ON PSEUDO-SIMPLE UNIVERSAL ALGEBRAS

DONALD MONK

A universal algebra is simple if and only if it has more than one element and there are no proper homomorphisms defined upon it. In this note we study a related notion: an algebra is *pseudo-simple* if and only if it has more than one element and is isomorphic to all its proper (i.e., non-one-element) homomorphic images. The two concepts simplicity and pseudo-simplicity are examples of concepts of irreducibility in universal algebra. Several of these notions of irreducibility may be equivalently expressed in terms of the lattice of congruence relations of the given algebra. Thus an algebra is simple if and only if the corresponding lattice is a chain of length two; sub-directly irreducible if the lattice has a smallest nonzero element; and weakly sub-directly irreducible if the non-identity congruences themselves form a lattice. It is natural to inquire about a similar equivalent expression for the notion of pseudo-simplicity.[1] In this note we characterize those lattices which can be the lattice of all congruence relations of a pseudo-simple algebra. We show that each of these lattices can also be the lattice of congruence relations on a non-pseudo-simple algebra. Thus there is no formulation of the notion of pseudo-simplicity solely in terms of the congruence lattice.

Where not otherwise stated, we shall use the notation of Birkhoff's book [2].

LEMMA. *If A is pseudo-simple, then the lattice $\mathfrak{L}(A)$ of all congruence relations on A has a smallest nonzero element.*

REMARK. As just mentioned, the conclusion means that A is sub-directly irreducible, although we shall not use this term.

PROOF. Let a and b be distinct elements of A. By Zorn's lemma there is a maximal congruence θ on A such that it is not the case that $a \equiv b(\theta)$. The algebra A/θ has more than one element, since $a/\theta \neq b/\theta$. Hence A is isomorphic to A/θ. If R is an arbitrary congruence of A/θ, then $a/\theta \equiv b/\theta(R)$. Hence the infimum of all non-identity congruences on A/θ is a non-identity congruence which is, clearly, the smallest non-identity congruence of $\mathfrak{L}(A/\theta)$. The lemma follows since A is isomorphic to A/θ.

Received by the editors May 29, 1961.

[1] The name "pseudo-simplicity", as well as the problem mentioned, were suggested by Professor Alfred Tarski during a seminar at the University of California, Berkeley, in 1959.

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

THEOREM 1. *If A is a pseudo-simple algebra, then $\mathfrak{L}(A)$ is a well-ordered chain. If the order type α of this chain is greater than 1, then α has the form $\omega^\beta+1$ for some ordinal β.*

PROOF. Assume that A is not simple.

1. **Order.** Suppose θ and θ' are incomparable congruence relations on A. In particular this implies that $A/(\theta\cap\theta')$ has more than one element and hence is isomorphic to A. But θ and θ' induce non-identity congruence relations R and R' on $A/(\theta\cap\theta')$ such that $R\cap R'$ is the identity congruence on $A/(\theta\cap\theta')$. This contradicts the lemma.

2. **Well-order (descending chain condition).** If θ_m, for positive integers m, is a strictly descending chain of congruences on A, then the infimum $\bigwedge\theta_m=\theta^*$ is a congruence such that A is isomorphic to A/θ^* while the latter is non-pseudo-simple by the lemma; this contradiction shows that there can be no such infinite descending chain.

3. **Conclusion.** Choose an ordinal γ and a function θ such that $\{\theta_\xi: \xi\leqq\gamma\}$ is the set of all congruences on A and $\theta_\xi<\theta_\eta$ whenever $\xi<\eta\leqq\gamma$. Suppose $\xi<\gamma$. Then A is isomorphic to A/θ_ξ, and it follows that $\xi+\gamma=\gamma$. This being true for every $\xi<\gamma$, γ is a γ-number, so that $\gamma=\omega^\beta$ for some ordinal β.[2] The order type of $\mathfrak{L}(A)$ is $\gamma+1=\omega^\beta+1$.

