ON FINITE GROUPOIDS AND $\mathscr{K}$-PRIME ALGEBRAS[1]

BY

RALPH McKENZIE

Introduction. By an *algebra* we shall here mean a system $\mathfrak{A}=\langle A; f_\kappa\rangle_{\kappa<\alpha}$ consisting of a nonempty set A and a sequence of finitary operations f_κ on A indexed by an ordinal α. The algebra $\mathfrak{A}$ is of type τ if τ is an α-termed sequence of nonnegative integers and for every $\kappa<\alpha$, the rank of f_κ is τ_κ. $\mathscr{K}_\tau$ denotes the class of all algebras of type τ. In what follows, no further restrictions are assumed other than those explicitly stated. However, we will employ common notation and concepts from the theory of algebras without a formal introduction.

In the study of direct decompositions of algebras, attention has thus far been mainly directed to the *unique factorization property* and to various *refinement properties*. For definitions, results and further bibliographical references concerning these properties see [2], [4], [6] and especially [5]. This paper deals with a closely related notion, the concept of a prime algebra. Let $\mathscr{K}\subseteq\mathscr{K}_\tau$. An algebra $\mathfrak{A}$ is said to be $\mathscr{K}$-prime or prime in the class $\mathscr{K}$, provided that $\mathfrak{A}\in\mathscr{K}$, $|A|>1$ and whenever $\mathfrak{B},\mathfrak{C}\in\mathscr{K}$, $\mathfrak{A}|\mathfrak{B}\times\mathfrak{C}$ implies $\mathfrak{A}|\mathfrak{B}$ or $\mathfrak{A}|\mathfrak{C}$. Here $\mathfrak{A}|\mathfrak{B}$ means that there exists $\mathfrak{D}$ such that $\mathfrak{B}\cong\mathfrak{A}\times\mathfrak{D}$[2].

Assume that $\mathscr{K}$ has the following properties. (I) Whenever $\mathfrak{A}\times\mathfrak{B}\in\mathscr{K}$, then $\mathfrak{A}\in\mathscr{K}$. (II) Whenever $\mathfrak{A}\cong\mathfrak{B}\in\mathscr{K}$, then $\mathfrak{A}\in\mathscr{K}$. Then it is clear that every finite $\mathscr{K}$-prime algebra is directly indecomposable. In [6] it is proved for certain extensive classes $\mathscr{K}$ that conversely every nontrivial finite directly indecomposable algebra in $\mathscr{K}$ is $\mathscr{K}$-prime. On the other hand, as observed in the same monograph [6, p. 60], the properties of being $\mathscr{K}$-prime and of being indecomposable are not so simply related for infinite algebras in these same classes. Of course, assuming (I) and (II), if every algebra in $\mathscr{K}$ is finite and has the unique factorization property and if $\mathscr{K}$ is closed under.the taking of direct products of finitely many algebras, then $\mathscr{K}$-prime algebras and nontrivial indecomposable algebras in $\mathscr{K}$ are the same.

This paper is mainly concerned with the determination of the $\mathscr{K}$-prime algebras in case $\mathscr{K}$ is either $\mathscr{K}_\tau$ or the class of all finite algebras of type τ. In the former case a complete solution is easily obtained from our results. In the finite case our results are far from complete.

Received by the editors August 15, 1966 and, in revised form, October 5, 1966.

[1] Research supported by the National Science Foundation. The author thanks Professor Donald Monk for many helpful suggestions. Most of the results contained herein were announced in McKenzie [7], [8].

[2] This definition, as well as the problem of the existence of prime algebras in the most general classes, was formulated in correspondence by Alfred Tarski.

The principal theorem in §1 states that if the type τ includes at least one operation of positive rank, then there are no $\mathscr{K}_\tau$-prime algebras. A similar result for certain equational subclasses of $\mathscr{K}_\tau$ is included for completeness.

The main result is attained in §2. Let $\tau=\langle 2\rangle$ so that $\mathscr{K}_\tau$ is the class of all groupoids.

THEOREM. *Let* $\mathfrak{G}=\langle G, \cdot\rangle$ *be a group and let* $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ *be finite groupoids such that* $\mathfrak{A}\times\mathfrak{B}\cong\mathfrak{G}\times\mathfrak{C}$. *Then* $\exists\mathfrak{G}'$, $\mathfrak{G}''$, $\mathfrak{A}'$, $\mathfrak{B}'$ *such that* $\mathfrak{G}\cong\mathfrak{G}'\times\mathfrak{G}''$, $\mathfrak{C}\cong\mathfrak{A}'\times\mathfrak{B}'$, $\mathfrak{A}\cong\mathfrak{A}'\times\mathfrak{G}'$ *and* $\mathfrak{B}\cong\mathfrak{B}'\times\mathfrak{G}''$.

The proof of this theorem requires a simple but involved counting argument. As an immediate corollary: *Every finite indecomposable group with more than one element is prime in the class of all finite groupoids.* This theorem and corollary are valid for loops as well as for groups.

In §3 we apply the refinement theorem of §2 to derive the unique factorization property for certain finite semigroups; more explicitly, for finite groupoids $\mathfrak{A}=\langle A, \cdot\rangle$ satisfying the following two conditions: (1) For every $x, y, z\in A$, $x\cdot(y\cdot z)=(x\cdot y)\cdot z$; (2) Whenever $x\neq y$, $x, y\in A$, there exist $u, v\in A$ depending on x and y, such that $x\cdot u\neq y\cdot u$ and $v\cdot x\neq v\cdot y$.

The problem of the existence of prime algebras in the class of all finite algebras of type τ, where τ is unrestricted, remains unsettled. This problem, the possibility of extending the results presented here, and other topics are discussed in §4.

1. **Algebras prime in their similarity type.** Throughout this section, α denotes a nonzero ordinal number, $\tau\in{}^{\alpha}\omega$ and $\mathscr{K}_\tau$ denotes the class of all algebras of type τ. We assume additionally that $\tau_0>0$.

DEFINITION 1.1. If $\mathscr{K}\subseteq\mathscr{K}_\tau$, then $\mathscr{K}^p$ is the class of all $\mathscr{K}$-prime algebras. $\mathfrak{A}\in\mathscr{K}^p$ iff $\mathfrak{A}\in\mathscr{K}$, A has more than one element and whenever $\mathfrak{B}$, $\mathfrak{C}\in\mathscr{K}$, $\mathfrak{A}|\mathfrak{B}\times\mathfrak{C}$ implies that $\mathfrak{A}|\mathfrak{B}$ or $\mathfrak{A}|\mathfrak{C}$.

THEOREM 1.1. $(\mathscr{K}_\tau)^p=0$.

The characterization of $\mathscr{K}_\sigma$-prime algebras in the cases not covered by Theorem 1.1 is very easy, and of little interest. The proof of this theorem does not lie very deep. In order to prove it, we adopt the following conventions and definitions: Every cardinal number $\mathfrak{m}$ is a set—$\mathfrak{m}$ is the set of all ordinals of cardinal number $<\mathfrak{m}$. If A is a set, then $|A|$ is the cardinal number of A.

DEFINITION 1.2. (1) Let $\mathfrak{m}>0$ be a cardinal number. Then $\mathfrak{D}_{\mathfrak{m}}=\langle\mathfrak{m}; f_\kappa\rangle_{\kappa<\alpha}$ is defined by letting $f_\kappa(x)=0$ for every $\kappa<\alpha$, $x\in{}^{\tau_\kappa}\mathfrak{m}$.

(2) If $\mathfrak{A}\in\mathscr{K}_\tau$, then $R_{\mathfrak{A}}=\{y\in A : (\exists\kappa<\alpha)(\exists x\in{}^{\tau_\kappa}A)(f_\kappa(x)=y)\}$.

(3) If $\mathfrak{A}\in\mathscr{K}_\tau$, then $\sim_{\mathfrak{A}}$ is the congruence relation on $\mathfrak{A}$ determined by setting $w\sim_{\mathfrak{A}}x$ if and only if for every $\kappa<\alpha$, $i<\tau_\kappa$, $y\in{}^{i}A$ and $z\in{}^{\tau_\kappa-i-1}A$, it is true that

$$f_\kappa(y^\frown\langle w\rangle^\frown z) = f_\kappa(y^\frown\langle x\rangle^\frown z).$$

To illustrate these notions, we observe that if $\alpha=1$ and $\tau_0=2$ (i.e. if $\mathscr{K}_\tau$ is the class of all groupoids) then for $\mathfrak{A}\in\mathscr{K}_\tau$, $w, x\in A$,

$$w \sim_{\mathfrak{A}} x \leftrightarrow (\forall y\in A)(f_0(y, w) = f_0(y, x) \wedge f_0(w, y) = f_0(x, y)).$$

Also note that $\sim_{\mathfrak{D}_\mathfrak{m}} = {}^2\mathfrak{m}$ and that, for arbitrary $\mathfrak{A}\in\mathscr{K}_\tau$, $\sim_{\mathfrak{A}} = {}^2A$ if and only if for every $\kappa<\alpha$, $f_\kappa^{\mathfrak{A}}$ is constant. Finally, observe that $\mathfrak{A}\cong\mathfrak{D}_{|A|}$ if and only if $|R_{\mathfrak{A}}|=1$.

