COLLOQUIUM MATHEMATICUM

XIV WARSZAWA—WROCŁAW 1966

THE UNIQUE FACTORIZATION PROBLEM FOR FINITE RELATIONAL STRUCTURES*

BY

B. JÓNSSON (MINNEAPOLIS, MINN.)

INTRODUCTION

By a *relational structure* or, briefly, a *structure* we shall here mean a system $\mathfrak{A} = \langle A, 0, R_t\rangle_{t\in T}$ consisting of a set A, an indexed family of relations R_t of finite rank over A, and a distinguished element $0\in A$ which is reflexive, i. e., satisfies the condition $\langle 0, 0, \ldots, 0\rangle \in R_t$ for all $t\in T$. In the principal theorems it will also be assumed that A is finite, but it may turn out to be of some significance for future investigations to observe that many of the auxiliary results are independent of this condition, and the finiteness will therefore not be assumed unless it is explicitly stated.

Every finite structure $\mathfrak{A}$ is isomorphic to a direct product of directly indecomposable structures. $\mathfrak{A}$ is said to have the *unique factorization property* provided this representation is unique up to isomorphism; i. e., provided the condition

$$\mathfrak{A} \cong \boldsymbol{P}_{i\in I}\mathfrak{B}_i \cong \boldsymbol{P}_{j\in J}\mathfrak{C}_j,$$

with $\mathfrak{B}_i$ and $\mathfrak{C}_j$ indecomposable for all $i\in I$ and $j\in J$, always implies that there exists a one-to-one map φ of I onto J such that $\mathfrak{B}_i \cong \mathfrak{C}_{\varphi(i)}$ for all $i\in I$.

Our primary concern here will be with the question which finite structures have the unique factorization property. Section 1 is devoted to a brief summary of earlier results concerning this problem. Sections 2 and 3 describe the terminology to be used in the remainder of the paper, and they also contain some simple technical results, mostly not new, that will be needed in the subsequent development. The results in Sections 4-8 are new, except for some simple lemmas; the principal

---

* The paper was presented to the Conference on General Algebra, held in Warsaw, September 7-11, 1964. These investigations were supported in part by the United States National Science Foundation Grant NSF-GP 1612.

results are generalizations of the Birkhoff-Ore Theorem and of the Jónsson-Tarski Theorem discussed in Section 1. In the ninth and final section we mention some open problems connected with the results presented here.

1. A SUMMARY OF EARLIER RESULTS

The meaning of the various technical terms used in this survey will be only roughly indicated here. In many cases the same concepts will be needed in the subsequent development, and more precise definitions can then be found in the next section, but in other cases the reader must be referred to the original sources.

There are three principal methods that have been used to attack the unique factorization problem. The first method is based on the notion of an inner direct product. Any representation

$$\mathfrak{A} \cong \boldsymbol{P}_{i \in I} \mathfrak{B}_i \tag{1}$$

of a structure $\mathfrak{A} = \langle A, 0, R_t \rangle_{t \in T}$ gives rise to a system of substructures $\mathfrak{B}'_i$ of $\mathfrak{A}$, isomorphic to the factors $\mathfrak{B}_i$. Suppose that among the relations R_t there is a partial binary operation $+$ such that, for all $x \in A$, $x+0$ and $0+x$ exist and are equal to x. We then say that $\mathfrak{A}$ is a *structure with a zero element.* For such structures it is possible to give an intrinsic characterization of those finite systems of substructures $\mathfrak{B}'_i$ that correspond to representations of $\mathfrak{A}$ as a direct product. This makes it possible to introduce the concept of an inner direct product of substructures of $\mathfrak{A}$, and to use this notion in place of the more combersome idea of an isomorphic representation of $\mathfrak{A}$ as a direct product. This is the method used in the earliest proof of the unique factorization property for (finite) groups, and in Jónsson-Tarski [7] inner direct products were used to prove that every finite algebra with a zero element has the unique factorization property. Actually it requires only minor changes in the argument given in [7] to prove the following:

THEOREM 1.1. *Every finite structure with a zero element has the unique factorization property.*

Since the conditions in the definition of a zero element seem to be as weak as one can make them and still obtain a workable notion of an inner direct product, this is a highly satisfactory result, and apart from the fact that the finiteness assumption can be replaced by weaker conditions the theorem seems to be the best that one can hope to obtain by this method.

The other two methods use the notion of a factor relation. With the representation (1) there is associated a system of homomorphisms of $\mathfrak{A}$ onto the factors $\mathfrak{B}_i$, and with each such homomorphism there is asso-

ciated an equivalence relation F_i over A, and these relations essentially characterize the representation. By a trivial generalization, for an arbitrary equivalence relation E over A one associates with each direct product representation of the quotient structure $\mathfrak{A}/E$ a system of equivalence relations over A, and one arrives in this manner at the notion of a direct product,

$$E = \prod_{i \in I} F_i \quad \text{or} \quad E = F \times F',$$

of a system of equivalence relations F_i, or of two equivalence relations F and F'. F is called a *factor relation* of E, in symbols

$$F \in \mathrm{FR}(\mathfrak{A}, E),$$

if $E = F \times F'$ for some F'. For simplicity let

$$\mathrm{FR}(\mathfrak{A}) = \mathrm{FR}(\mathfrak{A}, \mathrm{id}_A),$$

where id_A is the identity relation over A.

The second method is based on Ore's theorem for finite dimensional modular lattices. As developed by Birkhoff in [1] this method applies to algebras $\mathfrak{A}$ with a one-element subalgebra (a reflexive element) and having the property that all the congruence relations over $\mathfrak{A}$ are permutable, i. e.,

$$F|G = G|F \quad \text{for all} \quad F, G \in \Theta(\mathfrak{A}).$$

Here $\Theta(\mathfrak{A})$ is the lattice of all congruence relations over $\mathfrak{A}$, and $F|G$ is the relative product of F and G. In this case the lattice addition in $\Theta(\mathfrak{A})$ coincides with relative multiplication,

$$F + G = F|G,$$

and from this it follows that $\Theta(\mathfrak{A})$ is modular. It also follows that the notion of direct product of congruences relations over $\mathfrak{A}$ is a lattice theoretic notion, in fact, for $E, F, F' \in \Theta(\mathfrak{A})$,

$$E = F \times F' \quad \text{iff} \quad F \cap F' = E \text{ and } F + F' = {}^2A,$$

where ${}^2A$ is the universal relation over A. The last observation needed for the application of Ore's theorem is true in every structure $\mathfrak{A}$ with a reflexive element: For any equivalence relations E, F, G and H over A,

$$E = F \times G = F \times H \text{ implies } \mathfrak{A}/G \cong \mathfrak{A}/H.$$

Using these facts, Birkhoff inferred:

THEOREM 1.2. *Every finite algebra with a one-element subalgebra and ith permutable congruence relations has the unique factorization property.*

The third method uses, in addition to the factor relations, the decomposition function and the decomposition projections associated with a given decomposition

$$\mathrm{id}_A = F \times F'. \tag{1}$$

If (1) holds, then $F \cap F' = \mathrm{id}_A$ and $F|F' = {}^2A$. Hence, for all $x, y \in A$ there is a unique element $z \in A$ such that $xFzF'y$. The decomposition function associated with F and F' is the function $\bar{f}$ that correlates to each ordered pair $\langle x, y\rangle$ this unique element z, and the decomposition projections associated with F and F', or with $\bar{f}$, are the maps f and f' of A into itself such that, for all $x, y \in A$, $f(x) = \bar{f}(x, 0)$ and $f'(y) = \bar{f}(0, y)$. Let $\mathrm{DF}(\mathfrak{A})$ be the set of all decomposition functions and $\mathrm{DP}(\mathfrak{A})$ the set of all decomposition projections associated with direct decomposition of id_A.

Various conditions are known, expressed in terms of these concepts, which imply the unique factorization property. The most general results of this kind are probably the ones announced in Chang [2] and Jónsson-Tarski [6] and [8], with detailed proofs appearing in Chang-Jónsson-Tarski [3]. Among these results are the following:

THEOREM 1.3. *For any structure* $\mathfrak{A} = \langle A, 0, R_t\rangle_{t\in T}$ *the following conditions are equivalent to each other, and they imply that* $\mathfrak{A}$ *has the unique factorization property*:

(i) $\mathrm{FR}(\mathfrak{A})$ *is a Boolean algebra under the operations* $|$ *and* $\cap$.

(ii) *For all* $f, g \in \mathrm{DP}(\mathfrak{A})$, $fg = gf$.

(iii) *For all* $f, g \in \mathrm{DP}(\mathfrak{A})$ *and* $x \in A$, *if* $fg(x) = 0$, *then* $gf(x) = 0$.

Observe that in this theorem no finiteness assumptions are made. Actually the three conditions imply that any two decompositions

$$\mathrm{id}_A = \prod_{i\in I} F_i = \prod_{j\in J} G_j$$

have a common refinement

$$F_i = \prod_{j\in J} H_{i,j}, \qquad G_j = \prod_{i\in I} H_{i,j},$$

and from this it follows that id_A has, apart from the order of the factors, at most one decomposition into indecomposable factors. Of course it may happen that there is no such decomposition. Incidentally, in (i) and (ii) our hypothesis that 0 be reflexive can be replaced by the weaker assumption that $R_t \neq \emptyset$ for all $t \in T$.

Among the consequences of 1.3 are the following two theorems:

THEOREM 1.4. *Suppose in the structure* $\mathfrak{A} = \langle A, 0, R_t\rangle_{t\in T}$ *one of the relations* R_t *is a binary relation* $\leqslant$ *that satisfies conditions* (i)-(iii) *below*:

(i) *For all* $x \in A$, $x \leqslant x$.

(ii) *For all* $x \in A$, $x \leqslant 0 \leqslant x$ *implies* $x = 0$.

(iii) *For all* $x, y \in A$ *there exist a positive integer* n *and elements* $z_0 = x, z_1, z_2, \ldots, z_n = y$ *in* A *such that for each* $i < n$ *either* $z_i \leqslant z_{i+1}$ *or* $z_{i+1} \leqslant z_i$.

Then $\mathfrak{A}$ *has the unique factorization property.*

THEOREM 1.5. *Suppose in the structure* $\mathfrak{A} = \langle A, 0, R_t \rangle_{t \in T}$ *one of the relations* R_t *is a binary operation* $+$ *with the properties that, for all* $x, y \in A$,

(i) $0 + x = x + 0$.

(ii) $x + y = 0$ *implies* $x = y = 0$.

Then $\mathfrak{A}$ *has the unique factorization property.*

2. NOTATION AND TERMINOLOGY

The notation and terminology used here are to a large extent the same as in Chang-Jónsson-Tarski [3]. $B \times C$ and $\boldsymbol{P}_{i \in I} A_i$ are the Cartesian products, respectively, of the sets B and C and of the sets A_i $(i \in I)$, and ${}^I A$ is the set of all maps of I into A. We also write $f : I \to A$ for $f \in {}^I A$. A natural number n is identified with the set $\{0, 1, \ldots, n-1\}$, and ${}^n A$ is therefore the set of all n-termed sequences $x = \langle x_0, x_1, \ldots, x_{n-1} \rangle$ all of whose terms belong to A.

