Comm. Korean Math. Soc. 4 (1989), No. 2, pp. 303~320

ON ABELIAN UNIVERSAL ALGEBRAS

JUNG R. CHO

0. Introduction.

In the field of universal algebra, many people have been looking for properties of universal algebras which are close to properties of groups. One of the studies led some people in the study of "Abelian" universal algebras. Since J.D.H. Smith ([22]) introduced the notion of "Centrality", the idea has been simplified as "commutator" ([11], [12]), and lots of work has been done in connection with lattices of congruences and modules of over endomorphism rings ([3], [10], [12], [13]). Some of the material presented in this paper overlaps other persons' work already published, but the approach is different and there are some new results.

We will simply say 'algebra' for 'universal algebra' in this paper. It is also assumed that the readers have basic concepts of universal algebra such as: *subalgebra, homomorphism, direct product, variety, term-function*, and so on. One may refer to [2] and [9] for terminology.

Let $(A, \mathbf{\Omega})$ be an algebra. An equivalence relation θ on A is called a *congruence relation* (or simply a *congruence*) provided, if $a_i \equiv_\theta b_i$ for $i = 1, 2, \ldots, n$, then $f(a_1, a_2, \ldots, a_n) \equiv_\theta f(b_1, a_b, \ldots, b_n)$, for all $f \in \mathbf{\Omega}$ and $a_1, b_1, a_2, b_2, \ldots, a_n, b_n$ in A. An equivalence class of a congruence is called a *congruence class*.

For congruences θ and η of A, let $\theta \circ \eta$ denote the relational product of θ and η, $\theta \vee \eta$ denote the smallest congruence of A containing both θ and η, and $\theta \wedge \eta$ denote the largest congruence of A containing both θ and η. Two congruene θ and η are said to *permute* each other if $\theta \circ \eta = \eta \circ \theta$. It is well known that $\theta \wedge \eta = \theta \cap \eta$, and that $\theta \vee \eta = \theta \circ \eta$ if θ and η permute.

An algebra is called *permutable* if every pair of congruences permute, and a variety is *permutable* if every algebra in it is permutable. An

Received December 13, 1988. Revised May 4, 1989.

algebra is called *modular* if the lattice of congruenes of the algebra is modular, and a variety is *modular* if every algebra in it is modular.

An algebra is called *abelian* if there is a congruence ξ of $A \times A$ such that

$$\xi \vee \pi_1 = \xi \vee \pi_2 = I, \text{ and } \xi \wedge \pi_1 = \xi \wedge \pi_2 = \Delta,$$

where I is the universal congruence, and Δ is the diagonal, and π_1, π_2 are the kernels of the projections of $A \times A$ onto A.

We will study some properties of abelian universal algebras in permutable varieties and modular varieties. We also find some relation between the 'abelian' and 'medial' properties. Since quasigroups are good example of permutable algebras, we will consider quasigroups as special cases and most examples will be given by quasigroups.

LEMMA 1.1 (BIRKHOFF [1]). *Permutable algebras are modular.*[1]

COROLLARY. *Permutable varieties are modular.*

The following lemma characterizes permutable varieties by a term–function.

LEMMA 1.2 (MAL'CEV [18]). *A variety of algebras is permutable if and only if there is a term–function $p(x, y, z)$ in three variables such that every algebra in the variety satisfies the identities*

$$p(x, x, z) = z \quad \text{and} \quad p(x, z, z) = x.$$

Such a polynomial is called a *Mal'cev polynomial* of the variety and we will see this polynomial plays the single most important role for algebras in permutable varieties.

A quasigroup $(Q, \cdot, /, \backslash)$ is an algebra with three binary operations '$\cdot$', '/ ', and '\' such that ([8]), for all x, y and z in Q,

$$x \cdot (x \backslash y) = y, \ (y/x) \cdot x = y, \ x \backslash (x \cdot y) = y, \text{ and } (y \cdot x)/x = y.$$

[1] Later, B. Jónsson ([15], [16]) proved lattices of congruences of permutable algebras are Arguesian which in turn implies the modularity.

We will write xy for $x \cdot y$, omitting '$\cdot$'.

COROLLARY. *Varieties of quasigroups are permutable.*

Proof. Let $p(x,y,z) = (x/(y\backslash y))(y\backslash z)$, then

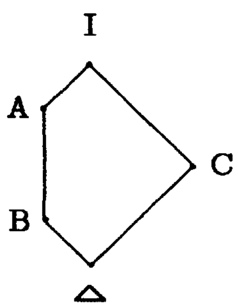
$$p(x,x,z) = (x/(x\backslash x))(x\backslash z) = x(x\backslash z) = z$$

and

$$p(x,z,z) = (x/(z\backslash z))(z\backslash z) = (x/z)z = x.$$

Thus $p(x,y,z)$ is a Mal'cev polynomial for varieties of quasigroups.