LEMMA 1.1. *If* $\mathfrak{m}>0$, *then* $\mathfrak{D}_\mathfrak{m}\notin(\mathscr{K}_\tau)^p$.

Proof. If $\mathfrak{m}=1$, then $\mathfrak{D}_\mathfrak{m}\notin(\mathscr{K}_\tau)^p$ by convention. We require two cases.

Case 1. $1<\mathfrak{m}<\aleph_0$. Define $\mathfrak{A}$, $\mathfrak{B}\in\mathscr{K}_\tau$. $\mathfrak{A}=\langle\mathfrak{m}^2; f_\kappa^{\mathfrak{A}}\rangle_{\kappa<\alpha}$ where $f_\kappa^{\mathfrak{A}}(x)=0$ if $\kappa>0$ and $x\in{}^{\tau_\kappa}(\mathfrak{m}^2)$; while

$$f_0^{\mathfrak{A}}(\langle i\cdot\mathfrak{m}+j\rangle^\frown x) = i$$

if $0\leqq i, j<\mathfrak{m}$ and $x\in{}^{\tau_0-1}(\mathfrak{m}^2)$. $\mathfrak{B}=\langle\mathfrak{m}\cdot(\mathfrak{m}+1); f_\kappa^{\mathfrak{B}}\rangle_{\kappa<\alpha}$ where $f_\kappa^{\mathfrak{B}}(x)=0$ if $\kappa>0$ and $x\in{}^{\tau_\kappa}(\mathfrak{m}\cdot(\mathfrak{m}+1))$; while

$$f_0^{\mathfrak{B}}(\langle i\cdot(\mathfrak{m}+1)+j\rangle^\frown x) = i$$

if $0\leqq i<\mathfrak{m}$, $0\leqq j\leqq\mathfrak{m}$ and $x\in{}^{\tau_0-1}(\mathfrak{m}\cdot(\mathfrak{m}+1))$.

Then $\mathfrak{D}_\mathfrak{m}\times\mathfrak{B}\cong\mathfrak{D}_{\mathfrak{m}+1}\times\mathfrak{A}$. The isomorphism takes

$$\begin{aligned} (i, j\cdot(\mathfrak{m}+1)+k) &\to (k, j\cdot\mathfrak{m}+i), \qquad 0 < j < \mathfrak{m}, \quad 0\leqq k\leqq\mathfrak{m},\\ (i, k) &\to (i, k), \qquad 0\leqq k<\mathfrak{m},\\ (i, \mathfrak{m}) &\to (\mathfrak{m}, i). \end{aligned}$$

But $\mathfrak{D}_\mathfrak{m}\nmid\mathfrak{D}_{\mathfrak{m}+1}$ since $\mathfrak{m}\nmid(\mathfrak{m}+1)$, and $\mathfrak{D}_\mathfrak{m}\nmid\mathfrak{A}$ since $0/\sim_{\mathfrak{A}}=\{0, 1, \ldots, \mathfrak{m}-1)\subseteq R_{\mathfrak{A}}$. Hence $\mathfrak{D}_\mathfrak{m}\notin\mathscr{K}_\tau^p$.

Case 2. $\mathfrak{m}\geqq\aleph_0$. Let t be any bijection from $\mathfrak{m}$ onto $\mathfrak{m}^2$ $(=\mathfrak{m}\times\mathfrak{m})$, and let s be any bijection from $\mathfrak{m}$ onto $(\mathfrak{m}\sim\{0\})\times\mathfrak{m}$. Define $\mathfrak{B}\in\mathscr{K}_\tau$. $\mathfrak{B}=\langle\mathfrak{m}\times\mathfrak{m}; f_\kappa^{\mathfrak{B}}\rangle_{\kappa<\alpha}$, where $f_\kappa^{\mathfrak{B}}(x)=(0, 0)$ if $\kappa>0$ and $x\in{}^{\tau_\kappa}(\mathfrak{m}\times\mathfrak{m})$; while

$$f_0^{\mathfrak{B}}(\langle(x, y)^\frown\rangle z) = t(x),$$

if $x, y\in\mathfrak{m}$ and $z\in{}^{\tau_0-1}(\mathfrak{m}\times\mathfrak{m})$.

Then $\mathfrak{D}_2\times\mathfrak{B}\cong\mathfrak{D}_\mathfrak{m}\times\mathfrak{B}$. The isomorphism:

$$\begin{aligned} (0, (x, y)) &\to (0, (x, y)),\\ (1, (x, y)) &\to (s_0(y), (x, s_1(y))) \end{aligned}$$

where $s(y)=(s_0(y), s_1(y))$. This concludes the proof for Case 2, since $\mathfrak{D}_\mathfrak{m}\nmid\mathfrak{D}_2$ and $\mathfrak{D}_\mathfrak{m}\nmid\mathfrak{B}$ $(R_{\mathfrak{B}}=B)$. Q.E.D.

LEMMA 1.2. *If* $\mathfrak{A}$ *is finite, then* $\mathfrak{A}\notin\mathscr{K}_\tau^p$.

Proof. By Lemma 1.1, we may assume that $|R_{\mathfrak{A}}|>1$ and that (consequently) $1<|A|<\aleph_0$. Pick $x_0\in A$ and let $\mathfrak{B}\in\mathscr{K}_\tau$ with $\mathfrak{A}\subset\mathfrak{B}$, $B=A\cup\{y_0\}$, $y_0\notin A$ and

$x_0 \sim_{\mathfrak{B}} y_0$. Clearly $\mathfrak{B}$ exists. There exists an isomorphism

$$\mathfrak{A} \times \mathfrak{D}_{\aleph_0} \cong \mathfrak{B} \times \mathfrak{D}_{\aleph_0}$$

which acts as follows:

$(x, 0) \to (x, 0)$, $x \in A$;

$(x/\sim_{\mathfrak{A}}) \times (\omega \sim \{0\}) \to (x/\sim_{\mathfrak{B}}) \times (\omega \sim \{0\})$, $x \in A$ and not $x \sim_{\mathfrak{A}} x_0$;

$(x_0/\sim_{\mathfrak{A}}) \times (\omega \sim \{0\}) \to [(x_0/\sim_{\mathfrak{B}}) \times (\omega \sim \{0\})] \cup \{(y_0, 0)\}$.

Since $|R_{\mathfrak{A}}| > 1$, $\mathfrak{A} \nmid \mathfrak{D}_{\aleph_0}$. Since $|B| = |A| + 1 < \aleph_0$, $\mathfrak{A} \nmid \mathfrak{B}$. Q.E.D.

Lemma 1.3. *If* $\sim_{\mathfrak{A}} \neq {}^2A$ *then* $\mathfrak{A} \notin \mathscr{K}_\tau^p$.

Proof. Let $\mathfrak{A} \in \mathscr{K}_\tau$ with $\sim_{\mathfrak{A}} \neq {}^2A$. Pick $x_0 \in A$ and let $\mathfrak{B} \in \mathscr{K}_\tau$ with $\mathfrak{A} \subset \mathfrak{B}$, $|B| = \mathfrak{m} > |A| \cup \aleph_0$ and $B \sim A \subset x_0/\sim_{\mathfrak{B}}$. Up to isomorphism over $\mathfrak{A}$ exactly one such $\mathfrak{B}$ exists for each $\mathfrak{m}$.

It is easily seen, as in the proof of Lemma 1.2, that

$$\mathfrak{A} \times \mathfrak{D}_{\mathfrak{m}} \cong \mathfrak{B} \times \mathfrak{D}_{\mathfrak{m}}.$$

Now, $\mathfrak{A} \nmid \mathfrak{D}_{\mathfrak{m}}$ since $\sim_{\mathfrak{A}} \neq {}^2A$. Suppose $\mathfrak{A} \times \mathfrak{C} \cong \mathfrak{B}$ for some $\mathfrak{C}$. Then, since $|x_0/\sim_{\mathfrak{B}}| = \mathfrak{m} > |A| \cup \aleph_0$, there exists $c \in C$ such that $|c/\sim_{\mathfrak{C}}| = \mathfrak{m}$. But since $\sim_{\mathfrak{A}} \neq {}^2A$, there exist $x, y \in \mathfrak{A} \times \mathfrak{C}$ such that $x \not\sim_{\mathfrak{A} \times \mathfrak{C}} y$ and $|x/\sim_{\mathfrak{A} \times \mathfrak{C}}| = |y/\sim_{\mathfrak{A} \times \mathfrak{C}}| = \mathfrak{m}$. But in $\mathfrak{B}$, there is only one set $x/\sim_{\mathfrak{B}}$ $(= x_0/\sim_{\mathfrak{B}})$ with $|x/\sim_{\mathfrak{B}}| = \mathfrak{m}$. Hence $\mathfrak{A} \nmid \mathfrak{B}$ and $\mathfrak{A} \notin \mathscr{K}_\tau^p$. Q.E.D.