If F is a binary relation we write xFy for $\langle x, y \rangle \in F$. $F|G$ is the relative product of the binary relations F and G, $\breve{F}$ is the converse of F, and id_A is the identity relation over A. If $f : A \to B$, then $\ker f$ is the kernel of of f, i. e., the set of all $\langle x, y \rangle \in {}^2 A$ such that $f(x) = f(y)$. From the calculus of binary relations we recall the modular laws:

$$\breve{F}|H \subset H \text{ implies } (F|G) \cap H \subseteq F|(G \cap H),$$

$$H|\breve{F} \subseteq H \text{ implies } H \cap (G|F) \subseteq (H \cap G)|F.$$

Also, if F and G are equivalence relations over the same set A, then the conditions $F|G \subseteq G|F$ and $F|G = G|F$ are equivalent to each other and are necessary and sufficient in order for $F|G$ to be an equivalence relation over A. If these conditions are satisfied, then $F|G$ is equal to the lattice sum $F+G$ of F and G in the lattice of all equivalence relations over A.

As was mentioned in the introduction, the word "structure" will here be understood to mean a system

$$\mathfrak{A} = \langle A, 0, R_t \rangle_{t \in T}$$

where A is a set, R_t is for each $t \in T$ a relation of some finite rank $\varrho(t)$ over A, i. e., a subset of ${}^{\varrho(t)} A$, and 0 is an element of A such that

$\langle 0, 0, \ldots, 0\rangle \in R_t$ for all $t \in T$. We shall actually confine ourselves to structures of some fixed similarity type; i. e., the relations in all the structures are assumed to be indexed by the same set T, and the ranks $\varrho(t)$ are assumed to be the same for all the structures involved.

The Cartesian product of a system of structures

$$\mathfrak{B}_i = \langle B_i, 0_i, S_{i,t}\rangle_{t\in T}, \quad i \in I,$$

is defined, as usual, to be the structure

$$\mathfrak{A} = \langle A, \theta, R_t\rangle_{t\in T}$$

where $A = \boldsymbol{P}_{i\in I} B_i$, $\theta(i) = 0_i$ for all $i \in I$ and, for each $t \in T$, R_t is the set of all $x \in {}^{\varrho(t)}A$ such that

$$\langle x_0(i), x_1(i), \ldots, x_{\varrho(t)-1}(i)\rangle \in S_{i,t} \quad \text{for all} \quad i \in I.$$

The Cartesian product $\mathfrak{B} \times \mathfrak{C}$ of two structures $\mathfrak{B}$ and $\mathfrak{C}$ is defined in a similar manner.

Given a map f of a set A onto a set B, the various maps induced by f will usually be denoted by the same symbol f. Thus if X is a subset of A, then $f(X)$ is the image of X under f, and if $x : I \to A$, then $f(x)$ is the superposition, fx or $f \circ x$, of f on x. In particular, for an n-termed sequence $x = \langle x_0, x_1, \ldots, x_{n-1}\rangle \in {}^nA$, $f(x)$ is the n-termed sequence

$$f \circ x = \langle f(x_0), f(x_1), \ldots, f(x_{n-1})\rangle \in {}^nB.$$

In this manner n-ary relations $R \subseteq {}^nA$ are mapped onto n-ary relations $f(R) \subseteq {}^nB$, and structures $\mathfrak{A} = \langle A, 0, R_t\rangle_{t\in T}$ are mapped onto structures $f(\mathfrak{A}) = \langle B, f(0), f(R_t)\rangle_{t\in T}$. Similar conventions apply to functions in several variables, e. g., if $f : A \times A \to A$ and $g, h : A \to A$, then $f(g, h) : A \to A$. When considering maps of a fixed set A into itself we sometimes identify the elements of A with the corresponding constant functions. Thus if $a \in A$ and $f : A \to A$, then $af = a$ and $fa = f(a)$.

Given an equivalence relation E over a set A, for $x \in A$ we let x/E be the E-class to which x belongs; i. e., x/E is the set of all y such that xEy. The same notation is applied to the various maps induced by the map $x \to x/E$. E. g., if $X \subseteq A$, then X/E is the set of all E-classes x/E with $x \in X$, if $x = \langle x_0, x_1, \ldots, x_{n-1}\rangle \in {}^nA$, then x/E is the member $\langle x_0/E, x_1/E, \ldots, x_{n-1}/E\rangle$ of ${}^n(A/E)$, if $R \subseteq {}^nA$, then R/E is the subset of ${}^n(A/E)$ consisting of all sequences x/E with $x \in R$, and if $\mathfrak{A} = \langle A, 0, R_t\rangle_{t\in T}$ is a structure, then $\mathfrak{A}/E$ is the quotient structure $\langle A/E, 0/E, R_t/E\rangle_{t\in T}$.

Given a structure $\mathfrak{A} = \langle A, 0, R_t\rangle_{t\in T}$ and a system of equivalence relations F_i $(i \in I)$ over A, the canonical epimorphisms of $\mathfrak{A}$ onto $\mathfrak{A}/F_i$ induce a homomorphism f of $\mathfrak{A}$ into the structure

$$\mathfrak{B} = \langle B, \theta, S_t\rangle_{t\in T} = \boldsymbol{P}_{i\in I}\, \mathfrak{A}/F_i.$$

The kernel of f is the equivalence relation

$$E = \bigcap \{F_i : i \in I\},$$

and f therefore induces a one-to-one map f_E of A/E onto B. We say that E is the *direct product* of the relations F_i, in symbols

$$E = \prod_{i \in I} F_i,$$

provided this map f_E is an isomorphism of $\mathfrak{A}/E$ onto $\mathfrak{B}$. In order for this to hold it is necessary and sufficient that the following two conditions be satisfied:

For each $x \in {}^I A$ *there exists* $u \in A$ *such that* $x_i F_i u$ *for all* $i \in I$.

For each $t \in T$ *and* $x \in {}^{\varrho(t)}A$, *if* $x/F_i \in R_t/F_i$ *for all* $i \in I$, *then* $x/E \in R_t/E$.

In the case of two equivalence relations F and F' over A, the direct product, if it exist, is written $F \times F'$. Applying the above criterion to this case, we see that $E = F \cap F'$ is the direct product of F and F' if and only if $F|F' = {}^2A$ and for all $t \in T$ and $x \in {}^{\varrho(t)}A$, the conditions $x/F \in R_t/F$ and $x/F' \in R_t/F'$ jointly imply that $x/E \in R_t/E$.

We say that F is a *factor relation* of E provided $E = F \times F'$ for some F', and we let $\mathrm{FR}(\mathfrak{A}, E)$ be the set of all factor relations of E. In particular, we let

$$\mathrm{FR}(\mathfrak{A}) = \mathrm{FR}(\mathfrak{A}, \mathrm{id}_A).$$

E is said to be *indecomposable* provided $\mathrm{FR}(\mathfrak{A}, E)$ has precisely two members, E and ${}^2A$.

The importance of factor relations is due to the fact that with any isomorphism

$$f : \mathfrak{A}/E \cong \boldsymbol{P}_{i \in I} \mathfrak{B}_i$$

there is associated a system of epimorphisms $g_i : \mathfrak{A} \to \mathfrak{B}_i$ with $g_i(x) = (f(x))_i$ for all $x \in A$, and that

$$E = \prod_{i \in I} (\ker g_i) \quad \text{and} \quad \mathfrak{A}/\ker g_i \cong \mathfrak{B}_i \quad (i \in I).$$

For this reason one can work interchangeably with representations of $\mathfrak{A}/E$ as a Cartesian product of structures and with representations of E as a direct product of factor relations. In particular, $\mathfrak{A}/E$ is indecomposable if and only if E is indecomposable.

3. DECOMPOSITION FUNCTIONS AND PROJECTION MAPS

We henceforth consider a fixed structure $\mathfrak{A} = \langle A, 0, R_t \rangle_{t \in T}$. With a decomposition $\mathrm{id}_A = F \times F'$ there is associated a unique map $\bar{f} : {}^2A \to A$ such that, for all $x, y \in A$, $xFf(x, y)F'y$, and we obtain two maps

$f, f' : A \to A$ by letting $f(x) = \bar{f}(x, 0)$ and $f'(y) = \bar{f}(0, y)$ for all $x, y \in A$. The maps $\bar{f}$ and ordered pairs $\langle f, f' \rangle$ obtained in this manner can be characterized intrinsically, and either one of them completely determines the decomposition.

Definition 3.1. By a *decomposition function* over $\mathfrak{A}$ we mean a map $\bar{f} : {}^2A \to A$ with the following properties:

(i) For all $x \in A$, $\bar{f}(x, x) = x$.

(ii) For all $x, y, z \in A$, $\bar{f}(\bar{f}(x, y), z) = \bar{f}(x, z) = \bar{f}(x, \bar{f}(y, z))$.

(iii) For all $t \in T$, $\bar{f}(R_t, R_t) \subseteq R_t$.

We let $\mathrm{DF}(\mathfrak{A})$ be the set of all decomposition functions over $\mathfrak{A}$.

Definition 3.2. (i) By an *orthogonal pair of projections over* $\mathfrak{A}$ we mean an ordered pair $\langle f, f' \rangle$ of maps $f, f' : A \to A$ with the following properties:

(i_1) $f^2 = f, f'^2 = f', ff' = 0 = f'f$.

(i_2) For all $x, y \in A$, if $f(x) = f(y)$ and $f'(x) = f'(y)$, then $x = y$.

(i_3) For all $x, y \in A$ there exists $z \in A$ such that $f(z) = f(x)$ and $f'(z) = f'(y)$.

(i_4) For all $t \in T$ and $x \in {}^{\varrho(t)}A$, $x \in R_t$ iff $f(x) \in R_t$ and $f'(x) \in R_t$.

(ii) By a *decomposition projection* of $\mathfrak{A}$ we mean a map $f : A \to A$ such that, for some map $f' : A \to A$, $\langle f, f' \rangle$ is an orthogonal pair of projections over $\mathfrak{A}$. We let $\mathrm{DP}(\mathfrak{A})$ be the set of all decomposition projections of $\mathfrak{A}$.

Corollary 3.3. *Let $\mathscr{A}$ be the set of all ordered pairs $\langle F, F' \rangle$ with $\mathrm{id}_A = F \times F'$, and let $\mathscr{B}$ be the set of all orthogonal pairs of projections over $\mathfrak{A}$. For $\langle F, F' \rangle \in \mathscr{A}$ let $\varphi(F, F')$ be the unique map $\bar{f} : {}^2A \to A$ such that*

$$xF\bar{f}(x, y)F'y \quad \text{for all} \quad x, y \in A,$$

for $\bar{f} \in \mathrm{DF}(\mathfrak{A})$ let $\psi(\bar{f}) = \langle f, f' \rangle$ where $f, f' : A \to A$,

$$f(x) = \bar{f}(x, 0) \quad \text{and} \quad f'(x) = \bar{f}(0, x) \text{ for all } x \in A,$$

and for $\langle f, f' \rangle \in A$ let

$$\eta(f, f') = \langle \ker f, \ker f' \rangle.$$

Then φ is a one-to-one map of $\mathscr{A}$ onto $\mathrm{DF}(\mathfrak{A})$, ψ is a one-to-one map of $\mathrm{DF}(\mathfrak{A})$ onto $\mathscr{B}$, η is a one-to-one map of $\mathscr{B}$ onto $\mathscr{A}$, and

$$\eta\psi\varphi(F, F') = \langle F, F' \rangle \quad \text{for all} \quad \langle F, F' \rangle \in \mathscr{A}.$$

Definition 3.4. In the notation of 3.3, a member $\langle F, F' \rangle$ of $\mathscr{A}$ and the members $\bar{f} = \varphi(F, F')$ of $\mathrm{DF}(\mathfrak{A})$ and $\langle f, f' \rangle = \psi(\bar{f})$ of B are said to be *associated* with each other.

