Factorization Properties Of Universal Algebras

Harry Wiggins

Thesis presented for the degree of Master of Science
in the Department of Mathematics and Applied Mathematics

University of Cape Town

December 10, 2010

Declaration

I know the meaning of Plagarism and declare that all of the work in the document, except for that which is properly acknowledged, is my own.

Abstract

This dissertation deals with algebraic structures that can be written as the product of directly indecomposable algebras in a unique way up to isomorphism, known as the Unique Factorization Property. Here we undertake the task of collecting all the major results discovered by a few mathematicians (A. Tarski, B. Jónsson, R. Mckenzie, C. Chang, G. Birkhoff, L. Lovasz, etc.) over the past century. Another goal of this thesis was to highlight important and to introduce fresh techniques. The scope of most of them is still unknown and hopefully they can be utilised further to yield new results to revive this beautiful branch of mathematics.

Acknowledgement

The work presented in this thesis is a product of many people to whom I owe much gratitude.

I would first and foremost like to thank my supervisors Dr. Peter Ouwehand, Prof. Hans-Peter Künzi and and Prof. C. Gilmour, for much advice given, time sacrificed bouncing off ideas and books lent. To all the other teachers and lecturers who have contributed to my mathematical education over the years, I thank you also.

I am extremely grateful for the financial support provided by the Harry Crossley Foundation, including the support from the friendly ladies at the PGFO : Stacey-Lee Harrison, Zerina Davis and Stacey Moses. I am also thankful for the National Research Foundation for their kind assistance.

A special thanks to the UCT Mathematics Department for giving me the freedom to tutor and share my passion for numbers with undergraduate students. Mrs. Di Loureiro and other secretaries in the Department for making administration matters disappear with their magic wands. Also for my fellow students (a notable element in this set is a dear friend, Bertus Labuschagne) who kept me sane and grounded during the writing process.

Lastly, a big thanks to my family for their love and support. My grandmother, mum, dad, brother and sister who made this journey worthwhile. Finally, to my late grandfather Harry Zandberg, who would have been proud.

" *If I have been able to see further than other men, it is because I have stood on the shoulders of giants.*" (Sir Isaac Newton)

Introduction

More than two millennia ago the ancient Greeks discovered that the simplest structures (finite sets or simply numbers) have an unique factorization in terms of prime factors. This result was practically proven by Euclid in book 7 of *Euclid's elements* (propositions 30 and 32). However the first correct proof of this 'obvious' result for natural numbers is to be found in *Disquisitiones Arithmeticae* by Carl Friedrich Gauss in 1798. Unexpectedly this is not true for more general number systems. A good example is the ring $\mathbb{Z}(\sqrt{-5})$ where

$$2 \times 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Ernest Kummer pointed this out in 1843 while working on Fermat's Last Theorem. This dissertation will explore this property for various algebraic structures. Here, directly indecomposable algebras will play the role of prime numbers, that is structures that can not be broken into the product of two smaller algebras. We follow the quest of a few mathematicians in their journey to investigate structures with this property.

Joseph Wedderburn [Wed09] was the first to ask in 1909 whether finite groups have the unique factorization property, that is a factorization into direct indecomposable algebras exist and is unique up to isomorphism. Not long after, a complete proof in the affirmative was found by Robert Remak [Rem11] in 1911. It should be noted that Leopold Kronecker [Kro70] already proved in 1870 that every finitely generated abelian group has this beautiful property, where the unique factors are cyclic groups. A few decades later Krull and Schmidt [Sch28] showed in 1928 that every infinite group with the finite chain condition also has this property.

So the obvious question to ask is which structures exist with this property and how we can completely classify all of them. Not unexpectedly, this turns out to be a very tough question to answer and only partial results are known.

We commence our journey by giving a formal description of the problem in Chapter 1. To further improve our understanding we list a few structures which do not possess the property. Here we also familiarise ourselves with the relevant theory and tools needed for later chapters.

Chapters 2 and 3 will generalize this group theoretical result into a more general setting by exposing important conditions needed for unique factorization. Chapter 2 extends this result by considering certain properties of the associated congruences lattice. Here we prove a major result published by Garrett Birkhoff [Bir48].

Suppose A is a congruence-permutable algebra whose congruence lattice has finite height. If A has a one-element subalgebra then A is uniquely factorable.

We also prove another unique factorization result due to Bjarni Jónsson [Jon66] published

in 1966.

If A is finite with a one-element subalgebra and a modular-congruence lattice then A is uniquely factorable.

These are all partial answers to the following open question :

If $Con\, A$ is a modular lattice of finite height and A has a one-element subalgebra, must A be uniquely factorable?

In Section 2.3 we provide counterexamples to illustrate the necessity of each condition in the open problem. We tie this chapter off by discussing a possible avenue of attack proposed by Ralph Freese [Fre1, Fre2].

Our task in Chapter 3 is to generalise the unique factorization property of groups in another direction. Here we concentrate on certain properties satisfied by the identity element. Introducing the class of zero-algebras, we modernise methods of Bjarni Jónsson and Alfred Tarksi [JT47] published in 1947 to show that :

Every zero-algebra with a finite center has an unique factorization, provided that each of its direct factors is decomposable into a finite product of indecomposable algebras.

To conclude this chapter, we study a related structure known as structures almost without zero-divisors. Curiously, I. Chajda [Cha76] showed that these algebras inherit an unique factorization property without needing a finiteness condition.

Chapter 4 explores the unique factorization property for infinite algebras. The ideas of refinement, intermediate refinement and strict refinement arises naturally when dealing with infinite structures. Here we discuss the relations between these concepts and include interesting results found in a paper by C. Chang, Bjarni Jónsson and Alfred Tarski [CJT] published in 1964. There, they showed that :

If $Con\, A$ is distributive then A has the strict refinement property.

If an algebra A possesses an idempotent element v such that (A, v) has the intermediate value property then algebra A has the refinement property.

Chapter 5 redirects our attention to the class of binary structures. These structures are abundant in mathematics and deserves special consideration. We mostly focus on connected structures and structures with binary operations satisfying certain equations. Here we show that :

If A is a connected ordered set, then A has the strict refinement property.

These solutions highlight the usefulness of the idea of decomposition functions. Also in this chapter, we show that if A is a connected reflexive binary structure with a strange finiteness condition, then A possesses the refinement property.

Chapter 6 is inspired by the open problem :

Does every finite idempotent structure possess the unique factorization property?

Examples of idempotent structures includes lattices. This section mainly concentrates on idempotent semigroups, also known as bands. Here we redevelop techniques by Ralph Mckenzie [Mck72] published in 1972 to ultimately show that :

Every finite idempotent semigroup has the UFP.

Finally, Chapter 7 studies other related factorization properties. Here we utilised new techniques from category theory, set theory and model theory. These methods still have plenty of room left for exploring. Included here is a beautiful result due to László Lovasz [Lov67] published in 1967 which states that :

For any two finite algebras A and B if $A^k \simeq B^k$ then $A \simeq B$.

We give two distinct proofs of this unexpected result for finite algebras. We close this chapter by providing a new result, which gives another explanation why finite abelian groups have the unique factorization property.

Let V be a variety where every directly indecomposable algebra is subdirectly irreducible. If A is a finite algebra with a one-element subalgebra, then A has the UFP.

Contents

1 Background **8**
- 1.1 Direct products . . . 8
- 1.2 Lattices . . . 10
  - 1.2.1 Modular lattices . . . 10
  - 1.2.2 Direct sums . . . 13
- 1.3 Congruences . . . 17

2 A Few Unique Factorization Results **22**
- 2.1 Congruence-permutable algebras . . . 22
- 2.2 Birkhoff-Ore Theorem . . . 23
  - 2.2.1 More congruence theory . . . 23
  - 2.2.2 Jónsson's Unique Factorization Theorem . . . 24
- 2.3 Counter-examples . . . 28
- 2.4 Freese's Unique Factorization Theorem . . . 30

3 Zero-algebras **34**
- 3.1 Inner products . . . 34
- 3.2 Central subuniverses . . . 38
- 3.3 More endomorphisms . . . 41
- 3.4 Algebras almost without zero-divisors . . . 46

4 Refinement properties **50**
- 4.1 Decomposition functions . . . 50
- 4.2 Intermediate refinement property . . . 57

5 More refinement properties **60**
- 5.1 Special binary structures . . . 60
- 5.2 Another refinement theorem . . . 66

6 Idempotent algebras **70**
- 6.1 More refinement results . . . 70
- 6.2 Applications to semigroups . . . 75

7 Other related properties **79**
- 7.1 kth roots and cancellation . . . 79
- 7.2 Another proof . . . 84
- 7.3 Absorbing algebras . . . 86
- 7.4 Subdirectly irreducible algebras . . . 89
- 7.5 Conclusion . . . 90

Chapter 1

Background

This chapter collects material from lattice theory and universal algebra to aid in establishing unique factorization results. We start the first section by giving a formal definition of the concept of unique factorization. Here we also include examples of structures that do not possess this nice property. The second section focuses on modular lattices and the concept of direct sums. We end this chapter by developing a language for understanding factorization in terms of congruences, which is vital for understanding later proofs.

1.1 Direct products

We adopt the usual notation/concepts from the theory of universal algebras, i.e. the definitions of fundamental operations, fundamental relations, algebraic structures, the product of structures of the same type, etc. First we remind the reader what an algebraic structure is and introduce the idea of direct product.

Definition 1.1.1. An **algebra** is a set A together with a collection of fundamental operations on A. An n-ary operation on A is a function that takes n elements of A and returns a single element of A. Thus, a 0-ary operation (or nullary operation) can be represented simply as an element of A or a constant. A 1-ary operation (or unary operation) is simply a function from A to A, often denoted by placing a symbol near the argument, like x'. A 2-ary operation (or binary operation) is often denoted by a symbol placed between its arguments, like $x * y$. Operations of higher or unspecified arity are usually denoted by function symbols, with the arguments placed in parentheses and separated by commas, like $f(x, y, z)$ or $f(x_1, ..., x_n)$. Sometimes operations of infinite cardinality are needed such as $\bigwedge_{\alpha \in I} x_\alpha$ where I is an infinite index set.

Definition 1.1.2. Let $\mathbf{A} = \{A_i : i \in I\}$ be a set of similar algebras, that is they have the same collection of fundamental operations. The **direct product** of $\mathbf{A} = \{A_i : i \in I\}$ is the algebra denoted by $\prod \mathbf{A}$, of the same similarity type, with underlying set $\prod_{i \in I} A_i$, such that for each fundamental operation F and all $x^1, x^2, \ldots, x^r \in \prod_{i \in I} A_i$, where r is the arity of F,

$$(F^{\prod A}(x^1, x^2, \ldots, x^r))_i = F^{A_i}(x_i^1, x_i^2, \ldots x_i^r)$$

for all $i \in I$.

Now before we do any mathematical reasoning about unique factorization we need to define this concept clearly.

Definition 1.1.3. Recall that an algebraic structure A is said to be **directly indecomposable** iff $|A| > 1$ and whenever $A \simeq B \times C$ then $|B| = 1$ or $|C| = 1$. For a given algebra A every isomorphism of the form $A \simeq \prod A_i$ is known as a **direct product representation** of A. □

Definition 1.1.4. We say algebra A possesses the **unique factorization property** or **UFP** iff it can be written as a product of directly indecomposable algebras and this representation is unique up to isomorphism, i.e. if

$$A \simeq \prod_{i \in I} B_i,$$

for some directly indecomposable algebras B_i and if

$$A \simeq \prod_{j \in J} C_j,$$

for some directly indecomposable algebras C_j then a bijection $\phi : I \longrightarrow J$ exists such that $B_i \simeq C_{\phi(i)}$. □

In other words, an algebra possesses the UFP whenever the direct product representation of an algebra is unique in terms of directly indecomposable algebras. It should be noted that any algebra of prime size is directly indecomposable and hence has the UFP. This observation allows us to manufacture many algebras with the unique factorization property. What about finding structures that do not have this property? It turns out that you do not have to look far to find them. The next two examples (unpublished by F. Galvin found in [MMT]) shows that even for finite algebras the UFP may not hold. Example 1.1.6 shows this is the case for some mono-unary algebras. Example 1.1.7 shows that even the number of directly indecomposable factors need not be invariant. Example 1.1.8 shows that this may also be true for structures with more than one fundamental operation. To do this we first define a binary operation for two mono-unary (that is algebras with exactly one unary operation) structures. This is known as the disjoint union.

Definition 1.1.5. Suppose (A, f) and (B, g) are mono-unary algebras with unary operations f and g respectively. Let $(A, f) \cup (B, g)$ be an algebra with underlying set $A \cup B'$ where B' is a set such that $A \cap B' = \emptyset$ and B' has the same cardinality as B (meaning a bijection b exists from B' to B). Let h be the unary operation on $A \cup B'$ such

$$h(x) = \begin{cases} f(x) & \text{if } x \in A, \\ b^{-1}g(b(x)) & \text{if } x \in B'. \end{cases}$$

Thus $(A \cup B', h)$ is another mono-unary algebra, known as the union of (A, f) and (B, g). Likewise, for any natural numbers k, let $k.(A, f)$ denote the disjoint union of mono-unary algebra (A, f) with itself n times.

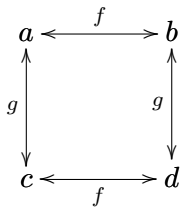
Example 1.1.6. Let A_n denote the n-element mono-unary algebra $(\{0, 1, \ldots, n-1\}, f)$ where $f(x) = x+1$ for $0 \leq x < n-1$ and $f(n-1) = 0$. Note, for example that $A_7 \times A_7 \simeq 7.A_7$ where $k.A_n$ is k copies of A_n. Let $B_{3k+1} = A_1 \cup k.A_3$ (a disjoint union of A_1 with k copies of A_3). It turns out $B_{3n+1} \simeq B_{3k+1} \times B_{3m+1}$ where $n = 3km + k + m$, since $B_{3n+1} \simeq A_1 \cup nA_3$ and $B_{3k+1} \times B_{3m+1} \simeq (A_1 \cup kA_3) \times (A_1 \cup mA_3) \simeq A_1 \cup (3km + k + m)A_3$. Furthermore B_{3n+1} can be factored in this manner if and only if a factorization of $3n + 1$ as $(3k + 1)(3m + 1)$ exists. In [MMT] it was shown that every mono-unary algebra is a disjoint union of connected mono-unary algebras. Therefore algebras B_4, B_{10} and B_{25} are all directly indecomposable algebras (only factorizations are $4 = 1 \times 4 = 2 \times 2, 10 = 1 \times 10 = 2 \times 5$ and $25 = 1 \times 25 = 5 \times 5$). Thus the following is a failure of the unique factorization property :

$$B_4 \times B_{25} \simeq B_{100} \simeq B_{10} \times B_{10}.$$

Example 1.1.7. We again use the same structures A_m, B_n as defined in the previous example. Put $C_{5k+1} = A_1 \cup k.B_5$. In a similar fashion we can show $C_{5k+1} \simeq C_{5n+1} \times C_{5m+1}$ if and only if $(5k+1) = (5n+1)(5m+1)$ for some positive integers. Note for example C_6, C_{16} and C_{81} are all directly indecomposable algebras (only factorizations are $6 = 1 \times 6 = 2 \times 3, 16 = 1 \times 16 = 2 \times 8 = 4 \times 4$ and $81 = 1 \times 81 = 3 \times 27 = 9 \times 9$). Thus the following shows C_{1296} does not possess the unique factorization property:

$$C_{16} \times C_{81} \simeq C_{1296} \simeq C_6 \times C_6 \times C_6 \times C_6.$$

Example 1.1.8. Suppose $A = \{a, b, c, d\}$ is an algebra with 2 unary functions f, g as indicated below. We see that $\theta_1 = \{(a,a),(a,b),(b,b),(b,a),(c,c),(c,d),(d,c),(d,d)\}$, $\theta_2 = \{(a,c),(a,a),(c,a),(c,c),(b,b),(b,d),(d,b),(d,d)\}$ and $\theta_3 = \{(a,d),(a,a),(d,a),(d,d),(b,b),(b,c),(c,b),(c,c)\}$ are congruences on A, that is $A/\theta_1 = \{\{a,b\},\{c,d\}\}$, $A/\theta_2 = \{\{a,c\},\{b,d\}\}$ and $A/\theta_3 = \{\{a,d\},\{b,c\}\}$. Observe that $A \simeq A/\theta_1 \times A/\theta_2 \simeq A/\theta_2 \times A/\theta_3 \simeq A/\theta_3 \times A/\theta_1$, but none of $A/\theta_1, A/\theta_2, A/\theta_3$ are isomorphic to one another. Finally, each structure $A/\theta_1, A/\theta_2, A/\theta_3$ is directly indecomposable as they have size 2, a prime number.



1.2 Lattices

It is remarkable what an essential role lattices play in the study of properties common to all algebraic structures such as abelian groups, boolean rings, Lie-algebras, etc. Sometimes the congruence lattice of an algebra can reveal interesting information about the algebra itself as we will soon discover. In this section we gather some important results about modular lattices and direct sums.

1.2.1 Modular lattices

This subsection is dedicated to modular lattices. They are also known as Dedekind lattices or Dedekind structures in honour of R. Dedekind who was the first to propose the modular law and some of its consequences [Ded00]. Their importance was realised by O. Ore in his papers [Ore35, Ore36a, Ore36b] while studying direct decompositions. First we need to define when a lattice is a modular lattice.

Definition 1.2.1. A **modular lattice** is any lattice that satisfies the modular law:

$$x \leq y \implies x \vee (y \wedge z) = y \wedge (x \vee z).$$

□

Notice that every distributive lattice is a modular lattice. To prove Dedekind's Transposition Principle for modular lattices or sometimes called the Diamond Isomorphism Theorem for lattices, we recall some basic definitions.

The binary relation $\leq$ where $a \leq b \iff a \vee b = b$ is a partial order on any lattice. If $a \leq b$ then we denote $[a, b]$ as the set $\{c : a \leq c \leq b\}$. Every sublattice of this form is known as an **interval**.

For every x and y the two intervals $[x \wedge y, x]$ and $[y, x \vee y]$ are called **transposes** of each other. The maps $a \mapsto a \vee y$ or $b \mapsto b \wedge x$ are known respectively as the associated **perspectivity maps**. Two intervals $[x, y]$ and $[x', y']$ are said to be **projective** iff there is a finite sequence of intervals $[x, y], [x_1, y_1], \ldots, [x_n, y_n], [x', y']$ where any two adjacent intervals are transposes of one another. The composition of the associated perspectivity maps is known as the **projectivity map**.

Dedekind's Transposition Principle. *Suppose L is a modular lattice and $x, y \in L$. The maps $\phi_y(a) = a \vee y$ and $\psi_x(b) = b \wedge x$ are inverse isomorphisms between $[x \wedge y, x]$ and $[y, x \vee y]$ respectively. Moreover subintervals are mapped into transposes under either map.*

Proof. Firstly note that ϕ_y and ψ_x are both order-preserving maps. Modularity immediately gives for all $a \in [x \wedge y, x]$ and for all $b \in [y, x \vee y]$ that

$$\begin{aligned} \psi_x(\phi_y(a)) &= (a \vee y) \wedge x = a \vee (x \wedge y) = a, \\ \phi_y(\phi_x(b)) &= (b \wedge x) \vee y = b \wedge (x \vee y) = b. \end{aligned}$$

Hence $\psi_x \circ \phi_y$ and $\phi_y \circ \psi_x$ are identity functions on $[x \wedge y, x]$ and $[y, x \vee y]$ respectively. Therefore ϕ_y is an isomorphism with ψ_x as its inverse.

For the second half of the result suppose $x \wedge y \leq a \leq b \leq x$. Thus ϕ_y is an injective map from $[a, b]$ to $[a \vee y, b \vee y]$. Finally to prove that these intervals are transposes it remains to show that $b \vee (a \vee y) = b \vee y$ and $b \wedge (a \vee y) = a$. The former follows from $a \leq b$. For the latter note $b \wedge y \leq x \wedge y \leq a$. Hence by modularity we have

$$b \wedge (a \vee y) = a \vee (b \wedge y) = a.$$

□

Corollary 1.2.2. *In any modular lattice the projective intervals are isomorphic.*

We proceed by discussing special lattices with a finiteness condition.

Definition 1.2.3. A lattice L has the **finite chain condition** iff every chain in L is finite. □

The Hausdorff Maximality Principle states that every ordered set has a maximal chain. Therefore every lattice has a maximal chain and hence lattices with the finite chain condition must have finite maximal chains. Not every such lattice has a bound on the length of chains, as seen in the Figure 1.1. However this pathology does not occur amongst modular lattices as deduced from Theorem 1.2.4, where $\prec$ denotes a covering in each "link" of a maximal chain.

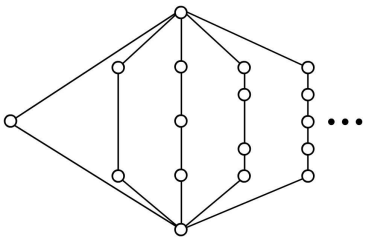


Figure 1.1: A lattice with an unbounded chain length.

Theorem 1.2.4. *Let L be a modular lattice and $a < b$ in L. If there is a finite maximal chain from a to b, then every chain from a to b is finite and all maximal chains have the same length. If*

$$a = a_0 \prec a_1 \prec \ldots \prec a_n = b$$

and

$$a = c_0 \prec c_1 \prec \ldots \prec c_m = b$$

are maximal chains then $n = m$ and the intervals $[a_i, a_{i+1}]$ and $[c_j, c_{j+1}]$ can be matched in a one-to-one correspondence such that matching intervals are projective.

Proof. We call two finite chains **equivalent** iff they have the same length and intervals can be matched in a one-to-one correspondence such that matching intervals are projective. This turns out to be an equivalence relation. We prove this claim by induction on the length of a finite maximal chain from a to b.

By definition it holds trivially when $n = 1$. Suppose $n > 1$ and the conclusions of the theorem hold for any two elements linked by a maximal chain of length less than n. Let C be another maximal chain from a to b. If $a_1 \in C$ then $C - \{a_0\}$ is a maximal chain from a_1 to b and the result follows immediately from the induction hypothesis. Otherwise there is $c \in C$ such that c and a_1 are incomparable. Let $d = a_1 \vee c$. Therefore $a_1 \wedge c = a_0$ and we have $[a_0, c]$ and $[a, d]$ are transposes of each other. Also the intervals $[a_0, a_1]$ and $[c, d]$ are transposes of one another.

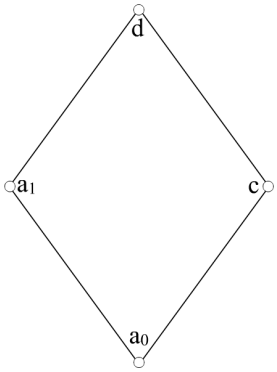


Figure 1.2: A sublattice.

Let $C_0 = \{c' \in C : c' < c\}$ and $C_1 = \{c' \in C : c \leq c'\}$. Let D_0 be the image of C_0 under the perspectivity map and D_1 be any maximal chain from d to b (it exists by the Hausdorff Maximality Principal). From the Dedekind Transposition Principle we have $D_0 \cup \{d\}$ is a maximal chain from a_1 to d. Thus $D_0 \cup D_1$ is a maximal chain from a_1 to b.

By the induction hypothesis we have that $D_0 \cup D_1$ and $a_1 \prec a_1 \prec \ldots \prec a_n$ are equivalent chains. Also by the Dedekind Transposition Principle we have that $a_0 \prec a_1 \prec \ldots \prec a_n$ and $C_0 \cup D_1 \cup \{c\}$ are equivalent. From the induction hypothesis we see that $\{c\} \cup D_1$ and C_1 are equivalent. Thus C is equivalent to $C_0 \cup D_1 \cup \{c\}$ and the result follows. □

Definition 1.2.5. A lattice L is said to be of **finite height** iff there is a finite upper bound to the length of chains in L. Thus for every $a \in L$ the interval $[0, a]$ is of finite height. Let $h(a)$ be the least upper bound to the length of chains in $[0, a]$. □

Not every lattice with the finite chain condition is of finite height, cf. Figure 1.1. However Theorem 1.2.4 proves that these concepts coincide for modular lattices. The next result illustrates another property of modular lattices of finite height.

Lemma 1.2.6. *Let L be a modular lattice of finite height. The following is true for all elements $a, b \in L$:*

(i) $h(0) = 0$.
(ii) If $a < b$ *then* $h(a) < h(b)$.
(iii) $h(a) + h(b) = h(a \wedge b) + h(a \vee b)$.

Proof. For (i) it is clear that $h(0) = 0$. If $a < b$ then $[0, a] \subset [0, b]$ which immediately implies $h(a) < h(b)$. Lastly, as L is a modular lattice the length of any maximal chain between two fixed elements x and y is a constant. Since $[a \wedge b, a]$ and $[b, a \vee b]$ are tranposes of one another we can apply Dedekind Transposition Principal to the sublattice $\{a \wedge b, a, b, a \vee b\}$ and we immediately get $h(a \vee b) - h(b) = h(a) - h(a \wedge b)$. □

1.2.2 Direct sums

Extending the results from the previous subsection we establish results concerning direct sums for modular lattices of finite height. Our main goal here is to prove Theorem 1.2.10, a version of the important Ore Theorem [Bir48]. It can be considered as a uniqueness result.

The results here will assist us in the next chapter to transform congruences in a lattice framework to harvest UFP results. But first we define the notion of direct sums for lattices with a bottom element. Compare the similarity between this definition and Lemma 1.3.6 for congruences.

Definition 1.2.7. In lattice L with a bottom 0 we say e is the **direct sum** of $\{e_i : 1 \leq i \leq n\}$ and denote this by $e = \bigoplus_{i=1}^{n} e_i$ if $e = \bigvee_{i=1}^{n} e_i$ and for all k we have

$$e_k \wedge \bigvee_{i \neq k} e_i = 0.$$

We also say element b is **indecomposable** if $b \neq 0$ and whenever $b = a \oplus a'$ implies either $a = 0$ or $a' = 0$. □

Note $a \oplus b$ may not necessarily exist. If it does it will equal $a \vee b$. In order for it to exist we must have $a \wedge b = 0$. Now we list three basic properties of $\oplus$ for modular lattices. This will be frequently used in Lemma 1.2.9. This powerful result (found in [CD]) has a lengthy proof and will do most of the work in proving Theorem 1.2.10.

Lemma 1.2.8. *Suppose L is a modular lattice of finite height and height function h. For all $a, b, c \in L$ we have that whenevever the left hand side expression exist, so does the right hand side expression (and vice versa) and that they then will be equal then.*

(i) $a \oplus b = b \oplus a$.
(ii) $a \oplus (b \oplus c) = (a \oplus b) \oplus c$.
(iii) $h(\bigoplus_{i \in I} a_i) = \sum_{i \in I} h(a_i)$ *for any finite set I, where $a_i \in L$ for all $i \in I$.*

Proof. The first part is obvious. Assume $d = a \oplus (b \oplus c)$. Therefore $h(d) = h(a) + h(b \oplus c) - h(a \wedge (b \oplus c)) = h(a) + h(b \oplus c) = h(a) + h(b) + h(c) - h(b \wedge c) = h(a) + h(b) + h(c)$. The result

will follow if we can show $a \wedge b = 0$ and $(a \vee b) \wedge c = 0$.

$$\begin{aligned} h((a \vee b) \wedge c) &= h(a \vee b) + h(c) - h(a \vee b \vee c) \\ &= h(a) + h(b) - h(a \wedge b) + h(c) - h(d) \\ &= -h(a \wedge b) \\ &\leq 0. \end{aligned}$$

Hence $h(a \wedge b) = 0 = h((a \vee b) \wedge c)$ which finishes part two. The last part is obvious. □

Lemma 1.2.9. *Let L be a modular lattice of finite height with elements $a, \overline{a}, b_1, b_2 \ldots, b_n$. If $a \oplus \overline{a} = b_1 \oplus b_2 \oplus \ldots \oplus b_n$ where a, b_i are indecomposable elements then $a \oplus \overline{a} = b_j \oplus \overline{a}$ for some element b_j.*

Proof. The fact that L is a modular lattice of finite height allows us to use Lemma 1.2.6. The proof proceeds using induction on the integer $h(a \oplus \overline{a})$. Now for all j, put $\overline{b_j} = b_1 \oplus \ldots \oplus b_{j-1} \oplus b_{j+1} \oplus \ldots \oplus b_n$ (omitting b_j). Thus $a \oplus \overline{a} = b_j \oplus \overline{b_j}$ for all indices j. Clearly $a \oplus \overline{a} \geq a \vee \overline{b_j}, a \oplus \overline{a} \geq \overline{a} \vee b_j$. Now we treat three cases: **Case I:** $a \vee \overline{b_j} = \overline{a} \vee b_j = a \oplus \overline{a}$ for some j. **Case II:** $a \vee \overline{b_j} < a \oplus \overline{a}$ for some j. **Case III:** $a \vee \overline{b_j} = a \oplus \overline{a}$ for all j but $\overline{a} \vee b_k < a \oplus \overline{a}$ for some k.

Case I : If $a \vee \overline{b_j} = \overline{a} \vee b_j = a \oplus \overline{a}$ for some j, then

$$\begin{aligned} h(a) &= h(a \vee \overline{b_j}) - h(\overline{b_j}) + h(a \wedge \overline{b_j}) \\ &= h(b_j \vee \overline{b_j}) - h(\overline{b_j}) + h(a \wedge \overline{b_j}) \\ &= h(b_j) + h(a \wedge \overline{b_j}) \\ &\geq h(b_j). \end{aligned}$$

In a similar fashion we can obtain $h(b_j) = h(a) + h(\overline{a} \wedge b_j) \geq h(a)$. Thus $h(a) = h(b_j)$ and $h(a \wedge \overline{b_j}) = h(\overline{a} \wedge b_j) = 0$. Therefore $a \wedge \overline{b_j} = 0 = \overline{a} \wedge b_j$ and we get the desired $b_j \oplus \overline{a} = a \oplus \overline{a}$.

Case II : Suppose $a \vee \overline{b_j} < a \oplus \overline{a}$ for some j. Assume $j = 1$ without loss of generality. Put

$$q_r = (a \vee \overline{b_r}) \wedge b_r.$$

If $a \vee \overline{b_1} \geq b_1$, then $a \vee \overline{b_1} \geq b_1 \vee \overline{b_1} = a \oplus \overline{a}$. This contradiction proves $q_1 = (a \vee \overline{b_1}) \wedge b_1 < b_1$ or $h(q_1) < h(b_1)$. Furthermore, since the b_r are indecomposable and $q_r \leq b_r$ it follows that

$$c = \bigvee_{r=1}^{n} q_r$$

is a direct sum of the q_r and

$$h(c) = \sum_{r=1}^{n} h(q_r) < \sum_{r=1}^{n} h(b_r) = h(a \oplus \overline{a}).$$

Define $d_r = a \vee \overline{b_r}$. By induction on n and modularity we show that

$$\bigvee_{r=1}^{n} q_r = \bigvee_{k=1}^{n} b_k \wedge \bigwedge_{k=1}^{n} d_k.$$

It is clearly true when $n = 1$, since $q_1 = b_1 \wedge d_1$. Then

$$\begin{aligned}
\bigvee_{r=1}^{n} q_r &= (b_1 \wedge d_1) \vee \big(\bigvee_{k=2}^{n} b_k \wedge \bigwedge_{k=2}^{n} d_k\big) && \text{(induction hypothesis)} \\
&= d_1 \wedge \big[b_1 \vee \big(\bigvee_{k=2}^{n} b_k \wedge \bigwedge_{k=2}^{n} d_k\big)\big] && \big(d_1 \geq \bigvee_{k=2}^{n} b_k\big) \\
&= d_1 \wedge \big[\bigvee_{k=1}^{n} b_k \wedge \bigwedge_{k=2}^{n} d_k\big] && \big(\bigwedge_{k=2}^{n} d_k \geq b_1\big) \\
&= \bigvee_{k=1}^{n} b_k \wedge \bigwedge_{k=1}^{n} d_k.
\end{aligned}$$

Now we are ready to show that $c \geq a$. Since

$$\begin{aligned}
c &= \bigvee_{k=1}^{n} b_k \wedge \bigwedge_{k=1}^{n} d_k \\
&= a \oplus \overline{a} \wedge \bigwedge_{k=1}^{n} d_k \\
&\geq \bigwedge_{k=1}^{n} d_k \\
&= \bigwedge_{k=1}^{n} (a \vee \overline{b_k}) \\
&\geq a.
\end{aligned}$$

Therefore by modularity it follows that $(c \wedge \overline{a}) \vee a = c \wedge (a \vee \overline{a}) = c$ and $c \wedge \overline{a} \wedge a = 0$ giving $c = a \oplus (c \wedge \overline{a})$.

Suppose now $q_r = \bigoplus e_{rk}$ where e_{rk} are indecomposable factors. Thus

$$c = a \oplus (c \wedge \overline{a}) = \bigoplus_{r,k} e_{rk}.$$

By induction, since $h(c) < h(a \oplus \overline{a})$, we may replace a with some indecomposable factor e_{rk} of q_r for some r. Put $e = e_{rk} \leq q_r \leq b_r$. Therefore

$$\begin{aligned}
e \vee \overline{a} &= e \vee (c \wedge \overline{a}) \vee \overline{a} \\
&= c \vee \overline{a} \\
&= a \vee (c \wedge \overline{a}) \vee \overline{a} \\
&= a \oplus \overline{a}.
\end{aligned}$$

Thus $h(e) = h(a)$, since $c = a \oplus (c \wedge \overline{a}) = e \oplus (c \wedge \overline{a})$. Hence $e \wedge \overline{a} = 0$ and $a \oplus \overline{a} = e \oplus \overline{a}$. Moreover e must be b_r, since $e \wedge (b_r \wedge \overline{a}) \leq e \wedge \overline{a} = 0$ and $e \vee (b_r \wedge \overline{a}) = (e \vee \overline{a}) \wedge b_r = (a \oplus \overline{a}) \wedge b_r = b_r$ by modularity. Therefore $b_r = e \oplus (b_r \wedge \overline{a})$. Knowing b_r is indecomposable we get $e = b_r$ and $a \oplus \overline{a} = b_r \oplus \overline{a}$ where $r \neq 1$, because $q_1 < b_1$.