Theorem 1 gives a necessary condition for the pseudo-simplicity of an algebra A. Naturally one is inclined to ask whether there can exist a pseudo-simple algebra A with $\mathfrak{L}(A)$ of order type $\omega^\beta+1$ no matter what β is. The answer is yes, and is essentially known.

THEOREM 2 (GRÄTZER-SCHMIDT). *For each ordinal β there is a pseudo-simple lattice A such that $\mathfrak{L}(A)$ forms a well-ordered chain of order type $\omega^\beta+1$.*

For the construction, see [3, proof of Theorem 1, *Case of chains*]; they do not say that $\mathfrak{L}(A)$ for their lattice A is pseudo-simple when $\mathfrak{L}(A)$ has the required form, but this is easily seen.

The major contribution of this note is the following theorem.

THEOREM 3. *For each ordinal $\beta>0$ there is a non-pseudo-simple algebra A such that $\mathfrak{L}(A)$ is a well-ordered chain of type $\omega^\beta+1$.*

PROOF. Let $A=\omega^\beta$. We define equivalence relations ϕ and θ_η for each $\eta\leqq A$ on A by specifying their equivalence classes, as follows. The equivalence classes of ϕ are $\{1, 2\}$, $\{0\}$, and $\{\xi\}$ for $2<\xi<A$. For each $\eta\leqq A$ let the equivalence classes of θ_η be $\{\xi: \xi<1+\eta\}$ and $\{\xi\}$ for $1+\eta\leqq\xi<A$.

---

[2] See [1, p. 68].

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

Now with each equivalence relation ψ on A such that $\psi \notin \{\theta_\eta : \eta \leqq A\}$ we shall associate a unary operation $-_\psi$ on A. Obviously $\theta_A \not\leqq \psi$; hence there is a least $\gamma \leqq A$ such that $\theta_\gamma \not\leqq \psi$. Clearly $\gamma \neq 0$, and γ is not a limit ordinal, so write $\gamma = \delta + 1$. Thus $\theta_\delta < \psi$. Choose $x, y \in A$ such that $x \equiv y(\theta_\gamma)$ while $x \not\equiv y(\psi)$, and choose $u, v \in A$ such that $u \equiv v(\psi)$ and $u \not\equiv v(\theta_\delta)$. For each $t \in A$ let

$$-_\psi t = \begin{cases} x & \text{if } u \equiv t(\theta_\delta), \\ y & \text{if } u \not\equiv t(\theta_\delta). \end{cases}$$

We assert that θ_η is a congruence relation with respect to $-_\psi$, for each $\eta \leqq A$. This is obvious if $\gamma \leqq \eta$. Suppose that $\eta < \gamma$, $t_1 \equiv t_2(\theta_\eta)$, and $-_\psi t_1 \not\equiv -_\psi t_2(\theta_\eta)$. Then we have, say, $-_\psi t_1 = x$ and $-_\psi t_2 = y$. Consequently, $u \equiv t_1(\theta_\delta)$ and $u \not\equiv t_2(\theta_\delta)$; thus $t_1 \not\equiv t_2(\theta_\delta)$. On the other hand, $\eta < \gamma$ implies that $\theta_\eta \leqq \theta_\delta$ and so $t_1 \equiv t_2(\theta_\delta)$, and we have arrived at a contradiction. Thus our assertion is true.

It is also true that ψ is not a congruence with respect to $-_\psi$. For, $u \equiv v(\psi)$ but $-_\psi u = x \not\equiv y = -_\psi v(\psi)$.