One can significantly increase the generality of many results by observing that the set $\mathrm{FR}(\mathfrak{A})$ is unchanged if we adjoin to $\mathfrak{A}$ certain additional relations, provided the new relations are obtained from the old ones by means of certain admissible constructions. Alternatively, we associate with $\mathfrak{A}$ a family $\Delta(\mathfrak{A})$ of relations, and observe that $\mathrm{FR}(\mathfrak{A})$ depends only on this family. To describe $\Delta(\mathfrak{A})$ we introduce some additional notation. If x is an m-termed sequence and y is an n-termed sequence, then we let xy be their juxtaposition, i. e., the sequence

$$\langle x_0, x_1, \ldots, x_{m-1}, y_0, y_1, \ldots, y_{n-1}\rangle.$$

If S_0 and S_1 are relations we let S_0S_1 be the set of all xy with $x \in S_0$ and $y \in S_1$. If $n > 1$ and $S \subseteq {}^nA$, then we let $P(S)$ be the $(n-1)$-ary relation such that, for all $x \in {}^{n-1}A$, $x \in P(S)$ iff $x\langle y\rangle \in S$ for some $y \in A$. If $S \subseteq {}^nA$ and φ is a permutation of n, then we let $S\varphi$ be the set of all sequences of the form $x \circ \varphi = \langle x_{\varphi(0)}, x_{\varphi(1)}, \ldots, x_{\varphi(n-1)}\rangle$ with $x \in S$. Finally, if i, j and n are natural numbers with $i < j < n$, then we let $I_{i,j,n}$ be the set of all $x \in {}^nA$ with $x_i = x_j$.

Definition 3.5. We let $\Delta(\mathfrak{A})$ be the intersection of all families $\mathscr{F}$ with the following properties:

(i) $R_t \in \mathscr{F}$ for all $t \in T$, ${}^nA \in \mathscr{F}$ for every positive integer n, and $I_{i,j,n} \in \mathscr{F}$ whenever i, j and n are natural numbers with $i < j < n$.

(ii) For every integer $n > 1$ and every $S \in {}^nA$, if $S \in \mathscr{F}$, then $P(S) \in \mathscr{F}$ and $S\varphi \in \mathscr{F}$ for every permutation φ of n.

(iii) For all $S_0, S_1 \in \mathscr{F}$, $S_0S_1 \in \mathscr{F}$.

(iv) For every non-empty subfamily $\mathscr{F}'$ of $\mathscr{F}$, $\bigcap \mathscr{F}' \in \mathscr{F}$.

(v) For every directed subfamily $\mathscr{F}'$ of $\mathscr{F}$, $\bigcup \mathscr{F}' \in \mathscr{F}$.

Corollary 3.6. *Suppose F_i $(i \in I)$ are equivalence relations over A, and let*

$$E = \bigcap \{F_i : i \in I\}.$$

Then

$$E = \prod_{i \in I} F_i$$

iff the following conditions hold:

(i) *For each $x \in {}^IA$ there exists $u \in A$ such that $x_i F_i u$ for all $i \in I$.*

(ii) *For all $S \in \Delta(\mathfrak{A})$ and $x \in {}^nA$, where n is the rank of S, if $x/F_i \in S/F_i$ for all $i \in I$, then $x/E \in S/E$.*

Corollary 3.7. *A map $\bar{f} : {}^2A \to A$ belongs to* $\mathrm{DF}(\mathfrak{A})$ *iff* 3.1(i), (ii) *hold and $\bar{f}(S, S) \subseteq S$ for all $S \in \Delta(\mathfrak{A})$.*

Corollary 3.8. *In order for an ordered pair $\langle f, f'\rangle$ of maps $f, f' : A \to A$ to be an orthogonal pair of projections over $\mathfrak{A}$ it is necessary and sufficient that* $3.2(\mathrm{i}_1)$-(i_3) *be satisfied, as well as the following condition:*

(i_4') *For all* $S \in \Delta(\mathfrak{A})$ *and* $x \in {}^n A$, *where* n *is the rank of* S, $x \in S$ *iff* $f(x) \in S$ *and* $f'(x) \in S$.

We conclude this section with a short list of additional properties of decomposition functions and of decomposition projections. These properties will be frequently used in the subsequent sections without being explicitly referred to.

COROLLARY 3.9. *If* $\bar{f} \in \mathrm{DF}(\mathfrak{A})$, *anf if* $\langle f, f' \rangle$ *is the orthogonal pair of projections associated with* $\bar{f}$, *then for all* $x, y, z, u \in A$ *the following conditions hold*:

(i) $\bar{f}(x, y) = \bar{f}\big(f(x), f'(y)\big)$.

(ii) $\bar{f}(x, y) = \bar{f}(z, u)$ *iff* $f(x) = f(z)$ *and* $f'(y) = f'(u)$.

(iii) $\bar{f}\big(f(x), f'(x)\big) = x$.

(iv) $\bar{f}(x, y) = z$ *iff* $f(x) = f(z)$ *and* $f'(y) = f'(z)$.

(v) $f\bar{f}(x, y) = f(x)$ *and* $f'\bar{f}(x, y) = f'(y)$.

(vi) $f(x) = x$ *iff* $f'(x) = 0$.

4. *DIVISIBILITY AND SET-INCLUSION*

In the proof of the unique factorization theorem for finite algebras with a zero element a fundamental lemma asserts that if $A = B \times B' = C \times C'$ and $B \subseteq C$, then B is a factor of C. In other words, among the factors of A the relations of set-inclusion and divisibility coincide. If $\mathfrak{A}$ is an algebra with permutable congruence relations, and if F and G are members of $\mathrm{FR}(\mathfrak{A})$ with $F \subseteq G$, then $G \in \mathrm{FR}(\mathfrak{A}, F)$. Thus it is also the case here that set-inclusion and divisibility coincide. Although these two results sound similar, it is easy to see that in situations where both of them apply they do not say the same thing. In fact the former, when translated into the language of factor relations, is a special case of 4.2 below, a result that applies to arbitrary structures. On the other hand, in generalizing the second result, in 4.6, we are forced to retain at least one instance of the permutability assumption.

LEMMA 4.1. *If* $\langle f, f' \rangle$ *and* $\langle g, g' \rangle$ *are orthogonal pairs of projections over* $\mathfrak{A}$, *then the conditions* $\ker f \subseteq \ker g$ *and* $gf = g$ *are equivalent, and they imply that*

$$gf' = 0, \quad g'f' = f' \quad \text{and} \quad g'fg' = fg'.$$

Proof. By 3.2(i), $f(x) = f\big(f(x)\big)$. Hence, if $\ker f \subseteq \ker g$, then $g(x) = gf(x)$. Conversely, if $g = gf$, then $\ker g = \ker gf \supseteq \ker f$.

Assuming that $gf = g$, we have $gf' = gff' = g0 = 0$. Also, the conditions $g'(x) = x$ and $g(x) = 0$ are equivalent, and applying this with x replaced by $f'(x)$ we find that $g'f' = f'$. The same argument with x

replaced by $fg'(x)$ yields the formula $g'fg' = fg'$, since we know that $gfg' = gg' = 0$.

THEOREM 4.2. *If*

$$\mathrm{id}_A = F \times F' = G \times G' \quad \text{and} \quad F \subseteq G,$$

and if $\langle f, f' \rangle$ *and* $\langle g, g' \rangle$ *are the orthogonal pairs of projections associated with* $\langle F, F' \rangle$ *and* $\langle G, G' \rangle$, *then*

$$G' = (\ker fg') \times (\ker f'g').$$

Proof. Let H and H' be the kernels of fg' and $f'g'$, respectively. Obviously the kernel G' of g' is contained in both H and H'. On the other hand, the conditions $f(x) = f(y)$ and $f'(x) = f'(y)$ jointly imply that $x = y$, and applying this with x and y replaced by $g'(x)$ and $g'(y)$ we see that $H \cap H' \subseteq G'$. Thus $G' = H \cap H'$.

To prove that $H|H' = {}^2A$ we consider two elements $x, y \in A$ and wish to find $z \in A$ such that $xHzH'y$. By $3.2(\mathrm{i}_3)$ we can find $z \in A$ such that $f(z) = fg'(x)$ and $f'(z) = f'g'(y)$. Consequently, by 4.1, $g(z) = gf(z) = gfg'(x) = gg'(x) = 0$, whence it follows that $g'(z) = z$. Thus $fg'(z) = f(z) = fg'(x)$ and $f'g'(z) = f'(z) = f'g'(y)$, and therefore $xHzH'y$.

Finally suppose $S \in \Delta(\mathfrak{A})$ is of rank k, and $x \in {}^kA$ is such that $x/H \in S/H$ and $x/H' \in S/H'$. Then there exist $y, z \in S$ such that $x/H = y/H$ and $x/H' = z/H'$. Thus $fg'x = fg'y \in S$ and $f'g'x = f'g'z \in S$, which implies that $g'x \in S$, $x/G' = g'x/G' \in S/G'$. This proves that $G' = H \times H'$, as was to be shown.

LEMMA 4.3. *Assume that the hypothesis of* 4.2 *is satisfied. Then* $\ker fg' = G'$ *iff* $F = \mathrm{id}_A$, *and* $\ker f'g' = G'$ *iff* $0/F = 0/G$. *In case* A *is finite,* $\ker fg' = G'$ *iff* $F = G$.

Proof. If $\ker fg' = G'$, then $\ker f'g' = {}^2A$, hence $f'g'(x) = f'g'(y)$ for all $x, y \in A$. Since $f'g'(0) = 0$, this implies that $f'g' = 0$. But then, by 4.1, $f' = f'g'f' = 0f' = 0$, $F' = {}^2A$, $F = \mathrm{id}_A$. Conversely, if $F = \mathrm{id}_A$, then $f = \mathrm{id}_A$, $fg' = g'$, $\ker fg' = \ker g' = G'$.

If $\ker f'g' = G'$, then $\ker fg' = {}^2A$, $fg' = 0$. From this it follows that if $g(x) = 0$, and therefore $g'(x) = x$, then $f(x) = 0$. I. e., it follows that $0/G \subseteq 0/F$. But $F \subseteq G$, so that $0/F = 0/G$. Conversely, if $0/F = 0/G$, then for all $x \in A$ the condition $g(x) = 0$ implies that $f(x) = 0$. Thus from the fact that $gg' = 0$ we infer that $fg' = 0$, $f'g' = g'$, $\ker g'f' = G'$.

Finally, if A is finite, then all the F-classes have the same number of elements, and all the G-classes have the same number of elements. Under these conditions, if $0/F = 0/G$, then it cannot happen that x/F is a proper subset of x/G, and we must therefore have $F = G$.

Suppose $\mathrm{id}_A = G \times G'$. If G' is not indecomposable, then $G' = H \times H'$ with $G' \neq H, H'$. Hence it follows that $G' \subset H \subset {}^2A$ and $\mathrm{id}_A \subset G \cap H \subset G$,

and that both H and $G \cap H$ are members of $\mathrm{FR}(\mathfrak{A})$. In other words, regarding $\mathrm{FR}(\mathfrak{A})$ as a partially ordered set under set-inclusion, we see that if either G' is covered by ${}^2A$ or G covers id_A, then G' is indecomposable. For finite structures we are now able to obtain a converse of the second implication. A partial converse of the first implication will be given in 4.7.

COROLLARY 4.4. *If A is finite, $\mathrm{id}_A = G \times G'$, and G' is indecomposable, then G covers id_A in* $\mathrm{FR}(\mathfrak{A})$.