Speaking of permutable algebras, a permutable algebra may not belong to a permutable variety, even to a modular variety.



A = {{(0,0)}, {(0,1), (1,0), (1,1)}}
B = {{(0,0)}, {(0,1)},{(1,0),(1,1)}}
C = {{(0,0),(1,0)},{(0,1),(1,1)}}

Figure

EXAMPLE 1.3. *Let $S = \{0,1\}$ be two–element left–zero semigroup, that is a semigroup such that $xy = x$ for all x and y. Since S has only two elements, S has only the trivial congruences, I and Δ, which permute trivially. Thus S is permutable. The relation $\{\{(0,0),(1,1)\}, \{(0,1),(1,0)\}\}$ is a congruence of $S \times S$, and this is a common complement of the kernels of the projections. Thus S is an abelian semigroup. Since $S \times S$ is also a left–zero semigroup, any partition is a congruence. However, the lattice of congruences of $S \times S$ is not modular. A non–modular sublattice of it is shown in the Figure above. Thus, any variety* *containing S, which must contain $S \times S$, is not modular, and so this variety is not permutable by Lemma 1.1.*

2. Abelian Algebras in Permutable Varieties.

For an abelian group $(A, +)$, an n-ary operation f on A is called *linear* over $(A, +)$ if f is an homomorphism of $(A, +)^n$ into $(A, +)$, and is called *affine* if there is a linear operation g and an element d in A such that

$$f(x_1, x_2, \ldots, x_n) = g(x_1, x_2, \ldots, x_n) + d,$$

for all $x_1, x_2, \ldots, x_n$ in A. An algebra $(A, \mathbf{\Omega})$ is called linear if there can be defined an abelian group $(A, +)$ such that every operation in $\mathbf{\Omega}$ is linear over $(A, +)$, and is called affine if every operation in $\mathbf{\Omega}$ is affine.[2] A quasigroup $(Q, \cdot, /, \backslash)$ is called *medial* if $(xy)(zw) = (xz)(yw)$ for all x, y, z, w in Q. It is not hard to see that if Q is a medial quasigroup then $(x \circ_1 y) \circ_2 (z \circ_1 w) = (x \circ_2 z) \circ_1 (y \circ_2 w)$ for all x, y, z, w in Q, where $\circ_1$ and $\circ_2$ are any operations among '$\cdot$', '$/$ ', and '$\backslash$' ([3], [6]).

Let $(Q, \cdot, /, \backslash)$ be a medial quasigroup. It is shown that ([3], [14], [24]) there can be defined an abelian group $(Q, +)$ with two commuting automorphisms φ and ψ of $(Q, +)$ such that $x \cdot y = \varphi x + \psi y + d$, for all x, y in Q, where d is a fixed element of Q. The rest two operations of the quasigroup are then defined by $x/y = \varphi^{-1}x - \varphi^{-1}\psi y - \varphi^{-1}d$, and $y\backslash x = \psi^{-1}\varphi y - \psi^{-1}x - \psi^{-1}d$. Thus we can easily see that $(Q, \cdot, /, \backslash)$ is affine over $(Q, +)$. Furthermore, if we define a relation ξ on $Q \times Q$ by $(x, y) \equiv_\xi (x', y')$ if and only if $xy = x'y'$, then ξ can be shown to be a congruence. It is not hard to see ξ is in fact a common complement of the kernels of the two projections of $Q \times Q$ into Q. Consequently, every medial quasigroup is affine as well as abelian.

This is not a property of medial quasigroups only. The next nice theorem of P. Gumm shows some equivalent conditions for algebras to be abelian.

Two operation f and g, m-ary and n-ary respectively, on an algebra

[2] These are definitions of R. McKenzie ([17]). For other equivalent definitions, see [12] and [13].

A are said to *commute* each other if

$$f(g(x_{11}, x_{12}, \ldots, x_{1n}), g(x_{21}, x_{22}, \ldots, x_{2n}), \ldots, g(x_{m1}, x_{m2}, \ldots, x_{mn})$$
$$= g(f(x_{11}, x_{21}, \ldots, x_{m1}), f(x_{12}, x_{22}, \ldots, x_{m2}), \ldots, f(x_{1n}, x_{2n}, \ldots, x_{mn}),$$

for all $x_{ij} \in A$, for $1 \leq i \leq m$ and $1 \leq j \leq n$. An algebra $(A, \mathbf{\Omega})$ is said to be *medial* if any two operation in $\mathbf{\Omega}$, not necessarily distinct, commute each other.