We will now complete the proof of Theorem 1.1 by considering the cases not excluded by the preceding three lemmas. Thus we assume $\mathfrak{A} \in \mathscr{K}_\tau$, $|A| \geqq \aleph_0$, $\sim_{\mathfrak{A}} = {}^2A$ and $|R_{\mathfrak{A}}| = \mathfrak{n} > 1$. For every $\kappa < \alpha$, $f_\kappa^{\mathfrak{A}}$ is a constant operation, and we denote the value of the constant by $\bar{f}_\kappa$ $(\bar{f}_\kappa \in A)$. Thus $R_{\mathfrak{A}} = \{\bar{f}_\kappa : \kappa < \alpha\}$. The argument splits into two additional cases:

In the first case, $R_{\mathfrak{A}} \neq A$. Let $\mathfrak{R}_{\mathfrak{A}} = < R_{\mathfrak{A}}, f_\kappa^{\mathfrak{A}} \restriction R_{\mathfrak{A}} >_{\kappa < \alpha}$. Clearly $\mathfrak{R}_{\mathfrak{A}} \in \mathscr{K}_\tau$. Also

$$\mathfrak{A} \times \mathfrak{D}_{|A|} \cong \mathfrak{R}_{\mathfrak{A}} \times \mathfrak{D}_{|A|}.$$

Moreover $\mathfrak{A} \nmid \mathfrak{D}_{|A|}$ since $|R_{\mathfrak{A}}| > 1$; and $\mathfrak{A} | \mathfrak{R}_{\mathfrak{A}}$ since $R_{\mathfrak{A}} \neq A$ while $R_{\mathfrak{R}_{\mathfrak{A}}} =$ "universe of $\mathfrak{R}_{\mathfrak{A}}$" $(= R_{\mathfrak{A}})$. Hence $\mathfrak{A} \notin \mathscr{K}_\tau^p$.

In case $R_{\mathfrak{A}} = A$, let x_1, x_2, x_3 be three distinct members of A, say $x_j = \bar{f}_{\iota_j} (j = 1, 2, 3)$. Let θ be the equivalence relation on A which identifies x_1 with x_2 with no further identification. Let ψ be the similar minimal equivalence relation identifying x_2 with x_3. Since $\sim_{\mathfrak{A}} = {}^2A$, θ, ψ are congruence relations on $\mathfrak{A}$. It is clear that if $\mathfrak{B} = \mathfrak{A}/\theta \times \mathfrak{A}/\psi$, then $\mathfrak{A} \cong \mathfrak{R}_{\mathfrak{B}}$ as in the last paragraph. Hence $\mathfrak{A} \times \mathfrak{D}_{|A|} \cong \mathfrak{A}/\theta \times \mathfrak{A}/\psi \times \mathfrak{D}_{|A|}$ also as above. Now $\mathfrak{A} \nmid \mathfrak{A}/\theta$ since $\bar{f}_{\iota_1} \neq \bar{f}_{\iota_2}$ while $f_{\iota_1}^{\mathfrak{A}/\theta} = f_{\iota_2}^{\mathfrak{A}/\theta}$. Similarly, $\mathfrak{A} \nmid (\mathfrak{A}/\psi \times \mathfrak{D}_{|A|})$. Thus $\mathfrak{A} \notin \mathscr{K}_\tau^p$. This concludes our proof of Theorem 1.1.

The more general theorem which follows is easily derived from an examination of the preceding argument.

Theorem 1.2. *Let $\mathscr{E}$ be any equational subclass of $\mathscr{K}_\tau$ containing the algebra $\mathfrak{D}_2$. Then for every $\mathscr{E}$-prime algebra $\mathfrak{A}$, $\mathfrak{A} \cong \mathfrak{D}_{|A|}$.*

Note that the assumption $\mathfrak{D}_2 \in \mathscr{E}$ actually implies that $\mathfrak{D}_{\mathfrak{m}} \in \mathscr{E}$ for every cardinal $\mathfrak{m}$ and is equivalent to the assumption that no nontrivial equation holding in $\mathscr{E}$ has a variable for one of its terms.

2. **Finite groups and groupoids.** Throughout this section, $\mathscr{K}$ denotes $\mathscr{K}_{\langle 2\rangle}$. Members of $\mathscr{K}$, written as ordered pairs $\mathfrak{A}=\langle A, \circ\rangle$, are called groupoids. $\mathscr{G}$ denotes the subclass of groups. We use the notation $\mathscr{K}_\omega$, for the class of finite algebras in $\mathscr{K}$, and of course a similar notation for any other class of algebras. The main theorem follows.

Theorem 2.1. *Let* $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C} \in \mathscr{K}_\omega$, *let* $\mathfrak{G} \in \mathscr{G}_\omega$ *and assume that*

$$\mathfrak{A} \times \mathfrak{B} \cong \mathfrak{G} \times \mathfrak{C}. \tag{1}$$

Then there exist $\mathfrak{G}'$, $\mathfrak{G}'' \in \mathscr{G}_\omega$ *and* $\mathfrak{A}'$, $\mathfrak{B}' \in \mathscr{K}_\omega$, *such that*

$$\mathfrak{A} \cong \mathfrak{A}' \times \mathfrak{G}', \quad \mathfrak{B} \cong \mathfrak{B}' \times \mathfrak{G}'', \quad \mathfrak{C} \cong \mathfrak{A}' \times \mathfrak{B}' \quad \text{and} \quad \mathfrak{G} \cong \mathfrak{G}' \times \mathfrak{G}''. \tag{2}$$

There are several obvious corollaries to this theorem, the first of which contrasts strongly with Theorem 1.1.

Corollary 2.1. $\mathscr{G}^p_\omega \subset \mathscr{K}^p_\omega$.

If $\mathfrak{A} \in \mathscr{K}_\omega$, then clearly there exist $\mathfrak{G} \in \mathscr{G}_\omega$ and $\mathfrak{B} \in \mathscr{K}_\omega$ such that $\mathfrak{A} \cong \mathfrak{G} \times \mathfrak{B}$ and every factor of $\mathfrak{B}$ which belongs to $\mathscr{G}$ is a one element group.

Corollary 2.2. $\mathfrak{G}$ *and* $\mathfrak{B}$ *are determined up to isomorphism by* $\mathfrak{A}$.

Corollary 2.3. *If* $\mathfrak{G} \in \mathscr{G}_\omega$, $\mathfrak{A}$, $\mathfrak{B} \in \mathscr{K}_\omega$ *and* $\mathfrak{G} \times \mathfrak{A} \cong \mathfrak{G} \times \mathfrak{B}$, *then* $\mathfrak{A} \cong \mathfrak{B}$.

Corollaries 2.1 and 2.2 are immediate from Theorem 2.1. Corollary 2.3 can be derived from 2.2, together with the well-known fact that it holds with $\mathscr{K}_\omega$ replaced by $\mathscr{G}_\omega$ [6, Theorem 3.11]. Theorem 2.1 follows by an inductive argument from its special case in which $\mathfrak{G}$ is directly indecomposable. The remainder of this section is devoted to a proof of the special case.

Thus we assume that $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C} \in \mathscr{K}_\omega$, that $\mathfrak{G}$ is a finite indecomposable group, and that

$$\Psi: \mathfrak{A} \times \mathfrak{B} \cong \mathfrak{G} \times \mathfrak{C} \tag{I}$$

is a fixed isomorphism from $\mathfrak{A} \times \mathfrak{B}$ onto $\mathfrak{G} \times \mathfrak{C}$. We use the symbols p_0 and p_1 for the first and second projections on a cartesian product. Thus if $X = X_0 \times X_1$, then

$$(\forall x \in X)(x = (p_0(x), p_1(x))).$$

The proof takes the form of a sequence of seven lemmas, but its general outline is simple.