Proof. According to 4.2 and 4.3 the existence of a factor relation F with $\mathrm{id}_A \subset F \subset G$ would yield a direct decomposition $G' = H \times H'$ with $H, H' \neq G'$.

Observe that if every element of A is known to be reflexive, then the finiteness condition in the preceding corollary may be omitted. In fact, if $F \in \mathrm{FR}(\mathfrak{A})$ is such that $\mathrm{id}_A \subset F \subset G$, then $u/F \subset u/G$ for some $u \in A$, and we may apply 4.2 and 4.3 with 0 replaced by u to infer that G' is not indecomposable.

LEMMA 4.5. *If $\mathrm{id}_A = F \times F = G \times G'$, and if $\langle f, f' \rangle$ and $\langle g, g' \rangle$ are the orthogonal pairs of projections associated with $\langle F, F' \rangle$ and $\langle G, G' \rangle$, then the following conditions are equivalent*:

(i) $(F \cap G)|F' = F'|(F \cap G)$.

(ii) $F \cap \big(F'|(F \cap G)|F'\big) \subseteq G$.

(iii) $F \cap G = F \cap \ker gf'$.

(iv) $\ker gf' = (F \cap G)|F'$.

Proof. That (i) implies (ii) is an easy consequence of the modular law. Assume (ii). If $\langle x, y \rangle \in F \cap G$, then

$$f'(x)F'xF \cap GyF'f'(y) \quad \text{and} \quad f'(x)Ff'(y),$$

which by (ii) implies that $f'(x)Gf'(y)$, $gf'(x) = gf'(y)$, $\langle x, y \rangle \in \ker gf'$. On the other hand, if $\langle x, y \rangle \in F \cap \ker gf'$, then

$$xF'f'(x)F \cap Gf'(y)F'y \quad \text{and} \quad xFy,$$

and an application of (ii) yields $\langle x, y \rangle \in G$. Thus (ii) implies (iii).

Assume (iii). If $a(F \cap G)|F'b$, then there exists an element x such that $aF \cap GxF'b$. Since $F'|F = {}^2A$, there also exists an element y such that $aF'yFb$. In order to prove (i) it suffices to show that yGb.

We have

$$\begin{aligned} f(a) &= f(x), \quad g(a) = g(x), \quad f'(x) = f'(b), \\ f'(a) &= f'(y), \quad f(y) = f(b). \end{aligned} \tag{1}$$

From the first two of these formulas we infer by (iii) that $gf'(a) = gf'(x)$. In view of the third and fourth formulas in (1) this can also be written $gf'(y) = gf'(b)$, and from this and the last formula in (1) we infer by (iii) that yGb, as was to be shown.

Obviously F' is contained in the kernel of gf', and if (iii) holds, then $F \cap G \subseteq \ker gf'$, and hence

$$(F \cap G)|F' \subseteq \ker gf'.$$

On the other hand, if $gf'(x) = gf'(y)$, then

$$xF'f(x)F \cap Gf'(y)F'y.$$

Thus

$$\ker gf' \subseteq F'|(F \cap G)|F',$$

and reference to (i) completes the proof of (iv). Finally, if (iv) holds, then $(F \cap G)|F'$ is an equivalence relation, and this implies that (i) holds.

THEOREM 4.6. *If* $\mathrm{id}_A = F \times F' = G \times G'$, $F \subseteq G$ *and* $F|G' = G'|F$, *then* $F = G \times (F|G')$.

Proof. By 4.5, $\ker fg' = F|G'$, and by 4.2,

$$\mathrm{id}_A = G \times (\ker fg') \times (\ker f'g').$$

Therefore $G \times (\ker fg')$ exists. Furthermore, by 4.5,

$$F = F \cap G = G \cap (\ker fg'),$$

so that

$$F = G \times (\ker fg') = G \times (F|G').$$

COROLLARY 4.7. *If, for all* $F, G, G' \in \mathrm{FR}(\mathfrak{A})$ *with* $\mathrm{id}_A = G \times G'$, *the condition* $F \subseteq G$ *implies that* $F|G' = G'|F$, *then the indecomposable members of* $\mathrm{FR}(\mathfrak{A})$ *are precisely the members covered by* ${}^2A$.

Proof. Obviously every member of $\mathrm{FR}(\mathfrak{A})$ that is covered by ${}^2A$ is indecomposable. On the other hand, if $F, G \in \mathrm{FR}(\mathfrak{A})$ and $F \subset G \subset {}^2A$, then it follows from 4.6 that $G \in \mathrm{FR}(\mathfrak{A}, F)$, so that F is not indecomposable.

5. A GENERALIZATION OF THE BIRKHOFF-ORE THEOREM

Most of the known unique factorization theorems make use of the fact that if two factor relations F and G of a structure $\mathfrak{A}$ (with a reflexive element) have a common complement, then $\mathfrak{A}/F$, and $\mathfrak{A}/G$ are isomorphic. This is usually combined with some kind of an exchange property in order to show that in two decompositions into indecomposable factors the factors can be paired off in such a way that corresponding quotient structures are isomorphic. In the next lemma we formulate a rather weak exchange property that still turns out to be sufficient for this purpose. The fact that it involves decompositions into two factors only turns out to be convenient, although probably not essential, for the applications both in the present section and in Section 8.

LEMMA 5.1. *Suppose A is finite, and assume that the conditions*

$$\mathrm{id}_A = F \times F' = G \times G', \qquad F \text{ is indecomposable},$$

always imply that there exists H such that $\mathrm{id}_A = H \times F'$ and either $H \supseteq G$ or $H \supseteq G'$. Then $\mathfrak{A}$ has the unique factorization property.

Proof. We shall prove by induction on m that if

$$\mathrm{id}_A = F_0 \times F_1 \times \ldots \times F_{m-1} \times K = G_0 \times G_1 \times \ldots \times G_{n-1} \times K,$$

where all the factors F_i and G_j are indecomposable, then $m = n$ and there exists a permutation φ of m such that $\mathfrak{A}/F_i \cong \mathfrak{A}/G_{\varphi(i)}$ for $i = 0, 1, \ldots, m-1$.

Let $G' = G_1 \times G_2 \times \ldots \times G_{n-1} \times K$. By successive applications of the hypothesis we obtain $H_0, H_1, \ldots, H_{m-1}$, each of them containing either G_0 or G', such that

$$\mathrm{id}_A = H_0 \times H_1 \times \ldots \times H_{i-1} \times F_i \times \ldots \times F_{m-1} \times K \tag{1}$$

for $i = 1, 2, \ldots, m$. In particular, for $i = m$,

$$\mathrm{id}_A = H_0 \times H_1 \times \ldots \times H_{m-1} \times K.$$

Consequently the direct product of all those factors H_i that contain G_0 must be G_0, and the direct product of all the remaining factors (including K) must be G'. Since G_0 is indecomposable, this implies that $H_p = G_0$ for some $p < m$. Thus

$$\begin{aligned} \mathrm{id}_A &= H_0 \times H_1 \times \ldots \times H_{p-1} \times H_{p+1} \times \ldots \times H_{m-1} \times (G_0 \times K) \\ &= G_1 \times G_2 \times \ldots \times G_{n-1} \times (G_0 \times K). \end{aligned}$$

By comparing two successive values of i in (1) we see that $\mathfrak{A}/F_i \cong \mathfrak{A}/H_i$ for $i = 0, 1, \ldots, m-1$ and, in particular, $\mathfrak{A}/F_p \cong \mathfrak{A}/G_0$. The proof is therefore easily completed by induction.

LEMMA 5.2. *If A is finite, and if*

$$\mathrm{id}_A = F \times F' = G \times G' = G \cap F' = F \cap G',$$

then $\mathrm{id}_A = G \times F'$.

Proof. From the fact that

$$F \cap F' = \mathrm{id}_A \quad \text{and} \quad F \mid F' = {}^2A$$

it follows that each F-class has exactly one element in common with each F'-class. Consequently, if the number of F-classes is m and the number of F'-classes is m', then the order of A is mm', each F-class has exactly m' elements, and each F'-class has exactly m elements.

Since $G \cap F' = \mathrm{id}_A$, each G-class has at most one element in common with each F'-class. Consequently the number of elements in each G-

is at most m', and the number of G-classes is at least m. Hence, and by symmetry, the number of G'-classes and the number of elements in each G'-class must be equal to m and m', the corresponding numbers for F. Now the m' elements in each G-class belong to distinct F'-classes, and each G-class therefore has an element in common with each F'-class. Thus

$$G|F' = {}^2A. \tag{1}$$

To complete the proof it suffices to show that if $S \in \Delta(\mathfrak{A})$ is of rank k, and if $x, y, z \in {}^kA$ are such that

$$x/G = y/G, \quad y/F' = z/F', \quad x, z \in S, \tag{2}$$

then $y \in S$.

Let $\bar{f}$ be the decomposition function associated with $\langle F, F' \rangle$. Considering a fixed sequence $x \in S$, let $y' = \bar{f}(x, y)$ for all $y \in {}^kA$. The correspondence $y \to y'$ maps ${}^kA$ onto x/F. When restricted to x/G this map is one-to-one because the conditions $x/G = y/G$ and $y/F' = y'/F'$ completely determine y when y' is given. Thus x/G is mapped in a one-to-one manner onto x/F. Also, S is mapped into itself, and $S \cap (x/G)$ is therefore mapped into $S \cap (x/F)$. Thus the number of sequences in $S \cap (x/G)$ cannot exceed the number in $S \cap (x/F)$. By symmetry, the two sets must contain the same number of sequences, and the correspondence $y \to y'$ therefore maps the former onto the latter.

Assume now that relations (2) holds. Then $y \in x/G$ and $y' = \bar{f}(x, y) = \bar{f}(x, z) \in S$. Consequently $y \in S$, as was to be shown.

LEMMA 5.3. *If, for each $i \in I$, F_i and G_i are equivalence relations over A with $F_i \subseteq G_i$, and if the direct product*

$$\prod_{i \in I} F_i$$

exists, then the direct product

$$\prod_{i \in I} G_i$$

also exists.

Proof. By hypothesis, for each $x \in {}^IA$ there exists $u \in A$ such that $x_i F_i u$ for all $i \in I$. Clearly this implies the corresponding property with F_i replaced by G_i; in fact, we use the same element u. Also by hypothesis, if $S \in \Delta(\mathfrak{A})$ is of rank k, and if $x \in {}^kA$ is such that $S \cap (x/F_i) \neq \emptyset$ for all $i \in I$, then

$$S \cap \bigcap \{x/F_i : i \in I\} \neq \emptyset,$$

and in order to complete the proof it is sufficient to establish the corresponding property with F_i replaced by G_i.

Suppose therefore that $S \cap (x/G_i) \neq \emptyset$ for all $i \in I$. For each $i \in I$ we can then find a sequence $y^{(i)} \in S$ such that $x/G_i = y^{(i)}/G_i$. There exists a sequence $z \in {}^kA$ such that $z/F_i = y^{(i)}/F_i$ for all $i \in I$. Thus S has an element in common with each of the sets z/F_i, namely the sequence $y^{(i)}$, and it therefore has a member in common with their intersection. Inasmuch as $x/G_i = z/G_i$, it follows that

$$S \cap \bigcap \{x/G_i : i \in I\} \supseteq S \cap \bigcap \{z/F_i : i \in I\} \neq \emptyset.$$

We now prove the promised generalization of the Birkhoff-Ore Theorem, essentially by following step by step the proof given by Birkhoff in [1], pp. 94-95.