THEOREM 2.1 (P. GUMM [10]). *For an algebra A in a permutable variety, the following conditions are equivalent:*

(i) *A is abelian.*
(ii) *A is affine.*
(iii) *Fundamental operations commute with a Mal'cev polynomial of the variety.*
(iv) *$\mathbf{\Delta} = \{(x, x) \mid x \in A\}$ is a congruence class of a congruence of $A \times A$.*

Especially, the property (iii) above implies that the property of being abelian in a permutable variety can be defined by a set of identities, and so the class of abelian algebras in a permutable variety from a subvariety.

An algebra is called *hamiltonian* if every subalgebra is an equivalence class of some congruence of the algebra, and a variety is hamiltonian if every algebra in it is so.[3]

COROLLARY 1. (P. GUMM [10]). *If A is an algebra in a permutable variety such that $A \times A$ is hamiltonian, then A is abelian.*

Proof. Since $\mathbf{\Delta}$ is a subalgebra of $A \times A$, it is a congruence class of a congruence of $A \times A$. Thus A is abelian by the preceding theorem.

We know that every subgroup of a group is normal if the group is abelian, but not conversely. An well known counterexample of this is the group of quaternion units. However, we can say a little more with the above corollary.

[3] This idea is developed by Norton ([21]). Also see [17].

COROLLARY 2. *Let G be a group. Then G is abelian if and only if every subgroup of $G \times G$ is a normal subgroup of $G \times G$.*

Since all operations and so all term–functions commute each other for medial algebras, medial algebras in a permutable variety is abelian, by (iii) of Theorem 2.1. However, not every abelian algebra in a permutable variety is medial.

EXAMPLE 2.2. *Let G be the ring of 2×2 matrices over the Galois field $GF(2)$, and let*

$$\alpha = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \beta = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Since α and β are invertible, they are automorphisms of G. Define a quasigroup on G by

$$x \cdot y = \alpha x + \beta y, \; x/y = \alpha^{-1}(x - \beta y), \text{ and } x\backslash y = \beta^{-1}(y - \alpha x),$$

then $(G, \cdot, /, \backslash)$ is linear over the additive group $(G, +)$ of the ring, and so it is abelian. Since quasigroups are permutable it belongs to the permutable variety of all quasigroups. However, $(G, \cdot, /, \backslash)$ is not medial because

$$(\overline{0} \cdot I)(\overline{0} \cdot \overline{0}) = \alpha \cdot \beta = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \beta \cdot \alpha = (\overline{0} \cdot \overline{0})(I \cdot \overline{0}),$$

where $\overline{0}$ denote the zero matrix and I the identity matrix.

The following lemma gives a condition for an abelian quasigroup to be medial.

LEMMA 2.3. *Let Q be an abelian quasigroup with an idempotent element e. Then Q is medial if and only if $e(xe) = (ex)e$ for all x in Q.*

Proof. Let $p(x, y, z)$ be a Mal'cev polynomial of Q, then

$$p(xe, e, ey) = p(xe, ee, ey) = p(x, e, e)p(e, e, y) = xy$$

by (iii) of Theorem 2.1. Thus

$$\begin{aligned}(xy)(zw) &= p(xe,e,ey)p(ze,e,ew)\\ &= p(p(xe,e,ey)e,e,ep(ze,e,ew))\\ &= p(p(xe,e,ey)p(e,e,e),p(e,e,e),p(e,e,e)p(ze,e,ew)\\ &= p(p((xe)e,ee,(ey)e),p(e,e,e),p(e(ze),ee,e(ew)))\\ &= p(p((xe)e,e,e(ze)),p(ee,e,ee),p((ey)e,e,e(ew)))\\ &= p(p((xe)e,e,(ez)e),p(ee,e,ee),p(e(ye),e,e(ew)))\\ &= p(p(xe,e,ez)p(e,e,e),p(e,e,e),p(e,e,e)p(ye,e,ew)\\ &= p(p(xe,e,ez)e,e,ep(ye,e,ew))\\ &= p(xe,e,ez)p(ye,e,ew)\\ &= (xz)(yw).\end{aligned}$$

Thus, Q is medial. Conversely, if e is an idempotent element of a medial quasigroup, $e(xe) = (ee)(xe) = (ex)(ee) = (ex)e$.

A *loop* is a quasigroup with a neutral element 1 such that $1x = x1 = 1$ for all x in the quasigroup.

COROLLARY 1. *A loop L is an abelian group if and only if $L \times L$ is hamiltonian.*

Proof. The necessity is trivial since very abelian group is hamiltonian. If $L \times L$ is hamiltonian, then L is abelian by the corollary to Theorem 2.1. If 1 is the identity element of L, 1 is idempotent and $1(x1) = (1x)1$ for all x in L. Thus L is medial by the preceding lemma. It is not hard to see a medial quasigroup with an identity element is an abelian group ([3], [20]).