Case III : Suppose $a \oplus \overline{a} = a \vee \overline{b_j} > \overline{a} \vee b_j$ for all indices j - the remaining possibility. Let

$$a \oplus \overline{a} = a_1 \oplus a_2 \oplus \ldots \oplus a_m$$

for some indecomposable elements a_i where $a = a_1$ (recall a is a directly indecomposable element). Also for all indices i let $\overline{a_i} = a_1 \oplus \ldots \oplus a_{i-1} \oplus a_{i+1} \oplus \ldots \oplus a_m$ (omitting a_i). Apply Case II with the roles of a_1 and b_1 reversed. Therefore an index k exists such that $b_1 \oplus \overline{b_1} = a_k \oplus \overline{b_1}$ and $k \neq 1$. We can safely assume $k = m$ by relabelling. Then $x \mapsto (x \vee a_m) \wedge \overline{a_m}$ is a lattice isomorphism from $[0, \overline{b_1}]$ to $[0, \overline{a_m}]$. Put $b_j^* = (b_j \vee a_m) \wedge \overline{a_m}$, then

$$\begin{aligned} \overline{a_m} &= a_1 \oplus a_2 \oplus \ldots \oplus a_{m-1} \\ &= b_2^* \oplus b_3^* \oplus \ldots \oplus b_n^*. \end{aligned}$$

By induction on the height of the lattice, since $h(\overline{a_m}) < h(a + \overline{a})$, we have $a_1 \oplus a_2 \oplus \ldots \oplus a_{m-1} = b_j^* \oplus a_2 \oplus \ldots \oplus a_{m-1}$ for some b_j^* in $[0, \overline{a_m}]$. Modularity gives

$$\begin{aligned} b_j^* \vee a_m &= ((b_j \vee a_m) \wedge \overline{a_m}) \vee a_m \\ &= (b_j \vee a_m) \wedge (\overline{a_m} \vee a_m) \\ &= b_j \vee a_m \\ &\leq b_j \vee \overline{a_1}. \end{aligned}$$

Therefore $\overline{a} \vee b_j = b_j \vee \overline{a_1} \geq b_j^* \vee a_2 \vee a_3 \vee \ldots \vee a_{m-1} \vee a_m = a \oplus \overline{a}$. This contradiction completes the proof. □

Now we are ready to prove an important version of the Ore Theorem [Bir48].

Theorem 1.2.10. *Let L be any modular lattice of finite height. If $a_1 \oplus a_2 \oplus \ldots \oplus a_m = b_1 \oplus b_2 \oplus \ldots \oplus b_n$ for some indecomposable elements then $m = n$ and a relabelling exists such that $a_1 \oplus a_2 \oplus \ldots \oplus a_n = a_1 \oplus a_2 \oplus \ldots \oplus a_{k-1} \oplus a_k \oplus b_{k+1} \oplus \ldots \oplus b_n$ for $k = 1, 2, \ldots, n$. Likewise a relabelling exists such that $b_1 \oplus b_2 \oplus \ldots \oplus b_n = b_1 \oplus b_2 \oplus \ldots \oplus b_{k-1} \oplus b_k \oplus a_{k+1} \oplus \ldots \oplus a_n$ for all k.*

Proof. Without loss of generality, assume $m \leq n$. Suppose the claim holds for all values less than or equal to k, that is a relabelling exists such that

$$a_1 \oplus a_2 \oplus \ldots \oplus a_m = a_1 \oplus a_2 \oplus \ldots \oplus a_{k-1} \oplus a_k \oplus b_{k+1} \oplus b_{k+2} \oplus \ldots \oplus b_n.$$

Note the case $k = 1$ is covered by Lemma 1.2.9. Suppose the result is true for k, then by Lemma 1.2.9 we have

$$a_1 \oplus a_2 \oplus \ldots \oplus a_m = a_j \oplus (a_1 \oplus a_2 \oplus \ldots \oplus a_{k-1} \oplus a_k \oplus b_{k+2} \oplus \ldots \oplus b_n),$$

for some index j. Noting that $j \notin \{1, 2, \ldots, k\}$ the result follows by induction, since

$$a_1 \oplus a_2 \oplus \ldots \oplus a_m = a_1 \oplus a_2 \oplus \ldots \oplus a_{k-1} \oplus a_k \oplus a_j \oplus b_{k+2} \oplus \ldots \oplus b_n.$$

Finally, looking at $k = m$ we get

$$a_1 \oplus a_2 \oplus \ldots \oplus a_m = a_1 \oplus a_2 \oplus \ldots \oplus a_m \oplus b_{m+1} \oplus \ldots \oplus b_n.$$

Indecomposability now shows that $m = n$. □

1.3 Congruences

This section develops a beautiful language in terms of congruences to study direct product factorizations of algebraic structures. To achieve this goal, like [MMT], we consider isomorphisms of the following form :

$$A \overset{f}{\simeq} \prod_{i \in I} A_i.$$

First recall that for any homomorphism $h : C \longrightarrow D$ between algebraic structures of the same type, the set $\ker h = \{(c_1, c_2) \in C^2 : h(c_1) = h(c_2)\}$ is a congruence on C. It turns out that this direct product factorization is completely determined up to isomorphism by certain congruences α_i on A where $\alpha_i = ker(p_i \circ f)$ and p_i is the projection of $\prod_{i \in I} A_i$ onto A_i for each $i \in I$. Clearly $A_i \simeq A/\alpha_i$ by considering the map $f_i : A/\alpha_i \longrightarrow A_i$ where $f_i(a/\alpha_i) = (p_i \circ f)(a)$. This simple observation allows us to study factorization properties by only considering a single algebra with some of its congruences. If $\Gamma \subseteq Con\, A$, then there is a natural map

$$f : A \longrightarrow \prod_{\theta \in \Gamma} A/\theta$$

given by $(f(a))_\theta = a/\theta$. It turns out to be more useful to study a further general map

$$f : A/\psi \longrightarrow \prod_{\theta \in \Gamma} A/\theta \tag{1.1}$$

given by $(f(a/\psi))_\theta = a/\theta$ where $\psi \in Con\, A$ and for all $\theta \in \Gamma$ we have $\theta \geq \psi$, i.e. that $\bigwedge \Gamma \geq \psi$. The following lemma is straightforward :

Lemma 1.3.1. *(i) f is injective if and only if $\bigcap \Gamma = \psi$.*

(ii) f is surjective if and only if $(\forall a \in A^\Gamma)(\exists b \in A)(\forall \theta \in \Gamma)\{(a_\theta, b) \in \theta\}$.

This lemma will be invoked later in Chapter 4. Now part (ii) of Lemma 1.3.1 motivates the next definition.

Definition 1.3.2. We say $\prod_{\theta \in \Gamma} \theta$ exists if $(\forall a \in A^\Gamma)(\exists b \in A)(\forall \theta \in \Gamma)[(a_\theta, b) \in \theta]$. If $\prod_{\theta \in \Gamma} \theta$ exists and $\bigcap \Gamma = \psi$ then we denote this by

$$\psi = \prod_{\theta \in \Gamma} \theta.$$

□

Even for two congruences θ_1 and θ_2 the product $\theta_1 \times \theta_2$ may not necessarily exist as seen by the next lemma. If it does it will equal $\theta_1 \wedge \theta_2$.

Lemma 1.3.3. *For the product $\theta_1 \times \theta_2$ to exist, we must have $\theta_1 \circ \theta_2 = 1$. Hence $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$.*

Proof. It is clear that for the product to exist, the conditions of Definition 1.3.2 need to be satisfied: That is for each (x, y) there is a z such that $(x, z) \in \theta_1$ and $(y, z) \in \theta_2$. Therefore $\theta_1 \circ \theta_2 = 1$. Hence θ_1 and θ_2 are permutable congruences. □

Note the associativity of product of congruences is clear, the next result demonstrates the connection between congruences and algebras.

Lemma 1.3.4. *If θ_1, θ_2 and θ are congruences on algebra A such that $\theta_1 \times \theta_2 = \theta$ then $A/\theta_1 \times A/\theta_2 \simeq A/\theta$.*

Proof. Consider the morphism $\phi : A/\theta_1 \times A/\theta_2 \longrightarrow A/\theta$ with $\phi(a/\theta_1, b/\theta_2) = c/\theta$ such that $(a, c) \in \theta_1$ and $(c, b) \in \theta_2$. The existence of this map follows from the fact $\theta_1 \circ \theta_2 = 1$. The uniqueness of this map follows from noting $\theta_1 \wedge \theta_2 = \theta$. The last remaining task is to show the map is bijective and preserves operations, which is clear. □

Again we emphasize, that we only write $\theta_1 \times \theta_2 = \psi$ whenever the product exists and the value is ψ. It should be mentioned that the relation $\theta = \alpha \times \beta$ is not lattice-theoretic, because $\alpha \times \beta$ cannot be determined by considering the lattice $Con\, A$ alone. An easy example of this is C_3, where C_n is the n-element chain lattice. It has two congruences θ_1 and θ_2 that satisfies $\theta_1 \vee \theta_2 = 1$ and $\theta_1 \wedge \theta_2 = 0$ but $\theta_1 \circ \theta_2 \neq \theta_2 \circ \theta_1$. Furthermore, note the lattice $C_2 \times C_2$ has a congruence lattice isomorphic to $Con(C_3)$, but $C_2 \times C_2$ is a decomposable lattice while C_3 is an indecomposable lattice.

The next lemma demonstrates that congruences are indeed a productive way of studying factorization problems as we do not lose any information. Lemma 1.3.6 and Lemma 1.3.8 are more properties of direct products of congruences.

Lemma 1.3.5. *Direct product decompositions of* 0 *in* $Con\, A$ *are in one-to-one correspondence with isomorphism classes of direct product representations of* A*.*

Proof. Suppose $f : A \xrightarrow{\simeq} \prod_{i \in I} A_i$ is a direct product decomposition. Then

$$0 = \prod_{i \in I} \alpha_i$$

in $Con\, A$ where $\alpha_i = ker(p_i \circ f)$ and p_i is the projection map from $\prod_{i \in I} A_i$ onto A_i. Also, note whenever $0 = \prod_{i \in I} \alpha_i$ for congruences α_i on A, then

$$A \simeq \prod_{i \in I} A/\alpha_i.$$

□

Knowing how to transform a direct product factorization into the language of congruences, we now proceed to connect these ideas of direct sums to give more insight and tools to manipulate congruences. This connection is shown in Lemma 1.3.7.

Lemma 1.3.6. *If* $0 = \prod_{i \in I} \alpha_i$ *then* $0 = \bigwedge_{i \in I} \alpha_i$ *and* $\alpha_i \vee \bigwedge\{\alpha_k : k \neq i\} = 1$

Proof. If $0 = \prod_{i \in I} \alpha_i$, then it follows by definition that their meet is 0. Given $(a, b) \in A \times A$ and some fixed $i \in I$. Let $c \in A^I$ such that $c_i = a$ and $c_k = b$ if $k \neq i$. Then by definition there is a $d \in A$ such that $(d, c_j) \in \alpha_j$ for each $j \in I$. In particular, $(a, d) \in \alpha_i$ and $(b, d) \in \bigwedge_{k \neq i} \alpha_k$. □

Lemma 1.3.7. *If* $0 = \prod_{i=1}^{n} \alpha_i$ *for some congruences* α_i *on* A*, then in the dual of* $Con\, A$ *we have*

$$\alpha_1 \oplus \alpha_2 \oplus \ldots \oplus \alpha_m = 1.$$

Proof. By Lemma 1.3.6 we have $0 = \bigwedge_{i \in I} \alpha_i$ and $\alpha_i \vee \bigwedge\{\alpha_k : k \neq i\} = 1$. So in the dual lattice we have $1 = \bigvee_{i \in I} \alpha_i$ and $\alpha_i \wedge \bigvee\{\alpha_k : k \neq i\} = 0$. Thus by Definition 1.2.7 we have $\alpha_1 \oplus \alpha_2 \oplus \ldots \oplus \alpha_m = 1$. □

Lemma 1.3.8. *Suppose A is an algebra with an one-element subalgebra. If α, β, θ are congruences on A such that $\alpha \times \theta = \beta \times \theta$ then $A/\alpha \simeq A/\beta$.*

Proof. Suppose $\{1\}$ is an one-element subalgebra of A. Let B denote the subalgebra $\{y \in A : (y, 1) \in \theta\}$ of A, where $\alpha|_B$ denotes the restriction of congruence α on subalgebra B. Now for each $x \in A$ there is an element y such that

$$x \overset{\alpha}{\text{———}} \boldsymbol{y} \overset{\theta}{\text{———}} 1,$$

since $\alpha \circ \theta = \alpha \vee \theta = 1$. This gives a well-defined map ϕ between A/α and $B/\alpha|_B$, mapping $x/\alpha \longrightarrow y/\alpha|_B$ (if $x/\alpha = x'/\alpha'$, $(x', y') \in \alpha$ and $(y', 1) \in \theta$ then $(y, y') \in \alpha \wedge \theta$ giving $y/\alpha|_B = y'/\alpha|_B$). Injectivity and surjectivity are immediate. Also the fact that $\{1\}$ is an one-element subuniverse gives that ϕ is a homomorphism. Hence ϕ is an isomorphism. Thus A/α and $B/(\alpha|_B)$ are isomorphic structures. Similarly, A/β and $B/(\beta|_B)$ are isomorphic structures. Note $\alpha \cap \theta = \alpha \times \theta = \beta \times \theta = \beta \cap \theta$ giving $B/(\alpha|_B) = (B)/(\beta|_B)$, which proves

$$A/\alpha \simeq B/(\alpha|_B) = B/(\beta|_B) \simeq A/\beta.$$

□

Remember that an algebra A is directly indecomposable if and only if $|A| > 1$ and whenever $A \simeq B \times C$ then $|B| = 1$ or $|C| = 1$. We are interested in factorising algebras into directly indecomposable algebras, so we need a similar notion for congruences.

Lemma 1.3.9. *For all $\theta \in Con\, A$, A/θ is directly indecomposable if and only if $\theta \neq 1$ and whenever $\theta = \alpha \times \beta$ then $\alpha = 1$ or $\beta = 1$.*

Proof. This follows immediately from recalling $\theta = \alpha \times \beta$ implies $A/\theta \simeq A/\alpha \times A/\beta$. And whenever $A/\theta \simeq B \times C$ then congruences θ_1 and θ_2 exist such that

$$\theta = \theta_1 \times \theta_2,$$

and $A/\theta_1 \simeq B, A/\theta_2 \simeq C$. □

Now we are ready to define what it means for a congruence to be directly indecomposable.

Definition 1.3.10. We say that congruence θ is **directly indecomposable** iff algebraic structure A/θ is directly indecomposable. □

Thus from Lemma 1.3.9 it follows that θ is a directly indecomposable congruence on A iff $\theta \neq 1$ and whenever $\theta = \alpha \times \beta$ then $\alpha = 1$ or $\beta = 1$ in $Con\, A$. Now that we have a language to study direct product factorizations in terms of congruences, it makes sense to find fertile ways of studying the congruence lattice of a given algebra. We direct our attention to congruence-distributive, congruence-modular and congruence-permutable algebras.

Definition 1.3.11. We say algebra A is **congruence-distributive** or **congruence-modular** iff the associated congruence lattice $Con\, A$ is distributive or modular respectively. □

In [BK47] it was shown that every algebra in a variety with a ternary majority term $M(x, y, z)$ such that $M(x, x, y) = M(x, y, x) = M(y, x, x) = x$ is congruence-distributive. Considering the term $M(x, y, z) = (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$ it follows readily that every lattice is congruence-distributive. Interestingly, Jonsson also showed in [Jon67] that every algebra in a

variety V is congruence-distributive if and only if there are ternary terms $p_1(x,y,z), p_2(x,y,z), \ldots, p_n(x,y,z)$ such that

$$\begin{aligned} p_i(x,y,x) &= x \quad \text{for all } i \leq n, \\ p_1(x,y,z) &= x, \\ p_n(x,y,z) &= z, \\ p_i(x,x,y) &= p_{i+1}(x,x,y) \quad \text{for } i \text{ even and } i \leq n, \\ p_i(x,y,y) &= p_{i+1}(x,y,y) \quad \text{for } i \text{ odd and } i \leq n. \end{aligned}$$

Similar conditions for congruence-modular varieties can be found in in [Day69] and [Gum81]. It should be mentioned again that every congruence-distributive algebra is congruence-modular, but the converse does not hold.

The next definition uses congruences again to introduce another useful class of algebras known as congruence-permutable algebras. They include important structures like groups and rings.

Definition 1.3.12. Suppose α and β are binary relations on algebraic structure A. Then

(i) By $\alpha \circ^n \beta$ where $n \geq 1$ we mean the relation $\alpha \circ \beta \circ \alpha \ldots$ which is a relation product alternating between α and β with n factors. Thus $\alpha \circ^1 \beta = \alpha$ and $\alpha \circ^n \beta = \alpha \circ (\beta \circ^{n-1} \alpha)$.

(ii) We say α and β n-**permute** where $n \geq 2$ iff $\alpha \circ^n \beta = \beta \circ^n \alpha$.

(iii) Algebra A is said to be n-**permutable** iff every pair of congruences of A n-permute. If algebra A is 2-permutable, we also say it is **permutable** or **congruence permutable**.

□

A.I. Mal'cev [Mal54] proved that every algebra in a variety with a ternary term $p(x,y,z)$ such that $p(x,x,y) = y$ and $p(x,y,y) = x$ for all elements x and y is congruence-permutable. It is actually an if and only if condition. This Mal'cev condition allows the reader to construct many algebras that are congruence-permutable. It also provides a simple reason why groups (consider the term $p(x,y,z) = xy^{-1}z$), rings (consider the term $p(x,y,z) = x - y + z$) and quasigroups (consider the term $p(x,y,z) = (x/(y\backslash y)).(y\backslash z)$) are congruence-permutable.

Given two congruences α and β, we clearly have $\alpha \vee \beta \geq \alpha \circ \beta$, however the concepts of join and permutable coincides for permutable algebras. And it should be highlighted that with permutable algebras the concept of factorization is lattice-theoretic, that is $\alpha \times \beta = 0$ iff $\alpha \vee \beta = 1$ and $\alpha \wedge \beta = 0$. Thus knowing the congruence lattice of a permutable algebra can reveal many of its factorization properties: For example if A is permutable and $Con(A) = C_3 \times C_4$ (where C_n is the n-element lattice chain) then A is decomposable. We end this section by showing that every permutable algebra is congruence-modular, but first we need Lemma 1.3.13.

Lemma 1.3.13. *(i) For even n, if $\alpha \circ^n \beta \subseteq \beta \circ^n \alpha$, then the congruences α and β n-permute.*

(ii) If an algebra A is n-permutable, then A is $n+1$-permutable.

Proof. (i) If ρ is a binary relation, like a congruence on an algebraic structure, let ρ' denote the converse relation of ρ, that is the relation

$$\rho' = \{(x,y) : (y,x) \in \rho\}.$$

Notice that for any two binary relations ρ and τ that $(\rho \circ \tau)' = \tau' \circ \rho'$ and for even $k > 0$ that $(\rho \circ^k \tau)' = (\tau') \circ^k (\rho')$. Since α, β are binary relations that are reflexive we have that

$$\begin{aligned} \beta \circ^n \alpha &= \beta' \circ^n \alpha' \\ &= (\alpha \circ^n \beta)' \\ &\subseteq (\beta \circ^n \alpha)' \\ &= \alpha' \circ^n \beta' \\ &= \alpha \circ^n \beta. \end{aligned}$$

Therefore $\alpha \circ^n \beta = \beta \circ^n \alpha$ and these congruences n-permute.

(ii) Thus $\alpha \circ^{n+1} \beta = \alpha \circ (\beta \circ^n \alpha) = \alpha \circ (\alpha \circ^n \beta) = \alpha \circ^n \beta$. In a similar fashion we can show that $\beta \circ^{n+1} \alpha = \beta \circ^n \alpha$. Therefore algebraic structure A is $n+1$-permutable.

□

Theorem 1.3.14. *If an algebra A is permutable, then A is 3-permutable. If A is 3-permutable, then A is congruence-modular.*

Proof. The first result follows by Lemma 1.3.13. For the second result suppose A is 3-permutable. Also $\alpha, \beta, \delta \in Con\, A$ such that $\alpha \leq \beta$. It remains to show that $\alpha \vee (\beta \wedge \delta) \geq \beta \wedge (\alpha \vee \delta)$. Suppose $(a, b) \in \beta \wedge (\alpha \vee \beta)$. Hence $(a, b) \in \beta$ and $(a, b) \in \alpha \vee \delta = \alpha \circ \delta \circ \alpha$. So there exists $c, d \in A$ such that $(a, c) \in \alpha, (c, d) \in \delta$ and $(d, b) \in \alpha$.

$$a \overset{\alpha}{\text{———}} \boldsymbol{c} \overset{\delta}{\text{———}} \boldsymbol{d} \overset{\alpha}{\text{———}} b$$

Using $\alpha \leq \beta$ we obtain $(c, d) \in \beta$. Thus $(c, d) \in \beta \wedge \delta$ which now shows that $(a, b) \in \alpha \vee (\beta \wedge \delta)$. □

Chapter 2

A Few Unique Factorization Results

In this chapter we finally prove some unique factorization results. This chapter includes partial answers to which congruence-permutable/congruence-modular algebras possess the unique factorization property.

2.1 Congruence-permutable algebras

Here we take the results from the previous chapter together and reproduce a unique factorization theorem for congruence-permutable algebras due to the American mathematician Garrett Birkhoff [Bir48] published in 1948. Another interesting proof of this theorem can be found in [MMT].

Before proving the first unique factorization result, we quickly recall the definition of a one-element subalgebra. Simple examples of one-element subalgebras include the set containing the identity element of any group.

Definition 2.1.1. We say $B = \{a\}$ is a one-element subalgebra of A iff B is closed under all the fundamental operations of A.

Theorem 2.1.2. *Suppose that A is a congruence-permutable algebra whose congruence lattice has finite height. If A has a one-element subalgebra then A is uniquely factorable.*

Proof. The congruence lattice of A is a modular lattice by Theorem 1.3.14. Also A has no infinite direct decomposition, because $Con\, A$ has finite height by Lemma 1.3.5. Suppose now

$$A \simeq \prod_{i=1}^{n} A_i \simeq \prod_{j=1}^{m} B_j,$$

for some directly indecomposable algebras A_i and B_j. Lemma 1.3.5 yields directly indecomposable congruences α_i, β_j such that

$$0 = \prod_{i=1}^{n} \alpha_i = \prod_{j=1}^{m} \beta_j$$

and $A/\alpha_i \simeq A_i$ and $A/\beta_j \simeq B_j$. Note that the dual of a modular lattice of finite height is still a modular lattice of finite height. Thus by Lemma 1.3.7 we have in the dual lattice of $Con\, A$ that

$$\alpha_1 \oplus \alpha_2 \oplus \ldots \oplus \alpha_m = 1 = \beta_1 \oplus \beta_2 \oplus \ldots \oplus \beta_n,$$

for some indecomposable congruences α_i and β_j. Applying Theorem 1.2.10 we have $m = n$. In this proof we showed a relabelling exist for all k such that

$$a_1 \oplus a_2 \oplus \ldots \oplus a_n = a_1 \oplus a_2 \oplus \ldots \oplus a_{k-1} \oplus a_k \oplus b_{k+1} \oplus b_{k+2} \oplus \ldots \oplus b_n.$$

Thus after a relabelling we can assume

$$\alpha_k \oplus \theta_k = 1 = \beta_k \oplus \theta_k$$

for some congruences θ_k for each k in the dual of $Con\, A$. Thus in the lattice $Con\, A$ we get $\alpha_k \times \theta_k = \alpha_k \wedge \theta_k = \beta_k \wedge \theta_k = \beta_k \times \alpha_k$. Therefore by Lemma 1.3.8 we get $A_k \simeq A/\alpha_k \simeq A/\beta_k \simeq B_k$ for each k. □

We commented earlier that every group, ring or quasi-group is congruence-permutable. Therefore by this theorem we have that every group or ring whose congruence lattice is of finite height is uniquely factorable. Also every quasigroup that has a congruence lattice of finite height and contains a one-element subalgebra must be uniquely factorable.

It should be noted that all the conditions in this theorem cannot be dropped. In section three of this chapter we give failures of the uniqueness property if just one of these conditions is omitted. Thus this result by itself is not easily generalized.

2.2 Birkhoff-Ore Theorem

In this section we reproduce a major unique factorization result due to the Icelandic mathematician Bjarni Jónsson [Jon66] for congruence-modular algebras. He carefully adapted the Birkhoff-Ore Theorem[1] discussed in the previous section to produce a new unique factorization theorem for finite congruence-modular structures.

2.2.1 More congruence theory

In this subsection we spend a little time proving three lemmas about congruences that will be used in the next subsection. The following result is an important for finite algebras and is vital in proving Theorem 2.2.6. Lemma 2.2.2 and Lemma 2.2.3 will respectively play roles in proving Theorem 2.2.6 and Theorem 2.2.7.

Lemma 2.2.1. *If A is a finite algebra and*

$$\alpha \times \alpha' = \beta \times \beta' = \alpha' \wedge \beta = \alpha \wedge \beta'$$

where $\alpha, \alpha', \beta, \beta' \in Con\, A$ then $\alpha \times \beta'$ exists and is equal to $\alpha \times \alpha'$.

Proof. We may safely replace A by $A/(\alpha \times \alpha')$. So we only need to show the result holds whenever $\alpha \times \alpha' = 0$. From the conditions it follows that $A \simeq A/\alpha \times A/\alpha' \simeq A/\beta \times A/\beta'$ and that A can be embedded into $A/\alpha' \times A/\beta$ and $A/\alpha \times A/\beta'$. If $a = |A/\alpha|, b = |A/\alpha'|, c = |A/\beta|$ and $d = |A/\beta'|$, then we have the following equalities and inequalities

$$\begin{aligned} |A| &= ab = cd, \\ |A| &\leq bc, \\ |A| &\leq ad. \end{aligned}$$

These inequalities imply that $a = c, b = d, |A| = bc$ and hence the embedding A into $A/\alpha' \times A/\beta$ is an isomorphism. □

[1] See [Bir48].

Lemma 2.2.2. *Suppose β, β' and γ are elements of Con A. If A is congruence-modular and $\beta \times \beta' = \gamma \times \gamma'$ then the following conditions are equivalent:*

(i) $(\beta \wedge \gamma) \circ \beta' = \beta' \circ (\beta \wedge \gamma)$.

(ii) $\beta \wedge (\beta' \circ (\beta \wedge \gamma) \circ \beta') \leq \gamma$.

Proof. To show (i) implies (ii) is a simple consequence of the modular law as seen in the calculation below:

$$\begin{aligned} \beta \wedge (\beta' \circ (\beta \wedge \gamma) \circ \beta') &\leq \beta \wedge (\beta' \vee (\beta \wedge \gamma)) \quad \text{by (i)} \\ &= (\beta \wedge \gamma) \vee (\beta \wedge \beta') \\ &= (\beta \wedge \gamma) \vee 0 \\ &\leq \gamma. \end{aligned}$$

To prove (ii) implies (i) suppose $(x, y) \in (\beta \wedge \gamma) \circ \beta'$. Therefore some element z exists such that $(x, z) \in \beta \wedge \gamma$ and $(y, z) \in \beta'$. Also $\beta \circ \beta' = \beta \vee \beta' = 1$ yields and element a such that $(x, a) \in \beta'$ and $(y, a) \in \beta$. Hence $(a, y) \in \beta \wedge (\beta' \circ (\beta \wedge \gamma) \circ \beta') \leq \gamma$ so that $(a, y) \in \beta \wedge \gamma$, showing that $(x, y) \in \beta' \circ (\beta \wedge \gamma)$. Therefore $(\beta \wedge \gamma) \circ \beta' \subseteq \beta' \circ (\beta \wedge \gamma)$ and hence by Lemma 1.3.13 they are actually equal. □

Lemma 2.2.3. *Suppose β, β', γ and γ' are elements of Con A. If $0 = \beta \times \beta' = \gamma \times \gamma'$, $\beta \leq \gamma$ and $\beta \circ \gamma' = \gamma' \circ \beta$ then $\beta = \gamma \times (\beta \circ \gamma')$.*

Proof. We first show $\gamma \wedge (\beta \circ \gamma') = \beta$. Noting $\gamma \wedge (\beta \circ \gamma') \geq \beta \wedge \beta = \beta$, we proceed to show that $\gamma \wedge (\beta \circ \gamma') \leq \beta$. If $(x, y) \in \gamma \wedge (\beta \circ \gamma')$ then $(x, y) \in \gamma$ and some element z exists such that $(x, z) \in \beta$ and $(z, y) \in \gamma'$. Using $\gamma \geq \beta$ we see that $(x, z) \in \gamma$. Therefore $(y, z) \in \gamma \wedge \gamma'$. Thus $y = z$ and $(x, y) \in \beta$. Now it remains to show that $\gamma \circ (\beta \circ \gamma') = 1 = (\beta \circ \gamma') \circ \gamma$.

$$\begin{aligned} \gamma \circ (\beta \circ \gamma') &= \gamma \circ (\gamma' \circ \beta) \\ &= (\gamma \circ \gamma') \circ \beta \\ &= \gamma \circ \gamma' \\ &= 1. \end{aligned}$$

Thus by Lemma 1.3.13 it follows that $\gamma \circ (\beta \circ \gamma') = 1 = (\beta \circ \gamma') \circ \gamma$ which finishes the proof. □

2.2.2 Jónsson's Unique Factorization Theorem

In this subsection we retrace B. Jónsson's original proof [Jon66] published in 1966. On our journey to proving Theorem 2.2.7 we encounter two other unique factorization results (Theorem 2.2.4 and Theorem 2.2.6) stated in terms of congruences.

Most unique factorization theorems make use of the fact that if two congruences α and β on the same structure A have a common complement, then $A/\alpha \simeq A/\beta$, provided A has an one-element subalgebra. The next result heavily relies on this fact, combined with some sort of exchange property.

Theorem 2.2.4. *Let A be a congruence-modular lattice of finite height with a one-element subalgebra. Suppose that, whenever β is a directly indecomposable congruence and*

$$0 = \beta \times \beta' = \gamma \times \gamma',$$

a congruence ϕ exists such that $0 = \phi \times \beta'$ and either $\phi \geq \gamma$ or $\phi \geq \gamma'$. If A has the above property, then A has the unique factorization property.

Proof. Without loss of generality, assume $m \leq n$ in the equation below. We proceed to show by induction on m that if the factors β_i and γ_j are directly indecomposable and

$$0 = \beta_1 \times \beta_2 \times \ldots \times \beta_m \times \phi = \gamma_1 \times \gamma_2 \times \ldots \times \gamma_n \times \phi,$$

for some congruence ϕ then $m = n$ and a bijection σ exists such that $A/\beta_i \simeq A/\gamma_{\sigma(i)}$ for $i = 1, 2, \ldots, m$. If $m = 1$ then

$$0 = \beta_1 \times \phi = \gamma_1 \times \ldots \gamma_n \times \phi.$$

Thus $A/\beta_1 \simeq A/\gamma_1 \times \ldots A/\gamma_n$, by Lemma 1.3.8. Therefore $n = 1$ and $A/\beta_1 \simeq A/\gamma_1$, proving the base case.

Let $\gamma' = \gamma_2 \times \gamma_3 \times \ldots \gamma_n \times \phi$. From consecutive applications of the hypothesis we find $\phi_1, \phi_2, \ldots, \phi_m$ (each containing either γ_1 or γ') such that

$$0 = \phi_1 \times \phi_2 \times \ldots \times \phi_{i-1} \times \beta_i \times \ldots \times \beta_m \times \phi = \gamma \times \gamma' \tag{2.1}$$

for $i = 2, 3, \ldots, m$. If above holds, then by applying the property of $Con\, A$ we know a congruence ϕ_i exists containing γ or γ' such that

$$0 = \phi_1 \times \phi_2 \times \ldots \times \phi_i \times \beta_{i+1} \times \ldots \times \beta_m \times \phi = \gamma \times \gamma' \tag{2.2}$$

Considering the case when $i = m$ we have

$$0 = \phi_1 \times \phi_2 \times \ldots \times \phi_m \times \phi \tag{2.3}$$

Hence the direct product of all those ϕ_i larger than γ_1 must be γ_1 and the direct product of those remaining factors (including ϕ) must be γ'. Therefore $\phi_j = \gamma_1$ for some $j \leq m$, since γ_1 is indecomposable. Comparing successive values of i in Equation 2.3 we see that $A/\beta_i \simeq A/\phi_i$ for all i. Thus $A/\beta_j \simeq A/\phi_j \simeq A/\gamma_1$ and $\beta_j = \gamma_1$, since β_j in $0 = \beta_1 \times \beta_2 \times \ldots \beta_j \times \ldots \beta_m \times \phi$ can be replaced by a congruence containing γ_1 or γ'. The rest of the proof now follows by induction replacing ϕ by $\phi \times \beta_j$. □

For the next theorem we introduce a new concept that singles out the most important congruences on an algebra in terms of direct product factorizations.

Definition 2.2.5. Let $FR(A, \alpha) = \{\beta : \beta \in Con\, A$ and some β' exists such that $\alpha = \beta \times \beta'\}$, i.e. $FR(A, \alpha)$ is the set of all direct factors of the congruence α on the algebra A. □

Theorem 2.2.6. *Let A be a finite congruence-modular algebra and $\mathcal{F}$ be the smallest family of congruences such that $0 \in \mathcal{F}$ and for all $\alpha \in \mathcal{F}$ and $\beta, \gamma \in FR(A, \alpha)$ we have $\beta \vee \gamma \in \mathcal{F}$. If for every $\alpha \in \mathcal{F}$ and $\beta, \beta', \gamma \in FR(A, \alpha)$ the property $\alpha = \beta \times \beta'$ implies $(\beta \wedge \gamma) \circ \beta' = \beta' \circ (\beta \wedge \gamma)$, then A is uniquely factorable.*

Proof. We show whenever $\alpha \in \mathcal{F}$ and

$$\alpha = \beta \times \beta' \times \phi = \gamma \times \gamma' \times \phi,$$

then congruences ψ and ψ' exist such that

$$\alpha = \psi \times \psi' \times \beta' \times \phi, \quad \gamma \leq \psi, \quad \gamma' \leq \psi'. \tag{2.4}$$

Observe the statement is trivial for $\alpha = 0$ or $\alpha = 1$, where 1 is the top element in $Con\, A$. Before continuing with induction we assume that the statement holds whenever α is replaced

by a bigger member of $\mathcal{F}$ or ϕ is replaced by a smaller congruence. Note if $\beta \wedge \gamma' \wedge \phi < \alpha$ and $\beta' \wedge \gamma \wedge \phi < \alpha$ then

$$\begin{aligned}(\beta \wedge \gamma' \wedge \phi) \wedge (\beta' \wedge \gamma \wedge \phi) &< \alpha \wedge \alpha \\ \alpha &< \alpha\end{aligned}$$

This contradiction shows that there is three cases to treat. Case I: $\beta \wedge \gamma' \wedge \phi = \beta' \wedge \gamma \wedge \phi = \alpha$, Case II: $\beta \wedge \gamma' \wedge \phi > \alpha$ or Case III: $\beta' \wedge \gamma \wedge \phi > \alpha$.

Case I: If $\beta \wedge \gamma' \wedge \phi = \gamma \wedge \beta' \wedge \phi = \alpha$. By Lemma 2.2.1 we have $\alpha = \gamma \times \beta' \times \phi$. Thus Equation 2.4 holds with $\psi = \gamma$ and $\psi' = 1$. Here we used Lemma 2.2.1, which immediately restricts us to finite algebras.