The first step is to correlate with the decomposition (I) congruence relations $\equiv$ on $\mathfrak{A}$, $\mathfrak{B}$ and $\mathfrak{C}$ and an isomorphism

$$\overline{\Psi}: \mathfrak{A}/{\equiv} \times \mathfrak{B}/{\equiv} \cong \mathfrak{G} \times \mathfrak{C}/{\equiv} \tag{I$'$}$$

such that $\mathfrak{A}/\equiv$, $\mathfrak{B}/\equiv$, and $\mathfrak{C}/\equiv$ are groups and for which the diagram

$$\begin{tikzcd}
\mathfrak{A}\times\mathfrak{B} \arrow[r, "\Psi"] \arrow[d] & \mathfrak{G}\times\mathfrak{C} \arrow[d] \\
\mathfrak{A}/\equiv\times\mathfrak{B}/\equiv \arrow[r, "\Psi"] & \mathfrak{G}\times\mathfrak{C}/\equiv
\end{tikzcd}$$

commutes. The two unnamed maps here are the obvious ones. Since the algebras occurring in (I′) are groups, it determines homomorphisms $\mathfrak{A}/\equiv\,\to\mathfrak{G}$, $\mathfrak{B}/\equiv\,\to\mathfrak{G}$ and similar mappings in the other direction. From our construction it follows that the first two mappings are injective. The assumption that $\mathfrak{G}$ is indecomposable allows the application of a theorem of Jónsson and Tarski and we conclude that one of the mappings $\mathfrak{G}\to\mathfrak{A}/\equiv$, $\mathfrak{G}\to\mathfrak{B}/\equiv$ is injective. Assume it is the latter. Then $\mathfrak{G}\to\mathfrak{B}/\equiv$ is an isomorphism.

Now the identity element of the group $\mathfrak{B}/\equiv$ is the universe of a subalgebra $\mathfrak{D}$ of $\mathfrak{B}$. The last part of the proof requires an examination of the behavior of the equivalence relation $\sim_{\mathfrak{B}}$ on $\mathfrak{B}$ and the behavior of the set $R_{\mathfrak{B}}$ (see Definition 1.2) relative to the isomorphisms (I), (I′). By comparing the cardinalities of equivalence classes, we are able to construct a homomorphism η from $\mathfrak{B}$ onto $\mathfrak{D}$. η is constructed in such a way that $\rho\times\eta : \mathfrak{B}\cong\mathfrak{B}/\equiv\times\,\mathfrak{D}$ where ρ is the quotient map, and that

$$\begin{tikzcd}
\mathfrak{C} \arrow[r] & \mathfrak{G}\times\mathfrak{C} \arrow[r, "\Psi^{-1}"] & \mathfrak{A}\times\mathfrak{B} \arrow[r, "\iota\times\eta"] & \mathfrak{A}\times\mathfrak{D}
\end{tikzcd}$$

is an isomorphism from $\mathfrak{C}$ onto $\mathfrak{A}\times\mathfrak{D}$. Thus we can take $\mathfrak{G}'$ to be the one element group, $\mathfrak{G}''=\mathfrak{G}$, $\mathfrak{A}'=\mathfrak{A}$ and $\mathfrak{B}'=\mathfrak{D}$ and the proof is complete.

The detailed proof begins with the definition of some auxiliary notions which will not be needed after the second lemma. Let $n=2\cdot|G|$.

DEFINITION 2.1. (i) $t*s=(\cdots((t\cdot s)\cdot s)\cdots)\cdot s$ (s occurs $n-1$ times).

(ii) $f(t)=t*t$.

Let m be the least integer $q>1$ such that the qth iterate of f is idempotent on A, B, C and G: $f^{(m)}=f^{(2m)}$ (m exists since A, B, C and G are finite).

(iii) $t\circ s=[\cdots[[(t*s)*f(s)]*f^{(2)}(s)]\cdots]*f^{(m-1)}(s)$.

LEMMA 2.1. *Ψ preserves $*$, f, and $\circ$. Moreover, if $g, h\in G$ and $t\in A(B, C$ or $G)$ then $f(g)=1$, $g\circ h=g\cdot h^{-1}$ and $t\circ t=(t\circ t)\circ(t\circ t)=f^{(m)}(t)$.*

This lemma is obvious. 1 and $^{-1}$ refer to the definable operations in the group $\mathfrak{G}$.

LEMMA 2.2. *Let $a, a'\in A$ and let $b, b'\in B$. Then*

(i) *If $p_0\Psi(a, b)=p_0\Psi(a, b')$, then for every $x\in A$, $p_0\Psi(x, b)=p_0\Psi(x, b')$.*

(ii) *If $p_0\Psi(a, b)=p_0\Psi(a', b)$, then for every $y\in B$, $p_0\Psi(a, y)=p_0\Psi(a', y)$.*

(This lemma is obvious if $\mathfrak{A}$ and $\mathfrak{B}$ are groups.)

Proof. By symmetry of assumptions, we need only prove (i). Assume that $a_0, \alpha_0 \in A$, $b_0, b'_0 \in B$, $c_0, c'_0, \gamma_0, \gamma'_0 \in C$, that $g_0, h_0, k_0 \in G$ with $h_0 \neq k_0$ and that

$$\begin{aligned} \Psi(a_0, b_0) &= (g_0, c_0), & \Psi(\alpha_0, b_0) &= (h_0, \gamma_0), \\ \Psi(a_0, b'_0) &= (g_0, c'_0), & \Psi(\alpha_0, b'_0) &= (k_0, \gamma'_0). \end{aligned} \tag{1}$$

Using Definition 2.1 (iii), define inductively for $i \in \omega$,

$$\begin{aligned} &g_{i+1} = g_i \circ h_i, \quad a_{i+1} = a_i \circ \alpha_i, \quad b_{i+1} = b_i \circ b_i, \quad c_{i+1} = c_i \circ \gamma_i, \\ &\gamma_{i+1} = \gamma_i \circ c_i, \\ &h_{i+1} = h_i \circ g_i, \quad \alpha_{i+1} = \alpha_i \circ a_i, \quad b'_{i+1} = b'_i \circ b_i, \quad c'_{i+1} = c'_i \circ \gamma_i, \\ &\gamma'_{i+1} = \gamma'_i \circ c_i, \\ &k_{i+1} = k_i \circ g_i. \end{aligned} \tag{2}$$

Then from (1), (2), and Lemma 2.1, we have for every natural number i,

$$\begin{aligned} \Psi(a_i, b_i) &= (g_i, c_i), & \Psi(\alpha_i, b_i) &= (h_i, \gamma_i), \\ \Psi(a_i, b'_i) &= (g_i, c'_i), & \Psi(\alpha_i, b'_i) &= (k_i, \gamma'_i) \text{ and } h_i \neq k_i. \end{aligned} \tag{3}$$

Now choose integers $q, p > 1$ such that

$$b'_p = b'_{p+q}. \tag{4}$$

Define another polynomial $\#$ by

$$s \# t = [\cdots[[(s \circ t) \circ (t \circ t)] \circ (t \circ t)] \cdots] \circ (t \circ t), \tag{5}$$

with $t \circ t$ occurring $q-1$ times. Now by (2) and Lemma 2.1, we have $b_p = b_p \circ b_p = b_i$ for $1 \leqq i$. Together with the recursive definition of b', (4) and (5), this gives $b'_p \# b_p = b'_p$.

(6)
(i) For $g, h \in G$, $g \# h = g \cdot h^{-1}$.
(ii) For $t \in A(B, C \text{ or } G)$, $t \# t = t \circ t = (t \# t) \# (t \# t)$.
(iii) $b'_p \# b_p = b'_p$.

Now from (3) and the fact that Ψ preserves $\#$,

$$\Psi((\alpha_p \# a_p) \# (a_p \# \alpha_p), (b'_p \# b'_p) \# (b'_p \# b'_p)) = (k_p \cdot g_p^{-1} \cdot k_p \cdot g_p^{-1}, \ldots)$$
$$\Psi((\alpha_p \# a_p) \# (a_p \# \alpha_p), (b'_p \# b_p) \# (b'_p \# b_p)) = (k_p \cdot g_p^{-1} \cdot h_p \cdot g_p^{-1}, \ldots).$$

The left sides are equal by (6) but the right sides are not equal since $k_p \neq h_p$. This contradiction proves the lemma. Q.E.D.

DEFINITION 2.2. (i) For $a, a' \in A$, let

$$a \equiv_{\mathfrak{A}} a' \leftrightarrow (\exists y \in B)(p_0 \Psi(a, y) = p_0 \Psi(a', y)).$$

(ii) For $b, b' \in B$, let

$$b \equiv_{\mathfrak{B}} b' \leftrightarrow (\exists x \in A)(p_0 \Psi(x, b) = p_0 \Psi(x, b')).$$

(iii) For $c, c' \in C$, let

$$c \equiv_{\mathfrak{C}} c' \leftrightarrow p_i\Psi^{-1}(1, c) \equiv p_i\Psi^{-1}(1, c') \qquad (i = 0, 1),$$

where 1 is the identity element of $\mathfrak{G}$.

