A CHARACTERIZATION OF MODULARITY FOR CONGRUENCE LATTICES OF ALGEBRAS*

Alan Day

(received June 28, 1968)

1. Introduction. Let us call an equational class (variety) K of algebras permutable if and only if every pair of congruences on each K-algebra is permutable. Similarly, we will call K modular (distributive) if the congruence lattice of each K-algebra is modular (distributive). Mal'cev [1] has characterized permutable equational classes by:

THEOREM. K *is permutable if and only if there exists a term (polynomial symbol),* p, *in three variables such that for every* a, b, *in each* K-*algebra*: (P1) $p(a, a, b) = b$

(P2) $p(a, b, b) = a$

Jonsson [2] has characterized distributive equational classes by:

THEOREM. K *is distributive if and only if there exists an* $n \in N$, *the set of natural numbers, and a sequence* $d_0, \ldots, d_n$ *of terms in three variables such that for every* a, b, c *in each* K-*algebra*:

(D1) $d_0(a, b, c) = a$ *and* $d_n(a, b, c) = c$,

(D2) $d_i(a, b, a) = a \ (i = 0, 1, \ldots, n)$,

(D3) $d_i(a, a, b) = d_{i+1}(a, a, b)$ (i *even*),

(D4) $d_i(a, b, b) = d_{i+1}(a, b, b)$ (i *odd*).

In this note we give a similar characterization of modular equational classes. We give definitions of n-modularity and n-distributivity that are suggested by these theorems and show that 2-modularity is equivalent to permutability and that n-distributivity implies (2n - 1)-modularity.

2. The characterization of modularity. For algebras $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$, we will use the respective upper case Latin letters A, B, C, ... to indicate the algebras' underlying set. For an algebra $\mathfrak{A}$ and $x, y \in A$, we let $\theta(x, y)$ be the smallest congruence relation on $\mathfrak{A}$ that contains

*This paper is based on a thesis submitted to McMaster University for an M.Sc. degree. The author expresses his gratitude to Professor G. Bruns for his guidance in this research.

Canad. Math. Bull. vol. 12, no. 2, 1969

(x, y). To simplify notation in this paper, we use the same symbol for a term and for its induced polynomials.

THEOREM 1. For an equational class K of algebras, the following are equivalent:

(a) K is modular;

(b) There is a natural number n and a sequence $\{m_i\}$ $(i = 0, 1, \ldots, n)$ of terms in four variables such that for every K-algebra $\mathfrak{A}$ and all $a, b, c, d \in A$

(M1) $m_0(a, b, c, d) = a$ and $m_n(a, b, c, d) = d$,

(M2) $m_i(a, b, b, a) = a \quad (i = 0, 1, \ldots, n)$,

(M3) $m_i(a, b, b, d) = m_{i+1}(a, b, b, d) \quad (i$ odd$)$,

(M4) $m_i(a, a, d, d) = m_{i+1}(a, a, d, d) \quad (i$ even$)$.

Proof. Without loss of generality, we may assume K to be non-trivial, i.e. containing at least one algebra with at least two elements.

(a) → (b). Let $\mathfrak{C}$ be an algebra with is K-freely generated by the four element set $\{a, b, c, d\}$. We define congruence relations on $\mathfrak{C}$ by:

$$\theta = \theta(b, c), \quad \psi = \theta(a, b) \vee \theta(c, d), \quad \phi = \theta(a, d) \vee \theta(b, c) .$$

By (a) we have $(a, d) \in \phi \wedge (\psi \vee (\phi \wedge \theta)) = (\phi \wedge \psi) \vee (\phi \wedge \theta)$. It follows that there exists a natural number n and a sequence $u_0, u_1, \ldots, u_n$ in $\mathfrak{C}$ satisfying:

(1) $$u_0 = a, \; u_n = d,$$

(2) $$u_i(\phi \wedge \theta) u_{i+1} \qquad (i \text{ odd}),$$

(3) $$u_i(\phi \wedge \psi) u_{i+1} \qquad (i \text{ even}).$$

Since $\mathfrak{C}$ is generated by $\{a, b, c, d\}$, there exists a sequence $m_0, m_1, \ldots m_n$ of terms in four variables such that

$$u_i = m_i(a, b, c, d) \quad (i = 0, 1, 2, \ldots, n).$$

Since every homomorphism of the term algebra in four variables into a K-algebra factors through $\mathcal{C}$ in such a way that the variables are mapped to a, b, c, d respectively, it is enough to show that the above identities hold in $\mathcal{C}$ for the free generators a, b, c, d.

(M1) follows easily from (1).