THEOREM 5.4. *Suppose A is finite, and let $\mathscr{F}$ be the smallest family of equivalence relations over A with the properties that $\mathrm{id}_A \in \mathscr{F}$ and that, for all $E \in \mathscr{F}$ and $F, G \in \mathrm{FR}(\mathfrak{A}, E)$, $F \cap G \in \mathscr{F}$. If, for all $E \in \mathscr{F}$ and for all $F, F', G \in \mathrm{FR}(\mathfrak{A}, E)$, the condition $E = F \times F'$ implies that $(F \cap G)|F' = F'|(F \cap G)$, then $\mathfrak{A}$ has the unique factorization property.*

Proof. We shall establish the following property, which includes the hypothesis of 4.1 as a special case, and therefore implies the theorem:

If $E \in \mathscr{F}$ and

$$E = F \times F' \times K = G \times G' \times K, \tag{1}$$

then there exist H, H' such that

$$E = H \times H' \times F' \times K, \quad H \supseteq G, \quad H' \supseteq G'. \tag{2}$$

This statement trivially holds when $E = {}^2A$ and, more generally, it is true whenever $E = K$. Proceeding by induction we may therefore assume that it holds whenever E is replaced by a larger member of $\mathscr{F}$, and also that for the relation E under consideration it holds whenever K is replaced by a smaller relation. We consider three cases.

Case 1. $F \cap G' \cap K = G \cap F' \cap K = E$.

In this case $E = G \times F' \times K$ by 5.2, and (2) therefore holds with $H = G$ and $H' = {}^2A$.

Case 2. $E \subset F \cap G' \cap K$.

Let

$$E_1 = F \cap G' \cap K, \quad F_1 = F, \quad F_1' = E_1|F', \quad G_1 = E_1|G, \quad G_1' = G'.$$

By hypothesis, F_1' and G_1 are equivalence relations over A, and by the modular law

$$F_1 \cap F_1' \cap K = (E_1|F') \cap (F \cap K) = E_1|(F' \cap F \cap K) = E_1|E = E_1,$$
$$G_1 \cap G_1' \cap K = (E_1|G) \cap (G' \cap K) = E_1|(G \cap G' \cap K) = E_1|E = E_1.$$

Consequently, by 5.3,

$$E_1 = F_1 \times F_1' \times K = G_1 \times G_1' \times K.$$

Since $E \subset E_1 \in \mathscr{F}$, it follows that there exist H, H' such that

$$E_1 = H \times H' \times F_1' \times K, \quad G \subseteq H, \quad G' \subseteq H'.$$

We have

$$H \cap H' \cap F' \cap K = E_1 \cap F' = (F \cap G' \cap K) \cap F' = E,$$
$$(H \cap H' \cap K)|F' = (H \cap H' \cap K)|E_1|F' = (H \cap H' \cap K)|F_1' = {}^2A.$$

In order to prove (2) for the present case it therefore suffices to show that if $S \in \Delta(\mathfrak{A})$, and if $x, y, z \in {}^kA$ are such that

$$x/H \cap H' \cap K = y/H \cap H' \cap K, \quad x/F' = z/F' \quad \text{and} \quad y, z \in S,$$

then there exists $u \in {}^kA$ such that

$$x/E = u/E \quad \text{and} \quad u \in S. \tag{3}$$

In any case, since $x/F_1' = z/F_1'$, there exists $v \in {}^kA$ such that

$$x/E_1 = v/E_1 \quad \text{and} \quad v \in S.$$

Thus

$$x/F \cap K = v/F \cap K, \quad x/F' = z/F', \quad v, z \in S,$$

and because of (1) this yields a sequence u that satisfies (3).

In the above argument H was so chosen that it contains E_1, which is not contained in G. Under the hypothesis of the second case we can therefore strengthen (2) by requiring H to contain G properly. This observation will be used in the treatment of the next case.

Case 3. $E \subset F' \cap G \cap K$.

According to Case 2 there exist H_1, H_1' such that

$$E = H_1 \times H_1' \times G' \times K, \quad F \subset H_1, \quad F' \subseteq H_1'.$$

Apply 4.6 to obtain $\overline{F}$ such that $F' = H_1' \times \overline{F}$. Then

$$E = F \times \overline{F} \times (H_1' \times K) = H_1 \times G_1' \times (H_1' \times K).$$

If $H_1' \neq {}^2A$, then $H_1' \times K \subset K$, so that the inductive hypothesis applies and yields H_2, H_2' such that

$$E = H_2 \times H_2' \times \overline{F} \times H_1' \times K, \quad H_1 \subseteq H_2, \quad G' \subseteq H_2'.$$

Again applying 4.6, we obtain $\bar{G}$ such that $G' = H_2 \times \bar{G}$. Thus

$$E = H_2 \times F' \times (H_2' \times K) = G \times \bar{G} \times (H_2' \times K). \tag{4}$$

Observe that H_2' cannot be equal to ${}^2A$, for this would yield $E = F \times F' \times K = H_2 \times F' \times K$, which is impossible because $F \subset H_2$. Thus $H_2' \times K \subset K$, and the inductive hypothesis applies to (4), yielding H_3, H_3' such that

$$E = H_3 \times H_3' \times F' \times H_2' \times K, \quad G \subset H_3, \quad \bar{G} \subseteq H_3'.$$

Consequently (2) holds with $H = H_3$ and $H' = H_3' \times H_2'$.

It only remains to consider the subcase when $H_1' = {}^2A$, and therefore

$$E = F \times F' \times K = H_1 \times G' \times K.$$

If $F \cap H_1 \cap K = E$, then $F \cap K = E$, $F' = {}^2A$, and we may take $H = G$ and $H' = G'$. If, on the other hand, $F \cap H_1 \cap K \supset E$, then Case 2 applies with G and G' replaced by G' and H_1, and yields H_2, H_2' such that

$$E = H_2 \times H_2' \times F' \times K, \quad H_1 \subseteq H_2, \quad G' \subset H_2'.$$

Observe that $F \subset H_2$, so that $H_2' \neq {}^2A$. By 4.6 there exists $\bar{G}$ such that $G' = H_2' \times \bar{G}$. Thus

$$E = H_2 \times F' \times (H_2' \times K) = G \times \bar{G} \times (H_2' \times K)$$

with $H_2' \times K \subset K$, and one more application of the inductive hypothesis yields H_3, H_3' such that

$$E = H_3 \times H_3' \times F' \times H_2' \times K, \quad G \subseteq H_3, \quad \bar{G} \subseteq H_3'.$$

As before, (2) holds with $H = H_3$ and $H' = H_3' \times H_2'$.

COROLLARY 5.5. *Suppose A is finite, and let $\mathscr{F}$ be as in* 5.4. *If the lattice of equivalence relations over A that is generated by $\mathscr{F}$ is modular, then $\mathfrak{A}$ has the unique factorization property.*

Proof. If $E \in \mathscr{F}$ and $E = F \times F' = G \times G'$, then F, F', G, G' belong to $\mathscr{F}$, and therefore

$$F \cap \big(F' \mid (F \cap G) \mid F'\big) \subseteq F \cap \big((F \cap G) + F'\big) = (F \cap G) + (F \cap F')$$
$$= F \cap G \subseteq G.$$

Applying 4.5 to the quotient structure $\mathfrak{A}/E$ we infer that $F \cap G$ and F' commute. Hence $\mathfrak{A}$ has the unique factorization property by 5.4.

In particular, when applied to algebras this shows that instead of assuming that the congruence relations permute we can make the weaker assumption that the lattice $\Theta(\mathfrak{A})$ of all congruence relations over $\mathfrak{A}$ is modular.

6. STRUCTURES WITH A CANCELABLE IDEMPOTENT

The next three sections will be devoted to the proof of the following result:

THEOREM 6.1. *Suppose A is finite, and assume that there exists a partial binary operation $+$ in $\Delta(\mathfrak{A})$ with the following properties:*

(Z_1) *For all $x \in A$, $0+x$ and $x+0$ exist and are equal.*

(Z_2) *For all $x, y \in A$, if $0+x = 0+y$, then $x = y$.*

Then $\mathfrak{A}$ has the unique factorization property.

The proof of this theorem will be based on a series of lemmas. In order to avoid repetition we assume once and for all that $+$ is a partial binary operation in $\Delta(\mathfrak{A})$ that satisfies (Z_1) and (Z_2), and that

$$\mathrm{id}_A = F \times F' = G \times G'.$$

As usual we let $\bar{f}$ and $\bar{g}$ be the decomposition functions associated with $\langle F, F' \rangle$ and $\langle G, G' \rangle$, and we let $\langle f, f' \rangle$ and $\langle g, g' \rangle$ be the associated orthogonal pairs of projections. An element $a \in A$ will be said to be *commuting* if, for all $x \in A$, $a+x$ and $x+a$ exist and are equal. If, for all $x, y \in A$, the condition that $a+x$ and $a+y$ exist and are equal implies that $x = y$, then a is said to be *cancelable*. (In every case where this property will be used, a will be known to be commuting.)

In this section we list a number of elementary consequences of these assumptions. Many of these properties can be found in Chang-Jónsson-Tarski [3], although there they are stated for binary operations only. It may be of some interest to observe that 6.2 holds for an arbitrary partial binary operation $+$ in $\Delta(\mathfrak{A})$, that the properties in 6.3 depend on (Z_1), and that in proving 6.4 we make use of both (Z_1) and (Z_2).

LEMMA 6.2. *For all $x, y, z, u \in A$, if $x+y$ and $z+u$ exist, then $\bar{f}(x, z) + \bar{f}(y, u)$ exists and is equal to $\bar{f}(x+y, z+u)$.*

Proof. Apply 3.7 with S replaced by $+$.

LEMMA 6.3. *For all $x, y, z, u \in A$, the following statements hold:*

(i) *$x+y$ exists iff $f(x)+f(y)$ and $f'(x)+f'(y)$ exist.*

(ii) *$x+y$ exists iff $f(x)+y$ and $f'(x)+y$ exist.*

(iii) *$x+y$ exist iff $x+f(y)$ and $x+f'(y)$ exist.*

(iv) *If $x+y$ exists, then $f(x+y) = f(x)+f(y)$.*

(v) $f(x)+f'(y) = \bar{f}(x, y)+0 = f'(y)+f(x)$.

(vi) $f(x)+f'(x) = x+0$.

(vii) *Suppose $x+y$ and $z+u$ exist. Then $x+y = z+u$ iff $f(x)+f(y) = f(z)+f(u)$ and $f'(x)+f'(y) = f'(z)+f'(u)$.*

(viii) *Suppose* $x+y$ *and* $y+x$ *exist. Then* $x+y = y+x$ *iff* $f(x)+y = y+f(x)$ *and* $f'(x)+y = y+f'(x)$.

(ix) $fgf'(x)+fg'f'(x) = 0$.

(x) $fgf'(x)+gf(x) = f'gf(x)+fg(x)$.

(xi) $fgf'(x)$ *is commuting.*

Proof. Assuming that $x+y$ exists, apply 6.2 with $z = u = 0$ to infer that $f(x)+f(y)$ exists and is equal to $f(x+y)$. Similarly one sees that $f'(x)+f'(y)$ exists and is equal to $f'(x+y)$. This proves (iv) and the "only if" part of (i). To prove the "if" part of (i), apply 6.2 with x, y, z and u replaced by $f(x)$, $f(y)$, $f'(x)$ and $f'(y)$, making use of the fact (3.9(iii)) that $\bar{f}\big(f(x), f'(x)\big) = x$.