COROLLARY 2. (EVANS [7]). *A variety of loops is hamiltonian if and only if it is a variety of groups.*

LEMMA 2.4. (MAL'CEV [18]). *Let $B_1, B_2, \ldots, B_k$ be pairwise disjoint subsets of an algebra (A, Ω). Then, $B_1, B_2, \ldots, B_k$ are congruence classes of a congruence of (A, Ω) if and only if, for every translation τ and $i = 1, 2, \ldots, k$, $\tau(B_i) \subseteq B_j$ for some j or $\tau(B_i) \cap B_j = \emptyset$ for all j.*

An algebra (A, Ω) is said to satisfy the *term condition* if for any n–ary termfunction w and elements $x, y, a_2, b_2, \ldots, a_n, b_n$ of A,

$$w(x, a_2, \ldots, a_n) = w(x, b_2, \ldots, b_n)$$

implies

$$w(y, a_2, \ldots, a_n) = w(y, b_2, \ldots, b_n).$$

It is not hard to see abelian algebras in a permutable variety satisfy the term condition: if $w(x, a_2, \ldots, a_n) = w(x, b_2, \ldots, b_n)$ then, with a Mal'cev polynomial $p(x, y, z)$,

$$\begin{aligned} w(y, a_2, \ldots, a_n) &= p(w(y, a_2, \ldots, a_n), w(x, a_2, \ldots, a_n), w(x, a_2, \ldots, a_n)) \\ &= p(w(y, a_2, \ldots, a_n), w(x, a_2, \ldots, a_n), w(x, b_2, \ldots, b_n)) \\ &= w(p(y, x, x), p(a_2, a_2, b_2), \ldots, p(a_n, a_n, b_n) \\ &= w(y, b_2, \ldots, b_n). \end{aligned}$$

For the converse, let $\Delta = \{(x, x) \mid x \in A\}$. Then, for any translation τ of $A \times A$, $\tau(\Delta) \subseteq \Delta$ or $\tau(\Delta) \cap \Delta = \emptyset$ by the term condition. By the preceding lemma, Δ is a congruence class of a congruence of $A \times A$. Hence, A is abelian by (iv) of Theorem 2.1. We have proved the following theorem in another way.

THEOREM 2.5 (GUMM [11]). *In a permutable variety, an algebra is abelian if and only if it satisfies the term condition.*

3. Module Representation of Abelian Algebras.

LEMMA 3.1 (GUMM [10]). *Let A be an algebra in a permutable variety and $p(x, y, z)$ a Mal'cev polynomial of the variety. Then, for all x, y, z, u, v and w of A,*

$$p(x, y, z) = p(z, y, x) \text{ and } p(x, y, p(u, v, w)) = p(p(x, y, u), v, w)).$$

An element e in an algebra (A, Ω) is called *idempotent* if $f(e, e, \ldots, e) = e$ for all $f \in \Omega$. An algebra is idempotent it every element of it is idempotent. We are now readv to define an abelian group on A which will serve as an underlying group of a module over a ring.

Let A be an abelian algebra with an idempotent element e and $p(x,y,z)$ be a Mal'cev polynomial of A. Define new operations '+' and '−' on A by

$$x+y=p(x,e,y) \text{ and } -x=p(e,x,e)$$

for all x and y in A. By the preceding lemma, '+' is commutative and associative. Because $e+x=x+e=p(x,e,e)=x$, e is the identity element with respect to '+'. Furthermore,

$$x+(-x)=p(x,e,p(e,x,e))=p(p(x,e,e),x,e)=p(x,x,e)=e.$$

Thus, $-x$ is the inverse of x with respect to '+'. We have proved:

LEMMA 3.2. *The algebra $(A,+,-,e)$ defined above is an abelian group.*

Let $(Q,\circ,/,\backslash)$ be an idempotent abelian quasigroup. Fixing an element e of Q, the abelian group is defined by the operation

$$x+y=p(x,e,y)=(x/(e\backslash e))(e\backslash y)=(x/e)(e\backslash y).$$

Thus $xy=(xe)+(ey)$. In particular, $x=xx=xe+ex$, and so

$$\begin{aligned} xe &= x+(-ex) \\ &= p(x,e,p(e,ex,e)) \\ &= p(p(x,e,e),p(e,e,e),p(e,ex,e)) \\ &= p(p(x,e,e),p(e,e,ex),p(e,e,e)) \\ &= p(x,ex,e) \end{aligned}$$

for all x in Q. Thus, for every y in Q,

$$e(ye)=p(e,e,e)p(y,ey,e)=p(ey,e(ey),ee)=(ey)e.$$

Hence, $(Q,\circ,/,\backslash)$ is medial by Lemma 2.3. We have shown:

THEOREM 3.3. *Idempotent abelian quasigroups are medial.*

A mapping $f: A^n \to A$ is called an *algebraic function* if there is a term function g of A and element $a_1,a_2,\ldots,a_k$ in A such that

$$f(x_1,x_2,\ldots,x_n)=g(a_1,a_2,\ldots,a_k,x_1,x_2,\ldots,x_n)$$

for all $x_1, x_2, \ldots, x_n$ in A.