Case II: If $\alpha < \beta \wedge \gamma' \wedge \phi$. Define $\alpha_1 = \beta \wedge \gamma' \wedge \phi, \beta_1 = \beta, \beta_1' = \alpha_1 \circ \beta', \gamma_1 = \alpha_1 \circ \gamma$ and $\gamma_1' = \gamma'$. From the hypothesis and the modular law

$$\begin{aligned}\beta_1 \wedge \beta_1' \wedge \phi &= (\alpha_1 \circ \beta') \wedge (\beta \wedge \phi) = \alpha_1 \vee (\beta \wedge \beta' \wedge \phi) = \alpha_1, \\ \gamma_1 \wedge \gamma_1' \wedge \phi &= (\alpha_1 \circ \gamma) \wedge (\gamma' \wedge \phi) = \alpha_1 \vee (\gamma \wedge \gamma \wedge \phi) = \alpha_1.\end{aligned}$$

Hence $\alpha_1 = \beta_1 \times \beta_1' \times \phi = \gamma_1 \times \gamma_1' \times \phi$. Now $\alpha < \alpha_1 \in \mathcal{F}$. So we know ψ and ψ' exist such that

$$\alpha_1 = \psi \times \psi' \times \beta_1' \times \phi, \quad \gamma_1 \leq \psi, \quad \gamma_1' \leq \psi'.$$

Therefore

$$\begin{aligned}(\psi \wedge \psi' \wedge \phi) \circ \beta' &= (\psi \wedge \psi' \wedge \phi) \circ \alpha_1 \circ \beta' \\ &= (\psi \wedge \psi' \wedge \phi) \circ (\alpha_1 \vee \beta') \\ &= (\psi \wedge \psi' \wedge \phi) \circ \beta_1' \\ &= 1,\end{aligned}$$

and

$$\begin{aligned}(\psi \wedge \psi' \wedge \beta' \wedge \phi) \vee \phi &= (\psi \wedge \psi' \wedge \beta' \wedge \phi) \vee \alpha_1 \vee \phi \\ &= (\psi \wedge \psi' \wedge (\beta' \vee \alpha_1)) \vee \phi \\ &= 1,\end{aligned}$$

and

$$\begin{aligned}\gamma \wedge \gamma' \wedge \beta' \wedge \gamma &= \alpha_1 \wedge \beta' \\ &= (\beta \wedge \gamma' \wedge \phi) \wedge \beta' \\ &= \alpha.\end{aligned}$$

These calculations shows $\alpha = \psi \times \psi' \times \beta' \times \phi$. Also note $\alpha_1 \not\leq \gamma$. So we can strengthen this case by selecting ϕ to contain γ properly.

Case III: If $\alpha < \beta' \wedge \gamma \wedge \phi$. By applying the stronger version of Case II, we know there are congruences ψ_1 and ψ_1' such that

$$\alpha = \psi_1 \times \psi_1' \times \gamma' \times \phi, \quad \beta < \psi_1, \quad \beta' \leq \psi_1'.$$

According to Lemma 2.2.3 there is a congruence $\overline{\beta}$ such that $\beta' = \psi_1' \times \overline{\beta}$. Thus

$$\alpha = \beta \times \overline{\beta} \times (\psi_1' \times \phi) = \psi_1 \times \gamma' \times (\psi_1' \times \phi).$$

If $\phi_1' = 1$, then we have

$$\alpha = \beta \times \beta' \times \phi = \psi_1 \times \gamma \times \phi.$$

Now $\beta \wedge \phi_1 \wedge \phi = \alpha$ forces $\beta \wedge \phi = \alpha$ and $\beta' = 1$. Thus $\psi = \gamma$ and $\psi = \gamma'$ works. However if $\beta \wedge \psi_1 \wedge \phi > \alpha$ then Case II produces ψ_2 and ψ_2 such that

$$\alpha = \psi_2 \times \psi_2' \times \beta' \times \phi, \quad \psi_1 \leq \psi_2, \quad \gamma' \leq \psi_2'.$$

Observe $\beta < \psi_2$. Thus $\psi_2' \neq 1$ and using Lemma 2.2.3 we find $\overline{\gamma}$ such that $\gamma' = \psi_2' \times \overline{\gamma}$ and

$$\alpha = \psi_2 \times \beta' \times (\psi_2' \times \phi) = \gamma \times \overline{\gamma} \times (\psi_2' \times \phi),$$

with $\psi_2' \times \phi < \phi$. Another application of the induction hypothesis gives ψ_3 and ψ_3' such that

$$\alpha = \psi_3 \times \psi_3' \times \beta' \times \psi_2' \times \phi, \quad \gamma \leq \psi_3, \quad \overline{\gamma} \leq \psi_3'.$$

Consequently Equation 2.4 holds with $\psi = \psi_3$ and $\psi' = \psi_2 \times \psi_3'$. The only remaining case is when $\psi_1' \neq 1$. If $\psi_1' \neq 1$ then $\psi_1 \times \phi < \phi$. Thus by the induction hypothesis we can produce ψ_2 and ψ_2' such that

$$\alpha = \psi_2 \times \psi_2' \times \overline{\gamma} \times \psi_1 \times \phi, \quad \psi_1 < \psi_2, \quad \gamma' \leq \psi_2'.$$

By Lemma 2.2.3 we can find $\overline{\gamma}$ such that $\gamma' = \psi_2 \times \overline{\gamma}$. Therefore

$$\alpha = \psi_2 \times \beta' \times (\psi_2' \times \phi) = \gamma \times \overline{\gamma} \times (\psi_2' \times \phi).$$

Observe $\psi_2' \neq 1$ as this would mean $\alpha = \beta \times \beta' \times \phi = \psi_2 \times \beta' \times \phi$ which contradicts $\beta < \psi_2$. Thus $\psi_2' \times \phi < \phi$ and the induction hypothesis applied to the above equation produce ψ_3 and ψ_3' such that

$$\alpha = \psi_3 \times \psi_3' \times \beta' \times \psi_2' \times \phi, \quad \gamma < \psi_3, \quad \overline{\gamma} \leq \psi_3'.$$

Therefore Equation 2.4 holds with $\psi = \psi_3$ and $\psi' = \psi_2' \times \psi_3'$.

These three cases together prove that Equation 2.4 holds for algebra A. Therefore, if $\alpha = 0 = \beta \times \beta' = \gamma \times \gamma'$ then a congruences ψ, ψ' exist by this result exist such that $0 = \beta \times \beta' = \psi \times \psi' \times \beta'$ such that $\gamma \leq \psi$ and $\gamma' \leq \psi'$. By Lemma 1.3.8 it follows that $A/\beta \simeq A/\gamma \times A/\gamma'$. So if β is directly indecomposable then the property in Theorem 2.2.4 holds and it follows that A is uniquely factorable. □

Notice the similarity between the proofs of Lemma 1.2.9 and Theorem 2.2.6. Also the use of Lemma 2.2.1 in Case I. Now we have the ingredients to prove the promised unique factorization result for finite congruence-modular algebras [Jon66]. Another interesting proof of this result can be found in [MMT].

Theorem 2.2.7. *If A is finite with a one-element subalgebra and a modular-congruence lattice then, A is uniquely factorable.*

Proof. Select $\alpha \in \mathcal{F}$ as defined in Theorem 2.2.6. If $\alpha = \beta \times \beta' = \gamma \times \gamma'$ then β, β', γ and γ' are elements of $\mathcal{F}$. Thus

$$\begin{aligned} \beta \wedge (\beta' \circ (\beta \wedge \gamma) \circ \beta') &\leq \beta \wedge ((\beta \wedge \gamma) \vee \beta') \\ &\leq (\beta \wedge \gamma) \vee (\beta \wedge \beta') \\ &\leq \beta \wedge \gamma \\ &\leq \gamma. \end{aligned}$$

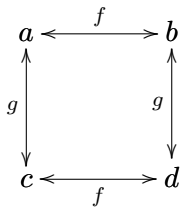
From Lemma 2.2.2 we see that $\beta \wedge \gamma$ and β' permute. Thus by Theorem 2.2.4 it follows that A is uniquely factorable. □

Therefore all finite congruence-modular structures that have a one-element subalgebra must be uniquely factorable. For example every finite group or finite ring has the unique factorization property. Also every finite lattice is congruence-distributive and hence congruence-modular and therefore possesses this property too. Just like Theorem 2.1.2 every condition is necessary. We demonstrate this by giving examples of failures in the next section.

2.3 Counter-examples

The first two sections have a natural generalization : If $Con\, A$ is a modular lattice of finite height and A has a one-element subalgebra, must A be uniquely factorable? The three examples found in [MMT] here demonstrate that if one those conditions is removed then A may fail to have the UFP.

Example 2.3.1. Suppose $A = \{a, b, c, d\}$ is an algebra with 2 unary functions f, g as indicated below. We see that $\theta_1 = \{(a,a),(a,b),(b,b),(b,a),(c,c),(c,d),(d,c),(d,d)\}$, $\theta_2 = \{(a,c),(a,a),(c,a),(c,c),(b,b),(b,d),(d,b),(d,d)\}$ and $\theta_3 = \{(a,d),(a,a),(d,a),(d,d),(b,b),(b,c),(c,b),(c,c)\}$ are congruences on A. Observe that $A \simeq A/\theta_1 \times A/\theta_2 \simeq A/\theta_2 \times A/\theta_3 \simeq A/\theta_3 \times A/\theta_1$, but none of $A/\theta_1, A/\theta_2, A/\theta_3$ are isomorphic to one another.



Notice in this example that A does not have an one-element subalgebra, but A is finite and hence $Con\, A$ is finite or of finite height. A simple calculation shows $Con\, A$ is permutable hence also congruence-modular. Therefore the condition that A must have an one-element subalgebra is necessary.

Example 2.3.2. For every natural number n, let A_n be the n-element semigroup and $c \in A_n$ such that $x.y = c$ for any $x, y \in A_n$. Let B_n denote the $2n$-element groupoid with the multiplication table shown below:

It turns out $A_2 \times B_3 \simeq A_3 \times B_2$, where each factor is a directly indecomposable algebra. Therefore it is a commutative semigroup that does not possess the unique factorization property, since all the factors are not isomorphic to one another.

This example illustrates that the condition of modularity is necessary, since finite algebra $A_2 \times B_3$ is not congruence-modular. Therefore also not congruence-permutable, but possess a one-element subalgebra.

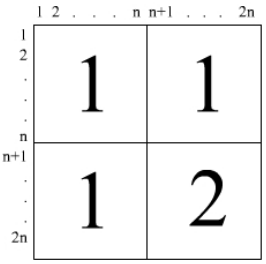


Figure 2.1: A depiction of an algebra that fails the UFP.

Example 2.3.3. Let V be a 4-dimensional vector space over the field of rational numbers with $\{x, y, z, u\}$ as a basis. Let P and Q be infinite disjoint sets of prime numbers with $5 \notin P \cup Q$. Let R and S be the set of all square-free positive integers whose prime factors belong to P and Q respectively. If

$$\begin{aligned}
A &= \left\{\tfrac{a}{r}x + \tfrac{b}{s}y + \tfrac{c}{5}(x+y) : a, b, c \in \mathbb{Z}, r \in R, s \in S\right\},\\
B &= \left\{\tfrac{a}{r}z + \tfrac{b}{s}u + \tfrac{c}{5}(z+u) : a, b, c \in \mathbb{Z}, r \in R, s \in S\right\},\\
C &= \left\{\tfrac{a}{r}(2x+z) + \tfrac{b}{s}(y+3u) + \tfrac{c}{5}(2x+2y+z+6u) : a, b, c \in \mathbb{Z}, r \in R, s \in S\right\},\\
D &= \left\{\tfrac{a}{r}(17x+9z) + \tfrac{b}{s}(y+2u) + \tfrac{c}{5}(17x+2y+9z+4u) : a, b, c \in \mathbb{Z}, r \in R, s \in S\right\},
\end{aligned}$$

then it can be shown that A, B, C and D are directly indecomposable abelian groups. Put

$$\begin{aligned}
x' &= 2x + z\\
y' &= y + 3u\\
z' &= 17 + 9z\\
u' &= y + 2u.
\end{aligned}$$

Note that $\{x', y', z', u'\}$ is also basis for V, since

$$\begin{aligned}
x &= 9x' - z'\\
y &= -2y' + 3u'\\
z &= -17x' + 2z'\\
u &= y' - u',
\end{aligned}$$

and that

$$\begin{aligned}
C &= \left\{\tfrac{a}{r}x' + \tfrac{b}{s}y' + \tfrac{c}{5}(x'+2y') : a, b, c \in \mathbb{Z}, r \in R, s \in S\right\},\\
D &= \left\{\tfrac{a}{r}z' + \tfrac{b}{s}u' + \tfrac{c}{5}(z'+2u') : a, b, c \in \mathbb{Z}, r \in R, s \in S\right\}.
\end{aligned}$$

It is clear that $A \simeq B$ and $C \simeq D$ and $A \cap B = \{0\} = C \cap D$. Note

$$\begin{aligned} x &= 9x' - z' \in C \cup D \\ y &= -2y' + 3u' \in C \cup D \\ z &= -17x' + 2z' \in C \cup D \\ u &= y' - u' \in C \cup D \\ \frac{x+y}{5} &= \frac{9}{5}(2x + 2y + z + 6u) - \frac{1}{5}(17x + 2y + 9z + 4u) - 3y - 10u \in C \cup D \\ \frac{u+z}{5} &= \frac{1}{5}(17x + 2y + 9z + 4u) - \frac{8}{5}(2x + 2y + z + 6u) - \frac{x+y}{5} + 5y + 9u \in C \cup D \end{aligned}$$

Hence $A+B \subseteq C+D$. Likewise it can be shown that $C+D \subseteq A+B$. Therefore $A+B = C+D$ giving $A^2 \simeq A+B = C+D \simeq C^2$. Next we proceed to show $A \not\simeq C$. Assume for a contradiction $\phi : A \longrightarrow C$ is an isomorphism. Note that the only elements $v \in A$ with the property that $\frac{v}{r} \in A \iff r \in R$ where $r \in \mathbb{Z}$ is $v = x$ or $v = -x$, since it is clear $v = kx$ for some integer k. However if $k \neq \pm 1$ then take any $r \in R$. Then $\frac{x}{r} = \frac{kx}{kr} \in A$ giving $kr \in R$. Likewise if $kr \in R$ we get $k^2 r \in R$, which is impossible if $|k| > 1$, since R is square-free, proving the claim. Likewise it can be shown the only elements $w \in C$ with the property that $\frac{w}{r} \in B \iff r \in R$ where $r \in \mathbb{Z}$ is $w = x'$ or $w = -x'$. Thus $\phi(x) \in \{x', -x'\}$. Likewise we can show $\phi(y) \in \{y', -y'\}$. Hence

$$\phi((x+y)/5) = \pm\frac{x' \pm y'}{5} \notin C.$$

Thus $A \not\simeq C$ but $A^2 \simeq C^2$.

This example due to Jónsson [Jon57] illustrates that the condition of finiteness or that the congruence lattice is of finite height is necessary. Here $Con\, A^2$ is not of finite height, but clearly congruence-permutable (it is a group), hence also congruence-modular.

2.4 Freese's Unique Factorization Theorem

This section explores Freese's [Fre1, Fre2] attempt at answering the open problem whether the common generalization of Theorem 1.2.10 and Theorem 2.2.7 holds:

If $Con\, A$ is a modular lattice of finite height and A has an one-element subalgebra, must A be uniquely factorable?

He found a substitute condition, for Lemma 2.2.1 (this was important in the proof of Theorem 2.2.7) to establish his own unique factorization result.

Definition 2.4.1. We say structure A has **Property P** if for any congruences $\alpha, \alpha', \beta, \beta'$ whenever

$$\alpha \times \alpha' = \beta \times \beta' = \alpha' \wedge \beta = \alpha \wedge \beta'$$

then $\alpha \times \beta'$ exists and is equal to $\alpha \times \alpha'$. □

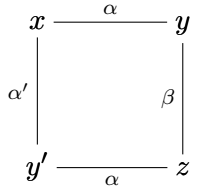
In [MMT] the authors showed whenever $Con\, A$ is a modular lattice of finite height where Property P can be proven then the generalization is valid. We start by proving a simple lemma concerning congruences.

Lemma 2.4.2. *Let L be a modular lattice of equivalence relations with elements α, α' and β.*

(i) If α, α' permute and $\alpha \wedge \alpha' \leq \beta \leq \alpha'$ then α and β permute.

(ii) If α, α' permute and $\alpha \leq \beta \leq \alpha \vee \alpha'$ then α' and β permute.

Proof. For part (i) suppose $(x, z) \in \alpha \circ \beta$. Thus an element y exists such that $(x, y) \in \alpha$ and $(y, z) \in \beta$. Therefore $(x, z) \in \alpha \vee \beta \leq \alpha \vee \alpha'$ and an element y' exists such that the relations in the following diagram holds:



By modularity we get $(x, y') \in \alpha' \wedge (\alpha \vee \beta) = (\alpha \wedge \alpha') \vee \beta = \beta$. Therefore $(x, z) \in \beta \circ \alpha$ and the result follows by Lemma 1.3.13. Proof of part (ii) is similar. □

Definition 2.4.3. *Suppose $FL(x, x', y, y')$ is a free lattice on the four generators x, x', y, y'. Define maps α_n and β_n on the set $\{a, a', b, b'\}$ to the free lattice $FL(x, x', y, y')$ such that $\beta_0(a) = x, \beta_0(a') = x', \beta_0(b) = y, \beta_0(b') = y'$ and*

$$\beta_{n+1}(a) = x \wedge [\beta_n(b) \vee \beta_n(a')] \wedge [\beta_n(b) \vee \beta_n(b')] \wedge [\beta_n(a') \vee \beta_n(b')].$$

Note the definition of β_n on b, b', a' is symmetric, α_n is defined dually.

For each n, $\alpha_n(b)$ or $\beta_n(a)$ is a term in the language of lattices. We let $\alpha_n^L(b)$ be the interpretation of this term in lattice L under the substitution $x = a, y = b, x' = a'$ and $y' = b'$. Similarly for $\beta_n^L(a)$. □

The next lemma will use the lattice depicted in Figure 2.2, which we label M_4.

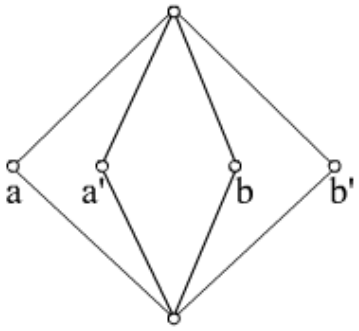


Figure 2.2: M_4 lattice.

The following result is due to R. Mckenzie [Mck72b] and is needed for Lemma 2.4.5.

Lemma 2.4.4. *If f is the unique homomorphism on the free lattice $FL(x, x', y, y')$ to M_4 such that $f(x) = a, f(y) = b, f(x') = a'$ and $f(y') = b'$ then $f(z) \geq w$ iff $z \geq \beta_n^L(w)$ for some n where $w \in \{a, a', b, b'\}$, the set of atoms of M_4.*

Proof. If $z \geq \beta_n^L(w)$ then $f(z) \geq f(\beta_n^L(w)) = w$, since inductively on n it turns out $f(\beta_n^L(w)) = w$. For the converse, we use induction on the length of expression z. For $z = x, x', y$ or y' the claim is obvious. To proceed we treat two cases :

Case I. Let $z = e_1 \wedge e_2$ for some smaller expressions e_1 and e_2. If $f(z) \geq w$ then $f(e_1) \geq w$ and $f(e_2) \geq w$. By the induction hypothesis we have $e_1 \geq \beta_n^L(w)$ for some n and $e_2 \geq \beta_m^L(w)$ for some m. Noting $\beta_r^L(w) \geq \beta_s^L(w)$ if $r > s$ we have $z = e_1 \wedge e_2 \geq \beta_{max(m,n)}^L(w)$.

Case II. Let $z = e_1 \vee e_2$ for some smaller expressions e_1 and e_2. If $f(z) = f(e_1 \vee e_2) \geq w$, then $f(e_1) \geq w, f(e_2) \geq w$ which means $e_1 \vee e_2 \geq e_1$ or $e_2 \geq \beta_n^L(w)$ for some n. The other remaining possibility is $f(e_1) = w_1$ and $f(e_2) = w_2$ where w, w_1 and w_2 are all distinct. Then by the induction hypothesis we have $e_1 \vee e_2 \geq \beta_m^L(w_1) \vee \beta_n^L(w_2)$ for some m and n. Hence $z = e_1 \vee e_2 \geq \beta_{max(m,n)}^L(w_1) \vee \beta_{max(m,n)}^L(w_2) \geq \beta_{max(m,n)+1}^L(w)$. □

Using this Lemma we can proof the next result which is needed for Theorem 2.4.6.

Lemma 2.4.5. *Suppose L is a lattice generated by x, y, x', y'. Let a, b, a', b' again be the atoms of M_4. The map $g(x) = a, g(y) = b, g(x') = a'$ and $g(y') = b'$ can be extended to a homomorphism of L into M_4 if and only if $\beta_n^L(a) \not\leq \alpha_n^L(b)$ for all $n \geq 0$.*

Proof. If $\beta_n^L(a) \leq \alpha_n^L(b)$ for some n then $a = g(\beta_n^L(a)) \leq g(\alpha_n^L(b)) = b$ if g was a homomorphism. This contradiction gives the one direction. For the other direction suppose g is a homomorphism and that $\beta_n^L(a) \leq \alpha_n^L(b)$ for some n. Using Lemma 2.4.4 we get $a \leq g(\alpha_n^L(b)) = b$ which is the desired contradiction. □

Theorem 2.4.6. *Suppose J is a modular lattice of finite height with equivalence relations α, α', β and β' satisfying*

$$\alpha \times \alpha' = \beta \times \beta' = \alpha' \wedge \beta = \alpha \wedge \beta'.$$

If there is no homomorphism of the sublattice of J generated by $\{\alpha, \beta, \alpha', \beta'\}$ onto M_4 then α and β' permute.

Proof. Let L be the lattice generated by $\{\alpha, \beta, \alpha', \beta'\}$. If

$$\alpha \wedge \alpha' = \alpha \wedge \beta = \alpha \wedge \beta' = \alpha' \wedge \beta = \alpha' \wedge \beta' = \beta \wedge \beta'$$

then a dimension argument shows

$$\alpha \vee \alpha' = \alpha \vee \beta = \alpha \vee \beta' = \alpha' \vee \beta = \alpha' \vee \beta' = \beta \vee \beta'$$

making $L \simeq M_4$, contrary to the hypothesis. Therefore we may assume without loss of generality $\alpha' \wedge \beta' > 0$. Let

$$\hat{\alpha} = \alpha \vee (\alpha' \wedge \beta'), \qquad \hat{\beta} = \beta \vee (\alpha' \wedge \beta').$$

and L_1 be the lattice generated by $\{\hat{\alpha}, \hat{\beta}, \alpha', \beta'\}$. Note $0 = \hat{\alpha} \times \alpha' = \hat{\beta} \times \beta' = \alpha' \wedge \hat{\beta} = \hat{\alpha} \wedge \beta'$. As in Lemma 2.4.5, we let $\beta_n^{L_1}$ be the interpretation of this term in L_1 under the substitution $x = \hat{\alpha}, x' = \alpha, y = \hat{\beta}, y' = \beta'$. Since L does not have M_4 as a homomorphic image, some n exists such that the following relation holds :

$$\beta_n^L(a) \leq \alpha_n^L(b). \tag{2.5}$$

Before we return to Equation 2.5 we will show that

$$\beta_n^{L_1}(a) = \beta_n^L(a) \vee (\alpha' \wedge \beta'). \tag{2.6}$$

Using induction on n and modularity we easily obtain $\beta_{n+1}(a) = \beta_n(a) \vee (\alpha' \wedge \beta')$ in L and L_1. From this we can conclude $\beta_{n+1}(a) = \beta_n(a) \wedge (\beta_n(a') \vee \beta_n(b'))$ in L and L_1. Modularity easily gives $\beta_n^{L_1}(a) \geq \beta_n^L(a) \vee (\alpha' \vee \beta')$. Using induction on n the next calculation establishes equality.

$$\begin{aligned} h(\beta_{n+1}^{L_1}(a)) &= h(\beta_n^{L_1}(a)) + h(\beta_n^{L_1}(a) \vee \beta_n^{L_1}(b')) - h(\beta_n^{L_1}(a) \vee \beta_n^{L_1}(a')) \\ &= [h(\beta_n^L(a)) + h(\alpha' \wedge \beta')] + [h(\beta_n^L(a) \vee \beta_n^L(b')) + h(\alpha' \wedge \beta')] \\ &\quad -[h(\beta_n^L(a) \vee \beta_n^L(a')) + h(\alpha' \wedge \beta')] \\ &= h(\beta_{n+1}^L(a)) + h(\alpha' \wedge \beta') \\ &= h(\beta_{n+1}^L(a) \vee (\alpha' \wedge \beta')). \end{aligned}$$

Hence Equation 2.6 gives

$$\begin{aligned} \beta_n^{L_1}(a) &= \beta_n^L(b) \vee (\alpha' \wedge \beta') \\ &\leq \alpha_n^L(b) \vee (\alpha' \wedge \beta') \\ &\leq \alpha_n^{L_1}(b). \end{aligned}$$

Therefore by Lemma 2.4.5, L_1 does not have M_4 as a homomorphic image. Thus by induction on the height of the lattice we can conclude $\hat{\alpha}$ and β permute. This fact with Lemma 2.4.2 gives

$$\begin{aligned} \alpha \vee \beta' &= \hat{\alpha} \vee \beta' \\ &= \hat{\alpha} \circ \beta' \\ &= [\alpha \vee (\alpha' \wedge \beta')] \circ \beta' \\ &= [\alpha \circ (\alpha' \wedge \beta')] \circ \beta' \\ &= \alpha \circ \beta'. \end{aligned}$$

□

As an immediate consequence of this theorem, we have Freese's [Fre1, Fre2] Unique Factorization Theorem.

Corollary 2.4.7. *Algebra A is said to have property Q if for any congruence α, α', β and β' on A, if*

$$\alpha \times \alpha' = \beta \times \beta' = \alpha' \wedge \beta = \alpha \wedge \beta',$$

and there is no homomorphism of the sublattice of J generated by $\{\alpha, \beta, \alpha', \beta'\}$ onto M_4, then α and β' permute. If A is a congruence-modular lattice of finite height with an one-element subalgebra with property Q, then A is uniquely factorable.

How does this result shine light on the unsolved problem : Does an algebra with a congruence-modular lattice of finite height with an one-element subalgebra have the UFP? It seems that this unsolved problem hinges on deducing Property P. Hypothetically speaking, if Property P holds for all infinite algebras then it must hold for an infinite set A with a binary operation $\cdot$ such that $x \cdot y = x$. Therefore $Con\, A = Eq\, A$ and we stripped the algebraic problem down to an easier set-theoretic problem. Unfortunately Ralph Freese found an example [Fre2] of a congruence-modular lattice of finite height that does not possess Property P, but is still uniquely factorable. So even though it seems that Property P is important, it is not vital for a structure to have the unique factorization property. Hence the door is still open for new attacks to this generalization.

Chapter 3

Zero-algebras

By 1947 it was already known that every finite group with or without operators has, up to isomorphism, an unique represention as a direct product of directly indecomposable subgroups. For groups without operators compare [Kro70], [MW09], [Rem11] and [Spe27]. For groups with operators see [Sch28]. Another proof can be found in [Fit34].

Inspired by these group theoretic results, Bjarni Jónsson extended them in his doctoral thesis [JT47] (under the supervision of Alfred Tarski) to a wider class of structures. He focussed on structures known as **zero-algebras**. We say $(A, 0, +, F_1, F_2, \ldots)$ is a **zero-algebra**, an **algebra with a zero** or a **Jónsson-Tarski algebra** if it has a one-element subalgebra $\{0\}$ and a binary operation $+$ such that for all $x \in A$ we have $x + 0 = x = 0 + x$. Thus groups, rings, lattices and H-spaces in algebraic topology are all examples of zero-algebras.

In this chapter we prove that any finite zero-algebra is uniquely factorable, giving all the other operators $F_1, F_2, \ldots$ more or less a free ride. Before we do this we introduce the notions of inner products and central subuniverses. After a series of lemmas (as modified from [MMT] and [JT47]) we establish something stronger which consequently proves that every finite zero-algebra is uniquely factorable.

We close this chapter by studying similar structures known as structures almost without zero-divisors. Following Ivan Chajda's [Cha76] arguments we produce an expected unique factorization result which does not require any finiteness.

3.1 Inner products

The idea of inner products is a well-studied concept for groups and was the earliest technique used to prove their unique factorization property. Here we demonstrate that the idea of inner products can be extended to zero-algebras, as explored in [Kro70], [MW09], [Rem11], [Spe27] and [Sch28]. The next result illustrates how to transform any direct product factorization into an inner product factorization.

Lemma 3.1.1. *If A is a zero-algebra and $A \simeq \prod_{i=1}^{n} A'_i$, then subalgebras A_i of A exist such that $A_i \simeq A'_i$ and $A \simeq \prod_{i=1}^{n} A_i$. Furthermore, for any $a \in A$ we can write $a = \sum_{i=1}^{n} a_i$ for unique elements $a_i \in A_i$. Also, if $a_i \in A_i$ then $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} a_{\sigma(i)}$ for any permutation σ of the set $\{1, 2, \ldots, n\}$. Lastly, for every fundamental operation F of arity r, if $a_k = \sum_{i=1}^{n} a_{ki}$ for*

some $a_k \in A$ *and* $a_{ki} \in A_i$ *then*

$$F(a_1, a_2, \ldots, a_r) = \sum_{i=1}^{n} F(a_{1i}, a_{2i}, \ldots, a_{ri}).$$

Proof. Suppose $\phi : \prod_{i=1}^{n} A_i' \longrightarrow A$ is an isomorphism. For each i, put

$$A_i = \{\phi(0, \ldots, a, \ldots, 0) : a \in A_i'\}.$$

Therefore $A_i \simeq A_i'$ and $A_i \subseteq A$ for all i. Suppose $\phi^{-1}(a) = (a_1', \ldots, a_n')$ where $a_i' \in A_i'$. If $a_i = \phi(0, \ldots, a_i', \ldots, 0)$ for each i then $a = \sum_{i=1}^{n} a_i$. Note the expression $\sum_{i=1}^{n} a_i$ does not depend on bracketing or rearrangement. Uniqueness follows from the fact that this representation is unique in $\prod_{i=1}^{n} A_i'$. For the last claim follows from the bijection ϕ. □

Before we give an official definition of inner product, we provide one example to demonstrate the previous result. The reader shoulder take note that the concepts of inner products will only apply to this chapter.

Example 3.1.2. Note that the cyclic group with 6 elements $\mathbb{Z}_6$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$ and that subalgebras $\{0, 3\}, \{0, 2, 4\}$ of $\mathbb{Z}_6$ are respectively isomorphic to $\mathbb{Z}_2$ and $\mathbb{Z}_3$.

In this chapter $\sum_{i=1}^{3} a_i$ means $(a_1 + a_2) + a_3$ and need not be $a_1 + (a_2 + a_3)$ as we do not always have associativity. However $0 + a + 0 = a$ no matter how the brackets are arranged. This behaviour is captured in a manner by the idea of inner product.

Definition 3.1.3. Suppose $\{A_1, A_2, \ldots, A_n\}$ is a collection of subalgebras of A such that for each $a \in A$ there are unique elements $a_i \in A_i$ such that $a = (((a_1 + a_2) + a_3) + \ldots) = \sum_{i=1}^{n} a_i$ (that is brackets been omitted by association on the left in $\sum_{i=1}^{n} a_i$). Suppose $a_i \in A_i$ and that σ is a permutation on the set $\{1, 2, \ldots, n\}$, then

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} a_{\sigma(i)}.$$

If for every fundamental operation F of arity r and any $a_k \in A$ where $a_k = \sum_{i=1}^{n} a_{ki}$ for some $a_{ki} \in A_i$ we have

$$F(a_1, a_2, \ldots, a_r) = \sum_{i=1}^{n} F(a_{1i}, a_{2i}, \ldots, a_{ri}),$$

then we say A is an **inner product** of the subalgebras A_i and denote this by $A = \prod_{i=1}^{n} A_i$. (Be careful not to confuse this idea with direct products, even though we use the same symbol.) □

Suppose $\{A_1, A_2, \ldots, A_n\}$ is a collection of subalgebras of A such that $A = \prod_{i=1}^{n} A_i$. If $a \in A$ then $a = \sum_{i=1}^{n} a_i$ for unique $a_i \in A_i$. Let $f_i : A \longrightarrow A$ be maps such that $f_i(a) = a_i$. It is easily established these maps are all endomorphisms with $f_i(A) = A_i$. They also satisfy the following conditions :

$$f_i^2 = f_i, \tag{3.1}$$

$$f_i f_j = 0 = f_j f_i \text{ whenever } i \neq j, \tag{3.2}$$

$$(\ldots(f_1 + f_2) + \ldots) + f_n = 1, \tag{3.3}$$

where 1 is id_A. Here fg is shorthand for $f \circ g$. By analogy with abelian group theory we abbreviate $f_1 \oplus \ldots \oplus f_n = 1$ if f_i are endomorphisms satisfying Equations (3.1) − (3.3). To summarize, we now have a natural way of turning any direct product factorization into a set of endomorphisms. The converse is also true, as seen from the next lemma.

Lemma 3.1.4. *If $f_1, f_2, \ldots, f_n$ are endomorphisms on zero-algebra A satisfying Equations (3.1) – (3.3) then*

$$A = \prod_{i=1}^{n} f_i(A).$$

Proof. By Equation 3.3 you get $a = \sum_{i=1}^{n} f_i(a)$ where $f_i(a) \in f_i(A)$ for each $1 \leq i \leq n$. Also if

$$a = \sum_{i=1}^{n} a_i$$

where $a_i \in f_i(A)$ for each i, then using Equation 3.1 and Equation 3.2 you get

$$\begin{aligned} f_i(a) &= \sum_{i=1}^{n} f_i(a_i) \\ f_i(a) &= f_i(a_i) = a_i. \end{aligned}$$

Thus the representation is unique. □

Endomorphisms will play an essential role, hence it would be wise to list a few elementary properties about them. For the next lemma $End\, A$ denotes the set of all endomorphisms of zero-algebra A.

Lemma 3.1.5. *Suppose A is a zero-algebra and a, b, c, d are any functions from A to A. Let $s, t, f, f', g, g', h, h'$ be endomorphisms of A such that $1 = f \oplus f' = g \oplus g' = h \oplus h'$. Then*

(i)

$$\begin{aligned} a(bc) = (ab)c, &\qquad (a+b)c = ac + bc, \\ a1 = 1a = a, &\qquad a + 0 = 0 + a = a, \\ s(a+b) = sa + sb, &\qquad 0a = 0 = s0, \end{aligned}$$

where 1 is the identity map $x \mapsto x$ and 0 is the map that takes $x \mapsto 0$.

(ii) If $fa = fb$ and $f'a = f'b$ then $a = b$.

(iii) $fs + f't \in End\, A$.

(iv) $s + hfgf't \in End\, A$.

(v) $a + hfgf'b = hfgf'b + a$.

(vi) $(a + hfgf'b) + c = a + (hfgf'b + c)$.

(vii) There is a function $x : A \longrightarrow A$ such that $x + hfgf'b = 0$.

(viii) If $c = hfgf'd$ or c is a finite sum of maps of this form then c is cancellative, that is $a + c = b + c$ implies $a = b$.

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

(x) $fgfg'f = fg'fgf$.