If $x+y$ exists, then by (i) the sum of $ff(x) = f(x)$ and $f(y)$ exists. Since the sum of $f'f(x) = 0$ and $f'(y)$ also exists, we infer by a second application of (i) that $f(x)+y$ exists, and a similar argument shows that $f'(x)+y$ exists. Conversely, if these last two sums exist, then by repeated use of (i), $f(x)+f(y) = ff(x)+f(y)$ and $f'(x)+f'(y) = f'f'(x)+f'(y)$ exist, and hence $x+y$ exists. This proves (ii), and (iii) can be proved similarly.

The existence of the sums involved in the remainder of the proof will be guaranteed by (i) and (iii) together with 6.2.

We have

$$\begin{aligned} f(x)+f'(y) &= \bar{f}(x, 0)+\bar{f}(0, y) = \bar{f}(x)+, (0+y) \\ &= \bar{f}(x+0, y+0) = \bar{f}(x, y)+\bar{f}(0, 0) \\ &= \bar{f}(x, y)+0. \end{aligned}$$

The other half of (v) is proved similarly, and (vi) follows by taking $y = x$.

(vii) is an easy consequence of (iv). Assuming that $x+y$ and $y+x$ exist, if $x+y = y+x$, then

$$f\big(f(x)+y\big) = f(x+y) = f(y+x) = f\big(y+f(x)\big),$$

$$f'\big(f(x)+y\big) = f'(0+y) = f'(y+0) = f'\big(y+f(x)\big),$$

so that $f(x)+y = y+f(x)$. Similarly $f'(x)+y = y+f'(x)$. Conversely, if these last two equations hold, then

$$f(x+y) = f\big(f(x)+y\big) = f\big(y+f(x)\big) = f(y+x)$$

and similarly $f'(x+y) = f'(y+x)$, so that $x+y = y+x$. This proves (viii). To prove (ix) we compute

$$fgf'(x)+fg'f'(x) = f\bar{g}\big(f'(x), f'(x)\big)+0 = ff'(x)+0 = 0+0 = 0.$$

Both sides of (x) are mapped onto the same element by f, namely $fg(x)+0$, and they are both mapped onto $0+f'gf(x)$ by f'. Consequently (x) holds.

The element $fgf'(x)$ commutes with $f'(y)$ by (v), and it commutes with $f(y)$ by (v) and (viii). By a second application of (viii) we infer that $fgf'(x)$ commutes with y. Thus (xi) holds.

LEMMA 6.4. *For all $x, y, z, u \in A$, the following statements hold:*

(i) $f(x)+f'(y) = f(z)+f'(u)$ *iff* $f(x) = f(z)$ *and* $f'(y) = f'(u)$.

(ii) *If $x+y$ and $x+z$ exist and if $f(x)+y = f(x)+z$, then $x+y = x+z$.*

(iii) *If x is cancelable, then so is $f(x)$.*

(iv) *$fgf'(x)$ is cancelable.*

(v) $fgf'g = fg'fg$.

(vi) $\ker fgf' = \ker fg'f'$.

(vii) *If $fg(x) = fg(y)$ and $fg'(x) = fg'(y)$, then $f(x) = f(y)$.*

(viii) *If $fg(x) = fg(y)$ and $fg'(x) = fg'(y)$, then $fgf'(x) = fgf'(y)$.*

(ix) *If $fg(x) = fg(z)$ and $fg'(y) = fg'(u)$, then $f\bar{g}(x, y) = f\bar{g}(z, u)$.*

(x) *If $fg(x) = fg(y)$ and $fg'f'(x) = fg'f'(y)$, then $fgf(x) = fgf(y)$.*

Proof. Applying f and f' to the first equation in (i) we obtain

$$f(x)+0 = f(z)+0 \quad \text{and} \quad 0+f'(y) = 0+f'(u),$$

and because of (Z_2) this yields $f(x) = f(z)$ and $f'(y) = f'(u)$. The implication in the opposite direction is obvious.

Under the hypothesis of (ii),

$$f(x+y) = f\big(f(x)+y\big) = f\big(f(x)+z\big) = f(x+z),$$

and applying f' to the equation $f(x)+y = f(x)+z$ we obtain

$$0+f'(y) = 0+f'(z), \quad f'(y) = f'(z), \quad f'(x+y) = f'(x+z).$$

Consequently, $x+y = x+z$.

If x is cancelable and $f(x)+y = f(x)+z$, then $f'(y) = f'(z)$ and $f(x)+f(y) = f(x)+f(z)$. From the latter equation it readily follows that $x+f(y)$ and $x+f(z)$ exist and hence in view of (ii) that $x+f(y) = x+f(z)$. Consequently $f(y) = f(z)$, $y = z$. Thus $f(x)$ is cancelable.

Suppose $fgf'(x)+y = fgf'(x)+z$. Then

$$fgf'(x)+f(y) = fgf'(x)+f(z) \quad \text{and} \quad 0+f'(y) = 0+f'(z).$$

From the latter equation it follows that $f'(y) = f'(z)$, and from the former we infer with the aid of (ii) that $f'(x)+f(y) = f'(x)+f(z)$, whence it follows by (i) that $f(y) = f(z)$. Thus $y = z$. This shows that $fgf'(x)$ is cancelable.

To prove (v) we observe, with the aid of 6.3(ix), that

$$fgf'g(x)+fg'f'g(x) = 0 = fg'fg(x)+fg'f'g(x)$$

and that $fg'f'g(x)$ is cancelable. (vi) follows from the fact that

$$fgf'(x)+fg'f'(x) = 0 = fgf'(y)+fg'f'(y),$$

and that all the summands are cancelable. Hence, if either $fgf'(x) = fgf'(y)$ or $fg'f'(x) = fg'f'(y)$, then both these equations hold. To prove (vii) it suffices to note that $fg(x)+fg'(x) = 0+f(x)$, Next, under the hypothesis of (viii),

$$fgf(x)+fgf'(x) = fgf(y)+fgf'(y),$$

since the two sides are equal to $0+fg(x)$ and $0+fg(y)$, respectively. Applying g' we obtain

$$g'fgf(x)+g'fgf'(x) = g'fgf(y)+g'fgf'(y).$$

Since $g'fgf(x)$ and $g'fgf(y)$ are equal by (vii) and cancelable by (iv), it follows that $g'fgf'(x) = g'fgf'(y)$. Similarly, $gfg'f(x) = gfg'f'(y)$, and since

$$gfg'f'(x)+gfgf'(x) = 0 = gfg'f'(y)+gfgf'(y),$$

it follows that $gfgf'(x) = gfgf'(y)$. Thus

$$gfgf'(x)+g'fgf'(x) = gfgf'(y)+g'fgf'(y),$$

and using 6.3(vi) and (Z_2) we conclude that $fgf'(x)+0 = fgf'(y)+0$, $fgf'(x) = fgf'(y)$.

Finally, (ix) is an immediate consequence of 6.3(v) and (Z_2), and under the hypothesis of (x) we have $fgf'(x) = fgf'(y)$ by (vi) and

$$fgf(x)+fgf'(x) = fgf(y)+fgf'(y)$$

by 6.3(v), and together with (iv) this yields $fgf(x) = fgf(y)$.

7. *GENERALIZATION OF THE FITTING-ŁOŚ LEMMA*

This section will be devoted to the proof of the main lemma on which the proof of 6.1 is based.

LEMMA 7.1. *If $(fgf)^n$ is idempotent, then it is a decomposition projection and its kernel is a factor of F.*

For the special case when A is an Abelian group with operators this lemma can be found in Fitting [5]. The generalization to algebras with a zero element is an unpublished result by J. Łoś. Since the proof of our lemma is rather long and not very intuitive, it may be helpful to outline first a proof for the case considered by Łoś. Let f' and g' be the decomposition projections orthogonal to f and g, and let $h = (fgf)^n$. Observe that, for $k = 1, 2, 3, \ldots$,

$$f = (fgf)^k+(fg'f+fg'fgf+fg'(fgf)^2+ \ldots +fg'(fgf)^{k-1}).$$

In fact, if this holds for a given value of k, then the corresponding formula with k replaced by $k+1$ is obtained by making use of the fact that

$$(fgf)^k = f(fgf)^k = (fgf+fg'f)(fgf)^k = (fgf)^{k+1}+fg'(fgf)^k,$$

and that $fg'(fgf)^k$ maps A into its center. Letting

$$q = fg'f+fg'fgf+\cdots+fg'(fgf)^{n-1},$$

we infer that $f = h+q$. Observe that fgf and $fg'f$ commute by 6.3(v), and therefore $hq = qh$. Consequently

$$hq = hqf = h^2q+hq^2 = hq+hq^2.$$

Since hq maps A into the center of the algebra, this implies that $hq^2 = 0$. Next,

$$q^2 = fq^2 = hq^2+q^3 = 0+q^3 = q^3,$$

so that q^2 is idempotent. Furthermore,

$$h = hf = h^2+hq = h+hq = (h+hq)+hq = h+2hq,$$
$$f = f^2 = (h+q)^2 = (h+2hq)+q^2 = h+q^2.$$

It is now easy to see that $\langle h, q^2+f'\rangle$ is an orthogonal pair of projections, and a straightforward argument completes the proof of the lemma for the special case of an algebra with a zero element.

Proof of Lemma 7.1. Our proof is to some extent suggested by the above argument, although many of the details will be considerably more involved. Let $p_1 = q_1 = f$, and for $k = 1, 2, \ldots$ let

$$p_{k+1} = fgp_k \quad \text{and} \quad q_{k+1} = \bar{f}(f, g'q_k).$$

Also let

$$h = fgp_n, \quad h' = (fg'q_n)^2, \quad \bar{h}(x, y) = f\bar{g}\big(p_n(x), q_nfg'q_n(y)\big),$$
$$H = \ker h, \quad H' = \ker h'.$$

We shall show that $F = H\times H'$. The proof will be based on a series of statements.

STATEMENT 1. *For* $k = 1, 2, \ldots$, $f = f\bar{g}(p_k, q_k)$.

Proof. For $k = 1$ this follows from 3.1, 3.2. Assuming that it holds for k we have

$$f\bar{g}(p_{k+1}, q_{k+1}) = f\bar{g}\big(fgp_k, \bar{f}(f, g'q_k)\big)$$
$$= f\bar{g}\big(fgp_k, \bar{f}\big(f\bar{g}(p_k, q_k), g'q_k\big)\big).$$

We wish to show that this is equal to $f\bar{g}(p_k, q_k)$, and hence to f. Actually it will be shown that, for all $x, y \in A$,

$$f\bar{g}\big(fg(x), \bar{f}(f\bar{g}(x, y), g'(y))\big) = f\bar{g}(x, y). \tag{1}$$

Observe that, for all $z, u, v, w \in A$, the conditions

$$f\bar{g}\big(z, f(u)\big) = f\bar{g}\big(v, f(w)\big), \quad fg'f'(u) = fg'f'(w) \tag{2}$$

jointly imply that

$$f\bar{g}(z, u) = f\bar{g}(v, w). \tag{3}$$

To verify this we compute

$$\begin{aligned} f\bar{g}\big(z, f(u)\big) + fg'f'(u) &= f\bar{g}\big(z, f(u)\big) + f\bar{g}\big(0, f'(u)\big) \\ &= f\bar{g}\big(z+0, f(u)+f'(u)\big) = f\bar{g}(z+0, u+0) \\ &= f\bar{g}(z, u) + f\bar{g}(0, 0) = f\bar{g}(z, u) + 0. \end{aligned}$$

Of course the corresponding formula with z and u replaced by v and w also holds. Consequently (2) implies that $f\bar{g}(z, u)+0 = f\bar{g}(v, w)+0$, which in turn yields (3).