Let the algebra A consist of the set A together with all the operations $-_\psi$ with ψ an equivalence relation on A such that $\psi \notin \{\theta_\eta : \eta \leqq A\}$. The congruence lattice of this algebra is, by the preceding two paragraphs, a well-ordered chain of type $\omega^\beta + 1$. A is not pseudo-simple. For, $\phi \notin \{\theta_\eta : \eta \leqq A\}$, so the operation $-_\phi$ is defined and in the algebra A. Clearly $\theta_0 < \phi$ and $\theta_1 \not\leqq \phi$. We defined $-_\phi$ by choosing $x, y \in A$ such that $x \equiv y(\theta_1)$ while $x \not\equiv y(\phi)$, choosing $u, v \in A$ such that $u \equiv v(\phi)$ and $u \not\equiv v(\theta_0)$, and defining $-_\phi t$ as above for each $t \in A$. Suppose f is an isomorphism of A/θ_1 onto A. Choose $a, b \in A$ such that $f(a/\theta_1) = u$ and $f(b/\theta_1) = v$. Since $x \equiv y(\theta_1)$ we have

$$x = -_\phi u = -_\phi f(a/\theta_1) = f(-_\phi a/\theta_1) = f(-_\phi b/\theta_1) = -_\phi f(b/\theta_1)$$
$$= -_\phi v = y,$$

which is a contradiction.

This completes the proof.[3]

The main problem left open by this note is as follows.

PROBLEM. *Characterize the notion of pseudo-simplicity intrinsically.*

This note shows that $\mathfrak{L}(A)$ is not the only intrinsic structure derived from A which needs to be considered to solve this problem. Among the other possibilities are the lattice of subalgebras and the number of argument places of the operations.

[3] It is easy to verify, moreover, that θ_η and θ_ξ are permutable for $\xi \leqq \eta \leqq A$. Hence our construction furnishes a counter-example to an assertion of Birkhoff, namely exercise 3 on p. 87 of [2].

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

REFERENCES

1. H. Bachmann, *Transfinite Zahlen*, Ergebnisse der Mathematik und ihrer Grenzgebiete (N.F.), vol. 1, Springer-Verlag, Berlin, 1955. vii+204 pp.

2. G. Birkhoff, *Lattice theory*, revised edition xiii+283 pp., Amer. Math. Soc., Providence, R. I., 1948.

3. G. Grätzer and E. T. Schmidt, *Two notes on lattice congruences*, Ann. Univ. Sci. Budapest. Eötvös. Sect. Math. 1 (1958), 83–87.

UNIVERSITY OF CALIFORNIA, BERKELEY

A NOTE ON FINITE FIELDS[1]

L. CARLITZ

1. Let q be a power of an odd prime and let $F=GF(q^n)$ denote the finite field of order q^n. Let F^* denote the multiplicative group of the nonzero elements of F and let Z be the subgroup of F^* of order $(q^n-1)/(q-1)$. It will be assumed that

$$\left(q-1, \frac{q^n-1}{q-1}\right) = 1. \tag{1}$$

Then every nonzero element ξ of F has a representation

$$\xi = \alpha\zeta \qquad (\alpha \in GF(q), \zeta \in Z), \tag{2}$$

and the representation is unique. For $\zeta \in Z$, $\zeta \neq 1$, put

$$1-\zeta = \tau(\zeta)\sigma(\zeta), \tag{3}$$

where $\tau(\zeta) \in GF(q)$, $\sigma(\zeta) \in Z$.

Put $Z_1 = Z - \{1\}$. In a letter to the writer, J. G. Thompson has raised the question whether the mapping $\zeta \to \sigma(\zeta)$ defined by (3) can be a permutation of Z_1. We shall show that the answer is negative.

Indeed let us assume that the mapping $\zeta \to \sigma(\zeta)$, is a permutation of Z_1. In view of (1) the mapping $\zeta \to \zeta^{q-1}$ is a permutation of Z_1 and consequently if we put

$$\zeta_1 = (1-\zeta)^{q-1} = (\sigma(\zeta))^{q-1},$$

then $\zeta \to \zeta_1$ is a permutation of Z_1. We recall that

Received by the editors June 29, 1961.

[1] Supported in part by National Science Foundation grant G 16485.

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use