Proof. Assertion (i) is obvious. The second assertion is immediate from $a = fa + f'a = fb + f'b = b$. For the third assertion, let F be any n-ary operation on A and $x_1, \ldots, x_n \in A$. We need

to show that $\alpha = (fs + f't)(F(x_1, \ldots, x_n))$ and $\beta = F(fs(x_1) + f't(x_1), \ldots, fs(x_n) + f't(x_n))$ are equal.

$$\begin{aligned} f(\beta) &= fF(fs(x_1) + f't(x_1), \ldots, fs(x_n) + f't(x_n)) \\ &= F(f^2s(x_1) + ff't(x_1), \ldots, f^2s(x_n) + ff't(x_n)) \\ &= F(f^2s(x_1), \ldots, f^2s(x_n)) \\ &= (f^2s)F(x_1, \ldots, x_n)) \\ &= (f^2s + ff't)F(x_1, \ldots, x_n)) \\ &= f(\alpha). \end{aligned}$$

Similarly we can show $f'(\beta) = f'(\alpha)$. From (ii) it follows that $\alpha = \beta$. Thus $fs + f't \in End\, A$.

Define λ, ϕ, ψ and δ to be the expression in the line that precedes it in the following calculations:

$$\begin{aligned} fa + (f'b + fc) &= f[fa + (f'b + fc)] + f'[fa + (f'b + fc)] \\ &= [f^2a + (ff'b + f^2c)] + [f'fa + (f'f'b + f'f'c)] \\ &= [fa + (0 + fc)] + [0 + (f'b + 0)] \\ &= (fa + fc) + f'b \\ &= \lambda. \\ fa + (gf'b + fc) &= g[fa + (gf'b + fc)] + g'[fa + (gf'b + fc)] \\ &= g(\lambda) + g'f(a + c) \\ &= \phi. \\ a + (fgf'b + c) &= f[a + (fgf'b + fc)] + f'[a + (fgf'b + c)] \\ &= f(\phi) + f'(a + c) \\ &= \psi. \\ a + (hfgf'b + c) &= h[a + (hfgf'b + c)] + h'[a + (hgf'b + c)] \\ &= h(\psi) + h'(a + c) \\ &= \delta. \end{aligned}$$

Putting $a = s, b = t, c = 0$ in the equation above, we get

$$s + hfgf't = h(\psi) + h'(s + t).$$

Thus assertion (iv) holds by applying assertion (iii). By very smilar calculations we can also show that

$$\begin{aligned} \lambda &= (f'b + fa) + fc, \\ \phi &= (gf'b + fa) + fc, \\ \psi &= (fgf'b + a) + c, \\ \delta &= (hfgf'b + a) + c. \end{aligned}$$

Thus $a + (hfgf'b + c) = (hfgf'b + a) + c$. Letting $c = 0$ we get assertion (v). From this we

readily obtain assertion (vi). For assertion (vii) use $x = hfg'f'b$, since

$$\begin{aligned} x + hfgf'b &= hfg'f'b + hfgf'b \\ &= hf(g' + g)f'b \\ &= hf1f'b \\ &= hff'b \\ &= h0b \\ &= 0. \end{aligned}$$

Assume $c = \sum_{i=1}^{n} h_i f_i g_i f_i' d_i$ for some functions. Assertions (v) and (vi) shows it does not matter how this sum is associated. Using (vii) we have for each i an inverse $x_i = h_i f_i g_i f_i' d_i$. Put $y = (\ldots(x_1 + x_2) + \ldots x_n$. Using (v) and (vi) we see that for any $a \in A$ that $(a + c) + y = a$. Therefore c is cancellative. For assertion (ix) we first note

$$\begin{aligned} fg'fg + fg'f'g = fg'(f + f')g = fg'1g = fg'g = 0, \\ fgf'g + fg'f'g = f(g + g')f'g = f1f'g = ff'g = 0. \end{aligned}$$

Using the fact that $fg'f'g$ is cancellative, it follows that $fg'fg = fgf'g$. Applying assertion (ix) twice we get $fgfg'f = fgf'gf = fg'fgf$. Hence endomorphisms fgf and $fg'f$ commute. □

We end this section with a simple cancellation theorem about inner direct products. This will used to prove Jónsson-Tarski Theorem, the major theorem of this chapter.

Theorem 3.1.6. *If B, C, D, E and F are subalgebras of zero-algebra A such that $A = B \times C \times D = E \times C \times F$ then $B \times D \simeq E \times F$*[1].

Proof. Select $b \in B$ and $d \in D$. Define map $\phi : B \times D \longrightarrow E \times F$ such that $\phi(b + d) = e + f$ if $b + 0 + d = e + c + f$ for unique elements $e \in E, c \in C$ and $f \in F$. Similarly, select $e \in E$ and $f \in F$. If $e + 0 + f = b + c + d$ for unique elements $b \in B, c \in C$ and $d \in D$ then let $\psi : E \times F \longrightarrow B \times D$ be a map such that $\psi(e + f) = b + d$. Both maps are easily seen to be homomorphisms.

Select $b \in B$ and $d \in D$. Suppose $b + d = e + c + f$ for some $e \in E, c \in C$ and $f \in F$ and $e + f = b' + c' + f'$ for some $b' \in B, c' \in C$ and $f' \in F$. Thus $\psi(\phi(b + d)) = \psi(e + f) = b' + d'$. On the other hand, by Lemma 3.1.1 we have $b + 0 + d = b + d = e + c + f = (e + f) + c = (b' + c' + d') + c = b' + (c + c') + d'$. Therefore $b = b'$ and $d = d'$, since $b' \in B, c + c' \in C$ and $d' \in D$. Hence $\psi(\phi(b + d)) = b + d$. Similarly, we can show $\psi(\phi(e + f)) = (e + f)$ for any $e \in E$ and $f \in F$. These maps can be restricted to give the desired isomorphism. □

Here we should highlight that this is a very simple cancellation theorem and does not constitute a proof that $B \times C \simeq B \times D \implies C \simeq D$ for zero-algebras B, C and D. Therefore the implication $B \times C \simeq B \times D$ is weaker than $B \times C = B \times D$. B. Jónsson did however show in [JT47] that $B \times C \simeq B \times D \implies C \simeq D$ holds whenever B is a finite algebra.

3.2 Central subuniverses

The study of groups had clearly shown that the properties of their direct product decomposition depends to some extent on their center. See [Spe27] for groups without operators and [Kor37] for groups with operators. Here we undertake to extend this concept to zero-algebras.

[1] For groups this was shown in [Kur32].

Definition 3.2.1. We say B is a **central subuniverse** of zero-algebra A iff B is a subuniverse and for all $b \in B$, an element $\overline{b} \in B$ exists such that

$$b + \overline{b} = 0,$$

and for all $a_1, \ldots, a_n \in A$ and all $b_1, \ldots, b_n \in B$ we have

$$F(a_1 + b_1, \ldots) \quad = \quad F(a_1, \ldots) + F(b_1, \ldots),$$

for every A-operation F of arity n. We also say element $b \in A$ is said to be **central** iff b lies in some central subuniverse. □

The next lemma shows if C is a central subuniverse of zero-algebra A, then $(C, +)$ is an abelian group.

Lemma 3.2.2. *Central elements commute with every element and associate with every two elements.*

Proof. If d is a central element then $d+a = (0+d)+(a+0) = (0+a)+(d+0) = a+d$. Hence central elements commute with every element of A. Let $t(a,d,b) = (a+d)+b$ and $r(a,d,b) = a+(d+b)$ be the ternary terms. If d is central we have $t(a,d,b) = t(a,0,b)+t(0,d,0) = (a+b)+d$ and $r(a,d,b) = r(a,0,b) + r(0,d,0) = (a+b)+d$. Hence associativity. □

Lemma 3.2.3. *The subuniverse generated by two central subuniverses is again a central subuniverse.*

Proof. Suppose P, Q are central subuniverses of A. Let R be the subuniverse generated by P and Q. Let $r \in R$. Then $r = t(\vec{p}, \vec{q})$ for some term t and $\vec{p} \in P^I$ and $\vec{q} \in Q^J$ for some index sets I and J. Since P, Q are central subuniverses, we can find $\vec{p'} \in P^I$ and $\vec{q'} \in Q^J$ such that $\vec{p} + \vec{p'} = \vec{0}$ and $\vec{q} + \vec{q'} = \vec{0}$. Let $r' = t(\vec{p'}, \vec{q'})$. By Lemma 3.2.2 and the fact that P, Q are central subuniverses we get

$$\begin{aligned} r + r' &= t(\vec{p}, \vec{q}) + t(\vec{p'}, \vec{q'}) \\ &= t(\vec{p}, \vec{0}) + t(\vec{0}, \vec{q}) + t(\vec{p'}, \vec{0}) + t(\vec{0}, \vec{q'}) \\ &= t(\vec{p}, \vec{0}) + t(\vec{p'}, \vec{0}) + t(\vec{0}, \vec{q}) + t(\vec{0}, \vec{q'}) \\ &= 0. \end{aligned}$$

Also if $r_i \in R^I$ then $r_i = t_i(\vec{p_i}, \vec{q_i})$ for some terms t_i and elements $\vec{p_i}$ and $\vec{q_i}$. Then for every fundamental operation F, using Lemma 3.2.2 and that fact that P, Q are central subuniverses we get

$$\begin{aligned} F(a_1 + r_1, \ldots) &= F(a_1 + t_1(\vec{p_1}, \vec{q_1}), \ldots) \\ &= F(a_1 + t_1(\vec{p_1}, \vec{0}) + t(\vec{0}, \vec{q_1}), \ldots) \\ &= F(a_1 + t_1(\vec{p_1}, \vec{0}), \ldots) + F(t_1(\vec{0}, \vec{q_1}), \ldots) \\ &= F(a_1, \ldots) + F(t_1(\vec{p_1}, \vec{0}), \ldots) + F(t_1(\vec{0}, \vec{q_1}), \ldots) \\ &= F(a_1, \ldots) + F(t_1(\vec{p_1}, \vec{q_1}), \ldots) \\ &= F(a_1, \ldots) + F(r_1, \ldots). \end{aligned}$$

□

Definition 3.2.4. We say $C(A)$ or C is the **center** of A if it is the union of all central subuniverses of A. This is also known as the Jónsson-Tarski center[2]. □

To get a feeling for this notion, we provide three examples.

Example 3.2.5.

- If A is a group or a ring, then C is the center in the usual sense. That is $C = \{c \in A : a + c = c + a \text{ for all } a \in A\}$ in the group case, since by Lemma 3.2.2 every element must commute and this set is clearly a central subuniverse.

  In the ring case, the center is $\{c \in A : a.c = 0 = c.a \text{ for all } a \in A\}$. From the multiplication operation we see for $b, \overline{b} \in C$ that $(0 + 0).(b + \overline{b}) = 0.0 + b.\overline{b}$ giving $b.\overline{b} = 0$. Similarly $\overline{b}.b = 0$ for $b, \overline{b} \in C$. Also $(0+b).(a+\overline{b}) = 0.a+b.\overline{b}$ and $(a+\overline{b}).(0+b) = a.0+\overline{b}.b$ for some element $a \in A$ shows $a.b = 0 = b.a$.

- If $(A, 0, +, F_1, F_2, \ldots)$ is a zero-algebra and $a_1 + a_2 = 0 \implies a_2 = 0$ for all $a_1 \in A$ then $\{0\}$ is the only central subuniverse and therefore $C = \{0\}$. Lattices are examples of structures which satisfy such a condition where $+$ will be the join operation.

- Let $(A, +)$ be an abelian group with more than one element. If a is not the identity element, define a fundamental operation F on it for every countable sequence of elements as

$$F(a_1, a_2, \ldots) = \begin{cases} 0 & \text{if the sequence } a_1, a_2, \ldots \text{ has finitely many distinct terms,} \\ a & \text{otherwise.} \end{cases}$$

  It is easily shown that subgroup C of $(A, +, F)$ is a central subuniverse if and only if C is finite. Hence the center of $(A, +, F)$ is the set of all elements of finite order. Thus, if A has infinitely many elements of a finite order, then the center of $(A, +, F)$ is not a central subuniverse. If the element a is of infinite order, then this center is not even a subuniverse.

As seen from the last example, the center of an zero-algebra need not be a subuniverse if we allow operations to be infinitary operations. The next lemma from [JT47] shows that this does not happen if all the operations are finite.

Lemma 3.2.6. *If the operations of A are finitary, then the central subuniverse is always a subuniverse.*

Proof. Suppose F is an operation of arity n and that $c_1, c_2, \ldots, c_n \in C$ the center of the algebra. Then $c_i \in B_i$ for some central subuniverses B_i. Applying Lemma 3.2.3 $n - 1$ times and we see why $F(c_1, c_2, \ldots, c_n) \in C$. □

The next lemma gives the relevance of the center to direct decompositions. As always assume f, f', g and g' are of endomorphisms on a zero-algebra A.

Lemma 3.2.7. *If $1 = f \oplus f' = g \oplus g'$ then f maps the center of A into itself and fgf' maps all of A into the center of A.*

[2]The term "center" is also used in the theory of lattices [Bir48] and rings [Jac43] with a different meaning.

Proof. Let C denote the center of A. For $b \in C$ we know there is a $\overline{b} \in C$ such that $b + \overline{b} = 0$. Thus $f(b) + f(\overline{b}) = f(b + \overline{b}) = f(0) = 0$. Now we have to show that $\alpha = \beta$ where

$$\begin{aligned} \alpha &= F(a_1 + f(b_1), \ldots), \\ \beta &= F(a_1, \ldots) + F(f(b_1), \ldots). \end{aligned}$$

for elements $a_i, b_i \in A$. This follows since $f(\alpha) = f(\beta)$ and $f'(\alpha) = f'(\beta)$. Therefore $f(b)$ is central if b is central. For the second part of the result consider the set $B = fgf'(A)$. Let

$$\begin{aligned} \gamma &= F(a_1 + fgf'(b_1), \ldots), \\ \delta &= F(a_1, \ldots) + F(fgf'(b_1), \ldots). \end{aligned}$$

Note that $f'(\gamma) = f'(\delta)$. By applying f and f' we see that

$$F(f(a_1) + f'(b_1), \ldots) = F(f(a_1), \ldots) + F(f'(b_1), \ldots).$$

Apply g and g' we see that

$$F(f(a_1) + gf'(b_1), \ldots) = F(f(a_1), \ldots) + F(gf'(b_1), \ldots).$$

Applying f and f' on both sides we obtain

$$F(f(a_1) + fgf'(b_1), \ldots) = F(f(a_1), \ldots) + F(fgf'(b_1), \ldots).$$

This means that $f(\gamma) = f(\delta)$. Hence $\gamma = \delta$. Finally, consider the set $D = B + B'$ where $B' = fg'f'(A)$. Note that D also has this property and that $fgf'(b) + fg'f'(b) = 0$. Therefore $fgf'(a)$ is central for all $a \in A$. □

3.3 More endomorphisms

In this section we collect the results from the previous two sections with a few new lemmas involving endomorphisms to show that every zero-algebra with a finite center is uniquely factorable. To achieve this we ultimately intend to compare two direct factorizations of a given zero-algebra A. Now before we do this we explore more connections between endomorphisms and inner products.

Lemma 3.3.1. *If f, f', ϕ, ψ are endomorphisms of zero-algebra A such that $1 = f \oplus f' = \phi \oplus \psi \oplus f'$ and $\phi + \psi = f$ then $f(A) = \phi(A) \times \psi(A)$.*

Proof. Assume $x \in \phi(A)$, that is $x = \phi(y)$ for some $y \in A$. Then

$$x = \phi(y) = (\phi + \psi)\phi(y) = f\phi(y) = f(x).$$

Hence $x \in f(A)$. Therefore $\phi(A) \subseteq f(A)$. In a similar fashion it follows that $\psi(A) \subseteq f(A)$. If $f(x) = a + b$, where $a \in \phi(A)$ and $b \in \psi(A)$ then $\phi(x) = \phi(f(x)) = \phi(a + b) = a$ and $\psi(b) = \psi(f(x)) = \psi(a + b) = b$. For every n-ary operation F and $a_1, a_2, \ldots, a_n \in \phi(A)$ and $b_1, b_2, \ldots, b_n \in \psi(A)$ we have

$$F(a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) = F(a_1, a_2, \ldots, a_n) + F(b_1, b_2, \ldots, b_n),$$

since

$$\begin{aligned}
\phi(F(a_1+b_1,a_2+b_2,\ldots,a_n+b_n)) &= \phi(F(a_1,a_2,\ldots,a_n)+F(b_1,b_2,\ldots,b_n)),\\
\psi(F(a_1+b_1,a_2+b_2,\ldots,a_n+b_n)) &= \psi(F(a_1,a_2,\ldots,a_n)+F(b_1,b_2,\ldots,b_n)),\\
f(F(a_1+b_1,a_2+b_2,\ldots,a_n+b_n)) &= f(F(a_1,a_2,\ldots,a_n)+F(b_1,b_2,\ldots,b_n)).
\end{aligned}$$

Together these results conclude that $f(A) = \phi(A) \times \psi(A)$. □

The following lemma was proved for groups by H. Fitting in 1934 and later by Jerzy Łoś for zero-algebras, but first we recall what it means for a map to be idempotent.

Definition 3.3.2. A function $\phi : A \longrightarrow A$ is said to be **idempotent** iff $\phi^2 = \phi$. □

Lemma 3.3.3. *If $\phi = (fgf)^n$ is idempotent then there is an endomorphism ψ of zero-algebra A such that $f = \phi + \psi$ and $1 = \phi \oplus \psi \oplus f'$.*

Proof. Put

$$q = (fg'f)[1 + (fgf) + \ldots + (fgf)^{n-1}].$$

From Lemma 3.1.5 (vi) it follows that no more parentheses are needed. From Lemma 3.1.5 (iv) se we see that q is an endomorphism of A. Next we show $q + \phi = f$. To do this, we apply Lemma 3.1.5 (v) and (vi).

$$\begin{aligned}
q+\phi &= (fg'f)[1+(fgf)+\ldots+(fgf)^{n-1}]+(fgf)^n\\
&= (fg'f)[1+(fgf)+\ldots+(fgf)^{n-2}]+[fg'f(fgf)^{n-1}+(fgf)^n]\\
&= (fg'f)[1+(fgf)+\ldots+(fgf)^{n-2}]+[(fg'f+fgf)(fgf)^{n-1}]\\
&= (fg'f)[1+(fgf)+\ldots+(fgf)^{n-2}]+(fgf)^{n-1}.
\end{aligned}$$

Inductively we may continue and obtain $q + \phi = fg'f(1) + fgf = f$. Similarly we can show $\phi + q = f$. We now take q^2 to be the desired ψ. From Lemma 3.1.5 (x) we have $\phi\psi = \psi\phi$. Next we show $\phi\psi = 0$. First note

$$\phi\psi + \phi q = \phi q^2 + \phi^2 q = \phi q^2 + \phi q\phi = \phi q(q+\phi) = \phi qf = \phi q = 0 + \phi q.$$

Since ϕq is cancellative we obtain $\phi\psi = 0$. To obtain $\psi^2 = \psi$ we first show

$$q^3 = 0 + q^3 = \phi q^2 + qq^2 = (\phi + q)q^2 = fq^2 = q^2.$$

Hence $\psi^2 = q^4 = q^3 = q^2 = \psi$. Now $\phi f' = \phi f f' = 0$. Likewise it can be shown that $\psi f' = f'\phi = f'\psi = 0$. All that remains now is to prove that $\phi + \psi = f$. First observe

$$\begin{aligned}
\phi+\phi q &= \phi^2+\phi q\\
&= \phi(\phi+q)\\
&= \phi f\\
&= \phi.
\end{aligned}$$

Therefore $\phi+\psi = \phi+q^2 = (\phi+\phi q)+q^2 = \phi+(\phi q+q^2) = (\phi^2+\phi q)+(q\phi+q^2) = (\phi+q)^2 = f^2 = f$ using (vi) from Lemma 3.1.5. □

The next lemma tells us slightly more than the previous lemma.

Lemma 3.3.4. *Let $1 = f \oplus f' = g \oplus g'$. If $n > 1$ and $(fgf)^n = f$ then an endomorphism ψ exist such that the following three equations hold:*

$$\begin{aligned} g &= (gfg)^n + \psi, \\ 1 &= (gfg)^n \oplus \psi \oplus g', \\ 1 &= (fg)^n \oplus [(fgf)^{n-1}g' + 1]f'. \end{aligned}$$

Proof. It follows immediately that $(gfg)^n$ is idempotent. So the facts about ψ follows from Lemma 3.3.3 with the roles of f and g reversed. For the final equation we note that $(fg)^n$ is idempotent since $(fgf)^n = f$. The second summand is idempotent since it is of the form $(fh+1)f'$ for some endomorphism h. Next we calculate the composition of the summands.

$$[(fgf)^{n-1}g' + 1]f' \cdot (fg)^n = 0.$$

$$\begin{aligned} (fg)^n \cdot [(fgf)^{n-1}g' + 1]f' &= [(fgf)^{n-1}g' + (fgf)^{n-1}g]f' \\ &= (fgf)^{n-1}f' \\ &= 0. \end{aligned}$$

Finally we show that the two summands really do add up to 1 by applying (vi) from Lemma 3.1.5.

$$\begin{aligned} (fg)^n + [(fgf)^{n-1}g' + 1]f' &= [(fg)^n + (fgf)^{n-1}g'f'] + f' \\ &= (fg)^{n-1}[fg + fg'f'] + f' \\ &= (fg)^{n-1}[(fgf + fgf') + fg'f'] + f' \\ &= (fg)^{n-1}[fgf + (fgf' + fg'f)] + f' \\ &= (fg)^{n-1}[fgf + 0) + f' \\ &= f + f' \\ &= 1. \end{aligned}$$

□

The next two lemmas are useful observations about the map $(fgf)^n$ and will assist us in proving our final lemma, Lemma 3.3.7.

Lemma 3.3.5. *If $(fgf)^n = f$ for some positive integer n then algebras B, C, D and D' exist such that $A = B \times D$ and $C = B \times D'$ where $1 = f \oplus f' = g \oplus g'$ for some endomorphisms f, g, g' on zero-algebra A. In fact,*

$$\begin{aligned} B &= f(A) \\ C &= g(A) \\ D &= ([(fgf)^{n-1}g' + 1]f')(A) \\ D' &= \psi(A) \end{aligned}$$

works, where ψ as the same as the one from Lemma 3.3.4.

Proof. From Lemma 3.1.4, Lemma 3.3.1 and Lemma 3.3.4 we get

$$\begin{aligned} g(A) &= (gfg)^n(A) \times \psi(A) \\ A &= (fg)(A) \times ([(fgf)^{n-1}g' + 1]f')(A). \end{aligned}$$

So the result will follow if we can show $f(A) = (fg)(A) = (fg)^n(A) = (gfg)^n(A)$. Note $f(A) \supseteq (fg)(A) \supseteq (fg)^n(A) \supseteq g((fg)^n(A)) = (gfg)^n(A)$, using the fact $A \supseteq h(A)$ for any endomorphism h on A. Let $\phi : (gfg)^n(A) \longrightarrow (fg)(A)$ such that $\phi((gfg)^n(x)) = (fg)(x)$. Note $(gfg)^n(x) = (gfg)^n(x') \iff (fg)(x) = f(gfg)^n(x) = f(gf)^n(x') = (fg)(x')$. Thus ϕ is a well-defined bijective homomorphism. Also $fg(A) \subseteq f(A) = (fgf)^n(A) = fg(fgf)^{n-1}(A) \subseteq fg(A)$. Hence $fg(A) = f(A)$. □

Lemma 3.3.6. *For all positive integers n, we have $(fgf)^n(A) \cup (fg'f)^n(A) \neq \{0\}$ if f is a non-zero map where $1 = f \oplus f' = g \oplus g'$ for some endomorphisms f, f', g, g' on zero-algebra A.*

Proof. We first treat the case $n = 1$. Note $fgf(a) + fg'f(a) = f(a)$. Hence the result holds for this case. Let n be the smallest integer for which $(fgf)^n(A) \cup (fg'f)^n(A) = \{0\}$. Using Lemma 3.1.5 part (x) we have

$$\begin{aligned}
(fgf)^{n-1}(x) &= (fgf)^{n-1}(fgf(x) + fg'f(x)) \\
&= (fgf)^n(x) + (fgf)^{n-1}(fg'f)(x) \\
&= (fgf)^{n-1}(fg'f(x)) \\
&= (fgf)^{n-1}(fg'f)(fgf(x) + fg'f(x)) \\
&= (fgf)^{n-1}(fg'f)^2(x) \\
&= \dots \\
&= (fgf)^{n-1}(fg'f)^n(x) \\
&= 0.
\end{aligned}$$

In a similar fashion we obtain $(fg'f)^{n-1}(x) = 0$. This contradicts the fact that n is the smallest integer such that $(fgf)^n(A) = (fg'f)^n(A) = \{0\}$. Therefore no such n exists, completing the proof. □

Lemma 3.3.7. *If A is a zero-algebra with a finite center and $A = B \times B' = C \times C'$ for some directly indecomposable algebra B then algebras D and D' exist such that $A = B \times D$ and either $C = B \times D'$ or $C' = B \times D'$.*

Proof. As always, let $1 = f \oplus f' = g \oplus g'$ where $f(A) = B, f'(A) = B', g(A) = C$ and $g'(A) = C'$. For $m \geq 3$, let

$$h_m = (fgf) + \ldots + (fgf)^{m-2}.$$

Using Lemma 3.2.7, it is a map of the center into itself. Since the center is finite, we must have $h_m = h_{m+k}$ (as maps defined on the center) for some m and $k \geq 1$. Since the range of gfg' is contained in the center, we have

$$h_m gfg'f = h_{m+k} gfg'f.$$

Observe

$$\begin{aligned}
h_m gfg'f + (fgf)^m &= h_m gfg'f + (fgf)^m(g' + g)f \\
&= h_m gfg'f + ((fgf)^{m-1} gfg'f + (fgf)^{m+1}) \\
&= (h_m + (fgf)^{m-1})gfg'f + (fgf)^{m+1} \\
&= h_{m+1} gfg'f + (fgf)^{m+1}.
\end{aligned}$$

Repeating this calculation k times, we obtain $h_m gfg'f + (fgf)^m = h_{m+k} gfg'f + (fgf)^{m+k}$. Cancelling off we obtain $(fgf)^m = (fgf)^{m+k}$ as maps on A. A similar calculations yields

$(fg'f)^r = (fg'f)^{r+s}$ for some r and $s \geq 1$. Choosing n larger than both m and r and divisible by k and s we obviously have $(fgf)^{2n} = (fgf)^n$ and $(fg'f)^{2n} = (fg'f)^n$.

Thus by Lemma 3.3.6 we may assume $(fgf)^n(A) \neq \{0\}$. Since $(fgf)^n$ is idempotent we have by Lemma 3.3.3 that $1 = (fgf)^n \oplus \psi \oplus f'$ for some ψ with $(fgf)^n + \psi = f$. Applying Lemma 3.3.1 we get $f(A) = (fgf)^n(A) \times \psi(A)$. Knowing $f(A)$ is directly indecomposable and $(fgf)^n(A) \neq \{0\}$ we must have $f(A) = (fgf)^n(A)$.

We proceed to claim $(fgf)^n = f$. Choose $y \in A$. Now $f(y) = (fgf)^n(x)$ for some x. Then $(fgf)^n(y) = (fgf)^n(f(y)) = (fgf)^n(fgf)^n(x) = (fgf)^n(x) = f(y)$ justifying our claim. Lemma 3.3.5 concludes the proof. □

Jonssón-Tarski Theorem. *Every zero-algebra with a finite center has an unique factorization, provided that each of its direct factors is decomposable into a finite product of indecomposable algebras.*

Proof. Suppose A is a zero-algebra with a finite center such that

$$A \simeq \prod_{i=1}^{n} A_i' \simeq \prod_{j=1}^{m} B_j',$$

for some directly indecomposable algebras A_i', B_j' and $n \leq m$. We prove this theorem by induction on n by showing $m = n$ and after renumbering $A_i' \simeq B_j'$. The theorem is clearly true for $n = 1$, that is when A is a directly indecomposable algebra. Now we continue by supposing it holds for all smaller values of n. By Lemma 3.1.1 we know there are subalgebras A_i, B_j of A with $A_i \simeq A_i'$ (for each i),$B_j \simeq B_j'$ (for each j) such that

$$A = \prod_{i=1}^{n} A_i = \prod_{j=1}^{m} B_j.$$

Apply Lemma 3.3.7 with $B = A_1, B' = \prod_{i=2}^{n} A_i, C = B_1$ and $C' = \prod_{j=2}^{m} B_j$. Thus $A = D \times B$ and either $C = B \times D'$ or $C' = B \times D'$ for some subalgebras D and D'. In both cases we have $D \simeq B'$ by Theorem 3.1.6.

Case I : If $C = B \times D'$ then $D' = 1$ making $B_1 = C = B$, since C is directly indecomposable. If B were trivial, then it contradicts the fact that B is directly indecomposable. Hence $A_1 \simeq B_1$. Also $A = B \times D = C \times D = C \times C'$. By Theorem 3.1.6 it follows that $C' \simeq D \simeq B'$. The induction hypothesis gives $m - 1 = n - 1$ and a renumbering that completes this case.

Case II : If $C' = B \times D'$ then $A = B \times B' = C \times C' = C \times B \times D'$. By Theorem 3.1.6 it follows that $B' \simeq C \times D'$. Suppose $D' = \prod_{k=1}^{\ell} D_\ell$ for some directly indecomposable algebras D_ℓ. As B' and C' have $m - 1, n - 1$ indecomposable factors respectively, it follows by induction that $\{A_2, \ldots, A_n\}$ is an rearrangement of $\{B_1, D_1, \ldots, D_\ell\}$ and $\{B_2, \ldots, B_n\}$ is an rerrangement of $\{A_1, D_1, \ldots, D_\ell\}$ of zero-algebras up to isomorphism and $n = m$. □

Corollary 3.3.8. *Every finite zero-algebra is uniquely factorable.*

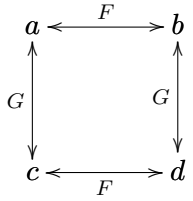
The Jónsson-Tarski Theorem explains why every group, ring or lattice with a finite center has the unique factorization property. In particular it proves that every finite group, ring or lattice is uniquely factorable. This theorem also allows us to modify the type of a structure to

produce more examples of algebras that is unique factorable.

It should be observed that Theorem 3.3 and Corollary 3.3.8 is still valid if a binary term operation + (that is definable in terms of the basic operations) exists such that $\{0\}$ is an one-element subuniverse and all elements x obey $x + 0 = x = 0 + x$.

The approach in this chapter is more modern than the original proof of Jónsson found in [JT47]. We utilised ideas of inner products and endomorphisms. These techniques seem to be intrinsic to zero-algebras and can not easily be applied to other structures as illustrated with the next example.

Example 3.3.9. Suppose $A = \{a, b, c, d\}$ is an algebra with 2 unary functions F, G as depicted below.



Although this algebra is not directly indecomposable, the only endomorphism on it is the identity morphism. This example illustrates why the techniques in this section are not useful in general.

3.4 Algebras almost without zero-divisors

Finiteness seems to be an important criteria for most of these results. This is no surprise, because for every finite structure we can guarantee at least one direct product decomposition into directly indecomposable algebras, but not for infinite structures. This section explores Ivan Chajda's [Cha76]unique factorization result which bears some resemblance to zero-algebras but has no finiteness restrictions.

In this section we concentrate on algebras almost without zero-divisors, that is a zero algebra with an extra operation which allows us to produce Ivan Chajda's unique factorization result [Cha76]. Theorem 3.4.7 will play a major role for producing this factorization result, but first some new concepts.

Definition 3.4.1. Algebra $(A, 0, +, f)$ is said to be **almost without zero-divisors** if it has a nullary element 0 and two operations + and f which has arity 2 and n respectively such that

(i) $a + 0 = a = 0 + a$ for all $a \in A$

(ii) for all $a_1, \ldots, a_n \in A$

$$f(a_1, \ldots, a_n) = 0 \text{ iff } a_j = 0 \text{ for some } j \in \{1, 2, \ldots, n\}.$$

□

Example 3.4.2. An interesting example of finite algebras almost without zero-divisors are $(\mathbb{Z}_p, f, h_m, g_n)$ where $f(a, b) = a + b, h_m(a, b) = a + b + m$ and $g_n(a_1, \ldots, a_n) = \prod_{i=1}^{n} a_i$ for some ring $\mathbb{Z}_p$ where p is a prime number. If $m \neq 0$ then these algebras almost without zero-divisors are not examples of zero-algebras.

Definition 3.4.3. Let pr_i denote the projection of $\prod_{i\in I} A_i$ onto the direct factor A_i. □

Lemma 3.4.4. *An algebraic structure almost without zero-divisors is directly indecomposable over the class of structures almost without zero-divisors.*

Proof. Suppose $A = \prod_{i\in I} A_i$ with $|I| \geq 2$ and $|A_i| > 1$ for all i. Select $i_1, i_2 \in I$ where $i_1 \neq i_2$. Choose $a \in A$ such that $pr_k(a) = 0$ if $k \in I - \{i_1\}$ and $pr_{i_1}(a) \neq 0$. Choose $a' \in A$ such that $pr_k(a') = 0$ if $k \in I - \{i_2\}$ and $pr_{i_2}(a') \neq 0$. Thus both a and a' are non-zero with $f(a, \ldots, a, a') = 0$. This contradiction completes the proof. □

Definition 3.4.5. Let $\{A_i : i \in I\}$ be a collection of structures without zero-divisors of the same type and $A = \prod_{i\in I} A_i$ for some algebra A. Let $\overline{A_i}$ denote the structure $\prod_{j\in I} A'_j$ where $A'_i = A_i$ and $A'_j = \{0\}$ whenever $j \in I - i$. □

Lemma 3.4.6. *Let $\{A_i : i \in I\}$ be similar algebraic structures almost without zero-divisors and $A = \prod_{i\in I} A_i$.*

(i) Suppose $a_1, \ldots, a_n \in A$. If for all $i \in I$ there is at least one $j \in \{1, 2 \ldots, n\}$ such that $pr_i(a_j) = 0$ then $f(a_1, \ldots, a_n) = 0$.

(ii) Suppose $a, a' \in A$ with either $pr_i(a) = 0$ or $pr_i(a') = 0$ for each $i \in I$. Then $a + b = b + a$ and $pr_i(a + b) = pr_i(a)$ or $pr_i(a + b) = pr_i(b)$ for each $i \in I$.

(iii) $\overline{A_i}$ for each $i \in I$ are also algebraic structures almost without zero-divisors of the same type.

Proof. (i) For each $i \in I$ we have

$$\begin{aligned} pr_i(f(a_1, \ldots, a_n)) &= f(pr_i(a_1), \ldots, pr_i(a_n)) \\ &= f(pr_i(a_1), \ldots, pr_i(a_{j-1}), 0, pr_i(a_{j+1}), \ldots, pr_i(a_n)) \\ &= 0. \end{aligned}$$

Hence $f(a_1, \ldots, a_n) = 0$. For (ii) note for each $i \in I$ that $pr_i(a)+pr_i(a') = pr_i(a')+pr_i(a)$. Thus $pr_i(a+a') = pr_i(a'+a)$ for each $i \in I$ and hence $a+a' = a'+a$. It is evident $pr_i(a+a') = pr_i(a)$ or $pr_i(a')$ from the fact $pr_i(a) = 0$ or $pr_i(a') = 0$. The last claim is obvious. □

Theorem 3.4.7. *Suppose $(A_i)_{i\in I}$ and $(B_j)_{j\in J}$ are similar algebraic structures almost without zero-divisors. If ϕ is an isomorphism from $\prod_{i\in I} A_i$ onto $\prod_{j\in J} B_j$ then an injection $\sigma : J \longrightarrow I$ exists such that*

$$\overline{B_j} \subseteq \phi(\overline{A_{\sigma(j)}}).$$

Proof. Fix some $j \in J$ and choose $b \in \overline{B_j} - \{0\}$. Put $b_j = pr_j(b)$. Then $b_j \neq 0$ and $pr_k(b) = 0$ for $k \neq j$. Realising ϕ is an isomorphism we have an unique element $a \in \prod_{i\in I} A_i = A$ such that $\phi(a) = b$. Hence for some $\sigma(j) \in I$ we have $pr_{\sigma(j)}(a) \neq 0$. Put $a_{\sigma(j)} = pr_{\sigma(j)}(a)$. Let c be an element of A such that $pr_i(c) = pr_i(a)$ for all $i \neq \sigma(j)$ and $pr_{\sigma(j)}(c) = 0$. By Lemma 3.4.6 we get $\overline{a_{\sigma(j)}} + c = a$.