Let (A, Ω) be an abelian algebra in a permutable variety with an idempotent element e, $p(x, y, z)$ a Mal'cev polynomial of A, and $(A, +, -, e)$ the abelian group defined above. Let R be the set of all unary algebraic functions of (A, Ω) with only e permitted as a constant, that is, for each f in R there is a binary term function $w(x, y)$ such that $f(x) = w(x, e)$ for all x in A. Define binary operations '+' and '$\cdot$' on R by

$$(f + g)(x) = f(x) + g(x) \text{ and } (f \cdot g)(x) = f(g(x)).$$

By the way they are defined, '+' is commutative and associative, and '$\cdot$' is associative. The zero mapping $x \mapsto e$ is the identity with respect to '+' since the zero mapping can be given as the unary algebraic function $p(e, x, x)$. The identity mapping $x \mapsto x$ is the unit element with respect to '$\cdot$' since it can be given by $p(x, e, e)$. For $f \in R$, the mapping $x \mapsto p(e, f(x), e)$ is the additive inverse of f. From the definition

$$((f+g)\cdot h)(x) = (f+g)(h(x)) = f(h(x))+g(h(x)) = (f\cdot h)(x)+(g\cdot h)(x).$$

Thus, $(R, +, \cdot)$ is right distributive. Now let $f, g, h \in R$ with $f(x) = w(x, e)$, then

$$\begin{aligned}(f \cdot (g + h))(x) &= f((g + h)(x)) \\ &= f(g(x) + h(x)) \\ &= w(g(x) + h(x), e) \\ &= w(p(g(x), e, h(x)), p(e, e, e)) \\ &= p(w(g(x), e), w(e, e), w(h(x), e)) \\ &= p(f(g(x)), e, f(h(x))) \\ &= (f \cdot g)(x) + (f \cdot h)(x),\end{aligned}$$

and so $(R, +, \cdot)$ is left distributive. Hence, $(R, +, \cdot)$ is a unitary ring. Suppose, furthermore, that A is medial. If $f, g \in R$ with $f(x) = u(x, e)$ and $g(x) = v(x, e)$ for some term–functions $u(x, y)$ and $v(x, y)$, then

$$\begin{aligned}(f \cdot g)(x) &= u(g(x), e) = u(v(x, e), v(e, e)) = v(u(x, e), u(e, e)) \\ &= v(f(x), e) = (g \cdot f)(x)\end{aligned}$$

and hence R is commutative. Putting these as a lemma, we have:

LEMMA 3.4. *If A is an abelian algebra in a permutable variety with an idempotent element e, then the set R of all unary algebraic functions, with only e permitted as a constant, is a unitary ring. If, furthermore, A is medial, R is commutative.*

With notations above, $(A, +, -, e)$ is a module over the ring R. The only thing that bothers is to show $f(x+y) = f(x)+f(y)$ for $f \in R$ and $x, y \in A$. If $f \in R$, then $f(x) = u(x, e)$ for some term–function $u(x, y)$. Thus, for all $x, y \in A$,

$$\begin{aligned} f(x+y) &= u(x+y, e) \\ &= u(p(x, e, y), p(e, e, e)) \\ &= p(u(x, e), u(e, e), u(y, e)) \\ &= p(f(x), e, f(y)) \\ &= f(x) + f(y). \end{aligned}$$

Since all operations of A is linear over $(A, +)$, so is every term–function of A. Let w be an n–ary term–function of A. Then, for $x_1, x_2, \ldots, x_n \in A$,

$$\begin{aligned} w(x_1, x_2, \ldots, x_n) &= w(x_1, +e + \cdots + e, \ldots, e + \cdots + e + x_n) \\ &= w(x_1, e, \ldots, e) + \cdots + w(e, \ldots, e, x_n). \end{aligned}$$

Let $w_i(x) = w(e, \ldots, e, x, e, \ldots, e)$ with x at the i–th position, then $w_i \in R$ for $i = 1, 2, \ldots, n$, and $w(x_1, x_2, \ldots, x_n) = w_1(x_1)+w_2(x_2)+\cdots+w_n(x_n)$. Thus w is expressed as a polynomial of the module $(A, +, -, e)$.

Conversely, every polynomial of the module $(A, +, -, e)$ can be expressed as an algebraic function of (A, Ω) by replacing every occurrence of $x+y$ with $p(x, e, y)$ and $-x$ with $p(e, x, e)$, while replacing $f \in R$ with the corresponding term–function.