(M2): From (1), (2) and (3) above, it follows that $m_i(a, b, c, d)\ \phi\ a$ holds for all $i = 0, 1, \ldots, n$. This, together with $a\ \phi\ d$ and $b\ \phi\ c$ gives us $m_i(a, b, b, a)\ \phi\ a$. But the congruence ϕ, restricted to the subalgebra of $\mathcal{C}$ generated by $\{a, b\}$ identifies $m_i(a, b, b, a)$ and a. Therefore,

$$m_i(a, b, b, a) = a \quad (i = 0, 1, \ldots, n).$$

(M3): For i odd, we get from (2) that $m_i(a, b, c, d)\ \theta\ m_{i+1}(a, b, c, d)$. Since $b\ \theta\ c$, this gives $m_i(a, b, b, d)\ \theta\ m_{i+1}(a, b, b, d)$. Again, the congruence relation θ on the subalgebra of $\mathcal{C}$ generated by $\{a, b, d\}$ identifies $m_i(a, b, b, d)$ and $m_{i+1}(a, b, b, d)$. Therefore,

$$m_i(a, b, b, d) = m_{i+1}(a, b, b, d) \quad (i \text{ odd}) .$$

The proof of (M4) is similar.

(b) → (a): Let θ, ψ, ϕ be congruence relations on a K-algebra $\mathfrak{a}$ satisfying $\theta \le \phi$. We have to show $(\theta \vee \psi) \wedge \phi \le \theta \vee (\psi \wedge \phi)$. For each $k \in N$, let $\Delta_k = \psi \circ \theta \circ \psi \circ \ldots \circ \theta \circ \psi$ ($2k + 1$ factors). Then $(\theta \vee \psi) \wedge \phi = \bigcup_{k \in N} (\phi \cap \Delta_k)$. Hence it suffices to show that $\phi \cap \Delta_k \le \theta \vee (\psi \wedge \phi)$ for every $k \in N$. We show this by induction over k.

For $k = 0$, this is obvious. For every k, the relation Δ_k is reflexive, symmetric and compatible with all operations. It follows easily that it is also compatible with all polynomials on $\mathfrak{a}$.

For $k \ge 0$, then $(a, d) \in \phi \cap \Delta_{k+1} = \phi \cap (\psi \circ \theta \circ \Delta_k)$ implies that there exists elements $b, c \in A$ such that

$$a\ \phi\ d, \quad a\ \Delta_k\, b, \quad b\ \theta\ c, \quad c\ \psi\ d .$$

https://doi.org/10.4153/CMB-1969-016-6 Published online by Cambridge University Press

Since $\theta \leq \phi$ and $\psi \leq \Delta_k$, we also have

$$b \, \phi \, c, \quad c \, \Delta_k d .$$

Define $u_i = m_i(a, b, c, d)$ $(i = 0, 1, \ldots, n)$. By (M1), $a = u_0$ and $u_n = d$.

For i odd we have:

$$u_i = m_i(a, b, c, d) \, \theta \, m_i(a, b, b, d) = m_{i+1}(a, b, b, d) \, \theta \, u_{i+1}$$

and hence

(4) $$u_i \, \theta \, u_{i+1} \quad (i \text{ odd}) .$$

For each i, we have

$$u_i \, \phi \, m_i(a, b, b, a) = a \text{ and } a = m_i(a, a, a, a) \, \phi \, m_i(a, a, d, d).$$

Therefore,

(5) $$u_i \, \phi \, m_i(a, a, d, d) \quad (i = 0, 1, \ldots, n).$$

For i even, $u_i \, \Delta_k \, m_i(a, a, d, d) = m_{i+1}(a, a, d, d) \, \Delta_k \, u_{i+1}$.
By combining this with (5) we have

$$u_i \, \phi \cap \Delta_k \, m_i(a, a, d, d) = m_{i+1}(a, a, d, d) \, \phi \cap \Delta_k \, u_{i+1} \quad (i \text{ even}).$$

By induction hypothesis, $\phi \cap \Delta_k \leq \theta \vee (\psi \wedge \phi)$ and this gives:

(6) $$u_i \, \theta \vee (\psi \wedge \phi) \, u_{i+1} \quad (i \text{ even}) .$$

https://doi.org/10.4153/CMB-1969-016-6 Published online by Cambridge University Press

This, together with (4) yields

$$(a, d) \in \theta \vee (\theta \vee (\psi \wedge \phi)) = \theta \vee (\psi \wedge \phi)$$

which was to be proved.

3. A relation between permutability and modularity. We define an equational class to be n-modular for some $n \in N$ if there exists a sequence of $n + 1$ terms in four variables satisfying statement (b) in Theorem 1. Clearly if K is modular, K is n-modular for some $n \in N$. Conversely, for any $n \in N$ if K is n-modular then K is modular.

THEOREM 2. An equational class is permutable if and only if it is 2-modular.