Lemma 3.4.6 gives $f(\overline{a_{\sigma(j)}}, c, \ldots, c) = 0$. Therefore

$$0 = \phi(0) = \phi(f(\overline{a_{\sigma(j)}}, c, \ldots, c)) = f(\phi(\overline{a_{\sigma(j)}}), \phi(c), \ldots, \phi(c)).$$

Thus $0 = pr_j(0) = f(pr_j(\phi(\overline{a_{\sigma(j)}})), pr_j(\phi(c)), \ldots, pr_j(\phi(c))$. Hence $pr_j(\phi(\overline{a_{\sigma(j)}})) = 0$ or $pr_j(\phi(c)) = 0$ for each $j \in J$.

If $\phi(\overline{a_{\sigma(j)}}) \notin \overline{B_j}$ then for some $j' \neq j$ we have $pr_{j'}(\phi(\overline{a_{\sigma(j)}})) \neq 0$ which implies $pr_{j'}(\phi(c)) = 0$. So $b = \phi(a) = \phi(\overline{a_{\sigma(j)}} + c) = \phi(\overline{a_{\sigma(j)}}) + \phi(c)$ but $0 = pr_{j'}(b) = pr_{j'}(\phi(\overline{a_{\sigma(j)}})) + pr_{j'}(\phi(c)) = pr_{j'}(\phi(\overline{a_{\sigma(j)}})) \neq 0$. This is a contradiction. Assuming $\phi(c) \notin \overline{B_j}$ we can reach a contradiction with a similar argument. Thus we must have $\phi(\overline{a_{\sigma(j)}}) \in \overline{B_j}$ and $\phi(c) \in \overline{B_j}$.

Therefore $pr_{j'}(\phi(\overline{a_{\sigma(j)}})) = 0 = pr_{j'}(\phi(c))$ if $j' \neq j$. Earlier we showed either $pr_j(\phi(\overline{a_{\sigma(j)}})) = 0$ or $pr_j(\phi(c)) = 0$. Thus either $\phi(\overline{a_{\sigma(j)}}) = 0$ or $\phi(c) = 0$. Suppose $\phi(c) \neq 0$ then $\phi(\overline{a_{\sigma(j)}}) = 0$. Then $b = \phi(a) = \phi(\overline{a_{\sigma(j)}} + c) = \phi(c)$. Hence $a = c$ as ϕ is an isomorphism. Therefore $0 = pr_{\sigma(j)}(c)$ and $pr_{\sigma(j)}(a) = a_{\sigma(j)} \neq 0$. This contradiction yields $\phi(c) = 0$. So $\phi(a) = \phi(\overline{a_{\sigma(j)}}) + \phi(c) = \phi(\overline{a_{\sigma(j)}})$ which implies $a = \overline{a_{\sigma(j)}}$. Thus far we have showed for each $b \in \overline{B_j} - \{0\}$ there is an index $\sigma(j) \in I$ and an element $\overline{a_{\sigma(j)}} \in \overline{A_{\sigma(j)}}$ with $\phi(\overline{a_{\sigma(j)}}) = b$.

Next we will show the index $\sigma(j)$ is the same for all $b \in \overline{B_j}$. Let $b_1, b_2 \in \overline{B_j} - \{0\}$. In the previous paragraph there is $i_1, i_2 \in I$ and elements $\overline{a}_{i_1} \in \overline{A_{i_1}}$ and $\overline{a}_{i_2} \in \overline{A_{i_2}}$ such that $\phi(\overline{a}_{i_1}) = b_1$ and $\phi(\overline{a}_{i_2}) = b_2$. Clearly $\overline{a}_{i_1} \neq 0 \neq \overline{a}_{i_2}$. If $i_1 \neq i_2$ then by Lemma 3.4.6 we have

$$f(b_1, b_2, \ldots, b_2) = \phi(f(\overline{a}_{i_1}, \overline{a}_{i_2}, \ldots, \overline{a}_{i_2})) = \phi(0) = 0.$$

Lemma 3.4.6 part (iii) gives $f(b_1, b_2, \ldots, b_2) \neq 0$ which is a contradiction. Therefore $i_1 = i_2$. Hence there is an unique index $\sigma(j) \in I$ such that for each $b \in \overline{B_j} - \{0\}$ there is $a \in \overline{A_{\sigma(j)}}$ satisfying $\phi(a) = b$. If $b = 0$, let $a = 0$ as $\phi(a) = b$ and $0 \in \overline{A_{\sigma(j)}}$. Thus $\phi(\overline{A_{\sigma(j)}}) \supseteq \overline{B_j}$. As $j \in J$ was arbitrary, this fact is true for every element in the set J.

Now we show this map is unique. Suppose $\overline{B_j} \subseteq \phi(\overline{A_{i_1}})$ and $\overline{B_j} \subseteq \phi(\overline{A_{i_2}})$ for some $i_1, i_2 \in I$ and $j \in J$. Choose $b \in \overline{B_j} - \{0\}$. Then $b = \phi(a_{i_1}) = \phi(a_{i_2})$ where $a_{i_1} \in \overline{A_{i_1}}$ and $a_{i_2} \in \overline{A_{i_2}}$. This is impossible if $i_1 \neq i_2$. Hence there is only one map from $\sigma : J \longrightarrow\!\!\!\!\!\rightarrow I$ with the desired properties.

It only remains to show the map is injective. To do this suppose $i \in I$ and $j_1, j_2 \in J$ such that $\overline{B_{j_1}} \subseteq \phi(\overline{A_i}), \overline{B_{j_2}} \subseteq \phi(\overline{A_i})$ and $j_1 \neq j_2$. Select $b_{j_1} \in \overline{B_{j_1}} - \{0\}$ and $b_{j_2} \in \overline{B_{j_2}} - \{0\}$. Then there exist some $a_1, a_2 \in \overline{A_i}$ such that $\phi(a_1) = b_{j_1}$ and $\phi(a_2) = b_{j_2}$. Note $a_1 \neq 0 \neq a_2$. By Lemma 3.4.6 (iii) we know $\overline{A_i}$ is almost without zero-divisors. Thus $f(a_1, a_2, \ldots, a_2) \neq 0$, but $0 = f(b_{i_1}, b_{i_2}, \ldots, b_{i_2}) = \phi(f(a_1, a_2, \ldots, a_2)) \neq \phi(0) = 0$ by Lemma 3.4.6 (i). This contradiction completes the proof. □

Now we are ready to prove I. Chajda's [Cha76] result. It should be highlighted that this result do not require $\{0\}$ to be a subuniverse and is applicable to the algebras in Example 3.4.2. We can even take the product of a finite collection of them and form a larger algebra which still has the UFP. However Theorem 3.3 can not be used directly to prove this fact and thus a new method was found to produce structures with the UFP.

Theorem 3.4.8. *If an algebraic structure is directly decomposable into structures almost without zero-divisors, then the factorization over the class of structures almost without zero-divisors is unique.*

Proof. Suppose $A \simeq \prod_{i \in I} A_i \simeq \prod_{j \in J} B_j$ where each A_i and B_j are algebraic structures almost without zero-divisors. By Lemma 3.4.4 it follows each A_i and B_j are directly indecomposable. Suppose ϕ is an isomorphism from $\prod_{i \in I} A_i$ onto $\prod_{j \in J} B_j$. By Theorem 3.4.7 we know an injective

map $\sigma : J \longrightarrow I$ exist such that for each $j \in J$ we have

$$\phi(\overline{A_{\sigma(j)}}) \supseteq \overline{B_j},$$

and an injective map $\tau : I \longrightarrow J$ exist such that for each $i \in I$ we have

$$\phi^{-1}(\overline{B_{\sigma(j)}}) \supseteq \overline{A_i}.$$

Note $\overline{A_i} \cap \overline{A_{i'}} = \{0\}$ if $i \neq i'$. Hence $\sigma(\tau(i)) = i$. Similarly we can show $\tau(\sigma(j)) = j$. Thus $\phi(\overline{A_{\sigma(j)}}) = \overline{B_j}$ and $\phi(\overline{B_{\tau(i)}}) = \overline{A_i}$. Hence τ and σ are bijections proving that $A_i \simeq B_{\tau(i)}$ for each $i \in I$. □

Chapter 4

Refinement properties

Having had some success with finite structures, we now continue our investigation of the unique factorization property aka UFP to study infinite algebras. Mathematicians quickly realised the UFP notion was insufficient to study these larger structures and they resolved this problem by introducing the new ideas of *refinement*, *strict refinement* and the *intermediate refinement property*. This chapter studies and connects these concepts. By building on previous techniques we proceed to show that every finite congruence distributive algebra is uniquely factorable. On our journey we also encounter other unique factorization results.

4.1 Decomposition functions

We commence this section by giving the precise definition of the term *refinement* which is a natural extension of the unique factorization property for infinite algebras. We also introduce the stronger concept of strict refinement. These concepts were introduced and brought to prominence when C. Chang [Cha61, Cha67], B. Jónsson, A. Tarski [CJT] and R. Mckenzie [Mck71] decided to tackle infinite algebras.

Definition 4.1.1. Algebra A has the **refinement property** for direct factorization iff if whenever

$$A \simeq \prod_{i\in I} B_i \simeq \prod_{j\in J} C_j,$$

then algebras D_{ij} exist such that $B_i \simeq \prod_{j\in J} D_{ij}$ and $C_j \simeq \prod_{i\in I} D_{ij}$. □

Definition 4.1.2. Algebra A has the **strict refinement property** whenever we have

$$0 = \prod_{i\in I} \beta_i = \prod_{j\in J} \gamma_j$$

in $Con\, A$, then congruences δ_{ij} exist such that $\beta_i = \prod_{j\in J} \delta_{ij}$ and $\gamma_j = \prod_{i\in I} \delta_{ij}$. □

Note that a finite structure is uniquely factorizable into directly indecomposable algebras if and only if it has the refinement property. The Klein four-group, the smallest non-cyclic group, illustrates that even for finite structures the refinement property does not necessarily imply the strict refinement property, however the converse is always true, as we will see shortly.

Theorem 4.1.3. *If algebra A has the strict refinement property then*
(i) A has the refinement property.
(ii) If $0 = \prod_{i\in I} \alpha_i = \prod_{j\in J} \beta_j$ where each α_i, β_j are directly indecomposable congruences then the sets $\{\alpha_i : i \in I\}$ and $\{\beta_j : j \in J\}$ are identical.
(iii) If $0 = \alpha \times \alpha'$ then A/α has the strict refinement property.

Proof. Assume for directly indecomposable algebras A_i, B_j we have

$$A \simeq \prod_{i\in I} A_i \simeq \prod_{j\in J} B_j.$$

Thus congruences α_i, β_j exist such that $A/\alpha_i \simeq A_i$ for each $i \in I$, $B/\beta_j \simeq B_j$ for each $j \in J$ and

$$0 = \prod_{i\in I} \alpha_i = \prod_{j\in J} \beta_j.$$

By the strict refinement property we can find congruences δ_{ij} such that $\alpha_i = \prod_{j\in J} \delta_{ij}$ and $\beta_j = \prod_{i\in I} \delta_{ij}$. Hence

$$A_i \simeq \prod_{j\in J} A/\delta_{ij} \text{ and } B_j \simeq \prod_{i\in I} B/\delta_{ij}.$$

The second and third part of the result follows immediately from the definition of strict refinement. □

Lemma 4.1.4. *Let α be a congruence on algebra A such that for all $i \in I$ and all $j \in J$, β_i, γ_j and δ_{ij} are congruences on A such that*

$$\alpha = \prod_{i\in I} \beta_i = \prod_{j\in J} \gamma_j,$$

and for all $i \in I$ and $j \in J$ we have

$$\beta_i = \prod_{j\in J} \delta_{ij} \text{ and } \gamma_j = \prod_{i\in I} \delta_{ij},$$

then $\delta_{ij} = \beta_i \circ \gamma_j = \gamma_j \circ \beta_i$ for all $i \in I$ and $j \in J$.

Proof. Fix $p \in I$ and $q \in J$. Let $M = \{(p, j) : j \in J\}$ and $N = \{(i, q) : i \in I\}$. Then $M \cap N = \{(p, q)\}$. Therefore

$$\prod_{(i,j)\in A\cup B} \delta_{ij}$$

exists by Lemma 1.3.1, since $\alpha = \prod_{i\in I, j\in J} \delta_{ij}$.

If $(x, y) \in \prod_{(i,j)\in M\cap N} \delta_{ij}$, then from above we know $z \in M$ exists such that $(x, z) \in \delta_{ij}$ for all $(i, j) \in M$ and $(y, z) \in \delta_{ij}$ for all $(i, j) \in N$. Thus $\prod_{(i,j)\in M\cap N} \delta_{ij} \subseteq \prod_{(i,j)\in M} \delta_{ij} \circ \prod_{(i,j)\in N} \delta_{ij}$.

Also note $\prod_{(i,j)\in M} \delta_{ij} \subseteq \prod_{(i,j)\in M\cap N} \delta_{ij}$ and $\prod_{(i,j)\in N} \delta_{ij} \subseteq \prod_{(i,j)\in M\cap N} \delta_{ij}$. Thus $\prod_{(i,j)\in M} \delta_{ij} \circ \prod_{(i,j)\in N} \delta_{ij} \subseteq \prod_{(i,j)\in M\cap N} \delta_{ij}$. Therefore

$$\begin{aligned} \beta_p \circ \gamma_q &= \prod_{(i,j)\in M} \delta_{ij} \circ \prod_{(i,j)\in N} \delta_{ij} \\ &= \prod_{(i,j)\in M\cap N} \delta_{ij} \\ &= \delta_{pq}. \end{aligned}$$

□

To further our study of refinement properties we take a brief detour into decomposition functions. They will serve roughly the same role as the endomorphisms associated with a direct decomposition of an algebra with a zero element as investigated in the previous chapter.

Definition 4.1.5. A **decomposition function** f on algebra A is a homomorphism $f : A^2 \longrightarrow A$ such that $f(x,x) = x$ and

$$f(f(x,y),z) = f(x,z) = f(x,f(y,z)).$$

If f is a decomposition function we define $f_v(x)$ to be $f(x,v)$ and $f'_u(y)$ to be $f(u,y)$. Suppose α and α' are congruences such that $\alpha \times \alpha' = 0$. Define the function $f_{\alpha,\alpha'} : A^2 \longrightarrow A$ such that $f_{\alpha,\alpha'}(x,y) = w$ where w is the unique element such that $(x,w) \in \alpha$ and $(w,y) \in \alpha'$. □

We will shortly see that decomposition functions are easier to manipulate then the algebraic structures themselves. Using decomposition functions we can capture direct product factorization properties as demonstrated with the example below.

Example 4.1.6. Suppose ϕ is an isomorphism from A to $B \times C$. For all $x, y \in A$ with $\phi(x) = (b_1, c_1)$ and $\phi(y) = (b_2, c_2)$, let $f(x,y) = \phi^{-1}(b_1, c_2)$. A simple calculation shows that f is a decomposition function with $\phi(A) = B \times C$. □

Obviously if f is a decomposition function and we put $g(x,y)$ to be $f(y,x)$ then g is also a decomposition function. The following lemma demonstrates the importance of decomposition functions.

Lemma 4.1.7. *If f is a decomposition function then $ker\, f_v$ and $ker\, f'_u$ are congruences on A that are independent of the choice of u and v. The correspondences*

$$\begin{aligned} (\alpha, \alpha') &\mapsto f_{\alpha,\alpha'} \\ f &\mapsto (ker\, f_v, ker\, f'_u) \end{aligned}$$

gives a bijection and its inverse between the set of pairs $(\alpha, \alpha') \in Con\, A^2$ with $\alpha \times \alpha' = 0$ and the set of decomposition functions on A.

Proof. We first show that the correspondence is independent on the choice of u and v. Let $v, v' \in A$. If $(x,y) \in ker\, f_v \implies f_v(x) = f_v(y) \implies f(x,v) = f(y,v) \implies f(f(x,v),v') = f(f(y,v),v') \implies f(x,v') = f(y,v') \implies (x,y) \in ker\, f_{v'}$. Thus $ker\, f_v = ker\, f_{v'}$. Similarly, it can be shown that $ker\, f'_u = ker\, f'_{u'}$ for all $u, u' \in A$.

Before we show the correspondence is a bijection, we show that the maps have the correct co-domains. It is clear $ker\, f_v$ is an equivalence relation. Say F is a n-ary operation and $(x_i, y_i) \in ker\, f_{F(v,v,\ldots,v)} = ker\, f_v$ for $1 \leq i \leq n$. The following calculation establishes that $ker\, f_v$ is a congruence.

$$\begin{aligned} f(F(x_1,x_2,\ldots,x_n),F(v,v,\ldots,v)) &= F(f(x_1,v),\ldots,f(x_n,v)) \\ &= F(f(y_1,v),\ldots,f(y_n,v)) \\ &= f(F(y_1,\ldots,y_n),F(v,\ldots,v)). \end{aligned}$$

Next we show $f_{\alpha,\alpha'}$ is a decomposition function. Clearly $f_{\alpha,\alpha'}(x,x) = x$. Suppose $f_{\alpha,\alpha'}(x,y) = w \implies (x,w) \in \alpha, (w,y) \in \alpha'$. If $f_{\alpha,\alpha'}(w,z) = t \implies (w,t) \in \alpha$ and $(t,z) \in \alpha'$. By transitivity we have $(x,t) \in \alpha$ and hence $f_{\alpha,\alpha'}(x,z) = t$. Thus $f_{\alpha,\alpha'}(f_{\alpha,\alpha'}(x,y),z) = f_{\alpha,\alpha'}(x,z)$. Similarly we can show $f_{\alpha,\alpha'}(x, f_{\alpha,\alpha'}(y,z)) = f_{\alpha,\alpha'}(x,z)$.

Let f be shorthand for $f_{\alpha,\alpha'}$. Suppose F is a n-ary operation and $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n) \in A^2$. Suppose $f(x_i, y_i) = z_i$ for each i. Thus $(x_i, z_i) \in \alpha$ and $(z_i, y_i) \in \alpha'$ for each i. Therefore $(F(x_1, \ldots, x_n), F(z_1, \ldots, z_n)) \in \alpha$ and $(F(z_1, \ldots, z_n), F(y_1, \ldots, y_n)) \in \alpha'$. Thus

$$\begin{aligned} F(f(x_1, y_1), \ldots, f(x_n, y_n)) &= F(z_1, \ldots, z_n) \\ &= f(F(x_1, \ldots, x_n), F(y_1, \ldots, y_n)). \end{aligned}$$

Suppose f is a decomposition function of algebra A. Let $(x, y) \in ker\, f_v \cap ker\, f'_v$. Then $(x, y) \in ker\, f_v$ and $(x, y) \in ker\, f'_v$. The next calculation shows that $ker\, f_v \cap ker\, f'_v = 0$.

$$\begin{aligned} x &= f(x, f(v, x)) \\ &= f(x, f(v, y)) \\ &= f(x, y) \\ &= f(f(x, v), y) \\ &= f(f(y, v), y) \\ &= f(y, y) \\ &= y. \end{aligned}$$

Let $(a, b) \in A^2$. Note $(a, f(a, b)) \in ker\, f_v$ since $f(f(a, b), v) = f(a, v)$ and $(b, f(a, b)) \in ker\, f'_v$ since $f(v, f(a, b)) = f(v, b)$. Hence $ker\, f_v \circ ker\, f'_v = 1$. From the previous paragraph it follows that $ker\, f_v \times ker\, f'_v = 0$.

Suppose $(\alpha, \alpha') \mapsto f_{\alpha,\alpha'}$, $(\beta, \beta') \mapsto f_{\beta,\beta'}$ and $f_{\alpha,\alpha'} = f_{\beta,\beta'}$. Note $(x, y) \in \alpha \iff f_{\alpha,\alpha'}(x, y) = y \iff f_{\beta,\beta'}(x, y) = y \iff (x, y) \in \beta$. Hence $\alpha = \beta$. Similarly, it follows that $\alpha' = \beta'$. Therefore the first map is injective. Suppose now, $ker\, f_v = ker\, g_v$ and $ker\, f'_u = ker\, g'_u$. If $(x, z) \in ker\, f_v = ker\, g_v$ and $(z, y) = ker\, f'_u = ker\, g'_u$, then $f(x, y) = z = g(x, y)$, by the independence of v and u. So the second map is also injective. Thus by the Cantor-Schröder-Bernstein Theorem it follows that the correspondence is indeed bijective.

Finally, noting $(a, b) \in \alpha \iff f_{\alpha,\alpha'}(a, b) = f_{\alpha,\alpha'}(b, b) \iff \langle (a, b), (b, b) \rangle \in \ker f_{\alpha,\alpha'}$ and $(a, b) \in \alpha' \iff f_{\alpha,\alpha'}(a, b) = f_{\alpha,\alpha'}(a, a) \iff \langle (a, b), (a, a) \rangle \in \ker f'_{\alpha,\alpha'}$ completes the correspondence. □

If A is an algebra with a zero and $u = v = 0$ then f_v, f'_u are f, f' as studied in the previous chapter. If A has an one-element subalgebra $\{e\}$ then f_e, f'_e are endomorphisms on A, but in general f_v, f'_u may not be. We list some elementary properties of decomposition functions without proof.

Lemma 4.1.8. *If f is a decomposition function and $a, b, c, d, e \in A$ then the following statements all hold:*

(i) $f_a(a) = a$.

(ii) $f_a f_b(c) = f_a(c)$.

(iii) $f'_a f_b(c) = f'_a(b)$.

(iv) $f_a(c) = c$ *iff* $f'_a(c) = a$.

(v) $f_a(c) = f_b(d)$ *implies* $f_e(c) = f_e(d)$.

(vi) $f_a(c) = f_a(d)$ *iff* $f_b(c) = f_b(d)$.

(vii) $f_a(c) = f_a(d)$ *and* $f'_a(c) = f'_a(d)$ *iff* $c = d$.

Before we continue to show that the strict refinement property is equivalent to the assertion that factor congruences form a Boolean sublattice on $Con\, A$, we quickly prove a result that will assist in this task.

Lemma 4.1.9. *If* $0 = \prod_{i\in I} \alpha_i$ *then the map*

$$K \mapsto \prod_{i\in I-K} \alpha_i$$

is a $(0,1)$*-morphism from the Boolean lattice of subsets of* I *into* $Con\, A$.

Proof. The hard part is to show the map preserves join and meet, that is for any subsets A and B of I that the following are true:

$$\begin{aligned}\prod_{I-A\cap B} \alpha_i &= \prod_{I-A} \alpha_i \wedge \prod_{I-B} \alpha_i,\\ \prod_{I-A\cup B} \alpha_i &= \prod_{I-A} \alpha_i \vee \prod_{I-B} \alpha_i.\end{aligned}$$

Using

$$\begin{aligned}\alpha &= \prod_{I-A\cup B} \alpha_i,\\ \beta &= \prod_{B-B\cap A} \alpha_i,\\ \gamma &= \prod_{A-A\cap B} \alpha_i,\\ \delta &= \prod_{A\cap B} \alpha_i,\end{aligned}$$

it turns out that it is enough to show that whenever $0 = \alpha \times \beta \times \gamma \times \delta$, then

$$(\alpha \times \beta) \wedge (\alpha \times \gamma) = \alpha \times \beta \times \gamma, \tag{4.1}$$

$$(\alpha \times \beta) \vee (\alpha \times \gamma) = \alpha. \tag{4.2}$$

Equation (4.1) is obvious, because $r \times s = r \wedge s$ and clearly $(\alpha \times \beta) \cup (\alpha \times \gamma) \leq \alpha$. For the reverse suppose $(x, y) \in \alpha$. Knowing that $\alpha \times \beta \times \gamma$ exists we can find u such that $(u, x) \in \alpha, (u, x) \in \beta, (u, y) \in \gamma$. Therefore $(x, u) \in \alpha \times \beta$ using transitivity. Hence $(u, y) \in \alpha$ giving $(u, y) \in \alpha \times \gamma$. Thus $(x, y) \in (\alpha \times \beta) \vee (\alpha \times \gamma)$ proving Equation (4.2). □

Before we give an equivalent list of statements, we recall a definition from Chapter 2.

Definition 4.1.10. For algebra A, α is a factor congruence iff $0 = \alpha \times \alpha'$ for some congruence α' on A. □

Theorem 4.1.11. *For any algebra* A *the following statements are equivalent:*

(i) A *has the strict refinement property.*

(ii) A *as the strict refinement property for finite index sets* I, J.

(iii) *The set of factor congruences of A forms a Boolean lattice.*

(iv) *If $0 = \alpha \times \alpha' = \beta \times \beta'$ for some $\alpha, \alpha', \beta, \beta' \in Con\, A$ then $(\alpha \vee \beta) \wedge \alpha' \leq \beta$.*

(v) *If $0 = \alpha \times \alpha' = \beta \times \beta'$ for some $\alpha, \alpha', \beta, \beta' \in Con', A$ then $\alpha \circ (\alpha' \wedge \beta) = (\alpha' \wedge \beta) \circ \alpha$ and $\beta \leq (\alpha' \wedge \beta) \vee \alpha$.*

(vi) *$f_v g_v = g_v f_v$ for all decomposition functions f, g and all $v \in A$.*

(vii) *There exists $v \in A$ such that $f_v g_v = g_v f_v$ for all decomposition functions f and g.*

(viii) *For any decomposition functions f, g and $a_1, a_2, a_3, a_4 \in A$ there exists $v \in A$ such that $f_v g_v(a_i) = g_v f_v(a_i)$ and $f'_v g_v(a_i) = g_v f'_v(a_i)$ for all $i \in \{1, 2, 3, 4\}$.*

Proof. $(i) \implies (ii) \implies (iii) \implies (iv)$ (since $(\alpha \vee \beta) \wedge \alpha' = (\alpha \wedge \alpha') \vee (\beta \wedge \alpha') \leq \beta$), $(iii) \implies (v)$ and $(vi) \implies (vii) \implies (viii)$ are obvious. Assume (vii) and suppose $0 = \prod_{i \in I} \beta_i = \prod_{j \in J} \gamma_j$. Define $\delta_{ij} = \beta_j \vee \delta_j$. To prove (i) it is sufficient to show that $\prod_{j \in J} \delta_{ij} = \beta_i$ and $\prod_{i \in I} \delta_{ij} = \gamma_j$.

By Lemma 4.1.7 there is a function $f_i : A \longrightarrow A$ such that $\beta_i = ker\, f_i = ker\, f_v$ for some v. Likewise $\gamma_j = ker\, g_j$ for some function $g_j : A \longrightarrow A$. By (vii) every f_i commutes with g_j. Next we show $\delta_{ij} = ker\, g_i f_i = ker f_i g_i$. Note $ker\, f_i \subseteq ker\, g_j f_i = ker\, f_i g_j$ and that $ker g_j \subseteq ker\, f_i g_j = ker\, g_j f_i$. Thus $\delta_{ij} = ker\, f_i \vee ker\, g_j \subseteq ker\, g_j f_i$. For the reverse if $(x, y) \in ker\, f_i g_j$ we have

$$x \overset{ker\, g_j}{\longrightarrow} g_j(x) \overset{ker\, f_i}{\longrightarrow} f_i g_j(x) = f_i g_j(y) \overset{ker\, f_i}{\longrightarrow} g_j(y) \overset{ker\, g_j}{\longrightarrow} y.$$

So $ker\, f_i g_j \subseteq ker\, f_i \vee ker\, g_j = \delta_{ij}$. Certainly $f_i(x) = f_i(y)$ iff $g_j f_i(x) = g_j f_i(y)$ for all j. So $\cap_{j \in J} \delta_{ij} = \beta_i$. It remains to show for all $a \in A^J$ there is a $b \in A$ with $f_i g_j(b) = f_i g_j(a_j)$ for all $j \in J$. This follows from the existence of element $b \in A$ with $g_j(b) = g_j(a_j)$ for all j which in turn is immediate from the existence of $\prod_{j \in J} \gamma_j$. A similar argument shows $\prod_{i \in I} \delta_{ij}$ exists and is equal to γ_j.

Assume (iv) and we will show $f_v g_v(x) = g_v f_v(x)$ for any decomposition functions f, g and any $v \in A$. Take $\alpha = ker\, f_v, \alpha' = ker\, f'_v, \beta = ker\, g_v$ and $\beta' = ker\, g'_v$. Thus $0 = \alpha \times \alpha' = \beta \times \beta'$. Now we proceed to proof the following two claims:

Claim 1: $(f_v g_v(x), g_v f_v(x)) \in \beta$.

$$f_v(x) \overset{\alpha}{\text{———}} \boldsymbol{x} \overset{\beta}{\text{———}} \boldsymbol{g_v(x)} \overset{\alpha}{\text{———}} f_v g_v(x).$$

$$f_v(x) \overset{\alpha'}{\text{———}} \boldsymbol{v} \overset{\alpha'}{\text{———}} f_v g_v(x).$$

So $(f_v(x), f_v g_v(x)) \in (\alpha \vee \beta) \wedge \alpha'$. Therefore $(f_v(x), f_v g_v(x)) \in \beta$. Moreover $(f_v(x), g_v f_v(x)) \in \beta$. Thus by transitivity $(f_v g_v(x), g_v f_v(x)) \in \beta$.

Claim 2: $(f_v g_v(x), g_v f_v(x)) \in \beta'$.

$$f_v g_v(x) \overset{\alpha}{\text{———}} \boldsymbol{g_v(x)} \overset{\beta'}{\text{———}} v.$$

$$f_v g_v(x) \overset{\alpha'}{\text{———}} v.$$

So $(f_v g_v(x), v) \in \alpha' \wedge (\alpha \vee \beta)$. Therefore $(f_v g_v(x), u) \in \beta'$. Also $(v, g_v f_v(x)) \in \beta'$. Thus $(f_v g_v(x), g_v f_v(x)) \in \beta'$ by transitivity.

We now assume assertion (v) and prove (iv). Note $\alpha \circ \beta \geq \alpha \circ (\beta \wedge \alpha')$. Also

$$\begin{aligned} \alpha \circ (\beta \wedge \alpha') &\geq \alpha \vee (\beta \wedge \alpha') \\ &\geq \beta. \end{aligned}$$

Therefore $\alpha \circ (\beta \wedge \alpha') \geq \alpha \circ \beta$ giving $\alpha \circ (\beta \wedge \alpha') = \alpha \circ \beta$. Also

$$\begin{aligned} \beta \circ \alpha &\leq ((\alpha' \wedge \beta) \vee \alpha) \circ \alpha \\ &= ((\alpha' \wedge \beta) \circ \alpha) \circ \alpha \\ &= (\alpha' \wedge \beta) \circ \alpha \\ &= \alpha \circ \beta. \end{aligned}$$

Thus $\alpha \vee \beta = \alpha \circ \beta = \beta \circ \alpha$. Hence $(\alpha \vee \beta) \wedge \alpha' = (\alpha \circ \beta) \wedge \alpha' = (\alpha \circ (\beta \wedge \alpha')) \wedge \alpha' \leq \alpha' \wedge \beta \leq \beta$, since if $(x, z) \in (\alpha \circ (\beta \wedge \alpha')) \wedge \alpha'$ then a y exists such that $(x, z) \in \alpha'$, $(x, y) \in \alpha$ and $(y, z) \in \beta \wedge \alpha'$. Thus $(x, y) \in \alpha'$ giving $(x, y) \in \alpha \wedge \alpha' = 0$ which implies $x = y$ and $(x, z) \in \beta$.

Finally assume $(viii)$. To prove (v) we first show α and $\alpha' \wedge \beta$ commute if $0 = \alpha \times \alpha' = \beta \times \beta'$. Let f and g be the decomposition functions associated with α and β respectively. Suppose $(x, y) \in \alpha \circ (\alpha' \wedge \beta)$. Thus $(x, z) \in \alpha$ and $(z, y) \in \alpha' \wedge \beta$ for some z, which means $(z, y) \in \beta$. Since z is the unique element such that $(x, z) \in \alpha$ and $(z, y) \in \alpha'$ we have $z = f(x, y)$. Suppose $u = f(y, x)$ and select $v \in A$ such that

$$f_v g_v(t) = g_v f_v(t) \text{ and } f'_v g_v(t) = g_v f'_v(t)$$

for $t = x, y, z, u$. Notice $f_v(z) = f_v(x), f'_v(z) = f'_v(y), f_v(u) = f_v(y), f'_v(u) = f'_v(x)$ and $g_v(z) = g_v(y)$. Therefore

$$\begin{aligned} f_v g_v(u) &= g_v f_v(u) \\ &= g_v f_v(y) \\ &= f_v g_v(y) \\ &= f_v g_v(z) \\ &= g_v f_v(z) \\ &= g_v f_v(x) \\ &= f_v g_v(x). \end{aligned}$$

Also $f'_v g_v(u) = g_v f'_v(u) = g_v g'_v(x) = f'_v g_v(x)$. Hence it follows that $g_v(u) = g_v(x)$ and $(u, x) \in \beta$. Thus we have $(x, y) \in (\alpha' \wedge \beta) \circ \alpha$. This establishes that α and $\alpha' \wedge \beta$ commute.

It remains to show that $\beta \leq \alpha \circ (\alpha' \wedge \beta)$. Suppose $(x, y) \in \beta$ and $z = f(x, y)$. Select $v \in A$ such that

$$f_v g_v(t) = g_v f_v(t) \text{ and } f'_v g_v(t) = g_v f'_v(t)$$

for $t = x, y, z$. Observe $g_v(x) = g_v(y), f_v(x) = f_v(z)$ and $f'_v(y) = f'_v(z)$. Hence $f_v g_v(y) = f_v g_v(x) = g_v f_v(x) = g_v f_v(x) = f_v g_v(z)$ and $f'_v g_v(y) = g_v f'_v(y) = g_v f'_v(z) = f'_v g_v(z)$. Therefore $g_v(y) = g_v(z)$ or equivalently $(y, z) \in \beta$. Thus $(x, y) \in \alpha \circ (\alpha' \wedge \beta)$, because

$$x \overset{\alpha}{\text{———}} z \overset{\alpha' \wedge \beta}{\text{———}} y.$$

□

Corollary 4.1.12. *If Con A is distributive then A has the strict refinement property.*

Proof. Note when *Con A* is distributive then condition (iv) of Theorem 4.1.11 holds. □

Corollary 4.1.13. *If A is an algebra with a zero and if the centre of A is* $\{0\}$ *then A has the strict refinement property.*

Proof. We only need to show $fg = gf$ whenever $1 = f \oplus f' = g \oplus g'$. By Lemma 3.1.5 $fgf', f'gf$ are both maps of A into the centre. Thus $fgf' = f'gf$.

$$\begin{aligned} fg &= fg(f + f') \\ &= fgf + fgf' \\ &= fgf + f'gf \\ &= (f + f')fg \\ &= gf. \end{aligned}$$

□

Corollary 4.1.14. *Every partially ordered set with a top and a bottom has the strict refinement property.*

Proof. Let P be a partially ordered set with a top and a bottom such that $P \simeq Q \times Q'$. Let f be the associated decomposition function. Then $f_{(0,0)}(a, a') = (a, 0) = (a, a') \wedge (1, 0)$, showing $f_0(x) = x \wedge y$ for some $y \in P$. Hence by Theorem 4.1.11 (vi) the result follows. □

In [FT52] we find a necessary and sufficient condition for an algebra to be a Boolean factor algebra, that is the set of factor congruences forms a Boolean lattice. They showed this happens whenever for every factor congruence α there is an unique congruence α' such that $0 = \alpha \times \alpha'$. Therefore by Theorem 4.1.11 these algebras also has the strict refinement property.