It follows directly from Lemma 2.2 that $\equiv_{\mathfrak{A}}$, $\equiv_{\mathfrak{B}}$, and $\equiv_{\mathfrak{C}}$ are congruence relations, yielding quotient algebras $\mathfrak{A}/\equiv$, $\mathfrak{B}/\equiv$, and $\mathfrak{C}/\equiv$ respectively.

Definition 2.3. If $a \in A$ and $b \in B$, let

$$\overline{\Psi}(a/\equiv_{\mathfrak{A}}, b/\equiv_{\mathfrak{B}}) = (p_0(\Psi(a, b)), p_1\Psi(a, b)/\equiv_{\mathfrak{C}}).$$

Lemma 2.3. $\mathfrak{A}/\equiv$, $\mathfrak{B}/\equiv$, $\mathfrak{C}/\equiv \in \mathscr{G}_\omega$. *$\overline{\Psi}$ is a well-defined isomorphism,*

$$(\text{I}') \qquad \overline{\Psi}\colon \mathfrak{A}/\equiv \times \mathfrak{B}/\equiv \;\cong\; \mathfrak{G}\times\mathfrak{C}/\equiv.$$

Proof. By Lemma 2.2 and Definition 2.2, $x, y, z \in A$ and $x \not\equiv y$ implies $x\cdot z \not\equiv y\cdot z$ and $z\cdot x \not\equiv z\cdot y$. Similarly in $\mathfrak{B}$. Thus, $\mathfrak{A}/\equiv$, $\mathfrak{B}/\equiv$ being finite, they are quasi-groups, i.e., $x, y \in A/\equiv$ implies $\exists z \in A/\equiv$ with $x\cdot z = y$, etc. Thus we can choose, $a, a_0 \in A$ and $b, b_0 \in B$ with $a\cdot a_0 \equiv a$ and $b\cdot b_0 \equiv b$. Then by Lemma 2.2, $p_0\Psi(a\cdot a_0, b\cdot b_0) = p_0\Psi(a, b)$. Hence $p_0\Psi(a_0, b_0) = 1$. Therefore

$$p_0\Psi(a, b_0\cdot b_0) = p_0\Psi(a\cdot a_0, b_0\cdot b_0) = p_0\Psi(a, b_0)$$

giving $b_0\cdot b_0 \equiv b_0$. And for any $x \in A$,

$$p_0\Psi(x\cdot a_0, b_0) = p_0\Psi(x\cdot a_0, b_0\cdot b_0) = p_0\Psi(x, b_0),$$

giving $x\cdot a_0 \equiv x$. A continuation of this argument shows that $a_0/\equiv$ and $b_0/\equiv$ are two-sided unit elements in $\mathfrak{A}/\equiv$ and $\mathfrak{B}/\equiv$ respectively.

$\mathfrak{A}/\equiv$ is now seen to be associative by the following calculation (a similar argument works for $\mathfrak{B}/\equiv$). Let $x, y, z \in A$. Then

$$\begin{aligned} p_0\Psi(x\cdot(y\cdot z), b_0) &= p_0\Psi(x\cdot(y\cdot z), b_0\cdot(b_0\cdot b_0)) = p_0\Psi((x\cdot y)\cdot z, (b_0\cdot b_0)\cdot b_0) \\ &= p_0\Psi((x\cdot y)\cdot z, b_0). \end{aligned}$$

Thus $x\cdot(y\cdot z) \equiv (x\cdot y)\cdot z$. The remainder of the proof is straightforward. Q.E.D.

From Theorem 3.7 of [6, p. 46] the assumption that $\mathfrak{G}$ is indecomposable implies that the image of $\mathfrak{G}$ under the group isomorphism $\overline{\Psi}^{-1}$ projects biuniquely either into $\mathfrak{A}/\equiv$ or into $\mathfrak{B}/\equiv$. There is no loss of generality in assuming that the latter case holds.

$$(\text{II}) \qquad p_1\overline{\Psi}^{-1} \text{ imbeds } \mathfrak{G} \text{ in } \mathfrak{B}/\equiv.$$

Since it follows from Definition 2.2 that the finite cardinality of $B/\equiv$ is no greater than that of G, we actually have the following.

Lemma 2.4. $\mathfrak{B}/\equiv \;\cong \mathfrak{G}$. *Moreover, if $b \in B$ and $c \in C$, then there is a unique element $g \in G$ such that $b \equiv p_1\Psi^{-1}(g, c)$.*

For the remaining discussion fix an element $a_0 \in A$ such that $a_0/\equiv$ is the identity element of $\mathfrak{A}/\equiv$, and a similar element $b_0 \in B$. Let $c_0 = p_1\Psi(a_0, b_0)$ so that $c_0/\equiv$ is the unit of $\mathfrak{C}/\equiv$.

Definition 2.4. (i) $\mathfrak{D} = \langle b_0/\equiv, \circ\rangle$. Thus $\mathfrak{D} \in \mathscr{K}_\omega$ and $\mathfrak{D} \subseteq \mathfrak{B}$. (ii) η_0 maps B into $b_0/\equiv$. Let $\eta_0(b) = d$ iff $d \equiv b_0$ and there exist $g, h \in G$ and $c \in C$ satisfying $\Psi(a_0 \cdot a_0, b) = (g, c)$, $p_1\Psi^{-1}(h, c) = d$.

By Lemma 2.4, η_0 is well defined. η_0 is a first approximation to a function $\eta\colon \mathfrak{B} \to \mathfrak{D}$ which we need to show that $\mathfrak{B} \cong \mathfrak{B}/\equiv \times \mathfrak{D} \cong \mathfrak{G} \times \mathfrak{D}$. From the further discussion it can be seen that η_0 need not have the required property of mapping each class $b/\equiv$ bijectively onto $b_0/\equiv$. The next few lemmas prepare the ground for the construction of η. Recall the introduction of the notions $\sim_{\mathfrak{B}}$ and $R_{\mathfrak{B}}$ in Definition 1.2 and the succeeding remark. Using the notation f^* for the set mapping induced by a function f, observe that

$$\bar{\Psi}(a/\equiv, b/\equiv) = (g, c/\equiv) \quad \text{iff} \quad \Psi^*(a/\equiv \times b/\equiv) = \{g\} \times c/\equiv,$$

that $\Psi(a, b) = (g, c)$ implies $\Psi^*(a/\sim_{\mathfrak{A}} \times b/\sim_{\mathfrak{B}}) = \{g\} \times c/\sim_{\mathfrak{C}}$, and that in general, $x \sim y$ implies $x \equiv y$.

Lemma 2.5. (i) *Let $g, h \in G$ and $c, c' \in C$. Then*

$$p_1\Psi^{-1}(g, c) \sim_{\mathfrak{B}} p_1\Psi^{-1}(g, c') \quad \textit{iff} \quad p_1\Psi^{-1}(h, c) \sim_{\mathfrak{B}} p_1\Psi^{-1}(h, c').$$

(ii) *η_0 is a homomorphism from $\mathfrak{B}$ into $\mathfrak{D}$.*

(iii) *If $b, b' \in B$ and $b \equiv b'$, then $b \sim b'$ iff $\eta_0(b) \sim \eta_0(b')$.*

Proof. (i) $u \sim_{\mathfrak{B}} v$ means that for every $x \in B$, $u \cdot x = v \cdot x$ and $x \cdot u = x \cdot v$. Now if $x \in B$ and $\Psi(a_0, x) = (k, c'')$, then $[p_1\Psi^{-1}(h, c)] \cdot x = [p_1\Psi^{-1}(g, c)] \cdot [p_1\Psi^{-1}(g^{-1}hk, c'')]$ and $[p_1\Psi^{-1}(h, c')] \cdot x = [p_1\Psi^{-1}(g, c')] \cdot [p_1\Psi^{-1}(g^{-1}hk, c'')]$. The continuation is obvious.

(ii) Let $b, b' \in B$ and choose $\bar{a}, \bar{a}', \bar{b}, \bar{b}'$, etc. with $\bar{b} \equiv b_0 \equiv \bar{b}'$ and $\Psi(a_0, b) = (g, c)$, $\Psi(\bar{a}, \bar{b}) = (h, c)$, $\Psi(a_0, b') = (g', c')$, $\Psi(\bar{a}', \bar{b}') = (h', c')$. This is possible by Lemma 2.4. Since $a_0 \equiv a_0 \cdot a_0$, it is clear from Definition 2.4 (ii) that (i) above applies and we have $\bar{b} \sim \eta_0(b)$ and $\bar{b}' \sim \eta_0(b')$. Moreover, clearly

$$\eta_0(b \cdot b') = \bar{b} \cdot \bar{b}' = \eta_0(b) \cdot \bar{b}' = \eta_0(b) \cdot \eta_0(b').$$

Part (iii) is immediate from part (i). Q.E.D.