Proof. If K is permutable, then by [1] there exists a term p in three variables satisfying (P1) and (P2) in every K-algebra. We define terms m_0, m_1, and m_2 in four variables by:

$$m_0(a, b, c, d) = a,$$

$$m_1(a, b, c, d) = p(a, p(a, b, c), d),$$

$$m_2(a, b, c, d) = d.$$

(M1) is satisfied by definition, and:

$$m_1(a, b, b, a) = p(a, p(a, b, b), a) = p(a, a, a) = a,$$

$$m_1(a, b, b, d) = p(a, p(a, b, b), d) = p(a, a, d) = d = m_2(a, b, b, d),$$

$$m_1(a, a, b, b) = p(a, p(a, a, b), b) = p(a, b, b) = a = m_0(a, a, b, b).$$

Therefore m_0, m_1, m_2 satisfy (M1) to (M4) and K is 2-modular.

If K is 2-modular, then by Theorem 1, there exists m_0, m_1, and m_2 satisfying the properties (M1) to (M4). We define

$$p(a, b, c) = m_1(c, c, b, a) .$$

https://doi.org/10.4153/CMB-1969-016-6 Published online by Cambridge University Press

We have

$$p(a, a, b) = m_1(b, b, a, a) = m_0(b, b, a, a) = b \text{ by (M4) and (M1) and}$$

$$p(a, b, b) = m_1(b, b, b, a) = m_2(b, b, b, a) = a \text{ by (M3) and (M1).}$$

Therefore, K is permutable.

4. A relation between distributivity and modularity. We define n-distributivity similarly to n-modularity (i.e. a sequence $d_0, \ldots, d_n$ of $n + 1$ terms in three variables satisfying (D1) to (D4) in Jónsson's Theorem). As any distributive lattice is modular, any distributive equational class is also modular. In this section we derive a sequence of terms characterizing modularity from a given sequence that determine distributivity.

THEOREM. *If an equational class* K *is* n-*distributive then it is* (2n - 1)-*modular*.

Proof. Assume K is n-distributive, i.e. there exists a sequence $d_0, \ldots, d_n$ of terms in three variables satisfying (D1) to (D4). We define for $k = 0, 1, \ldots, 2n - 1$

$$m_k(a, b, c, d) = \begin{cases} d_{(k+1)/2}(a, b, d) & k \equiv 1 \pmod 4, \\ d_{k/2}(a, c, d) & k \equiv 2 \pmod 4, \\ d_{(k+1)/2}(a, c, d) & k \equiv 3 \pmod 4, \\ d_{k/2}(a, b, d) & k \equiv 0 \pmod 4. \end{cases}$$

Now $m_0(a, b, c, d) = d_0(a, b, d) = a$ and $m_{2n-1}(a, b, c, d)$ is either $d_n(a, b, d)$ or $d_n(a, c, d)$ which are both identically d. Therefore (M1) is true. (M2) is clearly satisfied by applying (D2). For k odd, $m_k(a, b, b, d) = d_{(k+1)/2}(a, b, d) = m_{k+1}(a, b, b, d)$ and thus (M3) is satisfied.

For k even, we must consider two possible cases. If $k \equiv 2 \pmod 4$, then $\frac{k}{2}$ is odd and $k + 1 \equiv 3 \pmod 4$.

Therefore by (D4):

$$m_k(a, a, b, b) = d_{k/2}(a, b, b) = d_{(k+2)/2}(a, b, b) = m_{k+1}(a, a, b, b).$$

If $k \equiv 0 \pmod 4$ then, $k/2$ is even and $k + 1 \equiv 1 \pmod 4$. Then by (D3)

$$m_k(a, a, b, b) = d_{k/2}(a, a, b) = d_{(k+2)/2}(a, a, b) = m_{k+1}(a, a, b, b).$$

Therefore (M4) is satisfied and k is (2n - 1) modular.

Whether (2n - 1) is the best possible estimate in the above theorem is not known. We do know that in the equational class L of lattices, it can be no smaller. L is 2-distributive by the following terms:

$$d_0(a, b, c) = a,$$

$$d_1(a, b, c) = (a \vee b) \wedge (a \vee c) \wedge (b \vee c),$$

$$d_2(a, b, c) = c,$$

L is 3-modular by Theorem 3 and cannot be 2-modular by Theorem 2.

These results for permutability, modularity, distributivity, suggest the following general problem as raised by R. Wille: Can any non-trivial lattice identity that holds for all the congruence lattices of a given equational class be characterized by a sequence of equations?

REFERENCES

1. A.I. Mal'cev, On the general theory of algebraic system. Mat. Sb. (N.S.) 35 (77) (1954) 3-20.

2. B. Jónsson, Algebras who congruence lattices are distributive. Math. Scand. 21 (1967) 110-121.

3. G. Gratzer, Universal algebra. (D. Van Nostrand, to appear).

4. P.M. Cohn, Universal algebra. (Harper and Row, New York, 1965).

McMaster University
Hamilton, Ontario

https://doi.org/10.4153/CMB-1969-016-6 Published online by Cambridge University Press