4.2 Intermediate refinement property

Now we introduce and investigate a property that is weaker than the strict refinement property. This property with some additional conditions will still imply that a given structure has the refinement property.

Definition 4.2.1. (A, v) is said to have the **intermediate refinement** property iff the two formulas $f_v g_v(x) = v$ and $g_v f_v(x) = v$ are equivalent for each $x \in A$ and for all decomposition functions f and g, where structure A is an algebraic structure or an relational structure. □

Note if A has the strict refinement property then (A, v) has the intermediate refinement property for every element v of A. The following theorem translate this property to the language of congruences.

Theorem 4.2.2. *For any* $v \in A$ *the following conditions are equivalent:*

(i) (A, v) *has the intermediate refinement property.*

(ii) If $0 = \alpha \times \alpha' = \beta \times \beta'$ *then* $v/((\alpha \circ \beta) \wedge (\alpha' \circ \beta)) = v/\beta$.

(iii) If $0 = \alpha \times \alpha' = \beta \times \beta'$ *then* $v/((\alpha \circ \beta) \wedge (\alpha' \circ \beta)) \subseteq v/\beta$.

(iv) If $0 = \alpha \times \alpha' = \beta \times \beta'$ *then* $v/((\alpha \circ \beta) \wedge \alpha') \subseteq v/\beta$.

(v) If $0 = \alpha \times \alpha' = \beta \times \beta'$ *then* $v/\beta \subseteq v/(\alpha \circ (\alpha' \wedge \beta)) \subseteq v/((\alpha' \wedge \beta) \circ \alpha)$.

Proof. Clearly (iii) implies (iv) and (ii) and (iii) are equivalent. Imitating the proof in Theorem 4.1.11 we can show (v) implies (iv). We now assume (iv) holds and show (iii). Assume $(v,x) \in (\alpha \circ \beta) \wedge (\alpha' \circ \beta)$. Thus $(v,x) \in \alpha \circ \beta$ and $(v,x) \in \alpha' \circ \beta$. So elements m, n exists such that $(v,m) \in \alpha, (m,x) \in \beta, (v,n) \in \alpha'$ and $(n,x) \in \beta$. Therefore $(m,n) \in \beta$ giving $(v,n) \in \alpha \circ \beta$. Noting $(v,n) \in \alpha'$ we get $(v,n) \in (\alpha \circ \beta) \wedge \alpha'$. By (iv) we get $(v,n) \in \beta$ giving $(v,x) \in \beta$, since $(m,n) \in \beta$.

Assume (i) and we show (v) holds. Suppose $0 = \alpha \times \alpha' = \beta \times \beta'$. Let f and g be the associated decomposition functions. Suppose $x \in v/\beta$ and put $z = f(v,x)$. Thus $f'_v g_v(x) = f'_v g_v(v) = v = g_v f'_v(x) = g_v(z)$. Hence $g_v(z) = g_v(x)$ and $(z,x) \in \beta$ giving $(v,x) \in \alpha \circ (\alpha' \wedge \beta)$.

To show the second part let $x \in v/(\alpha \circ (\alpha' \wedge \beta))$. Thus $(v,z) \in \alpha$ and $(z,x) \in \alpha' \wedge \beta$ where $z = f(v,x)$. Put $y = f(x,v)$. This gives $f_v g_v(z) = g_v f_v(z) = g_v f_v f'_v(x) = v$. Therefore $g_v(y) = g_v f_v(x) = v$. Consequently $(v,y) \in \beta$ indicating that $(v,x) \in (\alpha' \wedge \beta) \circ \alpha$.

Assume (iii) and we show (i). For $x \in A$ the following conditions are equivalent :

$$f_v g_v(x) = v, \quad (g_v(x), v) \in \alpha, \quad (v,x) \in (\alpha \wedge \beta') \circ \beta, \quad x \in v/((\alpha \wedge \beta') \circ \beta).$$

Similarly for $f_v g_v(x) = v$. It therefore suffices to show that $v/((\alpha \wedge \beta') \circ \beta) = v/(\beta \circ (\alpha \wedge \beta'))$. Suppose $x \in v/((\alpha \wedge \beta') \circ \beta)$. Then $(v,z) \in \alpha \wedge \beta'$ and $(z,x) \in \beta$ for some element $z \in A$. Knowing $\alpha' \circ \alpha = 1$ there is an unique $y \in A$ such that $(v,y) \in \alpha'$ and $(y,x) \in \alpha$. Thus $(v,y) \in \alpha' \wedge (\alpha \circ \beta)$. Therefore $(v,y) \in \beta$ showing (i) holds. □

Before we prove Theorem 4.2.6 due to [CJT], the major result in this subsection, we first establish two lemmas to assist in this task.

Lemma 4.2.3. *Suppose* $v \in A$ *and* (A,v) *has the intermediate refinement property. If* $0 = \prod_{i \in I} \alpha_i = \beta \times \beta'$ *for some congruences then* $v/\beta = \bigcap_{i \in I} v/(\alpha_i \circ \beta)$.

Proof. It is evident that $v/(\alpha_i \circ \beta) \geq v/\beta$. Therefore $\bigcap_{i \in I} v/(\alpha_i \circ \beta) \geq v/\beta$. For the remainder of the proof suppose $x \in \bigcap_{i \in I} v/(\alpha_i \circ \beta)$. Thus for each $i \in I$ we have $x \in v/(\alpha_i \circ \beta)$ or in other words an element y_i exist such that $(v,y_i) \in \alpha_i$ and $(y_i,x) \in \beta$. Using the fact that some element $z \in A$ exists such that $(v,z) \in \beta'$ and $(z,x) \in \beta$ we have $(v,z) \in \beta' \wedge (\alpha_i \circ \beta)$. Therefore $(v,z) \in \alpha_i$ for each $i \in I$. Consequently $v = z$ and $(v,x) \in \beta$. □

We need the following definition for the next lemma.

Definition 4.2.4. An element v in algebra A is said to be **idempotent** iff for every fundamental operation F it satisfies the equation $F(v, \ldots, v) = v$.

Lemma 4.2.5. *If* $v \in A$ *is an idempotent element and* $0 = \alpha \times \alpha'$ *for some congruences on algebra* A *then* $v/\alpha \simeq A/\alpha'$.

Proof. It follows that v/α is a subalgebra of A as v is an idempotent element. Let $\phi : v/\alpha \longrightarrow A/\alpha'$ such that $\phi(x) = x/\alpha'$. We first show this map is bijective as its clear that the map is a homomorphism. If $y \in A$ then an element x exist such that $(v,x) \in \alpha$ and $(x,y) \in \alpha'$. Thus $\phi(x) = x/\alpha' = y/\alpha'$ and the map is onto. If $\phi(x) = \phi(y)$ then $(x,y) \in \alpha \wedge \alpha' = 0$. Hence $x = y$ and the map is injective completing the proof. □

Theorem 4.2.6. *If algebra* A *possess an idempotent element* v *such that* (A,v) *has the intermediate refinement property then algebra* A *has the refinement property.*

Proof. Suppose

$$A \simeq \prod_{i\in I} B_i \simeq \prod_{j\in J} C_j.$$

Then congruences β_i, γ_j exists such that $A/\beta_i \simeq B_i$ for each $i \in I$ and $A/\gamma_j \simeq C_j$ for each $j \in J$ and

$$0 = \prod_{i\in I} \beta_i = \prod_{j\in J} \gamma_j.$$

Let $\overline{\beta_p} = \prod_{i\in I-\{p\}} \beta_i$ and $\overline{\gamma_q} = \prod_{j\in J-\{q\}} \gamma_j$. Also let β_{pq}, γ_{pq} be the restriction of β_p, γ_q to $v/\overline{\gamma_q}$ and $v/\overline{\beta_p}$ respectively. By Lemma 4.2.5 we have for each $p \in I$ and $q \in J$ that

$$B_p \simeq A/\beta_p \simeq v/\overline{\beta_p}.$$

It turns out $0_{v/\overline{\beta_p}} = \prod_{j\in J} \gamma_{pj}$ (since $v/\overline{\beta_p} = \bigcap_{j\in J} \gamma_{pj}$ and if $x \in v/\overline{\beta_p}^J$ then $(x_j, v) \in \overline{\beta_p}$ for all $j \in J$. Using $\prod_{j\in J} \gamma_j = 0$ we see there is an element u such that $(x_j, u) \in \gamma_j$ for all $j \in J$. Thus $(u, v) \in \overline{\beta_p} \circ \gamma_j$ for each j, showing $(u, v) \in \overline{\beta_p}$ by Lemma 4.2.3. Hence $(x_j, u) \in \gamma_{pj}$ for each $j \in J$) giving

$$B_p \simeq v/\overline{\beta_p} \simeq \prod_{j\in J} (v/\overline{\beta_p})/\gamma_{pj}.$$

Similarly we can show

$$C_q \simeq \prod_{i\in I} (v/\overline{\gamma_q})/\beta_{iq}.$$

Put $\overline{\beta_{pq}} = \prod_{i\in I-\{p\}} \beta_{iq}$ and $\overline{\gamma_{pq}} = \prod_{j\in J-\{q\}} \gamma_{pj}$. Again by Lemma 4.2.5 we have

$$v/\overline{\beta_{pq}} = (v/\overline{\gamma_q})/\beta_{pq}, \qquad v/\overline{\gamma_{pq}} = (v/\overline{\beta_p})/\gamma_{pq}.$$

Hence by Lemma 4.2.3 we have

$$B_p \simeq \prod_{j\in J} v/\overline{\gamma_{pj}}, \qquad C_q \simeq \prod_{i\in I} v/\overline{\beta_{iq}}.$$

Thus A will have the refinement property if we can show $v/\overline{\beta_{pq}} = v/\overline{\gamma_{pq}}$. Now $x \in v/\overline{\beta_{pq}}$ is equivalent to each of the following statements:

$$\begin{aligned}
x &\in v/\overline{\beta_{pq}},\\
x &\in v/\beta_{iq} \text{ for all } i \in I - \{p\},\\
x &\in v/\overline{\gamma_q} \text{ and } x \in v/\beta_i \text{ for all } i \in I - \{p\},\\
x &\in v/\gamma_j \text{ and } x \in v/\beta_i \text{ for all } i \in I - \{p\} \text{ and } j \in J - \{q\}.
\end{aligned}$$

By symmetry the condition $x \in v/\overline{\gamma_{pq}}$ is equivalent to the last statement and therefore the conclusion follows. □

Chapter 5

More refinement properties

This chapter studies the class of relational structures. These structures are frequent in mathematics and need special consideration. Here we devote some space to them. We mostly deal with structures with binary operations satisfying certain equations and discover more refinement properties. In particular, we show that every connected partially ordered set has the strict refinement property. Using decomposition functions, we illustrate techniques to produce more structures with the refinement property. We end this chapter with a result that consequently proves that every finite connected symmetric binary structure is unique factorable.

5.1 Special binary structures

This section develops techniques published by C. Chang, B. Jónsson and A. Tarski [CJT] to study factorization properties of relational structures. Using decomposition functions in a clever way, we will produce more refinement properties for certain classes of binary structures.

Definition 5.1.1. Let $x^\frown y$ be the concatenation of the m-termed sequence x and the n-termed sequence y, that is by $x^\frown y$ we denote the sequence $(x_1, \ldots, x_m, y_1, \ldots, y_n)$. If R and S are two relations then $R^\frown S$ is the relation consisting of all sequences $x^\frown y$ where $x \in R$ and $y \in S$. If $n > 1$ and R is a relation of rank n then $P(R)$ and $Q(R)$ are the $n-1$-ary relations such that

$$\begin{aligned} P(R) &= \{x \in A^{n-1} : x^\frown\{y\} \in R \text{ for some } y \in A\}, \\ Q(R) &= \{x \in A^{n-1} : x^\frown\{y\} \in R \text{ for all } y \in A\}. \end{aligned}$$

Let $I_{i,j,n} = \{x \in A^n : x_i = x_j\}$ for all $i \leq j \leq n$. Lastly, if R is an n-ary relation and ϕ is a permutation of the set $\{1, 2, \ldots, n\}$ then define $\phi(R)$ to be the n-ary relation consisting of all the sequences $\phi(x) = (x_{\phi(1)}, x_{\phi(2)}, \ldots, x_{\phi(n)})$ where $x \in R$. □

Definition 5.1.2. For any relational algebra A, let $\Psi(A)$ denote the intersection of all families $\mathfrak{F}$ of relations having the following properties:

(i) $R \in \mathfrak{F}$ for every relation R of algebra A, $A^n \in \mathfrak{F}$ for every positive integer n and $I_{i,j,n} \in \mathfrak{F}$ for all natural numbers i, j and n where $i \leq j \leq n$.

(ii) For any n-ary relation R with $n > 1$, if $R \in \mathfrak{F}$ then $P(R) \in \mathfrak{F}$ and $Q(R) \in \mathfrak{F}$.

(iii) If R is an n-ary relation, ϕ a permutation of the set $\{1, 2, \ldots, n\}$ and $R \in \mathfrak{F}$ then $\phi(R) \in \mathfrak{F}$.

(iv) For any relations $R, S \in \mathfrak{F}$ we have $R^\frown S \in \mathfrak{F}$ and if R and S are relations of the same rank, then $R \cap S \in \mathfrak{F}$ and $R \cup S \in \mathfrak{F}$.

□

Lemma 5.1.3. *Suppose $R \subseteq A^n$ and $R \in \Psi(A)$. Let f be decomposition function on A and $x, y \in A^n$. Let $z_k = f(x_k, y_k)$ for $1 \leq k \leq n$. If $x, y \in R$ then $z = (z_1, z_2, \ldots, z_n) \in R$.*

Proof. Let $\mathfrak{F}$ be the class of relations with the property in the corollary. A simple calculation shows all the conditions of previous definition hold for $\mathfrak{F}$. Whence $R \in \Psi(A) \subseteq \mathfrak{F}$. □

Before we prove our first strict refinement theorem, we need some additional concepts for structures with a binary relation.

Definition 5.1.4. Let (A, R) be an algebra with a binary relation R. A relation R is said to be **symmetric** iff for all $x, y \in A$ whenever $(x, y) \in R$ then $(y, x) \in R$. Element x of the binary structure is called **anti-symmetric** iff $(x, y) \in R$ and $(y, x) \in R$ together imply $x = y$ for each $y \in A$. Algebra (A, x) is said to be **anti-symmetric** iff x is an anti-symmetric element of A. A relation R is said to be **anti-symmetric** iff every element x is anti-symmetric. Elements x and y are said to be **n-connected** whenever $(x, y) \in R^n = R \circ R \circ \ldots \circ R$ (R appears n times). A relation R is said to be **connected** iff any two elements $x, y \in A$ are n-connected for some positive integer n. A relation R is said to be **transitive** iff whenever $(x, y), (y, z) \in R$ then $(x, z) \in R$. Lastly, a relation R is said to be a **partial order** iff relation R is reflexive, anti-symmetric and transitive.

Now we are ready to establish a strict refinement result (due to [CJT]) that every connected symmetric binary relational structure with an anti-symmetric element has the strict refinement property.

Theorem 5.1.5. *If $\Psi(A)$ contains a symmetric and connected binary relation R and an element v such that (A, v) is anti-symmetric with respect to R then (A, v) has the intermediate refinement property.*

Proof. Let $\equiv_R$ or $\equiv$ be the smallest equivalence relation such that it contains the set $\{(x, y) : (x, y) \in R \text{ and } (y, x) \in R\}$. Observe $x \equiv v$ implies that $x = v$, since v is an anti-symmetric element. For $u \in A$ let $C(u)$ be the set of all elements $x \in A$ such that $f_u g_u(x) \equiv g_u f_u(x)$ for all decomposition functions f, g.

If we can establish that whenever x and u are n-connected then $x \in C(u)$ then the theorem follows readily, since connectedness gives that $C(v) = A$. If f, g are decomposition functions and $x \in A$ is such that $f_v g_v(x) = v$ then $g_v f_v(x) \equiv v$ and therefore $g_v f_v(x) = v$ proving that (A, v) has the intermediate refinement property.

Before we proceed we observe for any decomposition function f on A and $x, y, z, x', y', u, w \in A$ the following statements are all true :

(1) If $(x, x') \in R, (y, y') \in R$ then $(f(x, y), f(x', y')) \in R$.

(2) If $(x, y) \in R$ then $(f_u(x), f_u(y)) \in R$.

(3) If $(x, z) \in R, (y, z) \in R$ then $(f(x, y), z) \in R$.

(4) If $x \equiv x', y \equiv y'$ then $f(x, y) \equiv f(x', y')$.

(5) If $(f_u(x), f_u(y)) \in R$ and $(f'_u(x), f'_u(y) \in R$ then $(x, y) \in R$.

(6) If $f_u(x) \equiv f_u(y)$ and $f'_u(x) \equiv f'_u(y)$ then $x \equiv y$.

(7) If $x, u \in C(w)$ and $f_u(x), g_u f_u(x) \in C(w)$ for all decomposition functions f, g then $x \in C(u)$.

Most of the observations are immediate from definition. If $x \equiv x'$ then there are elements $x = r_1, r_2, \ldots, r_n = x'$ such that $(r_i, r_{i+1}) \in R$ and $(r_{i+1}, r_i) \in R$ for $1 \leq i < n$. Hence $(f(r_i, y), f(r_{i+1}, y)) \in R$ and $(f(r_{i+1}, y), f(r_i, y)) \in R$ and therefore $f(x, y) \equiv f(x', y)$. Adapting this argument one more time we can prove claim (2). Now we prove claim (8). By several applications of the hypothesis we get $f_w g_w f_u g_u(x) \equiv g_w f_w f_u g_u(x) = g_w f_w g_u(x) \equiv f_w g_w g_u(x) = f_w g_w(x) \equiv g_w f_w(x) = g_w f_w f_u(x) \equiv f_w g_w f_u(x) = f_w g_w g_u f_u(x)$ and $f'_w g_w f_u g_u(x) \equiv g_w f'_w g_u f_u(x) = g_w f'_w(v) = g_w f'_w f_u(x) \equiv f'_w g_w f_u(x) = f'_w g_w g_u f_u(x)$. Therefore by claim (7) we have $g_u f_u(x) = f_u g_u(x)$ and hence $x \in C(u)$. To complete the proof we show by induction that

$$\text{If } x \text{ and } u \text{ are } (R, n) \text{ connected then } x \in C(u). \tag{5.1}$$

We start the proof with the case $n = 1$, that is (x, u) are $(R, 1)$ connected. Assume without loss of generality $(u, x) \in R$. Thus by claim (2) we have $(u, f_u(x)) \in R$ and $(f_u(x), x) \in R$. Hence $(g_u f_u(x), f_u(x)) \in R$ and $(g_u f_u(x), g_u(x)) \in R$ giving $(g_u f_u(x), f(g_u(x), f_u(x)) \in R$. From $f(g_u(x), f_u(x)) = f(g_u(x), u) = f_u g_u(x)$ we get $(f_u g_u(x), g_u f_u(x)) \in R$. Similarly we can show $(g_u f_u(x), f_u g_u(x)) \in R$ and hence $x \in C(u)$.

Assume that statement 5.1 holds whenever n is replaced by a smaller integer. If x and u are (R, n) connected then elements $x = r_0, r_1, \ldots, r_n = u$ such that either (r_i, r_{i+1}) or (r_{i+1}, r_i) are R-related. Put $w = r_{n-1}$. Assume without loss of generality $(w, u) \in R$. Thus $x, u \in C(w)$. By claim (7) it is enough to show that $f_u(x), g_u f_u(x) \in C(w)$ for any decomposition functions f, g. We deal with two cases:

Case 1 : For some $j \leq n - 1$ we have $(r_{j+1}, r_j) \in R$. Let $r'_i = f_u(r_i)$ if $i \leq j$ otherwise let $r'_i = f_w(r_i)$. By the hypothesis we have w and $f_u(x)$ are $(R, n-1)$-connected. Let $r''_i = g_u f_u(r_i)$ if $i \leq j$ otherwise let $r''_i = g_w f_w(r_i)$. Again we have w and $g_u f_u(x)$ are $(R, n-1)$-connected. Thus $f_u(x), g_u f_u(x) \in C(w)$.

Case 2 : Suppose $(r_j, r_{j+1}) \in R$ for all j. Let $r'_i = f_u(r_i)$ and $r''_i = g_u f_u(r_i)$ for all i. Applying Case 1 we infer that both $f_u(x)$ and $g_u f_u(x)$ belong to $C(w)$. □

The conditions on R is necessary as there exist structures with a symmetric and symmetric binary relations R that is not uniquely factorable. See Example 7.2.14. We continue this chapter by giving more examples of structures with the strict refinement property due to Chang, Jónsson and Tarski [CJT].

Corollary 5.1.6. *Let $+$ be a binary operation on A such that $x + x = x$ for all $x \in A$. If for all $x, y \in A$ one of the following condition holds:*

(i) There exists $z \in A$ such that $x + z = z + x = x$ and $y + z = z + y = y$

(ii) There exists $z \in A$ such that $x + z = z + x = z$ and $y + z = z + y = z$

then A has the refinement property.

Proof. Let $R = \{(x, y) \in A^2 : x + y = y + x = x\}$. It is readily seen that the conditions in Theorem 5.1.5 are satisfied and by Theorem 4.2.6 the conclusion follows. □

Definition 5.1.7. If R is a binary relation let $T(R) = \{(x, y) : (x, z) \in R \iff (y, z) \in R \text{ and } (z, x) \in R \iff (z, y) \in R\}$. We say R is **thin** iff $T(R)$ is the equality relation. □

The proof of the following theorem is similar to the proof of Theorem 5.1.5. This turns out to be a stronger result than [Has51] where Hashimoto proved that every connected partially ordered set has the refinement property.

Theorem 5.1.8. *If (A, R) is a thin connected symmetric binary relational structure then A has the strict refinement property.*

Corollary 5.1.9. *Every connected partially ordered set has the strict refinement property.*

Earlier we studied Jónsson-Tarski algebras. They are algebraic systems with a binary operation $+$ and a zero element 0 such that $0 + x = x + 0 = x$ for all $x \in A$. In particular we showed whenever A is centerless then A has strict refinement property. We proceed now to prove more refinement properties by looking at the five properties below, where fixed element v takes over the rol of 0. We say element v has property P_i if

(P_1) for all $x \in A, v + x = x + v$.

(P_2) for all $x, y \in A$, $v+(x+y) = (v+x)+y, x+(v+y) = (x+v)+y$ and $x+(y+v) = (x+y)+v$.

(P_3) for all $x, y \in A$ if $v + x = v + y$ then $x = y$.

(P_4) for all $x \in A$ if $v + x = v + v$ then $x = v$.

(P_5) for all $x, y \in A$ if $x + y = v + v$ then $x = y = v$.

Lemma 5.1.10. *Suppose $+$ is a binary relation in $\Psi(A)$ such that v is an element satisfying property P_1. Then for all decomposition functions f, g on A we have*

(i) $f_v(x) + f'_v(x) = v + x$.

(ii) $f_v g_v f'_v(x) + f_v g'_v f'_v(x) = v + v$.

(iii) $f_v g_v f'_v(x) + g_v f_v(x) = f'_v g_v f_v(x) + f_v g_v(x)$.

(iv) $f_v(x) + f'_v(y) = f'_v(y) + f_v(x)$.

(v) $x + y = y + x$ *iff* $f_v(x) + y = y + f_v(x)$ *and* $f'_v(x) + y = y + f'_v(x)$.

(vi) $x + y = y + x$ *iff* $f_v(x) + f_v(y) = f_v(y) + f_v(x)$ *and* $f'_v(x) + f'_v(y) = f'_v(y) + f'_v(x)$.

(vii) $f_v g_v f'_v(x) + y = y + f_v g_v f'_v(x)$.

Proof. By Lemma 5.1.3 we see $f_v(x) + f_v(y) = f_{v+v}(x + y)$. Thus $f_v(x) + f'_v(x) = f(x, v) + f(v, x) = f(x + v, v + x) = f(v + x, v + x) = v + x$ giving (i). To prove (ii) we apply (i) and get $f_v g_v f'_v(x) + f_v g'_v f'_v(x) = f_{v+v}(g_v f'_v(x) + g'_v f'_v(x)) = f_{v+v}(v + f'_v(x)) = f_v(v) + f_v f'_v(x) = v + v$. The third claim follows from the following calculation :

$$\begin{aligned}
f_v g_v f'_v(x) + g_v f_v(x) &= f(g_v f'_v(x), v) + f(g_v f_v(x), g_v f_v(x)) \\
&= f(g_v f'_v(x) + g_v f_v(x), v + g_v f_v(x)) \\
&= f(g_{v+v}(f'_v(x) + f_v(x)), g_v f_v(x) + v) \\
&= f(g_{v+v}(v + x), g_v f_v(x) + v) \\
&= f(v + g_v(x), g_v f_v(x) + v) \\
&= f(v, g_v f_v(x)) + f(g_v(x), v) \\
&= f'_v g_v f_v(x) + f_v g_v(x).
\end{aligned}$$

Using P_1 we get $f_v(x) + f'_v(y) = f(x+v, v+y) = f(v+x, y+v) = f'_v(y) + f_v(x)$. Thus (iv) holds. To prove (v) we first assume $x + y = y + x$. Hence

$$\begin{aligned} f_v(x) + y &= f(x, v) + f(y, y) \\ &= f(x+y, v+y) \\ &= f(y+x, y+v) \\ &= f(y, y) + f(x, v) \\ &= y + f_v(x). \end{aligned}$$

Similarly we can show $f'_v(x) + y = y + f'_v(x)$. For the second half assume y commutes with $f_v(x)$ and $f'_v(x)$.Thus

$$\begin{aligned} x + y = f(y, y) + f(f_v(x), f'_v(x)) = f(y + f_v(x), y + f'_v(x)), \\ y + x = f(f_v(x), f'_v(x)) + f(y, y) = f(f_v(x) + y, f'_v(x) + y). \end{aligned}$$

For claim (vi) we apply (v) and (iv). Finally by (iv) we have $f'_v(x)$ commutes with $f_v(y)$. Thus $f_v g_v f'_v(x)$ also commutes with $f_v(y)$. Similarly we can show $f_v g_v f'_v(x)$ also commutes with $f'_v(y)$. Hence by (vi) we have that $f_v g_v f'_v(x)$ commutes with y. □

Theorem 5.1.11. *Suppose $+$ is a binary operation in $\Psi(A)$ and v is an element of A satisfying P_1 and P_4. Then (A, v) has the intermediate refinement property if and only if for all decomposition functions f, g and $x \in A$ we have $f_v g_v f'_v(x) = v$.*

Proof. If (A, v) has the intermediate refinement property then $g_v f_v(x) = v$ implies $f_v g_v(x) = v$. Since $g_v f_v f'_v(x) = u$ we have $f_v g_v f'_v(x) = v$. Conversely assume $f_v g_v f'_v(x) = v$ and $g_v f_v(x) = v$. Then $v + v = v + f_v g_v(x)$ by Lemma 5.1.10. Thus by P_4 it follows that $v = f_v g_v(x)$. □

Theorem 5.1.12. *Suppose $+$ is a binary operation in $\Psi(A)$ and v is an idempotent element of A satisifying P_1 and P_5, then algebra A has the refinement property.*

Proof. By Lemma 5.1.10 we have $f_v g_v f'_v(x) + f_v g'_v f'_v(x) = v + v$ for any decomposition functions f and g. Hence $f_v g_v f'_v(x) = v$ by property P_5. Consequently by Theorem 5.1.11 it follows that (A, v) has the intermediate refinement property giving the conclusion. □

Theorem 5.1.13. *Suppose $+$ is a binary operation in $\Psi(A)$ and v is an element of A satisfying P_1 and P_3. Then (A, v) has the intermediate refinement property if and only if A has the strict refinement property.*

Proof. If (A, v) has the intermediate refinement property then $f_v g_v f'_v(x) = v$ for any decomposition functions f, g and elements $x \in A$. Thus by Lemma 5.1.10 (iii) we have $v + g_v f_v(x) = v + f_v g_v(x)$. Hence by P_3 it follows that $g_v f_v(x) = f_v g_v(x)$. By Theorem 4.1.11 we get that A has the strict refinement property. The reverse implication is true for every structure A. □

Theorem 5.1.14. *Suppose $+$ is a binary operation in $\Psi(A)$ and v is an element of A satisfying P_1, P_4 and P_5 then A has the strict refinement property.*

Proof. From the proof of Theorem 5.1.12 we see that (A, v) has the intermediate refinement property. Therefore the conclusion follows by Theorem 5.1.13. □

Lemma 5.1.15. *Suppose $+$ is a binary operation in $\Psi(A)$ and v is an element of A satisfying P_2. If f, g are decomposition functions and $z \in A$ then the conditions of P_2 also hold when v is replaced by $f_v g_v f'_v(z)$.*

Proof. We will shortly prove that the following three statements are true for any decomposition functions f, g and $x, y, z \in A$.

(1) $(x + y) + z = x + (y + z)$ if and only if $(f_v(x) + f_v(y)) + f_v(z) = f_v(x) + (f_v(y) + f_v(z))$ and $(f'_v(x) + f'_v(y)) + f'_v(z) = f'_v(x) + (f'_v(y) + f'_v(z))$.

(2) $(f_v(x) + f_v(y)) + f'_v(z) = f_v(x) + (f_v(y) + f'_v(z))$.

(3) If $(x + y) + z = x + (y + z)$ then $(x + y) + f_v(z) = x + (y + f_z(z))$.

Here we mean x, y, z associate iff $(x+y)+z = x+(y+z)$. Note $f_v f_v g_v f'_v(z) = f_v g_v f'_v(z)$, $f'_v f_v g_v f'_v(z) = v$ and $f'_v(x), f'_v(y), v$ associate. So if these three statements hold then showing x, y and $f_v g_v f'_v(z)$ associate reduces to showing $f_v(x), f_v(y)$ and $f_v g_v f'_v(z)$ associate. By (2) we know that $f_v(x), f_v(y), f'_v(z)$ associate. Finally two applications of (3) gives the desired conclusion. Thus it remains to show these three statements are all true.

Put $u = (v + v) + v = v + (v + v)$. Thus

$$\begin{aligned} f_u((x + y) + z) &= (f_v(x) + f_v(y)) + f_v(z), \\ f_u(x + (y + z)) &= f_v(x) + (f_v(y) + f_v(z)). \end{aligned}$$

We also get similar formulas with f_u replaced with f'_u. From these formulas we can conclude statement (1). The formulas below are true whenever one of the elements involved is v. Thus these calculations proof statement (2).

$$\begin{aligned} f_u((x + y) + z) &= (f_v(x) + f_v(y)) + f_v(z), \\ f_u(x + (y + z)) &= f_v(x) + (f_v(y) + f_v(z)), \\ f'_u((x + y) + z) &= (f'_v(x) + f'_v(y)) + f'_v(z), \\ f'_u(x + (y + z)) &= f'_v(x) + (f'_v(y) + f'_v(z)). \end{aligned}$$

Lastly these calculations establishes claim (3).

$$\begin{aligned} f_u((x + y) + f_v(z)) &= (f_v(x) + f_v(y)) + f_v(z), \\ f_u(x + (y + f_v(z))) &= f_v(x) + (f_v(y) + f_v(z)), \\ f'_u((x + y) + f_v(z)) &= (f'_v(x) + f'_v(y)) + v, \\ f'_u(x + (y + f_v(z))) &= f'_v(x) + (f'_v(y) + v). \end{aligned}$$

□

Lemma 5.1.16. *Suppose $+$ is a binary operation in $\Psi(A)$ and v is an element of A satisfying P_1, P_2 and P_3. If f, g are decomposition functions and $z \in A$ then the conditions of P_3 also hold when v is replaced by $f_v g_v f'_v(z)$.*

Proof. Assume that $f_v g_v f'_v(z) + x = f_v g_v f'_v(z) + y$. By adding $f_v g'_v f'_v(z)$ on the left and using Lemma 5.1.15 and Lemma 5.1.10 (ii) we obtain that $(u + u) + x = (u + u) + y$. Consequently by property P_3 the result now follows. □

Theorem 5.1.17. *Suppose $+$ is a binary operation in $\Psi(A)$ and v is an element of A satisfying P_1, P_2 and P_3. Furthermore if there are no elements c, d in A such that $c \neq v$ and $c + d = v + v$ and the conditions P_1, P_2 and P_3 are all satisfied when v is replaced by c then A has the strict refinement property.*

Proof. For some decomposition functions let $c = f_v g_v f'_v(z)$ and $d = f_v g_v f'_v(z)$. Then $c + d = v + v$ by Lemma 5.1.10 (ii). Thus by Lemma 5.1.10 (vii), Lemma 5.1.15 and Lemma 5.1.16 we have that P_1, P_2 and P_3 are true when v is replaced by c. Therefore $c = u$ and according to Theorem 5.1.11 it follows that (A, v) has the intermediate refinement property. Applying Theorem 5.1.13 we get the desired result. □

Theorem 5.1.18. *Suppose $(A, +)$ is an algebra with a single binary operation $+$ and it has exactly one element v such that $x + v = v + x$. If $v + v = v$ then A has the refinement property.*

Proof. Define the binary relation R on A via $(x, y) \in R$ iff $x + y = y + x$. It is clear the $T(R)$-class of v is a singleton. Since $(v, x) \in R$ we see that (A, R) is a connected symmetric binary relation. Thus $((A, R), v)$ has the intermediate refinement property. If f is a decomposition function on $(A, +)$ then f is a decomposition function on (A, R), since if $((a, b), (c, d)) \in R^2$ then $f(a, b) + f(c, d) = f(a + c, b + d) = f(c + a, d + b) = f(c, d) + f(a, b)$. Thus (A, v) has the intermediate refinement property. Noting v is idempotent it follows that A has the refinement property. □

5.2 Another refinement theorem

The last result illustrates why every finite connected symmetric binary structure is uniquely factorable. This result is due to R. Mckenzie [MMT] and it only requires one of the $T(R)$ classes to be finite. Compare this result with Theorem 5.1.5.

