A NOTE ON THE UNIQUE FACTORIZATION OF ABSTRACT ALGEBRAS

FREDERICK B. THOMPSON

In their monograph[1] *Direct decompositions of finite algebraic systems*, Jónsson and Tarski have established the unique factorization theorem and several related results for a comprehensive class of finite abstract algebras. Every algebra $\mathfrak{A}$ of this class is constituted by a set A of arbitrary elements, by a binary operation $+$, and possibly by other operations 0_0, 0_1, $\cdots$; the only conditions imposed on $\mathfrak{A}$ are that A be closed under all the operations involved and that it contain an element z which is a (both-hand) zero element for the operation $+$ and is idempotent under the remaining operations. At the end of their paper, Jónsson and Tarski raised the problem of whether their results can be extended to an even more comprehensive class of algebras, in fact to algebras $\mathfrak{A}$ differing from those mentioned above in that the element z is only to be idempotent under all operations involved (not necessarily being a zero element for $+$). The purpose of this note is to show that the solution of the problem just mentioned is a negative one.

We consider algebras $\mathfrak{A}_{p,t}$ defined in the following way: p and t are positive integers; $\mathfrak{A}_{p,t}$ is constituted by the set A_t of all non-negative integers less than t, and by the operation $\oplus_p$ defined by the following formula:

$$(hp + m) \oplus_p (kp + n) = mp + n$$

where h, k, m, and n are non-negative integers, $m < p$ and $n < p$. In particular, $u \oplus_1 v = 0$ for all non-negative integers u and v. In what follows we shall be interested in only those algebras $\mathfrak{A}_{p,t}$ in which $p \mid t$ and $p^2 \leqq t$; we denote by K the class of all such algebras. As is easily seen, in every algebra $\mathfrak{A}_{p,t}$ of K the set of all elements A_t is closed under the operation $\oplus_p$ and contains an element, in fact 0, which is idempotent under this operation. The following two theorems express the fundamental properties of the algebras of the class K with respect to cardinal multiplication.

Presented to the Society, November 27, 1948; received by the editors September 27, 1948.

[1] B. Jónsson and A. Tarski, *Direct decompositions of finite algebraic systems*, Notre Dame Mathematical Lectures, No. 5, Notre Dame, Indiana, 1947. The notations of this monograph are applied in the present note, except that the relation of isomorphism between two algebras is denoted by the symbol $\cong$.

THEOREM 1. *If* $\mathfrak{A}_{m,r}$ *and* $\mathfrak{A}_{n,s}$ *are any two algebras in* K, *then* $\mathfrak{A}_{mn,rs}$ *is also an algebra in* K *and we have* $\mathfrak{A}_{mn,rs} \cong \mathfrak{A}_{m,r} \times \mathfrak{A}_{n,s}$.

PROOF. The first part of the conclusion is obvious. To obtain the second part, remember that $m \mid r$, and hence $r = um$ for some positive integer u. Consider any two elements: h of the algebra $\mathfrak{A}_{m,r}$ and k of the algebra $\mathfrak{A}_{n,s}$. Clearly we can write h and k in the forms $h = h_0 m + h_1$, $k = k_0 n^2 + k_1 n + k_2$, where $h_1 < m$, $k_1 < n$, $k_2 < n$. We now correlate with the ordered couple h, k the number:

$$f(h, k) = (k_0 un + h_0 n + k_1)mn + (h_1 n + k_2).$$

It is now a routine matter to check that this correlation establishes the desired isomorphism.

THEOREM 2. *Let* $\mathfrak{A}_{p,t}$ *be an algebra in the class* K, *and let* $\mathfrak{B}$ *and* $\mathfrak{C}$ *be any two algebras each constituted by a set of elements and a binary operation. If*

$$\mathfrak{A}_{p,t} \cong \mathfrak{B} \times \mathfrak{C},$$

then there are algebras $\mathfrak{A}_{m,r}$ and $\mathfrak{A}_{n,s}$ *in* K *such that*

$$\mathfrak{B} \cong \mathfrak{A}_{m,r}, \qquad \mathfrak{C} \cong \mathfrak{A}_{n,s}.$$

PROOF. Let $\mathfrak{B}$ consist of the set B of r elements and the binary operation $\bigcirc$; let $\mathfrak{C}$ consist of the set C of s elements and the binary operation $\square$. Clearly $rs = t$. Let f map $\mathfrak{B} \times \mathfrak{C}$ isomorphically onto $\mathfrak{A}_{p,t}$. For $b \in B$, let B_b denote the set of non-negative integers $a < p$ for which $f(b, c) \equiv a \pmod{p}$ for some $c \in C$. Similarly C_c will denote the set of non-negative integers $a < p$ for which $f(b, c) \equiv a \pmod{p}$ for some $b \in B$.

(1) For $b_1, b_2 \in B$, the sets B_{b_1} and B_{b_2} are either disjoint or identical.