Lemma 2.6. *If $b \in B$, then*

(i) $|b/\equiv| = |b_0/\equiv|$.

(ii) $|b/\equiv \cap R_{\mathfrak{B}}| = |b_0/\equiv \cap R_{\mathfrak{B}}|$.

(iii) $|b/\sim_{\mathfrak{B}}| = |\eta_0(b)/\sim_{\mathfrak{B}}|$.

(*Note that $\eta_0(b)/\sim_{\mathfrak{B}} \subseteq b_0/\equiv$.*)

Proof. Let $b \in B$ and let $S = \Psi^*(A \times b/\equiv)$. By Lemma 2.4, p_1 maps S biuniquely onto C. Hence $|A| \cdot |b/\equiv| = |S| = |C|$ is independent of b, giving (i). A similar observation, replacing S by $S \cap R_{\mathfrak{G} \times \mathfrak{C}} = \Psi^*[R_{\mathfrak{A}} \times (b/\equiv \cap R_{\mathfrak{B}})]$ gives (ii) ($p_1^*(S \cap R_{\mathfrak{G} \times \mathfrak{C}}) = R_{\mathfrak{C}}$).

To get (iii), fix g, h, c and a with $\Psi(a_0 \cdot a_0, b)=(g, c)$ and $\Psi(a, \eta_0(b))=(h, c)$. Then $\Psi^*(a_0/\equiv \times b/\equiv)=\{g\}\times c/\equiv$ and $\Psi^*(a/\equiv \times b_0/\equiv)=\{h\}\times c/\equiv$. Moreover, by Lemma 2.5 (i) there is a subset T of C with $\Psi^*(a_0/\equiv \times b/\sim_{\mathfrak{B}})=\{g\}\times T$ and $\Psi^*(a/\equiv \times \eta_0(b)/\sim_{\mathfrak{B}})=\{h\}\times T$. Putting these relations together with (i), (iii) follows. Q.E.D.

Remark 2.1. Putting Lemma 2.5 (iii) and Lemma 2.6 together we find that, by finiteness assumptions, η_0 maps any complete set of representatives of the $\sim_{\mathfrak{B}}$ classes contained in $b/\equiv$ onto a complete set of representatives for the $\sim_{\mathfrak{B}}$ classes contained in $b_0/\equiv$.

Lemma 2.7. *If $b \in B$, then η_0 maps $b/\equiv \cap R_{\mathfrak{B}}$ bijectively onto $b_0/\equiv \cap R_{\mathfrak{B}}$ and $b/\sim_{\mathfrak{B}} \cap R_{\mathfrak{B}}$ bijectively onto $\eta_0(b)/\sim_{\mathfrak{B}} \cap R_{\mathfrak{B}}$.*

Proof. By Lemma 2.5 (iii), Lemma 2.6 and finiteness, it will be seen that it suffices to prove that $\eta_0^*(b/\equiv \cap R_{\mathfrak{B}}) \supseteq b_0/\equiv \cap R_{\mathfrak{B}}$. Let $y \in b_0/\equiv \cap R_{\mathfrak{B}}$. Since η_0 is a homomorphism and the identity map on $b_0/\equiv$, choose $y_0, y_1 \in b_0/\equiv$ with $y=y_0 \cdot y_1$. Using Remark 2.1, choose $t \equiv b$ such that $\eta_0(t) \sim_{\mathfrak{B}} y_0$. Then $t \cdot y_1 \equiv b$, $t \cdot y_1 \in R_{\mathfrak{B}}$ and $\eta_0(t \cdot y_1)=\eta_0(t)\cdot\eta_0(y_1)=\eta_0(t)\cdot y_1=y_0\cdot y_1=y$. Q.E.D.

Now to conclude the proof of Theorem 2.1, let η be any function from B onto $b_0/\equiv$ such that η agrees with η_0 on $R_{\mathfrak{B}}$ while for every $b \in B$, η maps $(b/\sim)\sim R_{\mathfrak{B}}$ bijectively onto $(\eta_0(b)/\sim)\sim R_{\mathfrak{B}}$. By 2.6 and 2.7, such functions exist. That η maps $\mathfrak{B}$ into $\mathfrak{D}$ homomorphically is obvious. By 2.5, 2.6, 2.7, and Remark 2.1, η maps $b/\equiv$ bijectively onto $b_0/\equiv$ for each $b \in B$. Hence $\phi(b)=(b/\equiv, \eta(b))$ defines an isomorphism between $\mathfrak{B}$ and $\mathfrak{B}/\equiv \times \mathfrak{D}$. Thus $|C|=|A \times D|$. An isomorphism λ between $\mathfrak{C}$ and $\mathfrak{A} \times \mathfrak{D}$ is therefore defined by letting $\lambda(c)=(a, \eta(b))$ where $\Psi(a, b)=(1, c)$. (It is enough to show that λ is injective. But if $\Psi(a, b)=(1, c)$ and $\Psi(a, b')=(1, c')$ then $b \equiv b'$. Hence if $\eta(b)=\eta(b')$ then $b=b'$ and $c=c'$.)

3. **Finite semigroups.** $\mathcal{G}_\omega$ and $\mathcal{K}_\omega$ denote, as in the last section, the classes of finite groups and groupoids respectively. It is known from [6, Theorem 3.10, p. 49] that finite groupoids with a neutral element have the unique factorization property. Recent results of Chang, Jónsson, Tarski [2] and Jónsson [5] exhibit as special cases certain other classes of groupoids with this property. We give in this section yet another result of this sort.

Throughout the section, $\mathcal{S}$ denotes the class of all finite groupoids $\mathfrak{A}=\langle A, \cdot\rangle$ satisfying the following two conditions:

(1) $(\forall x, y, z \in A)((x\cdot y)\cdot z = x\cdot(y\cdot z))$.

(2) $(\forall x, y \in A)(\exists u, v \in A)(x \neq y \rightarrow u\cdot x \neq u\cdot y \wedge x\cdot v \neq y\cdot v)$.

It must be emphasized here that in (2) the existence of u, v with these properties independently of x, y is not asserted. Notice also that if $\mathfrak{A}, \mathfrak{B} \in \mathcal{K}_\omega$ then $\mathfrak{A} \times \mathfrak{B} \in \mathcal{S}$ iff $\mathfrak{A}, \mathfrak{B} \in \mathcal{S}$.

Theorem 3.1. *Every algebra in S has the unique factorization property.*

In other words, if $\mathfrak{A} \in \mathscr{S}$ and $\mathfrak{A} \cong P_{i\in I}\mathfrak{B}_i \cong P_{j\in J}\mathfrak{C}_j$ with $\mathfrak{B}_i$ and $\mathfrak{C}_j$ indecomposable (and having more than one element) for all $i \in I$ and $j \in J$, then there exists a one-to-one map ϕ of I onto J such that $\mathfrak{B}_i \cong \mathfrak{C}_{\phi(i)}$ for all $i \in I$.

Groupoids satisfying (1) are usually called semigroups. Before proving the theorem, it may be worthwhile to indicate why some condition such as (2) must be imposed in order to ensure that a finite semigroup have the unique factorization property. The example given below depends in an obvious way on a flagrant violation of (2). Since this semigroup is commutative, the example solves a question stated by Chang-Jónsson-Tarski in [2, p. 32].

Since we are assuming that each ordinal is identical with the set of all smaller ordinals, the example may be described as follows. For $0 \leqq x,\ y<6$, let $x \cdot_{\mathfrak{A}} y=1$ if both x and y are $\geqq 3$ and let $x \circ_{\mathfrak{A}} y=0$ otherwise. For $0 \leqq x,\ y<4$, let $x \cdot_{\mathfrak{B}} y=1$ if both x and y are $\geqq 2$ and let $x \cdot_{\mathfrak{B}} y=0$ otherwise. Clearly, $\mathfrak{A}=\langle 6, \circ_{\mathfrak{A}}\rangle$ and $\mathfrak{B}=\langle 4, \circ_{\mathfrak{B}}\rangle$ are commutative semigroups. Moreover it is easy to find isomorphisms between $\mathfrak{A} \times \mathfrak{O}_2$ and $\mathfrak{B} \times \mathfrak{O}_3$. Since $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{O}_2$ and $\mathfrak{O}_3$ are all indecomposable and mutually nonisomorphic, it follows that the semigroup $\mathfrak{A} \times \mathfrak{O}_2$ does not have the unique factorization property. (Recall that the definition of $\mathfrak{O}_{\mathfrak{m}}$ in Definition 1.2 specializes to groupoids and yields a semigroup.)