Lemma 5.2.1. *For any non-empty finite sets I and J, if g_i, h_j are natural numbers such that*

$$\prod_{i \in I} g_i = \prod_{j \in J} h_j,$$

then natural numbers k_{ij} exist such that

$$g_i = \prod_{j \in J} k_{ij},$$

and

$$h_j = \prod_{i \in I} k_{ij}.$$

Proof. The proof is by induction on $|I| + |J|$. Clearly this result holds for $|I| = 1 = |J|$. To continue we select an element $x \in I$ if $|I| > 1$. (A similar calculation can be done if $|J| > 1$). By the properties of natural numbers we can find k_{xj} such that k_{xj} is a factor of h_j for each $j \in J$ and

$$\prod_{j \in J} k_{xj} = g_x.$$

A possible way is to select $k_{x1} = gcd(g_x, h_1), k_{x2} = gcd(g_x/k_{x1}, h_2), k_{x3} = gcd(\frac{g_x}{k_{x1}k_{x2}}, h_3), \ldots$, etc if $J = \{1, 2, 3, \ldots, m\}$. Applying the induction hypothesis now on $I - \{x\}$ and J with the new $h'_j = h_j/k_{xj}$ the result follows. □

This result can also be seen as an immediate consequence of the Fundamental Theorem of Arithmetic. This Lemma will be useful in the next proof.

Theorem 5.2.2. *If (A, R) is a connected symmetric binary structure and if one equivalence class of $T(R)$ is finite then A has the refinement property.*

Proof. Suppose $A \overset{\phi}{\simeq} \prod_{i\in I} B_i$ and $A \overset{\psi}{\simeq} \prod_{j\in J} C_j$. For this proof we use the notation : for any binary structure E let $\overline{E}$ be the quotient structure of E by the special equivalence relation $T(R)$. The natural map $\phi : E \longrightarrow \overline{E}$ is a homomorphism and if $(a,b) \in T(R)$ in $\overline{E}$ then $(a,b) \in R$ in E.

It is also easy to verify that there are isomorphisms $\overline{\phi} : \overline{A} \longrightarrow \prod_{i\in I} \overline{B_i}$ and $\overline{\psi} : \overline{A} \longrightarrow \prod_{j\in J} \overline{C_j}$ such that the following diagram commutes.

$$\begin{array}{ccc} A & \xrightarrow{\phi} & \prod_{i\in I} B_i \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle\theta^I} \\ \overline{A} & \xrightarrow[\overline{\phi}]{} & \prod_{i\in I} \overline{B_i} \end{array}$$

Likewise there is a similar diagram for ψ and $\overline{\psi}$. For each i let $\overline{\beta_i}$ be the factor relation of $\overline{A}$, that is the kernel of $p_i \circ \overline{\phi}$ (with p_i the projection of $\prod_{i\in I} \overline{B_i}$ onto B_i). Also let $\overline{\gamma_j}$ be the factor relation of $\overline{A}$ that is the kernel of $p_j \circ \overline{\psi}$ (with p_j the projection of $\prod_{j\in J} \overline{C_j}$ onto C_j). Clearly $0 = \prod_{i\in I} \overline{\beta_i} = \prod_{j\in J} \overline{\gamma_j}$. By the thinness of $\overline{A}$ and Theorem 5.1.5 we know that $\overline{A}$ has the strict refinement property.

So there exist congruences $\overline{\delta_{ij}}$ on $\overline{A}$ such that $\overline{\beta_i} = \prod_{j\in J} \overline{\delta_{ij}}$ and $\overline{\gamma_j} = \prod_{i\in I} \overline{\delta_{ij}}$. Let $\overline{D_{ij}}$ be the quotient structure A/δ_{ij}. So there are isomorphisms $\overline{\lambda_i} : \overline{B_i} \longrightarrow \prod_{j\in J} \overline{D_{ij}}$ and $\overline{\mu_j} : \overline{C_j} \longrightarrow \prod_{i\in I} \overline{D_{ij}}$, such that for each i and j we have

$$p_j \circ \overline{\lambda_i} \circ p_i \circ \overline{\phi} = p_i \circ \overline{\mu_j} \circ p_j \circ \psi.$$

Hence the following maps from A to $\prod_{ij} \overline{D_{ij}}$ are the same

$$A \xrightarrow{\phi} \prod_{i\in I} B_i \xrightarrow{\phi^I} \prod_{i\in I} \overline{B_i} \xrightarrow{\overline{\lambda}} \prod_{ij} \overline{D_{ij}}$$
$$A \xrightarrow{\psi} \prod_{j\in J} C_j \xrightarrow{\psi^I} \prod_{j\in J} \overline{C_j} \xrightarrow{\overline{\mu}} \prod_{ij} \overline{D_{ij}}$$

where $\overline{\lambda}$ is the map that takes $(\overline{b_i} : i \in I)$ to $(\overline{d_{ij}} : i \in I, j \in J)$ where $\overline{d_{ij}}$ is defined by $\overline{\lambda_j}(\overline{b_i}) = (\overline{d_{ij}})_{j\in J}$. Similar for $\overline{\mu}$. Now for each $x \in \prod_{ij} D_{ij}$ we define

$$\begin{aligned} F(x) &= \left|(\overline{\lambda} \circ \theta^I)^{-1}[x]\right| \\ F(x) &= \left|(\overline{\mu} \circ \theta^J)^{-1}[x]\right| \end{aligned}$$

That is the cardinal of the pre-images of x under either $\overline{\lambda} \circ \theta^I$ or $\overline{\mu} \circ \theta^J$. Thus $F(x)$ is just the cardinality of a $\equiv$-class of the original structure A. For each $y \in \overline{B_i}$ and $z \in \overline{C_j}$ let

$$\begin{aligned} G_i(y) &= \left|\theta_i^{-1}[y]\right| \\ H_j(z) &= \left|\theta_j^{-j}[z]\right|. \end{aligned}$$

Therefore by definition we have

$$\begin{aligned} F(x) &= \prod_{i\in I} G_i(\overline{\lambda}_i^{-1}(x_{i*})) \\ F(x) &= \prod_{j\in J} H_j(\overline{\mu}_j^{-1}(x_{*j})) \end{aligned}$$

where x_{*j} is the element of $\prod_{i\in I} \overline{D}_{ij}$ with $x_{*j}(i) = x(i,j)$ for each j and x_{i*} is the element of $\prod_{j\in J} \overline{D}_{ij}$ defined by $x_{i*}(j) = x(i,j)$. Let $Card$ be the collection of cardinal numbers. Knowing $F(x)$ is finite for some x we can show that there exist cardinal functions

$$K_{ij} : \overline{D}_{ij} \longrightarrow Card,$$

for each i and j such that

$$G_i(\overline{\lambda}_i^{-1}(y)) = \prod_{j\in J} K_{ij}(y(j)),$$

for each i and $y \in \prod_{j\in J} \overline{D}_{ij}$ and

$$H_j(\overline{\mu}_j^{-1}(z)) = \prod_{i\in I} K_{ij}(z(i)),$$

for each j and $z \in \prod_{i\in I} \overline{D}_{ij}$.

Given the cardinal functions K_{ij} we can now construct structures D_{ij} which will prove the refinement property. Fix $i \in I$ and $j \in J$. Let $Z = \{Z_x : x \in \overline{D}_{ij}\}$ be a disjoint family of sets such that $|Z_x| = K_{ij}(x)$ for each $x \in \overline{D}_{ij}$. We define the universe of D_{ij} to be $\cup Z$ and define $\theta_{ij} : D_{ij} \longrightarrow \overline{D}_{ij}$ via $\theta_{ij}(z) = x$ where Z_x is the unique Z that contains x. Lastly we define R to be the largest binary relation on D_{ij} such that θ_{ij} is a homomorphism. That is $x\overline{R}x'$ in D_{ij} if zRz' in D_{ij} for each $z \in Z_x$ and $z' \in Z_{x'}$. (Its easy to verify that the kernel of θ_{ij} is the $\equiv$relation of D_{ij}. Thus justifying the notation of $\overline{D}_{ij}$.)

Next we define $\overline{\theta}_i : \prod_{j\in J} D_{ij} \longrightarrow \prod_{j\in J} \overline{D}_{ij}$ by $\overline{\theta}_i((y_j)_{j\in J}) = (\theta_{ij}(y_j))_{j\in J}$ given that $y = (y_j)_{j\in J} \in \prod_{j\in J} \overline{D}_{ij}$.

$$\begin{aligned} |\theta_i^{-1}(y)| &= \prod_{j\in J} |\theta_{ij}^{-1}(y_j)| \\ &= \prod_{j\in J} K_{ij}(y_j) \\ &= G_i(\overline{\lambda}_i^{-1}(y)) \\ &= |\theta_i^{-1}\overline{\lambda}_i^{-1}(y)|. \end{aligned}$$

In otherwords if $\overline{\lambda}_i(x) = y$ then $\theta_i^{-1}(x)$ is a subset of B_i that is equipotent with the subset of $\theta_i^{-1}(y)$. Define $\lambda_i : B_i \longrightarrow \prod_{j\in J} D_{ij}$ to be any function that maps $\phi_i^{-1}(x)$ bijectively to $\theta_i^{-1}(x)$ to $\theta_i^{-1}(\lambda_i(x))$ for each $x \in \overline{B}_i$. Then λ_i will be a bijection of B_i with $\prod_{j\in J} D_{ij}$ such that

$$\theta_i' \circ \lambda_j = \overline{\lambda}_i \circ \theta_i.$$

It is readily checked that each λ_i maps the binary structure B_i isomorphically onto $\prod_{i\in I} D_{ij}$. By symmetry we can also show that $C_j \simeq \prod_{j\in J} D_{ij}$. $\square$

Chapter 6

Idempotent algebras

Another important open problem for finite algebras asks *whether every finite idempotent algebra have the unique factorization property?* Recall an algebra A is said to be idempotent iff every fundamental operation F satisfies the equation $F(x,\ldots,x) = x$. Simple examples include any lattice. This question was asked by A. Tarski in the middle of the 20th century and have been a challenging problem ever since (especially for algebras with more than one operation). Earlier we showed that this claim holds for finite lattices and for finite idempotent congruence-modular algebras.

Even for the simple case of idempotent groupoids the problem remains unsolved. None of the earlier techniques seems to be easily adapted to solve this problem. This chapter concentrates on the only major result known in this area regarding idempotent semigroups. Our first objective is to recreate the beautiful theory found in Mckenzie's paper [Mck72]. After that we apply these results to prove that every finite idempotent semigroup, that is an algebraic structure with a binary operation $+$ where the identities $(x+y)+z = x+(y+z)$ and $x+x = x$ are both true, has the refinement property.

6.1 More refinement results

The method introduced in this section is based on older refinement theory invented by Chang, Jónsson and Tarski in [Cha61],[Cha67],[CJT], [Jon66] and [JT47]. This was later improved by Mckenzie in [Mck68] and [Mck71]. The main consequence of this section is Theorem 6.1.13. However to understand this important refinement result we have to introduce some new definitions. We define the concept of the product of two classes of algebraic structures of the same type and the idea of D-ideals.

Definition 6.1.1. A class K of algebras (of the same similarity type) is said to be **algebraic** if for each of its members, it contains every structure isomorphic to it. □

Definition 6.1.2. By $A[B]$ we mean the **substructure** B of algebra A. By (A,R) we mean the **expansion** of structure A, by adding one more fundamental relation R to it. If $A \simeq B \times C$ then we say B is a **direct factor** of A and we denote this by $B \parallel A$. Lastly, let $DF(A)$ be the set of all decomposition functions on algebra A, as explained in Definition 4.1.5. □

For the following definition we assume K, K_1 and K_2 are non-empty algebraic classes of algebras of some fixed type such that $K_1 \cup K_2 \subseteq K$ and class K is closed under the operations of taking direct factors of an algebra and the direct product of two algebras.

Definition 6.1.3. We write $K = K_1 \times K_2$ if the following are all true:

(1) Suppose $A \simeq \prod_{i\in I} A_i$ and $A \in K$. Then $A \in K_j$ iff for all $i \in I, A_i \in K_j$, for $j = 1$ or $j = 2$.

(2) Whenever $A \in K$, there are algebras $k_1A \in K_1$ and $k_2A \in K_2$ such that $A \simeq k_1A \times k_2A$. Furthermore if $A \simeq A_1 \times A_2$ and $A_1 \in K_1, A_2 \in K_2$ then $A_1 \simeq k_1A$ and $A_2 \simeq k_2A$.

When this happens we say that K_1, K_2 are **complementary factor classes** of K. Note k_1 can be considered as a map from K to K_1 and k_2 as a map from K to K_2. □

Corollary 6.1.4. *Let $K = K_1 \times K_2$. If $A \in K$ and $A \simeq \prod_{i\in I} A_i$ then $k_jA \simeq \prod_{i\in I} k_jA_i$ for $j = 1$ or $j = 2$.*

Proof. The following calculation establishes this fact.

$$\begin{aligned} A &\simeq k_1A \times k_2A, \\ A &\simeq \prod_{i\in I} k_1A_i \times \prod_{i\in I} k_2A_i. \end{aligned}$$

□

Corollary 6.1.5. *Let $K = K_1 \times K_2$. Then K_1 and K_2 are both closed under finite products and direct factors. Furthermore, if $A \in K$ then $A \in K_j \iff k_jA \simeq A \iff k_{3-j}A \simeq 1$ for $j = 1, 2$.*

Proof. The first observation is clear and hence we conclude $1 \in K \cap K_1 \cap K_2$. The second observation is now immediate from the fact that $A \simeq 1 \times A$. □

Corollary 6.1.6. *Let $K = K_1 \times K_2$ and $A \in K$. Then A has the refinement property iff both k_1A and k_2A have the refinement property.*

Proof. Obvious from definitions and the fact that $A \simeq k_1A \times k_2A$. □

Next we introduce the notion of D-ideals.

Definition 6.1.7. Let $\triangle(A)$ be the class of relations R over algebraic structure A such that every direct product decomposition

$$A \simeq \prod_{i\in I} A_i$$

can be expanded to

$$(A, R) \simeq \prod_{i\in I} (A_i, R_i)$$

for some relation $(R_i)_{i\in I}$ with the same rank as R. □

By definition it follows that $\triangle(A)$ always includes all the fundamental operations and relations. It is also closed under most basic set-theoretic operations on relations: intersection, permutation of variables, directed union of finitary relations, etc. Lastly whenever the relations on the algebra are such that only the trivial decomposition exists then every relation over A belongs to $\triangle(A)$. In the following definition we use notation g_x, f_x, g_y as explained in Definition 4.1.5.

Definition 6.1.8. Let A be some structure. By a **D-equivalence** of structure A we mean an equivalence relation E that belongs to $\triangle(A)$ such that for any $f, g \in DF(A)$ and any elements $x, y \in A$ we have

$$xEg_xf_xg_yx.$$

By a **D-ideal** we mean a set U that is of the form $U = x/E$ for some $x \in A$ and D-equivalence E. □

Lemma 6.1.9. *Let $A \overset{\phi}{\simeq} A_1 \times A_2$ and U be any D-ideal of A. Then there exist D-ideals U_1 in A_1 and U_2 in A_2 such that*

$$(A, U) \overset{\phi}{\simeq} (A_1, U_1) \times (A_2, U_2)$$

and consequently

$$A[U] \overset{\phi}{\simeq} A_1[U_1] \times A_2[U_2].$$

Proof. Say $\phi(x) = (x_1, x_2)$ and $U = x/E$ for some D-equivalence E. Setting $U_1 = x_1/E_1$ and $U_2 = x_2/E_2$ works, where the D-equivalence E splits into E_1 and E_2. □

Lemma 6.1.10. *Let $U = \bigcap\{U_t : t \in T\}$ where each U_t is a D-ideal of A for all $t \in T$. Then U is a D-ideal in A if it is non-empty.*

Proof. Let $U_t = x_t/E_t$ for some D-equivalences E_t. If $x \in \bigcap\limits_{t\in T} U_t$ and $E = \bigcap\limits_{t\in T} E_t$ then $U = x/E$. □

Theorem 6.1.11. *Suppose A is a structure with U as a D-ideal. Also assume that*

$$A \overset{\psi}{\simeq} \prod_{i\in I} A_i \overset{\phi}{\simeq} \prod_{j\in J} B_j.$$

Then there exist algebraic structures $C_i, D_j, A_{i,j}, B_{i,j}$ (for all $i \in I, j \in J$) satisfying the following conditions for all $i \in I$ and $j \in J$:

$$\begin{aligned} C_p \parallel A[U] \quad & \textit{and} \quad D_q \parallel A[U], \\ \phi(C_p \times A_p) \quad &= \quad \prod_{j\in J} B_{p,j}, \\ \phi^{-1}(D_q \times B_q) \quad &= \quad \prod_{i\in I} A_{i,q}, \\ \phi(C_p \times A_{p,q}) \quad &= \quad D_q \times B_{p,q}. \end{aligned}$$

Proof. By definition there is a D-equivalence E on structure A and an element $x \in A$ such that $U = x/E$. From the fact that $E \in \triangle(A)$ there are unique equivalence relations E_i, F_j such that

$$(A, E) \overset{\psi}{\simeq} \prod_{i\in I} (A_i, E_i) \overset{\phi}{\simeq} \prod_{j\in J} (B_j, F_j).$$

Let $\psi(x) = (a_i)_{i\in I}$ and $\phi(\psi(x)) = (b_j)_{j\in J}$. Then we have

$$A[U] \overset{\psi}{\simeq} \prod_{i\in I} A_i[a_i/E_i] \overset{\phi}{\simeq} \prod_{j\in J} B_j[b_j/F_j].$$

Now put

$$\begin{aligned} C_p \quad &= \quad \prod_{i\in I-\{p\}} A_i[a_i/E_i], \\ D_q \quad &= \quad \prod_{j\in J-\{q\}} B_j[b_j/F_j]. \end{aligned}$$

Hence the first condition of the theorem follows readily. To satisfy the middle two conditions we are forced to define $B_{p,j}$ as the j-th image of $\phi(C_p \times A_p)$, a substructure of B_j. Likewise let

$A_{i,q}$ be the i-th projection of $\phi^{-1}(D_q \times B_q)$. The last formula follows immediately if we prove that the middle two hold, since $\phi(C_p \times A_{p,q})_q \subseteq \phi(C_p \times A_p)_q \subseteq B_{p,q}$. By symmetry we only need to prove the first formula. By definition we already have $\phi(C_p \times A_p) \subseteq \prod_{j\in J} B_{p,j}$. So it suffices to show that

$$\psi^{-1}\phi^{-1}(\prod_{j\in J} B_{p,j}) \subseteq \psi^{-1}(C_p \times A_p).$$

This can be stated in terms of decomposition functions. For a fixed $p \in I$ define $f \in DF(A)$ as follows:

$$\psi(f(x,y))_i = \begin{cases} \psi(x)_i & \text{for } i \neq p; \\ \psi(y)_p & \text{for } i = p. \end{cases}$$

For each $j \in J$ define $g^j \in DF(A)$ as follows:

$$\phi\psi(g^j(x,y))_{j'} = \begin{cases} \phi\psi(x)_j & \text{for } j' = j; \\ \phi\psi(y)_{j'} & \text{for } j' \neq j. \end{cases}$$

So the second condition is equivalent to showing for every $y \in A$ such that for all $j \in J$ there exists u_j satisfying $f_{x_0}g^j(y,u_j)Ex_0$ then $f_{x_0}yEx_0$. From $f_{x_0}g^j(y,u_j)Ex_0$ it follows that $f_y g^j(y,u_j)Ef_y x_0$ since $f_y f_{x_0} = f_y$. By the fact that E is a D-equivalence we have for all $j \in J$ that

$$yEg^j_y f_y g^j(y,u_j)Eg^j_y f_y x_0.$$

By definition of the decomposition functions we have $yEg^j_y f_y x_0$ for all $j \in J \iff yEf_y x_0 \iff f_{x_0}yEx_0$ as desired. □

Theorem 6.1.12. *Let $A \in K$ and $K = K_1 \times K_2$. If A has a D-ideal U such that $A[U] \in K_1$ then k_2A has the refinement property.*

Proof. Note $A[U] \simeq A_1[U_1] \times A_2[U_2]$ for some D-ideals U_1, U_2 and $A_2[U_2] \in K_1$. So we may safely assume $A \in K_2$ and deduce the refinement property. Suppose

$$A \simeq \prod_{i\in I} A_i \simeq \prod_{j\in J} B_j.$$

By Theorem 6.1.11 there are structures such that

$$\begin{aligned} C_p \times A_p &\simeq \prod_{j\in J} B_{p,j}, \\ D_q \times B_q &\simeq \prod_{i\in I} A_{i,q}, \\ C_p \times A_{p,q} &\simeq D_q \times B_{p,q}. \end{aligned}$$

Then all $C_p, D_q \in K_1$ and hence $k_2C_p \simeq 1 \simeq k_2D_q$. From the fact that $A \in K_2$ it follows that $k_2A_p \simeq A_p$ and $k_2B_q \simeq B_q$. Applying the k_2 operator to the above formulas we obtain the common refinement:

$$\begin{aligned} A_p &\simeq \prod_{j\in J} k_2B_{p,j}, \\ B_q &\simeq \prod_{i\in I} k_2A_{i,q}, \\ k_2A_{p,q} &\simeq k_2B_{p,q}. \end{aligned}$$

□

Theorem 6.1.13. *Let $K = K_1 \times K_2$. Assume that each member of K_1 has the refinement property and every $A \in K_2$ has a D-ideal such that $A[U] \in K_1$. Then every member of K possesses the refinement property.*

Proof. Let $A \in K$. Then $A \simeq k_1A \times k_2A$. Thus $k_1A \in K_1$ and has the refinement property. By Theorem 6.1.12 we know that k_2A also has the refinement property. □

Next we provide a few examples of D-ideals. We conclude this section by providing a way of producing many more D-ideals.

Example 6.1.14.

- The centre of any group or center of any ring is a D-ideal.
- Suppose $(A, \cdot)$ is a binary algebra with an element $a \in A$ such that $ax = xa$ for all $x \in A$. Then the set of all such "central elements" forms a D-ideal with the corresponding D-equivalence E where $xEy \iff$ for all z the relations $xz = zx$ and $yz = zy$ are equivalent.
- Suppose $(A, \cdot)$ is a binary algebra with an element $u \in A$ such that $ux = u = xu$ for all x. Then the set of all elements y such that $xy = u = yx$ forms a D-ideal with the corresponding D-equivalence E where $xEy \iff \forall z[xz = u \iff yz = u$ and $zx = u \iff zy = u]$.

Definition 6.1.15. For any α-ary relation S (where α is an ordinal) on a set A we define the quasi-identity relation $\approx_S$ on A as follows : $u \approx_s v$ iff for every ordinal $0 \leq \delta < \alpha$ the formulas $S(x(\delta/u))$ and $S(x(\delta/v))$ are equivalent. ($x(\delta/z)$ is the sequence obtained by replacing the δ^{th} term x_δ by z in sequence x.) □

Definition 6.1.16. Let S be any α-ary relation on a set A. We say that relation S is **special** if it is possible to partition α into two disjoint sets, ie. $\alpha = I \cup J$ so that both binary relations $S_I = S_\star|\breve{S}_\star$ and $S_J = \breve{S}_\star|S_\star$ are connected over A^I and A^J respectively. We write $S_\star(x, y)$ with $x \in A^I$ and $y \in A^J$ to mean $x \cup y$ and $\breve{S}_\star$ to mean $y \cup x$ where $y \in A^J$ and $x \in A^I$. □

Example 6.1.17. In the second example the equivalence E is $\approx_S$ where S is the special binary relation $S(x_0, x_1)$ iff $x_0x_1 = x_1x_0$. In the third example the equivalence E is $\approx_S$ where S is the special binary relation $S(x_0, x_1)$ iff $x_0x_1 = u$.

As a consequence of the next result, it follows immediately that both these quasi-identity relations defined in the previous examples are D-equivalences. This result will be stated without proof as some undeveloped machinery is needed.

Theorem 6.1.18. *Let A be a structure and assume that S is a special relation over A and that $S \in \triangle(A)$. Then $\approx_S$ is a D-equivalence on A. Furthermore for all $f, g \in DF(A)$ and for all $x, y \in A$ we have*

$$f_x g_x y \approx_s g_x f_x y.$$

It should be noted that it is clear that $\approx_S$ is an equivalence and belongs to $\triangle(A)$. Also $y = f_y g_y g_x y \approx_S g_y f_y g_x y$ (if the final part of theorem is true). Thus $\approx_S$ is a D-equivalence. A similar result can be found in [Mck71].

6.2 Applications to semigroups

This section is completely devoted to idempotent semigroups, that is a semigroup satisfying the identity $x+x=x$. They are also labelled as **bands** in literature by Clifford and Preston in [Cli61]. We use the theory developed in the previous section to yield a result that will show why every finite band is uniquely factorable. To achieve this goal, we need the following equivalence relation to produce D-ideals.

Definition 6.2.1. For every band A we define the congruence $\approx_A$ as the relation $a \approx b \iff \forall x, y \in A$ we have $x+a+y = x+b+y$. □

Note brackets are not needed in the definition due to associativity. Next we show the importance of this equivalence relation.

Lemma 6.2.2. *If A is a band then $\approx_A$ is a D-equivalence.*

Proof. Let S be the ternary relation such that $S(x_0, x_1, x_2) \iff x_0 + x_1 + x_2 = x_0 + x_2$. By definition we have $S \in \triangle(A)$. Next we show that S is special with $\alpha = 3, I = \{1\}$ and $J = \{0, 2\}$. Now S_I is the relation over A where

$$S_I(x, y) \iff \exists u, v \text{ such that } u + x + v = u + v \text{ and } u + y + v = u + v.$$

From idempotency we have $x + x + y = x + y = x + y + y$ and conclude that S_I is indeed connected. Now S_J is the binary relation on A such that

$$S_J(x, y) \iff \exists u \text{ such that } x_0 + u + x_1 = x_0 + x_1 \text{ and } y_0 + u + y_1 = y_0 + y_1.$$

From the fact that $S_J(x, (x_0, y_1))$ and $S_J((x_0, y_1), y)$ we see that S_J is also connected. So by Theorem 6.1.18 it follows immediately that $\approx_S$ is a D-equivalence. It turns out that $\approx_S$ and $\approx_A$ are equal and hence the result follows. (For the harder part assume (u, v) lies in $\approx_S$. Thus $u + v + u = u$. Next a simple calculation shows $x + v = x + v + v = x + u + v$ and $v+y = v+v+y = v+u+y$. Finally we obtain $x+v+y = (x+u+v)+v+(v+u+y) = x+u+y$, giving (u, v) lies in $\approx_A$.) □

This naturally leads to the known concept of a **rectangular band**: That is, an idempotent semigroup satisfying the identity $x + y + z = x + z$ for all $x, y, z \in A$. Also note that if U is a D-ideal of the D-equivalence $\approx_A$ then $A[U]$ is a rectangular band. It should be mentioned that not all rectangular bands have the refinement property, but shortly we will see that finite rectangular bands however does.

Definition 6.2.3. $\mathfrak{B}^{\square}$ is the class consisting of all finite rectangular bands.
$\mathfrak{B}^r$ is the class of all finite right-zero semigroups, ie. those satisfying the identity $x + y = y$.
$\mathfrak{B}^l$ is the class of all finite left-zero semigroups, ie. those satisfying the identity $x + y = x$.
$\mathfrak{B}$ is the class of all bands A such that at least one of the structures $A[U]$ (where U is an $\approx_A$-coset) is finite.
$\mathfrak{B}^\star$ is the class of all $A \in \mathfrak{B}$ such that every direct factor belonging to $\mathfrak{B}^{\square}$ is isomorphic to 1, the trivial band with one element. □

Definition 6.2.4. Suppose $A \in \mathfrak{B}$.

(i) Define $\theta^l(A)$ to be the smallest congruence θ on A such that A/θ is a left-zero semigroup. Analogously $\theta^r(A)$ is the smallest congruence θ on A such that A/θ is a right-zero semigroup.

(ii) Let $P, Q \in A/\theta^l(A)$. We write $P \overset{l}{\simeq} Q$ if there is a bijection $\phi : P \longrightarrow Q$ satisfying

both $y + \phi(x) = y + x$ and $\phi(x + y) = \phi(x) + y$ for all $x \in P$ and $y \in A$. Analogously for $P, Q \in A/\theta^r(A)$ we write $P \overset{r}{\simeq} Q$ if there is a bijection $\phi : P \longrightarrow Q$ such that $\phi(x) + y = x + y$ and $\phi(y + x) = y + \phi(x)$ for all $x \in P$ and $y \in A$.

(iii) We define $l(A)$ to be the largest cardinal that divides the cardinals of the sets $\{Q \in A/\theta^l(A) : P \overset{l}{\simeq} Q\}$. Analogously $r(A)$ is the largest cardinal that for each $P \in A/\theta^r(A)$ divides the cardinals of the sets $\{Q \in A/\theta^r(A) : P \overset{r}{\simeq} Q\}$ for each $P \in A/\theta^l(A)$.

(iv) Lastly, define $\chi(A)$ to be the pair of cardinals $(l(A), r(A))$. □

Lemma 6.2.5. *For each $A \in \mathfrak{B}, \chi(A)$ is a pair of positive integers.*

Proof. By definition we know there is a finite $\approx_A$-coset U. Choose $P_l \in A/\theta^l(A)$ and $P_r \in A/\theta^r(A)$ meeting U. If $P_l \overset{l}{\simeq} Q$ or $P_r \overset{r}{\simeq} Q$ then $x \approx_A \phi(x)$ for each x in the domain of ϕ. Hence Q also meets U and both the sets $\{Q : P_l \overset{l}{\simeq} Q\}$ and $\{Q : P_r \overset{r}{\simeq} Q\}$ are finite. □

Before we give a classical result about finite bands, we need the following definition.

Definition 6.2.6. For each positive integer n let L_n be a fixed left-zero semigroup and R_n be a fixed right-zero semigroup each with a n-element subuniverse. □

Lemma 6.2.7. *Let $A \in \mathfrak{B}^\square$ and m, n are positive integers. Then $\chi(L_m \times R_n) = (m, n)$ and $\chi(A) \simeq L_m \times R_n$ iff $\chi(A) = (m, n)$.*

Proof. Suppose $A \overset{\psi}{\simeq} L_m \times R_n$. Now $\theta^l(A)$ is generated by the pairs $\{(x, x + y) : x, y \in A\}$. It follows trivially that $\theta^l(A)(x, y)$ iff $\psi(x)$ and $\psi(y)$ have the same first component. Thus $\psi(x/\theta^l(A)) = \{a\} \times R_n$ where a is the first component of $\psi(x)$. Select $x, y \in L_m$ and let $\phi : x/\theta^l(A) \longrightarrow y/\theta^l(A)$ such that $\phi(x, a) = (y, a)$. Then it follows that $(c, d) + \phi(x, b) = (c, d) + (x, b)$ and $\phi((x, b) + (c, d)) = \phi(x, b) + (c, d)$. Therefore $x/\theta^l(A) \overset{l}{\simeq} y/\theta^l(A)$ and hence $l(A) = m$. In a similar fashion we can show $r(A) = n$.

For the reverse direction suppose $A \in B^\square$ an select and element $e \in A$. Then we define

$$\begin{aligned} A^l &= \{x + e : x \in A\}, \\ A^r &= \{e + x : x \in A\}. \end{aligned}$$

From $(x+e)+(x'+e) = x+(e+x'+e) = x+(e+e) = x+e$ we see that A^l is indeed a left-zero semigroup. In a similar fashion we can show that A^r is a right-zero semigroup. Next we show $A \overset{\phi}{\simeq} A^l \times A^r$ where $\phi(x) = (x+e, e+x)$. Noting $(x+e)+(y+e) = (x+e+y)+e = x+y+e$ and $(e+x)+(e+y) = e+(x+e+y) = e+x+y$ it follows that ϕ is indeed a homomorphism. If $\phi(x) = \phi(x')$ then $x+e = x'+e$ and $e+x = e+x'$. Hence $x = (x+e)+(e+x) = (x'+e)+(e'+x) = x'$. Surjectivity follows from the fact that $\phi(x + y) = (x + y + e, e + x + y) = (x + e, e + y)$. Hence ϕ is an isomorphism. Lastly suppose $\chi(A) = (m, n)$. If $A \simeq L_t \times R_s$ (such a decomposition exists by the previous paragraph) then $\chi(A) = (t, s) = (m, n)$. Thus $t = m$ and $s = n$ and the result follows. □

Lemma 6.2.8. *If $A, B \in \mathfrak{B}$ then $\chi(A \times B) = \chi(A) \times \chi(B)$. That is $l(A \times B) = l(A) \times l(B)$ and $r(A \times B) = r(A) \times r(B)$.*

Proof. We proof this for 'left' numbers as the proof for 'right' numbers is dual. We start by showing

$$\theta^l(A \times B) = \theta^l(A) \times \theta^l(B).$$

$\theta^l(A \times B)$ is the congruence generated by all the pairs $\{(x, x+y) : x, y \in A \times B\}$. So all the pairs $\{(a,b),(a+c,b) : a, c \in A \text{ and } b \in B\}$ and $\{(a,b),(a,b+d) : a \in A \text{ and } b, d \in B\}$ generates it. The set of these pairs turns out to be a generating set for $\theta^l(A) \times \theta^l(B)$. Therefore there is a natural isomorphism

$$\sigma : (A/\theta^l(A) \times B/\theta^l(B)) \simeq (A \times B)/\theta^l(A \times B)$$

where $\sigma(P,Q) = P \times Q$ with $P \in A/\theta^l(A)$ and $Q \in B/\theta^l(B)$. Next we show if $P_1, P_2 \in A/\theta^l(A)$ and $Q_1, Q_2 \in B/\theta^l(B)$ then $P_1 \times Q_1 \overset{l}{\simeq} P_2 \times Q_2$ in $A \times B$ iff $P_1 \overset{l}{\simeq} P_2$ in A and $Q_1 \overset{l}{\simeq} Q_2$ in B. From this we conclude the result for 'left' numbers using a simple combinatorial argument.

The "if" part is clear. For the converse suppose $\phi : P_1 \times Q_1 \overset{l}{\simeq} P_2 \times Q_2$. We will show there exist maps $f : P_1 \longrightarrow P_2$ and $g : Q_1 \longrightarrow Q_2$ such that $\phi(a,b) = (f(a), g(b))$ when $a \in P_1$ and $b \in Q_1$. In so doing we get $f : P_1 \overset{l}{\simeq} P_2$ and $g : Q_1 \overset{l}{\simeq} Q_2$. To establish this we need to show $\phi(a,b)$ and $\phi(a,b')$ have the same first part. Also $\phi(a,b)$ and $\phi(a',b)$ have the same second part where $a, a' \in P_1$ and $b, b' \in Q_1$. Suppose $a \in A$ and $b, d \in B$. If $\phi(a,b) = (u,v)$ then

$$\phi(a,b) = \phi((a,b) + (a,b)) = \phi(a,b) + (a,b) = (u+a, v+b)$$

and

$$\phi(a,b+d) = \phi((a,b) + (a,d)) = \phi(a,b) + (a,d) = (u+a, v+d).$$

Hence $\phi(a,b)$ and $\phi(a,b+d)$ share the same first part. Noting that Q_1 is connected under the relation $\{(b,b+d) : b \in Q_1 \text{ and } d \in A\}$ it follows that for any $a \in P_1$ and $b, b' \in Q_1$ that $\phi(a,b)$ and $\phi(a,b')$ share the same first part. In a similar way we can show if $a, a' \in P_1$ and $b \in Q_1$ that $\phi(a,b)$ and $\phi(a',b)$ have the same second part. □

Lemma 6.2.9. *Suppose $A \in \mathfrak{B}^\square$ and $C, D \in \mathfrak{B}$. If $A \times C \simeq A \times D$ then $C \simeq D$.*

Proof. By Lemma 6.2.7 it is enough to show it holds for $A = L_m$ and $A = R_n$ where m and n are positive integers. We assume the former (the proof for the latter is similar); that is, $\phi : L_m \times C \simeq L_m \times D$. By Lemma 6.2.8 we have a natural isomorphism

$$\sigma : L_m \times C/\theta^l(C) \simeq L_m \times D/\theta^l(D)$$

where $\sigma(x,P) = (y,Q)$ iff $\phi(\{x\} \times P) = \{y\} \times Q$ since $L_m \simeq L_m/\theta^l(L_m)$. Using this isomorphism we have two ways of partitioning $L_m \times C/\theta^l(C)$ into m-element subsets. Firstly put (x_1, P_1) and (x_2, P_2) into the same class if $P_1 = P_2$. For the second way put (x_1, P_1) and (x_2, P_2) in the same class if $\sigma(x_1, P_1)$ and $\sigma(x_2, P_2)$ have the same second component. By a result of De Bruijn [Bru47] there exists a common selector set $T \subseteq L_m \times C/\theta^l(C)$, that is for each partition, T has exactly one member from each class.