For suppose $a_1 \in B_{b_1} \cap B_{b_2}$ (that is, a_1 is in the common part of B_{b_1} and B_{b_2}), $a_2 \in B_{b_1}$, $a_2 \notin B_{b_2}$. Then there are integers a_1', a_1'', a_2', a_3, a_3' such that

$$f(b_1, c_1) = a_1' p + a_1, \qquad f(b_2, c_1') = a_1'' p + a_1,$$
$$f(b_1, c_2) = a_2' p + a_2, \qquad f(b_2, c_2) = a_3' p + a_3,$$

for some c_1, c_1', $c_2 \in C$. We see that $a_3 \in B_{b_2}$, thus $a_3 \neq a_2$.

$$\begin{aligned} f(b_1 \bigcirc b_1, c_1 \square c_1) &= f(b_1, c_1) \oplus f(b_1, c_1) = (a_1' p + a_1) \oplus (a_1' p + a_1) \\ &= a_1 p + a_1 = (a_1'' p + a_1) \oplus (a_1'' p + a_1) \\ &= f(b_2, c_1') \oplus f(b_2, c_1') = f(b_2 \bigcirc b_2, c_1' \square c_1'). \end{aligned}$$

Therefore since f is biunique, $b_1 \bigcirc b_1 = b_2 \bigcirc b_2$. Thus, by a similar manipulation:

$$a_2 p + a_2 = f(b_1 \bigcirc b_1, c_2 \square c_2) = f(b_2 \bigcirc b_2, c_2 \square c_2) = a_3 p + a_3.$$

Consequently $a_2 = a_3$, which contradicts the above assertion that $a_2 \neq a_3$.

(2) For $c \in C$ and $b \in B$, the set $C_c \cap B_b$ contains exactly one element.

Indeed, let $f(b, c) = a'p + a$; thus $a \in C_c \cap B_b$. Suppose $a_1 \neq a$ were also in $C_c \cap B_b$. Thus for some b_1 and c_1, $f(b_1, c) = a_1' p + a_1$ and $f(b, c_1) = a_1'' p + a_1$. Thus

$$f(b_1 \bigcirc b_1, c \square c) = a_1 p + a_1 = f(b \bigcirc b, c_1 \square c_1);$$

and since f is biunique, $b \bigcirc b = b_1 \bigcirc b_1$, $c \square c = c_1 \square c_1$. Therefore

$$f(b \bigcirc b, c \square c) = ap + a = a_1 p + a_1$$

and $a = a_1$.

(3) For $b_1, b_2 \in B$, the sets B_{b_1} and B_{b_2} have the same number of elements.

For suppose $B_{b_1} = \{a_1, a_2, \cdots, a_n\}$, $B_{b_2} = \{a_1', \cdots, a_m'\}$, with $n > m$. Let $c_i \in C$ be such that $C_{c_i} \cap B_{b_1} = \{a_i\}$ for $i = 1, \cdots, n$. Clearly $C_{c_i} \cap B_{b_2} = C_{c_j} \cap B_{b_2}$ for some i, j, $i \neq j$. Therefore C_{c_i} and C_{c_j} are neither disjoint nor, by (2), are they identical, thus contradicting (1).

(4) For $b \in B$, let b/C be the set of all $f(b, c)$ for $c \in C$. Either B_b and b/C are disjoint or $B_b \subset b/C$.

Suppose $a_1 \in B_b \cap b/C$ and $a_2 \in B_b$. Then, for some c_1, $c_2 \in C$ and integer a_2', $f(b, c_1) = a_1$, $f(b, c_2) = a_2' p + a_2$. Let b_0, c_0 be such that $f(b_0, c_0) = 0$. Thus $f(b_0 \bigcirc b, c_0 \square c_1) = 0 \oplus a_1 = a_1$; therefore $b_0 \bigcirc b = b$. Consequently

$$f(b, c_0 \square c_2) = f(b_0 \bigcirc b, c_0 \square c_2) = 0 \oplus (a_2' p + a_2) = a_2;$$

and $a_2 \in b/C$.

Let n be the number of elements in each B_b; let m be the number of elements in each C_c.

$$mn = p. \tag{5}$$

This follows immediately from (1) and (2).

$$m^2 \leqq r; \qquad n^2 \leqq s. \tag{6}$$

Suppose $a_1, a_2 \in B_b$. Thus $f(b, c_1) = a_1' p + a_1$, $f(b, c_2) = a_2' p + a_2$. $f(b \bigcirc b, c_1 \square c_2) = a_1 p + a_2$. Therefore the set $b \bigcirc b/C$ of all $f(b \bigcirc b, c)$ for

$c \in C$ contains at least n^2 elements. But $b \bigcirc b/C$ contains s elements. Thus $n^2 \leqq s$. Similarly $m^2 \leqq r$.