We now take

$$z = fg(x), \quad u = \bar{f}(f\bar{g}(x, y), g'(y)), \quad v = x, \quad w = g'(y).$$

Since, by 3.9(ii), $f\bar{g}\big(x, g'(y)\big) = f\bar{g}(x, y)$, (1) is equivalent to (3), and it is therefore sufficient to show that (2) holds. Since $f(u) = f\bar{g}(x, y)$ and $f'(u) = f'g'(y)$, the second equation in (2) is obviously true, and the first one can be written

$$f\bar{g}\big(fg(x), f\bar{g}(x, y)\big) = f\bar{g}\big(x, fg'(y)\big).$$

To prove this we compute

$$\begin{aligned} f\bar{g}\big(fg(x), f\bar{g}(x, y)\big) + 0 &= f\bar{g}\big(fg(x), f\bar{g}(x, y)\big) + f\bar{g}(0, 0) \\ &= f\bar{g}\big(fg(x)+0, f\bar{g}(x, y)+0\big) = f\bar{g}\big(fg(x)+0, fg(x)+fg'(y)\big) \\ &= f\bar{g}\big(fg(x), fg(x)\big) + f\bar{g}\big(0, fg'(y)\big) = fg(x)+fg'fg'(y) \\ &= f\bar{g}\big(x, fg'(y)\big) + 0, \end{aligned}$$

and then cancel 0.

STATEMENT 2. *For* $k, l = 1, 2, \ldots$, $(fgp_k)(fg'q_l) = (fg'q_l)(fgp_k)$.

Proof. Since $fgp_k = (fgf)^k$, it is sufficient to show that fgf commutes with fgq_l. For $l = 1$ this follows from 6.4(v). Assuming that it holds for $l = m$, we wish to show that it holds for $l = m+1$. Observe that $fg'fq_{m+1}$

is equal to $fg'f$, which is already known to commute with fgf. Also $fg'f'q_{m+1} = fg'f'g'q_m$, and using 6.4(v) and the inductive hypothesis we find that

$$\begin{aligned} fgffg'f'q_{m+1} &= fgfg'f'g'q_m = fgfgfg'q_m \\ &= fgfg'q_mfgf = fg'f'g'q_mfgf \\ &= fg'f'q_{m+1}fgf. \end{aligned}$$

Thus fgf commutes with both $fg'fq_{m+1}$ and $fg'f'q_{m+1}$, and hence commutes with their sum $fg'q_{m+1}+0$. Canceling 0 we see that fgf commutes with $fg'q_{m+1}$.

STATEMENT 3. $(fgp_n)(fgq_n)^2 = 0$.

Proof. We shall actually prove the stronger assertion that $fgp_nfg'q_ng' = 0$ or, what by Statement 2 is equivalent, $fg'q_nfgp_ng' = 0$. Using Statement 1 we find that

$$\begin{aligned} fgp_ng' &= ffgp_ng' = f\bar{g}(p_n, q_n)fgp_ng' \\ &= f\bar{g}(p_nfgp_ng', q_nfgp_ng') = f\bar{g}(p_ng', q_nfgp_ng'). \end{aligned}$$

The last step uses 6.4(ix) and the hypothesis $(fgp_n)^2 = fgp_n$. Adding 0 we obtain

$$fgp_ng' + 0 = fgp_ng' + fg'q_nfgp_ng'.$$

Since fgp_ng' is cancelable, the conclusion follows.

STATEMENT 4. $(fg'q_n)^3 = (fg'q_n)^2$.

Proof. By Statement 1,

$$\begin{aligned} (fg'q_n)^2 &= f(fg'q_n)^2 = f\bar{g}(p_n, q_n)(fg'q_n)^2 \\ &= f\bar{g}\big(p_n(fg'q_n)^2, q_n(fg'q_n)^2\big). \end{aligned}$$

Hence, by 6.4(ix) and Statement 3,

$$(fg'q_n)^2 = f\bar{g}\big(0, q_n(fg'q_n)^2\big) = (fg'q_n)^3.$$

STATEMENT 5. *For all* $x \in A$, $\bar{h}(x, x) = f(x)$.

Proof. This is equivalent to the formula

$$fgp_n + (fg'q_n)^2 = f + 0 \tag{4}$$

which in turn is equivalent to the conjunction of the two equations obtained by applying fgp_n and $fg'q_n$ to (4), i. e., the equations

$$(fgp_n)^2 + fgp_n(fg'q_n)^2 = fgp_n + 0, \tag{5}$$

$$fg'q_nfgp_n + (fg'q_n)^3 = fg'q_n + 0. \tag{6}$$

That (5) holds follows from Statement 3 and the hypothesis. By Statements 4 and 2 and 6.3(v) the left-hand side of (6) is equal to

$$f\bar{g}(p_n, q_n)fg'q_n + 0,$$

and hence (6) follows by Statement 1.

STATEMENT 6. *For all* $x, y, z \in A$,

$$\bar{h}(\bar{h}(x, y), z) = \bar{h}(x, z) = \bar{h}(x, \bar{h}(y, z)).$$

Proof. It is clearly sufficient to show that, for all $u \in A$,

$$f\bar{g}(p_n\bar{h}(x, y), u) = f\bar{g}(p_n(x), u),$$

$$f\bar{g}(u, q_nfg'q_n\bar{h}(y, z)) = f\bar{g}(u, q_nfg'q_n(z))$$

and by 6.4(ix) these equations hold provided

$$fgp_n\bar{h}(x, y) = fgp_n(x), \tag{7}$$

$$(fg'q_n)^2\bar{h}(y, z) = (fg'q_n)^2(z). \tag{8}$$

By 6.3(v) together with Statement 3,

$$\begin{aligned} fgp_n\bar{h}(x, y) + 0 &= (fgp_n)^2(x) + fgp_n(fg'q_n)^2(y) \\ &= fgp_n(x) + 0, \end{aligned}$$

and we cancel 0 to obtain (7). Using, in addition, Statements 2 and 4 we find that

$$\begin{aligned} (fg'q_n)^2\bar{h}(y, z) + 0 &= (fg'q_n)^2fgp_n(y) + (fg'q_n)^4(z) \\ &= 0 + (fg'q_n)^2(z), \end{aligned}$$

whence (8) follows.

STATEMENT 7. $F = H \times H'$.

Proof. Since $hf = h$ and $h'f = h'$, the condition $f(x) = f(y)$ always implies that

$$h(x) = h(y) \quad \text{and} \quad h'(x) = h'(y). \tag{9}$$

On the other hand,

$$\bar{h}(x, y) + 0 = fgp_n(x) + (fg'q_n)^2(y) = h(x) + h'(y).$$

In particular, taking $x = y$ and applying Statement 5 we find that

$$h(x) + h'(x) = f(x) + 0.$$

From this and the corresponding formula with x replaced by y it is clear that (9) implies that $f(x) = f(y)$. Thus

$$F = H \cap H'.$$

For all $x, y \in A$, if $z = \bar{h}(x, y)$, then

$$h(z) = \bar{h}(\bar{h}(x, y), 0) = \bar{h}(x, 0) = h(x)$$

and, similarly, $h'(y) = h'(z)$. Therefore $xHzH'y$. This shows that

$$H \mid H' = {}^2A.$$

Since, obviously, for all $S \in \Delta(\mathfrak{A})$ and $x, y \in S$ the sequence $\bar{h}(x, y)$ belongs to S, the conclusion follows.

According to Statement 7 the kernel of the map $fgp_n = (fgf)^n$ is a factor of F. Furthermore, if $x \in A$ and $y = fgp_n(x)$, then $fgp_n(y) = fgp_n(x)$. Also $f'(y) = 0$ and $h'(y) = (fgq_n)^2 fgp_n(x) = 0$, so that $y \in 0/(F \cap H')$. Consequently fgp_n is a decomposition projection. This completes the proof.

8. PROOF OF THE FUNDAMENTAL THEOREM

We now complete the proof of 6.1 by showing that $\mathfrak{A}$ has the exchange property described in 5.1.

LEMMA 8.1. *If $(fgf)^n$ is idempotent and F is indecomposable, then $(fgf)^n = f$ or $(fgf)^n = 0$.*

Proof. By 7.1 the kernel of $(fgf)^n$ is a factor of $F = \ker f$, and must therefore be either ${}^2A$ or E. In the former case it is obvious that $(fgf)^n = 0$, but in the latter case we claim that $(fgf)^n = f$. In fact, $(fgf)^n(x)$ is in this case a member of the range of f which is in the relation $\ker(fgf)^n = F$ to x, and the only element with this property is $f(x)$.

LEMMA 8.2. *If F is indecomposable and A/F is finite, then there exists a positive integer n such that either $(fgf)^n = f$ or $(fg'f)^n = f$.*

Proof. The range of fgf is contained in the range $0/F'$ of f and is therefore finite. Hence some power of fgf must be idempotent. Similarly, some power of $fg'f$ must be idempotent, and we finally infer that there exists a positive integer n such that both $(fgf)^n$ and $(fg'f)^n$ are idempotent. According to the preceding corollary, the proof will be complete if we show that $(fgf)^n$ and $(fg'f)^n$ cannot both be 0. The proof of this is based on a simple set-theoretic observation:

STATEMENT. *Suppose h and h' are maps of a set U into itself with the properties that $hh' = h'h$ and that, for all $x, y \in A$, the conditions $h(x) = h(y)$ and $h'(x) = h'(y)$ jointly imply that $x = y$. Then, for every positive integer k and for all $x, y \in A$, the conditions $h^k(x) = h^k(y)$ and $h'^k(x) = h'^k(y)$ jointly imply that $x = y$.*

In fact, assuming that the conclusion holds for $k = m$, consider the case $k = m+1$. Given $x, y \in A$, with $h^{m+1}(x) = h^{m+1}(y)$ and $h'^{m+1}(x) = h'^{m+1}(y)$, let

$$u = h^m h'^m(x) \quad \text{and} \quad v = h^m h'^m(y).$$

Then $h(u) = h(v)$ and $h'(u) = h'(v)$, so that $u = v$. Thus $h^m h'^m(x) = h^m h'^m(y)$. Certainly we also have $h'^m h^{m'}(x) = h'^m h'^m(y)$, and it follows that $h'^m(x) = h'^m(y)$. Similarly $h^m(x) = h^m(y)$, and we infer by the inductive hypothesis that $x = y$.

LEMMA 8.3. *If, for some positive integer* n, $(fgf)^n = f$, *then* $\mathrm{id}_A = \big((F \cap G')|G\big) \times F'$.

Proof. We first prove that $F \cap G'$ and G permute:

$$(F \cap G')|G = G|(F \cap G'). \tag{1}$$

By 4.5 this is equivalent to the assertion that

$$G' \cap F = G' \cap \ker fg. \tag{2}$$

According to 6.4(vii), the right-hand side of this equation is contained in the left-hand side, and to prove the opposite inclusion it suffices to show that if $fg'(x) = fg'(y)$ and $f(x) = f(y)$, then $fg(x) = fg(y)$. In fact, we have

$$gfg(x) + gfg'(x) = gfg(y) + gfg'(y),$$

the two sides being equal to $gf(x) + 0$ and $gf(y) + 0$, respectively. The second summand is the same on both sides of this equation, and since it is cancelable we infer that $gfg(x) = gfg(y)$. Consequently

$$fg(x) = (fgf)^n g(x) = (fgf)^n g(y) = fg(y).$$

Next we show that

$$\big((F \cap G')|G\big) \cap F' = \mathrm{id}_A. \tag{3}$$

From (2) it follows that

$$(F \cap G')|G \subseteq \ker fg.$$

Therefore, if $\langle x, y\rangle$ belongs to the left-hand side of (3), then

$$fg(x) = fg(y) \quad \text{and} \quad f'(x) = f'(y). \tag{4}$$

Consequently

$$fgf(x) + fgf'(x) = fgf(y) + fgf'(y),$$

since the two sides are equal to $fg(x) + 0$ and $fg(y) + 0$, respectively. Canceling $fgf'(x) = fgf'(y)$ we infer that $fgf(x) = fgf(y)$, and since $f = (fgf)^n$, this implies that $f(x) = f(y)$. Together with the second equation in (4) this implies that $x = y$. Thus (3) holds.