For the purpose of proving Theorem 3.1 let $\mathscr{E}$ denote a one-element groupoid and, whenever $\mathfrak{A} \in \mathscr{K}_\omega$ let $g(\mathfrak{A}) \in \mathscr{G}_\omega$ and $s(\mathfrak{A}) \in \mathscr{K}_\omega$ denote ambiguously any group and groupoid such that $\mathfrak{A} \cong g(\mathfrak{A}) \times s(\mathfrak{A})$ and such that every factor of $s(\mathfrak{A})$ which belongs to $\mathscr{G}_\omega$ is isomorphic to $\mathscr{E}$. By Corollary 2.2, $g(\mathfrak{A})$ and $s(\mathfrak{A})$ are determined up to isomorphism by $\mathfrak{A}$.

LEMMA 3.1. *If* $\mathfrak{A}, \mathfrak{B} \in \mathscr{K}_\omega$ *then* $g(\mathfrak{A} \times \mathfrak{B}) \cong g(\mathfrak{A}) \times g(\mathfrak{B})$ *and* $s(\mathfrak{A} \times \mathfrak{B}) \cong s(\mathfrak{A}) \times s(\mathfrak{B})$.

The lemma is an easy consequence of Theorem 2.1. Before continuing, we need a few simple facts from the theory of semigroups [3, Chapter 1].

Every finite semigroup has idempotent elements, in particular some power of each element is idempotent. (An element e is idempotent iff $e \cdot e=e$. We can speak of powers because the operation satisfies (1).)

If e is an idempotent in the semigroup $\mathfrak{A}$, then we use the notation $\mathfrak{A}^e=\langle A^e, \circ\rangle$ for the largest subgroup of $\mathfrak{A}$ containing e as its identity element. Thus

$$A^e = \{x \in A : e \cdot x \cdot e = x \wedge (\exists y \in A)(x \cdot y = y \cdot x = e)\}.$$

The following lemma gives the only essential application of the condition (2) required in our proof of Theorem 3.1.

LEMMA 3.2. *Let* $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D} \in \mathscr{S}$, *let* $e \in A$ *be any idempotent element of* $\mathfrak{A}$ *and assume that* $\phi : \mathfrak{A} \times \mathfrak{B} \cong \mathfrak{C} \times \mathfrak{D}$. *Then*

$$\phi^*(\mathfrak{A}^e \times \mathfrak{B}) = \mathfrak{C}_0 \times \mathfrak{D}_0$$

for some $\mathfrak{C}_0 \subseteq \mathfrak{C}$ *and* $\mathfrak{D}_0 \subseteq \mathfrak{D}$.

Proof. (Of course a similar statement holds if the idempotent is chosen from any of $\mathfrak{B}$, $\mathfrak{C}$, or $\mathfrak{D}$.) Let $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, e, and ϕ be given satisfying the hypotheses. Given $(a, b), (a', b') \in A^e \times B$ and $(c, d), (c'd') \in C \times D$ with $\phi(a, b) = (c, d)$ and $\phi(a', b') = (c', d')$ it must be shown that $\phi^{-1}(c', d) \in A^e \times B$. Let $(a'', b'') = \phi^{-1}(c', d)$.

(1) $e \cdot a'' = a''$.

Assume that (1) is false. Then by the definition of $\mathscr{S}$, pick $x \in A$ such that $x \cdot e \cdot a'' \neq x \cdot a''$. Let $\phi(x, b) = (u, v)$, $\phi(x \cdot e, b) = (r, s)$. Then since $(x, b) \cdot (a, b)$ $(xe, b)(a, b)$ we have $v \cdot d = s \cdot d$. Similarly, $u \cdot c' = r \cdot c'$. Thus $(u, v) \cdot (c', d) = (r, s) \cdot (c', d)$ and $x \cdot e \cdot a'' = x \cdot a''$ contradicting the choice of x. Thus (1) is true.

(2) $a'' \cdot e = a''$.

The proof is similar.

(3) $(\exists x \in A)(x \cdot a'' = a'' \cdot x = e)$.

To prove this let $m > 1$ be such that the mth powers of (a, b) and (a', b') are both idempotent. Then $a^m = (a')^m = e$. And

$$(c, d)^m \cdot (c', d)^m \cdot (c', d')^m = (c^m \cdot (c')^m, d^m(d')^m).$$

Hence

$$(a'')^m = e \cdot (a'')^m \cdot e = a^m \cdot (a'')^m (a')^m = (a^m) \cdot (a')^m = e.$$

We can take $x = (a'')^{m-1}$ in (3).

(1–3) give $a'' \in A^e$ completing the proof. Q.E.D.

Theorem 3.1 is easily seen to be equivalent to the following theorem which will now be proved.

THEOREM 3.2. *Let $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D} \in \mathscr{S}$ with $\mathfrak{A}$ directly indecomposable and $\mathfrak{A} \times \mathfrak{B} \cong \mathfrak{C} \times \mathfrak{D}$. Then $\exists \mathfrak{C}', \mathfrak{C}'', \mathfrak{D}', \mathfrak{D}'' \in \mathscr{S}$ such that $\mathfrak{A} \cong \mathfrak{C}' \times \mathfrak{D}'$, $\mathfrak{B} \cong \mathfrak{C}'' \times \mathfrak{D}''$, $\mathfrak{C} \cong \mathfrak{C}' \times \mathfrak{C}''$ and $\mathfrak{D} \cong \mathfrak{D}' \times \mathfrak{D}''$. (Either $\mathfrak{C}' \cong \mathscr{E}$ or $\mathfrak{D}' \cong \mathscr{E}$.)*

Proof. Under the given assumptions, choose an isomorphism ϕ from $\mathfrak{A} \times \mathfrak{B}$ onto $\mathfrak{C} \times \mathfrak{D}$ and pick idempotent elements $e \in A$, $e' \in B$, $f \in C$ and $f' \in D$ such that $\phi(e, e') = (f, f')$. Also assume that $\mathfrak{A} \cong s(\mathfrak{A})$ and $g(\mathfrak{A}) \cong \mathscr{E}$. Otherwise Theorem 3.1 applies. (Since $\mathfrak{A}$ is directly indecomposable, either $g(\mathfrak{A}) \cong \mathscr{E}$ or $\mathfrak{A} \cong g(\mathfrak{A})$.)

By Lemma 3.2 we have

$$
\begin{aligned}
\phi^*(\mathfrak{A} \times \mathfrak{B}^{e'}) &= \mathfrak{C}_0 \times \mathfrak{D}_0, \\
\phi^*(\mathfrak{A}^e \times \mathfrak{B}) &= \mathfrak{C}_1 \times \mathfrak{D}_1, \qquad (1) \\
\phi^*(\mathfrak{A}_0 \times \mathfrak{B}_0) &= \mathfrak{C} \times \mathfrak{D}^{f'},
\end{aligned}
$$

where $\mathfrak{A}_0 \subseteq \mathfrak{A}$, $\mathfrak{B}_0 \subseteq \mathfrak{B}$, $\mathfrak{C}_0, \mathfrak{C}_1 \subseteq \mathfrak{C}$, and $\mathfrak{D}_0, \mathfrak{D}_1 \subseteq \mathfrak{D}$. Since $\mathfrak{A}$ is indecomposable and $\mathfrak{A} \cong s(\mathfrak{A}) \cong s(\mathfrak{C}_0) \times s(\mathfrak{D}_0)$ by Lemma 3.1, we may assume that $s(\mathfrak{D}_0) \cong \mathscr{E}$ and consequently that $\mathfrak{D}_0$ is a group.

(2) $\mathfrak{D}_0 = \mathfrak{D}^{f'}$, $\mathfrak{A}_0 = \mathfrak{A}$ and $\mathfrak{D}_1 = \mathfrak{D}$. Moreover,

$$\phi^*(\mathfrak{A}^e \times \mathfrak{B}_0) = \mathfrak{C}_1 \times \mathfrak{D}^{f'}.$$

That $\mathfrak{D}_0 = \mathfrak{D}^{f'}$ is now obvious from the preceding remark and the observation that $\phi^*(\mathfrak{A}^e \times \mathfrak{B}^{e'}) = \mathfrak{C}^f \times \mathfrak{D}^{f'}$. From this and (1) it follows that $\mathfrak{A}_0 = \mathfrak{A}$. To see that

$\mathfrak{D}=\mathfrak{D}_1$, let d be an arbitrary element of D and let $(a, b)=\phi^{-1}(f, d)$. Since also $\phi(e, e')=(f, f')$, by Lemma 3.2 $\phi(a, e')\in C^f\times D$. But by (1) and the fact that $\mathfrak{D}_0=\mathfrak{D}^{f'}$, $\phi(a, e')\in C\times D^{f'}$. Thus $\phi(a, e')\in C^f\times D^{f'}$ implying $a\in A^e$. This in turn gives $(a, b)\in A^e\times B$ and $d\in D_1$. Thus $\mathfrak{D}=\mathfrak{D}_1$. The last statement is immediate by taking intersections.