$$m \mid r; \qquad n \mid s. \tag{7}$$

For some $b_0 \in B$, consider B_{b_0}. There are nt/p elements of A_t whose residues mod p are in B_{b_0}. If k is the number of sets b/C such that $B_{b_0} = B_b$, then $nt/p = ks$, since b/C contains s elements. Thus $k = nt/ps = nrs/nms = r/m$; therefore $m \mid r$. Similarly $n \mid s$.

$$\mathfrak{B} \cong \mathfrak{A}_{m,r}; \qquad \mathfrak{C} \cong \mathfrak{A}_{n,s}. \tag{8}$$

By (1), (3), (4), and (5), we see that there are just m elements $b \in B$ such that $B_b \subset b/C$. Let these elements be $b_0, b_1, \cdots, b_{m-1}$, where the numbering is arbitrary except that $0 \in B_{b_0}$. Let $b_i \bigcirc b_j = b_{im+j}$, $i, j < m$. It is easily checked that this definition is permissible. For each i, $0 \leqq i < m$, we assign (in arbitrary order) indices m^2+i, m^2+m+i, m^2+2m+i, $\cdots$, $r-m+i$ to all those elements $b \in B$ which have not been previously numbered and for which $B_b = B_{b_i}$. Let $\phi(b_i) = i$. Clearly ϕ is biunique on B to A_r, the set of elements of $\mathfrak{A}_{m,r}$. Consider $b_{hm+k}, b_{um+v} \in B$, $k, v < m$;

$$\begin{aligned} f(b_{hm+k} \bigcirc b_{um+v}, c \square c') &= (k'p + k) \oplus (v'p + v) = kp + v \\ &= f(b_k \bigcirc b_v, c'') = f(b_{km+v}, c'') \end{aligned}$$

for some $c'' \in C$. Thus $b_{hm+k} \bigcirc b_{um+v} = b_{km+v}$. Therefore

$$\phi(b_{hm+k} \bigcirc b_{um+v}) = \phi(b_{hm+k}) \oplus_m \phi(b_{um+v}).$$

Consequently $\mathfrak{B} \cong \mathfrak{A}_{m,r}$. Similarly $\mathfrak{C} \cong \mathfrak{A}_{n,s}$.

The theorem is now a consequence of (5), (6), (7), and (8).

If, instead of algebras $\mathfrak{A}_{p,t}$ of the class K, we speak of their isomorphism types $\alpha_{p,t}$, and denote the class of all such isomorphism types by K', then an essential part of the contents of Theorems 1 and 2 can be expressed in the following way.

COROLLARY 3. *The cardinal product $\beta \times \gamma$ of two isomorphism types is in K' if and only if both β and γ are in K'.*

Furthermore, in each particular case we can easily determine whether an isomorphism type $\alpha_{p,t}$ is decomposable and can describe all of its decompositions into indecomposable factors. We apply here Theorems 1 and 2 and make use of the obvious facts that $\alpha_{1,1}$ is the unit type (the isomorphism type of a one element algebra) and that two isomorphism types $\alpha_{m,r}$ and $\alpha_{n,s}$ are identical if and only if $m = n$ and $r = s$. In this way we see, for instance, that the isomorphism

type $\alpha_{2,4}$ is indecomposable; $\alpha_{2,8}$ has, apart from order, the unique decomposition into indecomposable factors:

$$\alpha_{2,8} = \alpha_{1,2} \times \alpha_{2,4};$$

and finally $\alpha_{2,12}$ has two different decompositions into indecomposable factors:

$$\alpha_{2,12} = \alpha_{2,6} \times \alpha_{1,2} = \alpha_{2,4} \times \alpha_{1,3}.$$

Thus the last example shows that the refinement theorems 4.7 and 4.8, as well as the unique factorization theorem 4.9, of Jónsson and Tarski cannot be extended to algebras which have an idempotent element but not a zero element. The problem whether the cancellation theorem 4.10 can be extended to such algebras still remains open.

UNIVERSITY OF CALIFORNIA

NOTE ON A PAPER BY C. E. RICKART

R. P. DILWORTH AND MORGAN WARD

In a recent issue of this Bulletin,[1] C. E. Rickart proves the following two theorems:

THEOREM 1. *Any one-to-one multiplicative mapping of a Boolean ring onto an arbitrary ring is necessarily additive.*

THEOREM 3. *Any one-to-one meet preserving mapping of a distributive lattice onto a distributive lattice is also join preserving.*

We should like to point out that both of these theorems are simple consequences of the following well known principle of lattice theory:

Any one-to-one mapping of one lattice onto another lattice which preserves order both ways is a lattice isomorphism.

Now a one-to-one meet preserving mapping of one lattice onto another preserves order both ways; for if x and x' denote corresponding elements,

$$a \geqq b \rightleftarrows a \cap b = b \rightleftarrows a' \cap b' = b' \rightleftarrows a' \geqq b'.$$

CALIFORNIA INSTITUTE OF TECHNOLOGY

Received by the editors September 20, 1948.

[1] Vol. 54 (1948) pp. 758–764.