Varieties of modules over a fixed ring is permutable since the lattice of congruences of module is a sublattice of the lattice of congruences of the underlying group,which is permutable. We note that modules are abelian since Δ is a congruence class of the congruence ξ defined by $(x, y) \equiv_\xi (x', y')$ if $x - y = x' - y'$.

Two algebras (A, Ω) and (B, Ψ) are said to be *polynomially equivalent* if there is a bijection $\rho : A \to B$ such that for every Ω–term function w there exists a Ψ–term function w' such that $w(x_1, x_2, \ldots, x_n) = w'(\rho(x_1), \rho(x_2), \ldots, \rho(x_n))$ for all $x_1, x_2, \ldots, x_n$ in A, and vice versa. That is they are representations of each other in another form of algebras.

Summarizing the results in previous paragraphs, we have the following theorem. The first part of the theorem is shown also by P. Gumm ([10]).

THEOREM 3.5. *Let (A, Ω) be an algebra in a permutable variety with an idempotent element e. Then, (A, Ω) is abelian if and only if, taking e as a nullary operation, (A, Ω) is polynomially equivalent to a module over a unitary ring. Furthermore, (A, Ω) is medial if and only if the ring is commutative.*

We can show the following corollaries without much difficulties.

COROLLARY 1. *Let (A, Ω) be an abelian algebra in a permutable variety, with an idempotent element e. If*

$$\begin{aligned} &f(g(e, \ldots, e), \ldots, g(e, \ldots, x, \ldots, e), \ldots, g(e, \ldots, e)) \ x \text{ at } (i, j) \\ =&g(f(e, \ldots, e), \ldots, f(e, \ldots, x, \ldots, e), \ldots, f(e, \ldots, e)) \ x \text{ at } (j, i) \end{aligned}$$

for all $f, g \in \Omega$, $x \in A$, and i, j, then (A, Ω) is medial.

COROLLARY 2. *Every idempotent abelian algebra in a permutable variety is medial.*

The restriction that algebras have an idempotent element is a rather strong condition. Without an idempotent element, we can still say a lot about abelian algebras in permutable varieties. As we have seen in definitions, an affine operation is simply a *translation* of a linear operation. Thus, if there is a way of *shifting* or *linearizing* operations so that the algebra under new operations is abelian with an idempotent element, we will be happy. Luckily, this is the case.

For simplicity, we denote the sequence $(x_1, x_2, \ldots, x_n)$ by $\underline{x}$ and the sequence $(e, e, \ldots, e)$ by $\underline{e}$, for appropriate n. Let (A, Ω) be an abelian algebra in a permutable variety, and $p(x,y,z)$ be a Mal'cev polynomial. Fix an element e of A. For each operation $f \in \mathbf{\Omega}$, we define a new operation f^* by

$$f^*(\underline{x}) = p(f(\underline{x}), f(\underline{e}), e),$$

and let $\mathbf{\Omega}^* = \{f^* \mid f \in \mathbf{\Omega}\}$. For every term–function w of $(A, \mathbf{\Omega})$, let w^* be the term–function of $(A, \mathbf{\Omega}^*)$ corresponding to w.

LEMMA 3.6. *With the notations above,*

(i) *e is an idempotent element of $(A, \mathbf{\Omega}^*)$,*
(ii) *$w^*(\underline{x}) = p(w(\underline{x}), w(\underline{e}), e)$ for every term–function w of $(A, \mathbf{\Omega})$,*
(iii) *$p^*(x,y,z) = p(x,y,z)$,*
(iv) *$(A, \mathbf{\Omega}^*)$ is abelian,*
(v) *$w(\underline{x}) = p(w^*(\underline{x}), e, w(\underline{e}))$ for every term–function w of $(A, \mathbf{\Omega})$.*

Proof. (i). For every $f \in \mathbf{\Omega}$, $f^*(\underline{e}) = p(f(\underline{e}), f(\underline{e}), e) = e$.

(ii). We show this by an induction on the number of operations involved in w. The result is obvious by the definition if w involves only one operation. Let $w = f(u_1, \ldots, u_n)$ for some term–functions $u_1, \ldots, u_n$ and an operation $f \in \mathbf{\Omega}$. Suppose the result is true for term–functions involving less operations than w. Then,

