, $a(m)=\bar{v}$ otherwise. This yields

$$r_n^{\mathbf{F}}(\bar{u},\bar{v})=s_n^{\mathbf{F}}(\bar{u},\bar{v}),$$

so

$$r_n(\bar{u},\bar{v})=s_n(\bar{u},\bar{v}).$$

Thus for $r(\bar{u},\bar{v})\in F_{\mathbf{A(M)}}(\bar{u},\bar{v})$, the associated $\vec{r}\in R^*[M]$ is unique. □

THEOREM 3.3. $\mathbf{R}(\mathscr{A}(\mathbf{M}))\cong(\mathbf{R}(\mathscr{A}))[\mathbf{M}]$.

Proof. Let $\phi: R(\mathscr{A}(\mathbf{M}))\to R^*[M]$ be the bijection described in Lemma 3.2. Then for $r(u,v)$, $s(u,v)$ idempotent terms in the language of $\mathscr{A}(\mathbf{M})$ we have $\phi(r(\bar{u},\bar{v}))=\vec{r}$, $\phi(s(\bar{u},\bar{v}))=\vec{s}$ where

$$r(\bar{u},\bar{v})=\sum r_m(\bar{u},\bar{v})\cdot(m(\bar{u})-m(\bar{v}))$$

$$s(\bar{u},\bar{v})=\sum s_m(\bar{u},\bar{v})\cdot(m(\bar{u})-m(\bar{v})).$$

As $r_m(\bar{u},\bar{v})$, $s_m(\bar{u},\bar{v})$ and $m(\bar{u})-m(\bar{v})\in R(\mathscr{A}(\mathbf{M}))$, for $m\in M$, we can think of the above operations of addition and multiplication as being *ring* operations of $\mathbf{R}(\mathscr{A}(\mathbf{M}))$. But then

$$r(\bar{u},\bar{v})+s(\bar{u},\bar{v})=\sum(r_m(\bar{u},\bar{v})+s_m(\bar{u},\bar{v}))\cdot(m(\bar{u})-m(\bar{v})),$$

so $\phi(r(\bar{u},\bar{v})+s(\bar{u},\bar{v}))=\phi(r(\bar{u},\bar{v}))+\phi(s(\bar{u},\bar{v}))$. Also $\phi(\bar{v})=\vec{0}$ and $\phi(\bar{u})=\vec{1}$, and then $\phi(-r(\bar{u},\bar{v}))=-\phi(r(\bar{u},\bar{v}))$.

Finally to show that ϕ preserves multiplication we make use of the fact that the Mal'cev term $p(x,y,z)$ permutes with other terms in the language of $\mathscr{A}(\mathbf{M})$, and that for $\mathbf{A}\in\mathscr{A}(\mathbf{M})$ and $a\in A$,

$$p^{\mathbf{A}}(x,y,z)=x-y+z,$$

where the calculations on the right are done in $\mathbf{M}(\mathbf{A},a)$.
First note that for $m,n\in M$,

$$\begin{aligned}(m(\bar{u})-m(\bar{v}))\cdot(n(\bar{u})-n(\bar{v}))&=m(n(\bar{u})-n(\bar{v}))-m(\bar{v})\\&=m(p(n(\bar{u}),n(\bar{v}),\bar{v}))-m(\bar{v})\\&=p((m\cdot n)(\bar{u}),(m\cdot n)(\bar{v}),m(\bar{v}))-m(\bar{v})\\&=(m\cdot n)(\bar{u})-(m\cdot n)(\bar{v})+m(\bar{v})-m(\bar{v})\\&=(m\cdot n)(\bar{u})-(m\cdot n)(\bar{v}).\end{aligned}$$

Next, if $t(u, v)$ is an idempotent term in the language of $\mathscr{A}$, and if $m \in M$, then

$$\begin{aligned}(m(\bar{u})-m(\bar{v}))\cdot t(\bar{u},\bar{v}) &= m(t(\bar{u},\bar{v}))-m(\bar{v})\\ &= t(m(\bar{u}), m(\bar{v}))-m(\bar{v})\\ &= t(m(\bar{u}), m(\bar{v}))-t(m(\bar{v}), m(\bar{v}))+t(\bar{v},\bar{v})\\ &= p(t(m(\bar{u}), m(\bar{v})), t(m(\bar{v}), m(\bar{v})), t(\bar{v},\bar{v}))\\ &= t(p(m(\bar{u}), m(\bar{v}), \bar{v}), p(m(\bar{v}), m(\bar{v}), \bar{v}))\\ &= t(m(\bar{u})-m(\bar{v}), \bar{v})\\ &= t(\bar{u},\bar{v})\cdot(m(\bar{u})-m(\bar{v})).\end{aligned}$$

Thus elements of $\mathbf{R}^*$ commute with elements of $\mathbf{R}(\mathscr{A}(\mathbf{M}))$ of the form $m(\bar{u})-m(\bar{v})$.

Consequently we have

$$\begin{aligned}&\phi(r(\bar{u},\bar{v})\cdot s(\bar{u},\bar{v}))\\ &=\phi\left(\left(\sum_m r_m(\bar{u},\bar{v})\cdot(m(\bar{u})-m(\bar{v}))\right)+\left(\sum_m s_m(\bar{u},\bar{v})\cdot(m(\bar{u})-m(\bar{v}))\right)\right.\\ &=\phi\left(\sum_{m,n} r_m(\bar{u},\bar{v})\cdot(m(\bar{u})-m(\bar{v}))\cdot s_n(\bar{u},\bar{v})\cdot(n(\bar{u})-n(\bar{v}))\right)\\ &=\phi\left(\sum_{m,n} r_m(\bar{u},\bar{v})\cdot s_n(\bar{u},\bar{v})\cdot(m(\bar{u})-m(\bar{v}))\cdot(n(\bar{u})-n(\bar{v}))\right)\\ &\phi\left(\sum_{m,n} r_m(\bar{u},\bar{v})\cdot s_n(\bar{u},\bar{v})\cdot((mn)(\bar{u})-(mn)(\bar{v}))\right)\Bigg)\\ &=\phi(r(\bar{u},\bar{v}))\cdot\phi(s(\bar{u},\bar{v})).\end{aligned}$$

This completes the proof. □

REFERENCES

[1] W. BAUR, *Decidability and undecidability of theories of abelian groups with predicates for subgroups*, Compos. Math. *31* (1975), 23–30.

[2] ——, *Undecidability of the theory of abelian groups with a subgroup*, Proc. Amer. Math. Soc. *44* (1976), 125–128.

[3] S. BURRIS, *The first-order theory of Boolean algebras with a distinguished group of automorphisms*, (to appear in Algebra Universalis).

[4] S. BURRIS and R. MCKENZIE, *Decidability and Boolean Representations*, Memoirs Amer. Math. Soc. No. 246, July 1981.

[5] S. BURRIS and H. P. SANKAPPANAVAR, *A Course in Universal Algebra*, Graduate Texts in Math. No. *78*, Springer-Verlag 1981.
[6] S. BURRIS and H. WERNER, *Sheaf constructions and their elementary properties*, Trans. Amer. Math. Soc. *248* (1979), 269–309.
[7] W. TAYLOR, *Equational Logic*, Houston J. of Math., Survey 1979.

University of Waterloo
Waterloo, Ontario
Canada