From (1) and (2) we obtain

$$(3)\qquad s(\mathfrak{B}_0)\cong s(\mathfrak{C}_1),\ \mathfrak{B}\cong\mathfrak{D}\times[s(\mathfrak{C}_1)\times g(\mathfrak{C})],\quad\text{and}\quad \mathfrak{C}\cong\mathfrak{A}\times[s(\mathfrak{C}_1)\times g(\mathfrak{C})].$$

The first assertion follows from the last part of (2): $s(\mathfrak{B}_0)\cong s(\mathfrak{A}^e\times\mathfrak{B}_0)$ and $s(\mathfrak{C}_1)\cong s(\mathfrak{C}_1\times\mathfrak{D}^{f'})$. Also we have

$$\begin{aligned} g(\mathfrak{B}) &\cong \mathscr{E}\times g(\mathfrak{B})\\ &\cong g(\mathfrak{A}\times\mathfrak{B}) \cong g(\mathfrak{C})\times g(\mathfrak{D}),\\ s(\mathfrak{B}) &\cong s(\mathfrak{A}^e\times\mathfrak{B}) \cong s(\mathfrak{C}_1)\times s(\mathfrak{D}) \end{aligned}$$

by (1), (2), and Lemma 3.1. Hence

$$\mathfrak{B} \cong g(\mathfrak{B})\times s(\mathfrak{B}) \cong \mathfrak{D}\times[s(\mathfrak{C}_1)\times g(\mathfrak{C})].$$

In a similar vein,

$$\begin{aligned} s(\mathfrak{C}) &\cong s(\mathfrak{C}\times\mathfrak{D}^{f'}) \cong s(\mathfrak{A}\times\mathfrak{B}_0)\\ &\cong \mathfrak{A}\times s(\mathfrak{B}_0) \cong \mathfrak{A}\times s(\mathfrak{C}_1). \end{aligned}$$

Multiplying by $g(\mathfrak{C})$, we get (3).

Now let $\mathfrak{C}'=\mathfrak{A}$, $\mathfrak{D}'=\mathscr{E}$, $\mathfrak{C}''=s(\mathfrak{C}_1)\times g(\mathfrak{C})$, and $\mathfrak{D}''=\mathfrak{D}$ and Theorem 3.2 is completely proved. Q.E.D.

4. **Discussion.** To my knowledge, Theorem 2.1 presents a phenomenon not previously recognized: refinement theorems have always required all algebras occurring to satisfy some condition other than finiteness; e.g., in [5] and [6] all structures are required to possess a special element with most of the properties of a neutral element. Unfortunately, it seems likely that the phenomenon is limited to algebras with only one operation. Some evidence will be given at the end of this discussion.

By a neutral element in a groupoid $\mathfrak{A}$, we mean an element $1\in A$ satisfying $1\cdot x=x\cdot 1=x$ for each $x\in A$. By a loop we mean a groupoid with a neutral element and satisfying in addition: whenever $x, y\in A$, there exists a unique solution $u\in A$ of the equation $x\cdot u=y$, and a unique solution $v\in A$ of the equation $v\cdot x=y$. With this definition, all results of section two remain true with "group" replaced by "loop". The proofs are almost identical with those given, except that the proof of the modified form of Lemma 2.2 requires the fact that in every finite loop the function $f(x, y)=x\cdot z$ where $y\cdot z=1$, coincides with some polynomial in the basic operation. The question whether "group" may be replaced by "groupoid with a neutral element" in Theorem 2.1 or in some of its corollaries seems very interesting.

To continue, let us agree to speak only of finite algebras and to call a finite algebra *prime* iff it is $\mathscr{K}$-prime in the sense of Definition 1.1 where $\mathscr{K}$ is the class of all finite algebras of the same type. The following problems are open.

Problem 1. For which operational types τ are there prime algebras of type τ?

Problem 2. Characterize intrinsically the prime algebras of given type, or show that the problem is in some sense recursively unsolvable.

We have observed that indecomposable loops with more than one element are prime, but this result does not exhaust the prime groupoids (e.g. the semilattice with two elements and the Sheffer stroke operation on a two-element set are prime groupoids). The argument of §2 can be altered to produce prime algebras of type $\langle n\rangle$ for $n \geqq 2$. I know of no examples among unary algebras, i.e. algebras of type $\langle 1\rangle$. It can be verified that a prime unary algebra $\langle A, f\rangle$ must contain no cycles: if $x \in A$, $m \geqq 1$, and $f^{(m)}(x)=x$, then $f(x)=x$. According to an unpublished result of Ralph Seifert, every prime unary algebra is connected in the sense that if $x, y \in A$, then for some $m, n>0$, $f^{(n)}(x)=f^{(m)}(y)$.

We conjecture that prime algebras with more than one basic operation do not exist. This would rule out any extension of Theorem 2.1 to richer operational types. To conclude, we will present two examples which tend to reinforce this conjecture.

In the first example, $\tau=\langle 2, 2\rangle$. Let $\mathfrak{A}=\langle A, +, \cdot\rangle$ where $+$ and $\cdot$ coincide on A and $\langle A, +\rangle$ is a two-element group. Let $\mathfrak{B}=\langle B, +, \cdot\rangle$ where $\langle B, +\rangle$ and $\langle B, \cdot\rangle$ are the two distinct groups on a two-element base B. It is easy to see that $\mathfrak{A} \times \mathfrak{B} \cong \mathfrak{B} \times \mathfrak{B}$. Hence $\mathfrak{A}$ is not prime. $\mathfrak{B}$ is not prime but the proof will not be given.

In the second example, $\tau=\langle 2, 1\rangle$. Let $\mathfrak{P}=\langle 2, \cdot, -\rangle$ be a two-element boolean algebra with smallest element 0. Let $\mathfrak{B}_0=\langle 2, \cdot^0, -^0\rangle$, $\mathfrak{B}_1=\langle 4, \cdot^1, -^1\rangle$, and $\mathfrak{B}_2=\langle 4, \cdot^2, -^2\rangle$ with operations defined as follows. $-^0$ is the cyclic permutation (01) whereas $-^1$ and $-^2$ are both identical with the permutation (0123). Set $x \cdot^0 y=0$ for $0 \leqq x, y<2$ and set $x \cdot^2 y=0$ for $0 \leqq x, y<4$. Finally, let $3'=1'=1$ and $2'=0'=0$ and set $x \cdot^1 y=x' \cdot y'$ for $0 \leqq x, y<4$. Then it is fairly easy to see that $\mathfrak{B}_0 \times \mathfrak{B}_1 \cong \mathfrak{P} \times \mathfrak{B}_2$ whereas $\mathfrak{P} \nmid \mathfrak{B}_i$ $(i=0, 1)$.

This last example is particularly interesting because every finitary operation on the set 2 can be expressed as a polynomial in the operations of $\mathfrak{B}$. In addition, the example modifies to show that if $\mathfrak{O}$ is any set of operations on 2, then the algebra $\langle\mathfrak{P}, \mathfrak{O}\rangle$ with the additional operations is not prime.

Added April 12, 1968. In a paper which will soon appear in Acta Math. Acad. Sci. Hungar., László Lovász has constructed an embedding of the semigroup of isomorphism types of finite relational structures (of a fixed similarity class), under the operation of direct product, into a direct power of the integers under multiplication. In the process, he has established a very beautiful and general cancellation theorem which contains Corollary 2.3 of this paper.

Ralph Seifert, a student at Berkeley, has recently proved the nonexistence of prime unary algebras (Abstract 67T-446, Notices Amer. Math. Soc. **14** (1967), 554).

References

1. G. Birkhoff, *Lattice theory*, rev. ed., Amer. Math. Soc. Colloq. Publ., Vol. 25, Amer. Math. Soc., Providence, R. I., 1948.

2. C. C. Chang, B. Jónsson and A. Tarski, *Refinement properties for relational structures*, Fund. Math. **55** (1964), 249–281.

3. A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*, Vol. 1, Math. Surveys, No. 7, Amer. Math. Soc., Providence, R. I., 1961.

4. P. Crawley and B. Jónsson, *Refinements for infinite direct decompositions of algebraic systems*, Pacific J. Math. **14** (1964), 797–855.

5. B. Jónsson, *The unique factorization problem for finite relational structures*, Colloq. Math. **14** (1966), 1–32.

6. B. Jónsson and A. Tarski, *Direct decompositions of finite algebraic systems*, Notre Dame Math. Lectures No. 5, Univ. of Notre Dame, Ind., 1947.

7. R. McKenzie, *On the unique factorization problem for finite commutative semigroups*, Abstract 621-38, Notices Amer. Math. Soc. **12** (1965), 315.

8. ———, *Finite groupoids and K-prime algebras*, Abstract 66T-453, Notices Amer. Math. Soc. **13** (1966), 727.

University of California,
Berkeley, California