We now wish to show that

$$(F \cap G')|G|F' = {}^2A. \tag{5}$$

Consider arbitrary elements $x, y \in A$, and let

$$u = \bar{f}\big((fgf)^{n-1}\bar{g}(x, f'(y)), f'(y)\big), \qquad v = \bar{g}(x, u). \tag{6}$$

In order to prove (5) it is sufficient to show that, under these conditions,

$$xGv, \quad vFu, \quad vG'u, \quad uF'y. \tag{7}$$

All these formulas except the second are trivially true, and in view of (2) that one will hold provided $fg(u) = fg(v)$ or, equivalently, $fg(u) = fg(x)$. To verify this we compute

$$\begin{aligned} fg(u)+0 &= fg(fgf)^{n-1}\bar{g}(x, f'(y))+fgf'(y) \\ &= (fgf)^{n}\bar{g}(x, f'(y))+fgf'(y) \\ &= f\bar{g}(x, f'(y))+fgf'(y). \end{aligned}$$

Since the sum $x+f'(y)$ need not exist, we rewrite $f\bar{g}(x, f'(y))$ as $f\bar{g}((fg)^n(x), f'(y))$. This is justified by 6.4(ix) and the fact that $(fg)^{n+1}(x) = fg(x)$. Thus

$$\begin{aligned} fg(u)+0 &= f\bar{g}((fg)^n(x), f'(y))+f\bar{g}(f'(y), 0) \\ &= f\bar{g}((fg)^n(x)+f'(y), f'(y)+0) \\ &= f\bar{g}((fg)^n(x)+f'(y), 0+f'(y)) \\ &= f\bar{g}((fg)^n(x), 0)+f\bar{g}(f'(y), f'(y)) \\ &= (fg)^{n+1}(x)+ff'(y) \\ &= fg(x)+0. \end{aligned}$$

Canceling 0 we infer that $fg(u) = fg(x)$. Thus (7) holds.

To complete the proof of the lemma we need only observe that if $S \in \Delta(\mathfrak{A})$ and $x, y \in S$, and if the sequence u is defined by the formula (6), then $u \in S$. This is true because $f(S)$, $f'(S)$, $g(S)$, $\bar{f}(S, S)$ and $\bar{g}(S, S)$ are all contained in S.

Proof of Theorem 6.1. Under the hypothesis of 6.1, if $\mathrm{id}_A = F \times F' = G \times G'$ and F is indecomposable, then it follows by 8.2 and 8.3 that $\mathrm{id}_A = H \times F'$ where H is either $(F \cap G')|G$ or $(F \cap G)|G'$. Consequently, by 5.1, $\mathfrak{A}$ has the unique factorization property.

9. OPEN PROBLEMS

Although the unique factorization problem has been settled for large classes of structures, a great deal of work still remains to be done. We have here concentrated on finite structures. In the case of infinite structures (with a distinguished reflexive element) it is perhaps more natural

to consider the weak direct products rather than the full direct, or Cartesian, products. Also, since an infinite structure need not be isomorphic to a direct product (either weak or full) of indecomposable structures one usually replaces the unique factorization property by the so-called refinement property. A structure $\mathfrak{A}$ is said to have the *refiniment property* if for any two representations

$$\mathfrak{A} \cong \prod_{i \in I}^{w} \mathfrak{B}_i \cong \prod_{j \in J}^{w} \mathfrak{C}_j$$

there exist structures $\mathfrak{D}_{i,j}$ such that

$$\mathfrak{B}_p \cong \prod_{j \in J}^{w} \mathfrak{D}_{p,j} \quad \text{and} \quad \mathfrak{C}_q \cong \prod_{i \in I}^{w} \mathfrak{D}_{i,q}$$

for all $p \in I$ and $q \in J$. Here Π^w denotes weak direct products. In the case of algebras with a zero element, various conditions are known which imply the refinement property. A reasonably complete account of these results can be found in Crawley-Jónsson [4]. In Chang-Jónsson-Tarski [3, the refinement property is proved for certain other classes of structures] without any finiteness conditions, but these classes are necessarily rather restricted, since the methods actually yield a stronger refinement property that does not hold except for rather exceptional classes of structures.

It seems likely that most or all of the results on *algebras* with a zero element can be extended almost mechanically to *structures* with a zero element, although we have not checked this in detail. For other structures many of these results are not even meaningful, since they involve concepts that are not defined for such structures, namely the notions of an inner direct product and of center. The inner direct products of subalgebras can be replaced by (weak) direct products of factor relations, but so far no substitute has been offered for the notion of a center. It is well known that in the case of groups there is in a sense a duality between the center and the quotient modulo the commutator group, and the new notion should presumably specialize to this quotient in the case of group.

Lacking a suitable counterpart to the notion of a center, we shall concentrate on those results that do not involve this concept. As a counterpart to the exchange property that plays a basic role in Crawley-Jónsson [4], we propose the following property: A structure $\mathfrak{B}$ is said to have the *dual exchange property* if, for any structure $\mathfrak{A}$ and any decompositions

$$\mathrm{id}_A = F \times F' = \prod_{i \in I}^{w} G_i,$$

the condition $\mathfrak{A}/F \cong \mathfrak{B}$ implies that there exist equivalence relations H_i such that $H_i \supseteq G_i$ for all $i \in I$ and

$$\mathrm{id}_A = \prod_{i \in I}^{w} H_i \times F'.$$

Consider now structures with a commuting and cancelable reflexive element. More precisely, consider structures $\mathfrak{A} = \langle A, 0, R_t \rangle_{t \in T}$ with the following property:

$\Phi(\mathfrak{A})$. *There exists a partial binary operation* $+$ *in* $\Delta(\mathfrak{A})$ *such that, for all* $x \in A$, $0+x$ *and* $x+0$ *exist and are equal and, for all* $x, y \in A$, *the condition* $0+x = 0+y$ *implies that* $x = y$.

We conjecture that many of the results in Crawley-Jónsson [4] — or, rather, their "duals" — are valid for structures with the property Φ. In particular:

CONJECTURE 9.1. *Suppose* $\Phi(\mathfrak{A})$ *holds. If*

$$\mathrm{id}_A = \prod_{i \in I}^{w} F_i = \prod_{j \in J}^{w} G_j,$$

where the index sets I *and* J *are countable and all the quotient structures* $\mathfrak{A}/F_i$ *and* $\mathfrak{A}/G_j$ *have the dual exchange property, then these two decompositions have isomorphic refinements* **(P 508)**.

CONJECTURE 9.2. *If* $\Phi(\mathfrak{A})$ *holds, and if*

$$\mathrm{id}_A = \prod_{i \in I}^{w} F_i,$$

where all the quotients $\mathfrak{A}/F_i$ *have the dual exchange property, then* $\mathfrak{A}$ *has, up to isomorphism, at most one representation as a weak direct product of indecomposable structures* **(P 509)**.

CONJECTURE 9.3. *If* $\Phi(\mathfrak{A})$ *holds, if* A *is countable, and if*

$$\mathrm{id}_A = \prod_{i \in I}^{w} F_i,$$

where each of the quotient structures $\mathfrak{A}/F_i$ *has the dual exchange property, then* $\mathfrak{A}$ *has the refinement property* **(P 510)**.

CONJECTURE 9.4. *If* $\mathfrak{B}$ *is a finite structure, and if* $\Phi(\mathfrak{B})$ *holds, then* $\mathfrak{B}$ *has the dual exchange property* **(P 511)**.

CONJECTURE 9.5. *If* $\mathfrak{B}$ *is a finite structure and if* $\Phi(\mathfrak{B})$ *holds, then the condition* $\mathfrak{B} \times \mathfrak{C} \cong \mathfrak{B} \times \mathfrak{C}'$ *implies that* $\mathfrak{C} \cong \mathfrak{C}'$ **(P 512)**.

The results presented here suggest some more technical problems. The following permutability property played an important role in Sections 4 and 5:

$\Psi(\mathfrak{A})$. *For all* $F, F', G \in \mathrm{FR}(\mathfrak{A})$, *if* $\mathrm{id}_A = F \times F'$, *then* $(F \cap G) | F' = F' | (F \cap G)$.

According to 5.4, a finite structure $\mathfrak{A}$ has the unique factorization property provided $\mathfrak{A}$ and certain quotient structures of $\mathfrak{A}$ have this property. We do not know whether it is sufficient to assume this just for $\mathfrak{A}$ itself:

PROBLEM 9.6. *Is it true that if* $\mathfrak{A}$ *is a finite structure and* $\Psi(\mathfrak{A})$ *holds, then* $\mathfrak{A}$ *has the unique factorization property?* **(P 513)**.

Perhaps more interesting is the problem of finding a common generalization of 1.1 and 1.2, or preferably of 5.4 and 6.1. An affirmative answer to either one of the next two problems would yield such a generalization.

PROBLEM 9.7. *Does every structure* $\mathfrak{A}$ *with a zero element have the property* $\Psi(\mathfrak{A})$? *More generally, does* $\Phi(\mathfrak{A})$ *imply* $\Psi(\mathfrak{A})$? **(P 514)**.

PROBLEM 9.8. *Suppose* $\mathfrak{A}$ *is a finite structure with the property that, for all orthogonal pairs* $\langle f, f' \rangle$ *and* $\langle g, g' \rangle$ *of projections over* $\mathfrak{A}$, $(\ker fg) \cap (\ker fg') \subseteq \ker f$. *Does it follow that* $\mathfrak{A}$ *has the unique factorization property?* **(P 515)**.

We predict that the answer to 9.7 is negative, but make no conjecture concerning 9.8.

REFERENCES

[1] G. Birkhoff, *Lattice theory*, American Mathematical Society Colloquium Publications 25, New York 1948.

[2] C. C. Chang, *Two theorems on direct decompositions of relations*, Bulletin of the American Mathematical Society 60 (1954), p. 24.

[3] — B. Jónsson and A. Tarski, *Refinement properties for relational structures*, Fundamenta Mathematicae 55 (1964), p. 249-281.

[4] P. Crawley and B. Jónsson, *Refinements for infinite direct decompositions of algebraic systems*, Pacific Journal of Mathematics 14 (1964), p. 797-855.

[5] H. Fitting, *Über die direkten Produktzerlegungen einer Gruppe in direkt unzerlegbare Faktoren*, Mathematische Zeitschrift 39 (1934), p. 16-30.

[6] B. Jónsson and A. Tarski, *Decompositions of algebras*, Bulletin of the American Mathematical Society 59 (1953), p. 77.

[7] — *Direct decompositions of finite algebraic systems*, Notre Dame Mathematical Lectures 5 (1947).

[8] — *Factor relations over algebras*, Bulletin of the American Mathematical Society 59 (1953), p. 77.

Reçu par la Rédaction le 29. 1. 1965