$$\begin{aligned} w^*(\underline{x}) &= f^*(u_1^*(\underline{x}), \ldots, u_n^*(\underline{x})) \\ &= p(f(u_1^*(\underline{x}), \ldots, u_n^*(\underline{x})), f(u_1^*(\underline{e}), \ldots, u_n^*(\underline{e})), e) \text{ by induction} \\ &= p(f(p(u_1(\underline{x}), u_1(e\underline{e}), e), \ldots, p(u_n(\underline{x}), u_n(\underline{e}), e)), f(e, \ldots, e), e) \\ &= p(p(f(u_1(\underline{x}), \ldots, u_n(\underline{x})), f(u_1, (\underline{e}), \cdot, u_n(\underline{e})), f(e, \ldots, e)), f(\underline{e}), e) \\ &= p(p(w(\underline{x}), w(\underline{e}), f(\underline{e})), f(\underline{e}), e) \\ &= p(w(\underline{x}), w(\underline{e}), p(f(\underline{e}), f(\underline{e}), e) \text{ by Lemma 3.1} \\ &= p(w(\underline{x}), w(\underline{e}), e). \end{aligned}$$

(iii). By (ii), $p^*(x,y,z) = p(p(x,y,z), p(e,e,e), e) = p(p(x,y,z), e, e) = p(x,y,z)$.

(iv). By (iii), we can use p for p^*. Since every f^* is an algebraic function of $(A, \mathbf{\Omega})$ by definition, $p(x,y,z)$ commutes with f^*. Thus, $(A, \mathbf{\Omega}^*)$ is abelian by Theorem 2.1.

(v). For every term function w,

$$\begin{aligned} p(w^*(\underline{x}), e, w(\underline{e})) &= p(p(w(uxx), w(uee), e), p(e,e,e), p(e,e,w(\underline{e})) \\ &= p(p(w(\underline{x}), e, e), p(w(\underline{e}), e, e), p(e,e,w(\underline{e})) \\ &= p(p(w(\underline{x}), e, e), w(\underline{e}), w(\underline{e})) \\ &= p(w(\underline{x}), e, e) \\ &= w(\underline{x}). \end{aligned}$$

THEOREM 3.7. *Let (A, Ω) be an algebra in a permutable variety. Then, (A, Ω) is abelian if and only if the set of all algebraic functions of (A, Ω) coindides with that of a module over a unitary ring.*

Proof. By Lemma 2.4 and (iii) of the preceding lemma, (A, Ω^*) is an algebra in a permutable variety. Moreover, (A, Ω^*) is abelian with an idempotent element by (i) and (iv) above. Thus, by Theorem 3.5, (A, Ω^*) is equivalent to the module $(A, +, -, e)$ over the ring of unary algebraic functions of (A, Ω^*). Observe that the set of all algebraic functions of (A, Ω^*) coincides that of (A, Ω) by the preceding lemma.

COROLLARY. *Let (A, Ω) be a medial algebra in a permutable variety. Then, there is a module over a commutative unitary ring such that the set of all algebraic functions of (A, Ω) coincides with that of the module.*

The converse of this corollary is not true in generl. In fact, algebraic functions of a module over a commutative ring may not commute, although term–functions do commute over a unitary ring.

As mentioned earlier, every permutable variety is modular. Most of the story for abelian algebras in permutable varieties can be said also for abelian algebras in mudular varieties. Before closing this section, we state a couple of theorems.

LEMMA 3.8. (HERRMANN [13]). *If V is a modular variety, then there is a ternary term–function $p(x, y, z)$ such that $p(x, x, z) = x$ and $p(x, z, z) = z$ hold for every abelian in V.*[4]

[4] Taylor ([23]) later proved a little stronger theorem.

COROLLARY 1. *Abelian algebras in a modular variety are permutable.*

COROLLARY 2. *Abelian algebras in a modular variety form a subvariety.*

THEOREM 3.9. (HERRMANN [13], TAYLOR [23]). *Let (A, Ω) be an abelian algebra in a mudular variety. Then, the set of all algebraic functions of (A, Ω) coincides that of a module over a unitary ring.*[5] *If, furthermore, Ω has a nullary operation which form an one–element subalgebra then (A, Ω) is polynomially equivalent to a module over a unitary ring.*

All that we need for the above theorem is a Mal'cev polynomial, which is guaranteed to exist by Lemma 3.8. We do not know whether or not medial algebras in a modular variety have the similar property as medial algebras in permutable variety. Since the class of all abelian algebras in a modular variety is a permutable variety, this question boils down to whether or not medial algebras in modular varieties are permutable.

4. Algebras polynomially equivalent to Modules.

Besides the materials so far in this paper, there are independent works on algebras polynomially equivalent to modules. It is worthwhile to collect what has been done in that area.

Varieties of algebras are said to polynomially equivalent if free algebras of the varieties are polynomially equivalent. The *idempotent reduct* of an algebra (A, Ω) is the algebra (A, Ω^*), where Ω^* is the set of all idempotent term–functions of (A, Ω). An algebra is called *regular* if every congruence is uniquely determined by any one of its congruence classes.

Various combinations of conditions in List A describe varieties of algebras polynomially equivalent to one of the varieties of modules in List B, and the correspondence is listed in Table. For most cases, if we add

[5] Herrmann used the term 'polynomially equivalent' for this, which is a little bit misleading.

the mediality then the ring becomes commutative, and if we impose the equational completeness on the variety, then the ring becomes a division ring. Different combinations may give the same variety of modules.

(1) permutable

(2) modular

(3) hamiltonian

(4) regular

(5) idempotent

(6) abelian

(7) medial

(8) every subalgebra is a congruence class of a unique congruence

(9) every subalgebra is a congruence class of a congruence

(10) every congruence has a congruence class which is a subalgebra

(11) every congruence has a unique congruence class which is a subalgebra

(12) every congruence class of any congruence is a subalgebra

(13) there is a nullary operation symbol which is idempotent

(14) equationally complete

List A.

(A) modules over a unitary ring

(B) modules over a commutative unitary ring

(C) idempotent reduct of modules over a unitary ring

(D) idempotent reduct of modules over a commutative unitary ring

(E) idempotent reduct of modules over a division ring

(F) idempotent reduct of vector spaces over a field

List B.

conditions	equivalent module	references
(1),(6), (13)	(A)	[10]
(2), (6),(13)	(B)	[11], [12]
(1), (7), (13)	(B)	[5]
(8), (12)	(C)	[6]
(7), (8), (12)	(D)	[6]
(8), (12), (14)	(E)	[6]
(7), (8), (12), (14)	(F)	[6]
(8), (11)	(A)	[5]
(1), (3), (13)	(A)	[10]
(3), (4)	(C)	[6]
(3), (4), (5), (6)	(D)	[6]
(5), (9), (10), (13)	(C)	[4]

Table.

References

1. G. Birkhoff, *Lattice Theory*, Amer. Math. Soc. Colloq. Publ. No. 25, Providence, R.I. 1973.
2. P. Cohn, *Universal Algebra*, D. Reidel Publ. Co., 1981.
3. J. Cho, *Varieties of medial algebras*, Ph. D. thesis, Emory Univ. Atlanta, G.A. 1986.
4. B. Csákány, *Abelian properties of primitive classes of universal algebras*, Acta. Sci. Math. (Szeged) 24(1963), 157–164.
5. B. Csákány, *Varieties in which congruences and subalgebras are amicable*, Acta. Sci. Math. (Szeged) 38(1975), 25–32.
6. B. Csákány, *Varieties of affine modules*, Colloq. Math. 31(1970), 3–10.
7. T. Evans, *Properties of algebras almost equivalent to identities*, J. London Math. Soc. 37(1962), 53–59.
8. T. Evans, *Homomorphism of non-associative systems*, J. London Math. Soc. 24(1949), 254–260.

9. G. Grätzer, *Universal Algebra*, Springer–Verlag, 1979.
10. P. Gumm, *Algebras in permutable varieties: Geometrical property of affine algebras*, Alg. Univ. 9(1979), 8–34.
11. P. Gumm, *An easy way to commutators in modular varieties*, Arch. Math. 34(1980), 45–54.
12. J. Hagemann and C. Herrmann, *A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity*, Arch. Math. 32(1979), 234–245.
13. C. Herrmann, *Affine algebras in congruence modular variety*, Acta. Sci. Math. 41(1979), 119–125.
14. J. Jezek and T. Kepka, *Medial groupoids*, Monograph of Acad. Praha, 1983.
15. B. Jónsson, *On the representations of lattices*, Math. Scand. 1(1953), 193–206.
16. B. Jónsson, *Modular lattices and Desargues' theorem*, Math. Scand. 2(1954), 295–314.
17. L. Klukovits, *Hamiltonian varieties of universal algebras*, Acta. Sci. Math. 34(1973), 171–174.
18. A. Mal'cev, *On the general theory of algebraic systems*, (Translation). Math. Sb. (77) 35(1954), 3–20.
19. R. Mckenzie, *Para primal varieties: A study of finite axiomatizability and definable congruences in locally finite varieties*, Alg. Univ. 8(1978), 336–348.
20. D. Murdoch, *Structure of Abelian quasigroups*, Trans. Amer. Math. Soc. 49 (1941), 392–409.
21. D. Norton, *Homiltonian loops*, Proc. Amer. Math. Soc. 3(1953), 56–65.
22. J.D.H. Smith, *Mal'cev Varieties*, Lecture notes 544, Springer–Verlag, 1976.
23. W. Taylor, *Some applications of the term condition*, Alg. Univ. 14(1982), 11-24.
24. K. Toyoda, *On Axioms of linear functions*, Proc. Imp. Acad. Tokyo, 17(1941), 211–237.

Department of Mathematics
Pusan National University
Pusan, 609–735