Note if $b \in C$ then there is an unique $x \in L_m$ and $P \in C/\theta^l(C)$ such that $b \in P$ and $(x,P) \in T$. Define $\psi : C \longrightarrow D$ such that $\psi(b)$ is the second part of $\phi(x,b)$ where $x \in L_m$ and $b \in P \in C/\theta^l(C)$ and $(x,P) \in T$. This map turns out to be the desired isomorphism. □

Lemma 6.2.10. *If $A \in \mathfrak{B}$ and $\chi(A) = (m,n)$, then there exists $B \in \mathfrak{B}^\star$ such that $A \simeq L_m \times R_n \times B$. Moreover if $A \simeq C \times D$ where $C \in \mathfrak{B}^\square$ and $D \in \mathfrak{B}^\star$ then $C \simeq L_m \times R_n$ and $D \simeq B$.*

Proof. We start off by showing if $A \in \mathfrak{B}$ and $l(A) = m$ then $L_m \parallel A$. By definition of $l(A)$ there is a set $T \subseteq A/\theta^l(A)$ and a bijective map

$$\sigma : L_m \times T \longrightarrow A/\theta^l(A)$$

such that $\sigma(x,p) \overset{l}{\simeq} P$ for all $x \in L_m$ and all $P \in T$. Let $B = A[\cup T]$ be a subalgebra of A, where $\cup T$ is the set containing all the elements of A used in T. For each pair $(x,P) \in L_m \times T$ choose $\phi_{(x,P)} : P \overset{l}{\simeq} \sigma(x,P)$. Then the map $\phi : L_m \times B \longrightarrow A$ defined by

$$\phi(x,y) = \phi_{(x,P)}(y)$$

for $x \in L_m$ and $y \in P \in T$ is a bijection. In fact this map is an isomorphism. Dually we can show if $A \in \mathfrak{B}$ and $r(A) = n$ then $R_n \parallel A$. From these results it follows that if $B \in \mathfrak{B}$ then $B \in \mathfrak{B}^\star$ iff $\chi(B) = (1,1)$.

To finish the proof suppose $A \in \mathfrak{B}$ and $\chi(A) = (m,n)$. Thus there exists $B' \in \mathfrak{B}$ such that $A \simeq L_m \times B$ and $\chi(B') = (1,n)$. Also $B' = R_n \times B$ where $B \in \mathfrak{B}^\star$. Hence $A \simeq L_m \times R_n \times B$ where $B \in \mathfrak{B}^\star$. Finally, suppose $A \simeq C \times D$ with $C \in \mathfrak{B}^\square$ and $D \in \mathfrak{B}^\star$. By Lemma 6.2.8 we have $\chi(C) = (m,n)$ and hence $C \simeq L_m \times R_n$. By Lemma 6.2.9 we obtain $B \simeq D$. □

Lemma 6.2.11. *Assume $A \in \mathfrak{B}$ and $A \simeq \prod_{i\in I} A_i$. Then $A \in \mathfrak{B}^\square$ iff $A_i \in \mathfrak{B}^\square$ for all $i \in I$. Likewise $A \in \mathfrak{B}^\star$ iff $A_i \in \mathfrak{B}^\star$ for all $i \in I$.*

Proof. The only part that does not follow immediately is to show that if $A_i \in \mathfrak{B}^\star$ for all $i \in I$ then $A \simeq \prod_{i\in I} A_i \in \mathfrak{B}^\star$. To prove this we use the the fact that A contains a finite $\approx$-coset. Hence there is a finite set $F \subseteq I$ such that

$$B = \prod_{i \in I-F} A_i$$

has a 1-element $\approx$-coset. If $B \simeq C \times D$ and $C \in \mathfrak{B}^\square$ and $|C| > 1$ then every $\approx$-coset of B would have more than 1 element. Therefore $B \in \mathfrak{B}^\star$ and

$$\begin{aligned} A &\simeq B \times \prod_{i\in F} A_i \\ \chi(A) &= \chi(B) \times \prod_{i\in F} \chi(A_i). \end{aligned}$$

So $\chi(A) = (1,1)$ and $A \in \mathfrak{B}^\star$. □

Theorem 6.2.12. *Each of $\mathfrak{B}^\square, \mathfrak{B}^r, \mathfrak{B}^l, \mathfrak{B}$ and $\mathfrak{B}^\star$ is an algebraic class which is closed under finite direct products and direct factors. Furthermore $\mathfrak{B} = \mathfrak{B}^\square \times \mathfrak{B}^\star$ and $\mathfrak{B}^\square = \mathfrak{B}^l \times \mathfrak{B}^r$.*

Proof. Follows immediately from Lemma 6.2.7, Lemma 6.2.10 and Lemma 6.2.11. □

Now we have the necessary tools to prove the following theorem [Mck72] which trivally explains why every finite band is uniquely factorable.

Theorem 6.2.13. *If A is a band with one of its $\approx_A$-cosets finite then A has the refinement property.*

Proof. Clearly a finite left-zero or right-zero semigroup has the refinement property. Also each $A \in \mathfrak{B}$ has a D-ideal U satisfying $A[U] \in \mathfrak{B}^\square$. So by Theorem 6.1.12 it follows that $\mathfrak{B}$ has the refinement property. □

Corollary 6.2.14. *Every finite band has the unique factorization property.*

Chapter 7

Other related properties

In this chapter we divert our attention from studying unique factorization properties to investigating related factorization properties. Our main focus will be on the following three implications (for some positive integer k). These fundamental questions concerning direct products were raised for groups, boolean algebras and arbitrary structures by Sikorski [Sik48], Tarski [Tar48, Tar49] and Kaplanski [Kap54] respectively.

$$\begin{aligned} A^k \simeq B^k &\implies A \simeq B, \\ A \times C \simeq B \times C &\implies A \simeq B, \\ A \simeq A \times B \times C &\implies A \simeq A \times B. \end{aligned}$$

If A^k or $A \times C$ has the unique factorization property then the first two implications are trivially true. However these three conclusions do not generally hold for infinite algebras[1]. This chapter will showcase conditions when it does occur. Even the cancellation property may fail for infinite or finite algebras as demonstrated with these examples:

Example 7.0.15. Let $A = \mathbb{Z}_2$ and $B = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots$ be two abelian groups. It is clear that $A \times B \simeq B^2$ but $A \not\simeq B$.

Example 7.0.16. Let A and B be algebras with the same underlying set $\{a, b\}$ and unary functions f and g respectively such that $f(a) = g(b) = a$ and $f(b) = g(a) = b$. A simple calculation shows $A \times B \simeq B^2$, but $A \not\simeq B$.

Suprisingly Lovász [Lov67] showed that the first implication holds for any finite structure. He furthermore showed the cancellation law (which prominently features in many unique factorization results) holds whenever C has an one-element subuniverse. We follow this beautiful counting argument in the first section. The second section contains ideas from equational theory to prove these results in a fresh, maybe more enlightening way. The third section, like Mckenzie [Mck71], concentrates on denumerable structures (that is finite or countably infinite structures). Using simple set theory arguments we prove that whenever B or C is finite then the third implication follows. As a fitting end to this chapter, we use a result established twice here to produce another unique factorization theorem for certain varieties.

7.1 kth roots and cancellation

The main goal of this section is to show that whenever A and B are finite structures then $A^k \simeq B^k \implies A \simeq B$ if k is some positive integer. We proceed by modifying the arguments

[1] See [Jon57] for groups and [Han57, Kin53] for Boolean algebras.

found in [Lov67, Lov71] by showing these results holds in certain important categories. This is motivated by the next definition and example. Lastly some attention is paid to cancellation results.

Definition 7.1.1. We call a category $\mathbb{L}$ a **Lovász category** if it closed under products, closed under pullbacks, for all objects A and B the set $hom(A, B)$ is finite, each morphism up to isomorphism has an unique epi-mono factorization and if $f : A \longrightarrow A$ is a monomorphism or epimorphism then f is an isomorphism and lastly the collection of non-isomorphic objects forms a set with some ordinal (that is it is not a proper class). Let $1_{\mathbb{L}}$ denote the terminal object of this category. □

Example 7.1.2. Let $\mathbb{C}$ be a category of all the finite algebraic structures of a given similarity type (that is they have the same fundamental operations). It is easily shown (or see [Mac]) that this is a simple way of producing a plethora of Lovász categories using universal algebras.

The next lemma is crucial and gives a connection between homomorphisms and monomorphisms in Lovász categories.

Lemma 7.1.3. *For a fixed object B in Lovász category $\mathbb{L}$ we have that the system of cardinals $\{|hom(A, B)| : A \in \mathbb{L}\}$ is determined by the system of cardinals $\{|mono(A, B)| : A \in \mathbb{L}\}$, that is if you know all the cardinals $hom(A, B)$ you can determine all the cardinals $mono(A, B)$. The converse is also true, that is if you know all the cardinals $mono(A, B)$ you can determine all the cardinals $hom(A, B)$.*

Proof. First recall that every homomorphism $f : A \longrightarrow B$ factors uniquely as

$$A \xrightarrow{e} C \xrightarrow{m} B,$$

where e is an epimorphism and m is an embedding. Thus it follows that

$$|hom(A, B)| = \sum_{e:A\to C, e \text{ is epi}} |mono(C, B)|. \tag{7.1}$$

Next we define the order $C \prec A$ if there is an epimorphism from object A to object C. It is certainly clear this order is a partial order and the least element is the terminal object. Hence doing induction on this partial order will complete the proof. For the converse, rewrite equation (7.1) as

$$|mono(A, B)| = |hom(A, B)| - \sum_{C \text{ is an epi-image of } A, C\neq A} |mono(C, B)|.$$

Again by induction on $|A|$ the result follows. □

Therefore in the case where $\mathbb{L}$ is the category of finite structures of a fixed type we conclude that for every finite structure A there exists integers $\mu_\theta(\theta \in Con\, A)$ such that for all finite structures B of the same type

$$|mono(A, B)| = \sum_{\theta\in Con\, A} \mu_\theta |hom(A/\theta, B)|.$$

It is interesting to observe that these integers μ_θ depend only on the congruence lattice and the procedure[2] to extract them is known as **Möbius inversion**.

[2] See [Gra].

For a given Lovász category $\mathbb{L}$, let $\{A_i : i < \alpha\}$ be a collection of all structures $in\mathbb{L}$ up to isomorphism for some ordinal α. Now for any object B we define $h_i(B) = |hom(A_i, B)|$. Finally, let $h(B)$ be the entire sequence $\{h_i(B) : i < \alpha\}$ of cardinals. Now we are ready to prove our first major result which will assist in solving the problems posed in the beginning.

Theorem 7.1.4. *Let $\mathbb{L}$ be a Lovász category with objects A and B.*

(i) $h(A) = h(B) \iff A \simeq B$.

(ii) For all $i < \alpha$ we have $h_i(A \times B) = h_i(A) \times h_i(B)$.

(iii) If $hom(1_{\mathbb{L}}, A) > 0$ then $h_i(A) > 0$ for all $i < \alpha$.

Proof. For the first part, note that by definition h is isomorphism invariant, that is $A \simeq B$ implies $h(A) = h(B)$. On the other hand if $h(A) = h(B)$ then by Lemma 7.1.3 $mono(A, B) = mono(A, A) \geq 1$. In a similar fashion we can show $mono(B, A) \geq 1$. Therefore $A \simeq B$. Part (ii) is immediate from the categorial definition of products. For part (iii) recall $1_{\mathbb{L}}$ is a terminal object, ie. $hom(A_i, 1_{\mathbb{L}}) = 1$ for all $i < \alpha$. □

Corollary 7.1.5. *Suppose A, B, C and D are objects of Lovász category $\mathbb{L}$.*

(i) If k is a positive integer and $A^k \simeq B^k$ then $A \simeq B$.

(ii) If there is a homomorphism from D to C and $A \times C \simeq B \times C$ then $A \times D \simeq B \times D$.

(iii) If $hom(1_{\mathbb{L}}, C) > 0$ and $A \times C \simeq B \times C$ then $A \simeq B$.

Proof. (i) Using universal properties of products we have for any ordinal i that $(h_i(A))^k = h_i(A^k) = h_i(B^k) = (h_i(B))^k$. Thus $h_i(A) = h_i(B)$ for all ordinals i. Hence $A \simeq B$ by Theorem 7.1.4.

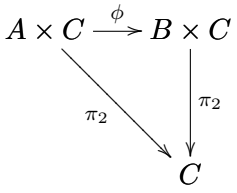
(ii) Note $h(D, C) > 0$ implies $h_i(D) = 0$ if $h_i(C) = 0$. By part (ii) of Theorem 7.1.4 we have $h_i(A).h_i(C) = h_i(B).h_i(C)$. From the previous remark it follows that $h_i(A).h_i(D) = h_i(B).h_i(D)$. Hence by Theorem 7.1.4 we have $A \times D \simeq B \times D$.

(iii) Either note $h_i(C) \neq 0$ for all i or using part (ii) of this corollary. Hence its an immediate conclusion that $1_{\mathbb{L}} \times A \simeq 1_{\mathbb{L}} \times B$ or in other words $A \simeq B$. □

This beautiful corollary makes a strong general statement about many finite structures. For example, if A, B and C are finite groups (maybe non-abelian) such that $A^5 \simeq B^5$ or $A \times C \simeq B \times C$ then $A \simeq B$, since $hom(1_{\mathbb{L}}, C) > 0$ holds for groups.

Now for the remainder of this section we continue studying factorization properties in terms of categorical concepts. We first translate the idea of isotopy which is needed to understand Lovász Isotopy Lemma.

Definition 7.1.6. Suppose $\mathbb{C}$ is a category closed under finite products. If there is an isomorphism $\phi : A \times C \longrightarrow B \times C$ that makes the following diagram commute

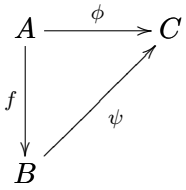


where π_2 is the second projection map, then we say object A is isotopic to object B over C and denote this by $A \sim_C B$. □

Using simple categorical arguments we prove a theorem which nearly looks like a cancellation theorem. This result was preceeded by J.D.H. Smith [Smi76] who proved under the hypothesis that A, B and C are finite structures and contained in a permutable variety that $A \times C \simeq B \times C$ implies A and B are isotopic.

Theorem 7.1.7. *Lovász Isotopy Lemma*
If A, B and C are objects in Lovász category $\mathbb{L}$ then $A \times C \simeq B \times C \iff A \sim_C B$.

Proof. The reverse direction is obvious. For the direct implication we create a new category $\mathbb{L}(C)$ for the object C. The objects in this category are the pairs (A, ϕ) where ϕ is a homomorphism from A to C. A morphism in $\mathbb{L}(C)$ between the objects (A, ϕ) and (B, ψ) is a morphism $f : A \longrightarrow B$ such that $\phi = \psi \circ f$, that is a homorphism ψ that makes the following diagram commute:



If A is object in $\mathbb{L}$ then $(A \times C, p_2)$ is an object in $\mathbb{L}(C)$ where p_2 is the second coordinate projection. We denote this object by A_C. It is known that products in $\mathbb{L}(C)$ correspond to pullbacks in $\mathbb{L}$. Also it can be checked that the product of A_C and B_C is isomorphic to $(A \times B)_C$.

Let $\{(A_i, \phi_i) : i < \alpha\}$ be a list of all objects in category $\mathbb{L}(C)$ up to isomorphism for some ordinal α. Let $h_i(A, \phi)$ the the number of $\mathbb{L}(C)$ morphisms from (A_i, ϕ_i) to (A, ϕ), that is

$$h_i(A, \phi) = |hom_{\mathbb{L}(C)}((A_i, \phi_i), (A, \phi))|$$

for some ordinal i. It is easily checked that $h_i((A, \phi) \times (B, \psi)) = h_i(A, \phi) \times h_i(B, \psi)$ and $(A, \phi) \simeq (B, \psi)$ iff $h_i(A, \phi) = h_i(B, \psi)$ for all i. Also note that for each i there is a $\mathbb{L}(C)$ morphism $f_i : (A, \phi_i) \longrightarrow C_C$ using the universal property. Thus $h_i(C_C) \neq 0$.

Suppose $A \times C \simeq B \times C$. Therefore in $\mathbb{L}(C)$ we have $(A \times C)_C \simeq (B \times C)_C$. So for each i we have $h_i(A_C).h_i(C_C) = h_i(B_C).h_i(C_C)$. Knowing $h_i(C_C)$ is non-zero we deduce that $h_i(A_C) = h_i(B_C)$ for each i. Thus $A_C \simeq B_C$ which is equivalent to saying $A \sim_C B$. □

It should be pointed out that the cancellation law also holds for structures other than those that possessing an one-element subuniverse. L. Fuchs [Fuc67] proved that the infinite cyclic group is cancellable in the class of all abelian groups. Here we proceed to apply Lovász Isotopy Lemma to algebraic structures (structures that only has fundamental operations) in conjunction with the next lemma to produce structures that do not have an one-element subuniverse but are still cancellable.

Lemma 7.1.8. *If algebraic structure A is isotopic to algebraic structure B then there is a bijective map ϕ_i for each fundamental operation f_i (they are indexed by set I) and a bijection ϕ such that*

$$\phi_i(f_i^A(a_1, \ldots, a_n)) = f_i^B(\phi(a_1), \ldots, \phi(a_n)),$$

for all $i \in I$ and $a_1, \ldots, a_n \in A$, where f_i has rank n.

Proof. Suppose A is isotopic to B over C. Thus for each $x \in C$ there is a bijection $\phi_x : A \longrightarrow B$ such that the map $\psi : A \times C \longrightarrow B \times C$ given by

$$(a, x) \mapsto (\phi_x(a), x)$$

is an isomorphism. Select an arbitrary element $c \in C$. We proceed to show $\phi(x) = \phi_c(x)$ and $\phi_i(x) = \phi_{f_i(c,c,\ldots,c)}(x)$ works.

$$\begin{aligned}
(\phi_{f_i^C(c,c,\ldots,c)}(f_i^A(a_1, a_2, \ldots, a_n), f_i^C(c, c, \ldots, c)) &= \psi(f_i^A(a_1, a_2, \ldots, a_n), f_i^C(c, c, \ldots, c)) \\
&= \psi(f_i^{A\times C}((a_1, c), (a_2, c), \ldots, (a_n, c))) \\
&= f_i^{B\times C}((\phi_c(a_1), c), (\phi_c(a_2), c), \ldots, (\phi_c(a_n), c)) \\
&= (f_i^B(\phi_c(a_1), \phi_c(a_2), \ldots, \phi_c(a_n)), f_i^C(c, c, \ldots, c)).
\end{aligned}$$

□

Corollary 7.1.9. *If* $\mathbf{C} = (C, f)$ *is a finite groupoid with elements* c, d *such that* $f(c, d) = f(d, d) = f(d, c) = c$ *then* $\mathbf{C}$ *is cancellable among finite algebras.*

Proof. Let $\mathbf{A} = (A, f^A)$ and $\mathbf{B} = (B, f^B)$ be finite groupoids such that $\mathbf{A} \times \mathbf{C} \simeq \mathbf{B} \times \mathbf{C}$. By Lovász Isotopy Lemma we know $\mathbf{A} \sim_{\mathbf{C}} \mathbf{B}$. Therefore for each $x \in C$ there is a bijection $\phi_x : \mathbf{A} \longrightarrow \mathbf{B}$ such that the map $\phi : \mathbf{A} \times \mathbf{C} \longrightarrow \mathbf{B} \times \mathbf{C}$ given by

$$(a, x) \mapsto (\phi_x(a), x)$$

is an isomorphism between $A \times C$ and $B \times C$. We claim ϕ_c is the desired isomorphism from $\mathbf{A}$ to $\mathbf{B}$. Invoking Lemma 7.1.8 we have

$$\begin{aligned}
\phi_c(f^A(a, a')) &= f^B(\phi_c(a), \phi_d(a')), \\
\phi_c(f^A(a, a')) &= f^B(\phi_d(a), \phi_d(a')), \\
\phi_c(f^A(a, a')) &= f^B(\phi_d(a), \phi_c(a')),
\end{aligned}$$

for all $a, a' \in A$. The next calculation proves why ϕ_c is an isomorphism.

$$\begin{aligned}
\phi_c(f^A(a, a')) &= \phi_c\phi_c^{-1}\phi_c(f^A(a, a')), \\
&= \phi_c\phi_c^{-1}(f^B(\phi_d(a), \phi_c(a'))), \\
&= \phi_c f^A(\phi_d^{-1}\phi_d(a), \phi_d^{-1}\phi_c(a')), \\
&= f^B(\phi_c\phi_d^{-1}\phi_d(a), \phi_d\phi_d^{-1}\phi_c(a')), \\
&= f^B(\phi_c(a), \phi_c(a')).
\end{aligned}$$

□

The example below effortlessly manufactures a large collection of algebras that are cancellable among finite structures, but do not have one-element subuniverses.

Example 7.1.10. Let $\mathbf{B} = (B, \wedge, \vee, ^-)$ be a Boolean algebra. Define groupoid $\mathbf{C} = (B, f)$ with $f(x, y) = (x \wedge y)^-$. Then $f(0, 0) = f(0, 1) = f(1, 0) = 1$ and by Corollary 7.1.9 it is cancellable among finite structures of this type.

7.2 Another proof

In this section we give another solution to the problem $A^k \simeq B^k \implies A \simeq B$. As an undergraduate the author was asked to prove that for any finite abelian groups A and B that $A^2 \simeq B^2 \implies A \simeq B$. This classroom problem intrigued the author and inspired the techniques found here, because it turns out to be true for any finite group, actually for any finite structure.

This fresh approach uses ideas from equational theory. These results will be applied to finite relational structures that may have an infinite set of finitary relations on the underlying set. To achieve this task we adopt terminology from [EF99]. First we define some notation, including the idea of a "counting function", that is useful for Lemma 7.2.5.

Definition 7.2.1. Let $X = \{x_1, \ldots, x_m\}$ be a finite set of variables. We say ϕ is an atomic formula if $\phi = r(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ where r is some equation/relation of arity n and σ is a map from $\{1, 2, \ldots, n\}$ to the set $\{1, 2, \ldots, m\}$. We denote $\mathcal{S}_X$ as the smallest set Z of formulas over X such that Z includes all the atomic formulas over X as well as all $x_i = x_j$ for $i, j \in \{1, \ldots, n\}$ and Z is closed under the NOT, OR and AND connectives. In fact S_X is the intersection of all sets Z as described. For a given $\phi \in \mathcal{S}_X$ we use $\phi(x_1, x_2, \ldots, x_n)$ if the order of the variables is important. □

Definition 7.2.2. If the variables $\vec{x}$ in a formula are interpreted $\vec{a}$ that is m-tuples of elements of A then ϕ makes a statement about A. This statement may be true or false. If it is true, we say ϕ is true of $\vec{a}$ in A or in symbols $A \models \phi(\vec{a})$. □

Definition 7.2.3. Let Υ denote the class of all cardinal numbers. For each algebra A and set of variables X we associate a "counting function" $C_A^X : \mathcal{S}_X \longrightarrow \Upsilon$ sending each formula ϕ to the number of solutions it has in A, ie. $C_A^X(\phi) = |\{\vec{a} : A \models \phi(\vec{a})\}|$. □

Next is an example to ground these concepts before we continue listing some elementary properties about the counting function.

Example 7.2.4. Let $X = \{x_1, x_2\}$, A be the group of order 2 and B be the non-cyclic group of order 4. If ϕ is the formula $(x_1^3 = x_2^2) \wedge (x_1 \neq x_2)$ then $C_A^X(\phi) = 2$, since $(0, 0)$ and $(0, 1)$ are both solutions for (x_1, x_2). Also $C_B^X(\phi) = 6$.

Lemma 7.2.5. *For all $\alpha, \beta \in \mathcal{S}_X$ we have*
(i) $C_A^X(\alpha) + C_A^X(\neg\alpha) = |A^X|$.
(ii) $C(\alpha) + C(\beta) = C(\alpha \vee \beta) + C(\alpha \wedge \beta)$.

Proof. (i) For each $f : X \longrightarrow A$ it either satisfies the formula or not.
(ii) Let S_ϕ be the set of solutions to the formula ϕ. Thus $S_{\alpha\wedge\beta} = S_\alpha \cap S_\beta$ and $S_{\alpha\vee\beta} = S_\alpha \cup S_\beta$ and the result follows.

□

Note if A, X are finite and we know the value of $C(\phi)$ then we can calculate $C(\neg\phi)$ using Lemma 7.2.5 part (i). However when A is infinite this is no longer the case. This observation indicates why finiteness is vital for this argument and breaks down otherwise.

In Example 7.2.4 we saw that $C_A^X(\phi) \times C_A^X(\phi) \neq C_B^X(\phi)$ but $A \times A \simeq B$. As we are interested in studying direct product properties we want to select the formulas that behave well under the counting function.

Definition 7.2.6. Let $\overline{S_X}$ be the smallest set of formulas containing atomic formulas and closed under the AND connective. □

Lemma 7.2.7. *Let $\phi \in \overline{S_X}$ then for any algebras A, B of the same type we have*
(i) $C_{A\times B}(\phi) = C_A(\phi) \times C_B(\phi)$.
(ii) $|Hom(A, B)| > 0$ and $C_A(\phi) > 0$ implies $C_B(\phi) > 0$.

The proof of Lemma 7.2.7 is straightforward and hence omitted. It should be noted that $\overline{S_X}$ is not the complete set of ϕ where $C_{A\times B}(\phi) = C_A(\phi) \times C_B(\phi)$ holds, but it is sufficient for our goal.

Now Theorem 7.2.10 below may look simple but it can be used to proof these powerful results about finite algebras, mentioned in the beginning of this section, in a simple manner. Before we prove this theorem we need a new definition and a lemma to assist us.

Definition 7.2.8. Let $\phi(x_1, x_2, \ldots, x_n) \in \mathcal{S}_X$. By substituting x_j with x_i we can make a new formula $\phi(x_j \rightsquigarrow x_i) = \phi(x_1, x_2, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots x_n)$ on the set $X - \{x_j\}$. □

Lemma 7.2.9. *If $\psi = \neg(x_i = x_j) \wedge \phi(x_1, \ldots, x_n)$ where $\phi \in \mathcal{S}_X$ for $X = \{x_1, \ldots x_n\}$, then for any algebra A we have $C_A^X(\psi) = C_A^X(\phi) - C_A^{X-\{x_j\}}(\phi(x_j \rightsquigarrow x_i))$.*

Proof. If you subtract all the solutions of ϕ in A from the solutions of $\phi(x_j \rightsquigarrow x_i)$ in A you get all the solutions of ψ in A. □

Theorem 7.2.10. *(i) If A, B are finite similar algebras which are not isomorphic then there is a formula $\tilde{\phi} \in \overline{S_X}$ for some X such that $C_A(\tilde{\phi}) \neq C_B(\tilde{\phi})$.*
(ii) $A \simeq B \iff C_A = C_B$.

Proof. (i) First we construct a formula ϕ such that $C_A^X(\phi) \neq C_B^X(\phi)$. Let X be a set such that $|X| = |A|$. Then a bijective function $\lambda : A \longrightarrow X$ exists. Thus we have natural bijections $\lambda^n : A^n \longrightarrow X^n$ for each natural number n. Let R_n be the set of all fundamental relations of arity n. Put

$$\begin{aligned} \hat{\phi} &= \bigwedge_{n \in \mathbb{N}; r \in R_n; \vec{a} \in r} r(\phi^n(\vec{a})), \\ \phi &= \hat{\phi} \wedge \bigwedge_{x,x' \in X; x \neq x'} \neg(x = x'). \end{aligned}$$

Clearly $C_A(\phi) \geq 1$. In fact $C_A^X(\phi) = |Aut(A)|$. If $C_A(\phi) = C_B(\phi)$ then $C_B(\phi) \geq 1$. Hence we can embed algebra A into algebra B. Similarly we can show that we can also embed algebra B into algebra A. Both being finite gives $A \simeq B$. This contradiction proves the existence of a formula ϕ with the desired property.

Now we proceed to modify ϕ to a formula $\tilde{\phi} \in \overline{S_Y}$ for some Y. By construction of ϕ we know a proposition ϕ_1 and variables x_i, x_j exist such that

$$\phi = \neg(x_i = x_j) \wedge \phi_1,$$

where ϕ_1 has less negations then ϕ. Using Lemma 7.2.9 we have $C_A^X(\phi_1) - C_A^{X-\{x_i\}}(\phi_1(x_i \rightsquigarrow x_j)) \neq C_B^X(\phi_1) - C_B^{X-\{x_i\}}(\phi_1(x_i \rightsquigarrow x_j))$. Thus either $C_A^X(\phi_1) \neq C_B(X)(\phi_1)$ or $C_A^{X-\{x_i\}}(\phi_1(x_i \rightsquigarrow x_j)) \neq C_B^{X-\{x_i\}}(\phi_1(x_i \rightsquigarrow x_j))$. Observe ϕ_1 and $\phi_1(x_i \rightsquigarrow x_j)$ have fewer atomic subformulas of the form $\neg(x = x')$ than ϕ. Therefore continuing by induction on the number of atomic subformulae completes the proof. □

Therefore knowing C_A on $\overline{S_X}$ we can determine the algebra up to isomorphism and hence calculate the counting function C_A completely. This is precisely what gets exploited in Corollary 7.2.12. Also the existence of an one-element subuniverse seems to be important for cancellation results. This strange phenomenon are understood better in light of Corollary 7.2.12.

Definition 7.2.11. We say element x of algebra A is an reflexive element if for all relations r we have $r(x, x, \dots (n \text{ times}), x)$ if r has arity n. □

Corollary 7.2.12. *Suppose A, B, C, D, E are finite relational algebras, that is algebras with only fundamental relations.*
(i) $A^k \simeq B^k \implies A \simeq B$ where k is a positive integer.
(ii) $A \times C \simeq B \times C$ and $|Hom(D, C)| > 0 \implies A \times D \simeq B \times D$
(iii) If E has an reflexive element then $A \times E \simeq B \times E \implies A \simeq B$.

Proof. (i) If $A \not\simeq B$ then there is a $\phi \in \overline{S_X}$ (where $\phi \in \mathcal{S}_X$ for some X) such that $C_A(\phi) \neq C_B(\phi)$. Then $C_A(\phi)^n \neq C_B(\phi)^n \implies C_{A^n}(\phi) \neq C_{B^n}(\phi)$. This contradiction gives the desired result.

(ii) Since $A \times D \not\simeq B \times D$ then there is a $\phi \in \overline{S_X}$ such that $C_{A\times D}(\phi) \neq C_{B\times D}(\phi) \implies C_A(\phi).C_D(\phi) \neq C_B(\phi).C_D(\phi) \implies C_A(\phi) \neq C_B(\phi)$ and $C_D(\phi) > 0$. Since $|Hom(D, C)| > 0$ we have $C_C(\phi) > 0$. So finally we get $C_{A\times C}(\phi) = C_A(\phi).C_C(\phi) \neq C_B(\phi).C_C(\phi) = C_{B\times C}(\phi)$. This contradiction gives the desired result.

(iii) The result follows from (ii) and Lemma 7.2.7. □

Using a natural way to transform a L-structure(a structure that potentially has both fundamental operations and fundamental relations) into a relational algebra(a structure that only has fundamental relations) while retaining its direct product properties we can easily conclude that these properties also hold for L-structures.

Corollary 7.2.13. *Suppose A, B, C, D, E are finite L-structures.*
(i) $A^k \simeq B^k \implies A \simeq B$ where k is a positive integer.
(ii) $A \times C \simeq B \times C$ and $|Hom(D, C)| > 0 \implies A \times D \simeq B \times D$
(iii) If E has an one-element subuniverse then $A \times E \simeq B \times E \implies A \simeq B$.

The next example illustrates that the extra condition on the cancellation law in Corollary 7.2.13 is necessary.

Example 7.2.14. Let V be a two-element set $\{a, b\}$ with binary relation $R = \{(a, a), (b, b)\}$ on it. Let W be a two-element set $\{c, d\}$ with binary relation $S = \{(c, d), (d, c)\}$ on it. It turns out that $V \times W \simeq W \times W$ but $V \not\simeq W$.

7.3 Absorbing algebras

Here we develop independent results to answer the question whether $A \simeq A \times B \times C \implies A \simeq A \times B \simeq A \times C$. This curious problem was raised by C. Chang's [Cha67] and answered by Mckenzie [Mck71]. Obviously this implication becomes more interesting when dealing with infinite structures. Unlike the other sections we strongly use ideas from set theory and even borrow a concept from analysis theory, but first a concept that applies to infinite structures.

Definition 7.3.1. We say that algebra A **absorbs** algebra B iff $A \simeq B \times A$. Algebra A is said to be **infinitely divisible** by B iff there are structures $(A_n)_{n\in\omega}$ such that $A \simeq B \times A_0$ and $A_n \simeq B \times A_{n+1}$ for each $n \in \omega$. □

Definition 7.3.2. We say two sequences $x = (x_0, x_1, x_2, \ldots)$ and $y = (y_0, y_1, y_2, \ldots)$ **eventually agree** if some integer n exists such that $x_m = y_m$ for all $m > n$. □

Now we are ready to connect the two notions of infinite divisibility and absorption. It should be noted that Corollary 7.3.4 was proved for countable complete Boolean algebras by Sikorski [Sik48] and Tarski [Tar48, Tar49].

Theorem 7.3.3. *If countable algebra A is infinitely divisible by finite algebra B then A absorbs B.*

Proof. Assume $A \simeq B \times A_0$ such that $a \mapsto (f_0(a), g(a))$ for some maps f_0 and g_0. Also for each i $A_i \simeq B \times A_{i+1}$ such that $a \mapsto (f_i(a), g_i(a))$ for some maps f_i and g_i. Therefore $\ker f_i \times \ker g_i = 0$ for every i in the appropriate lattice. Define $\psi_{-1} = id_A$ and

$$\begin{aligned} \psi_i &= g_i \circ \psi_{i-1} \\ \phi_i &= f_i \circ \psi_{i-1} \end{aligned}$$

for each $i \in \omega$. Thus $\ker \psi_0 \subseteq \ker \psi_1 \subseteq \ker \psi_2 \subseteq \ldots$ (since $\psi_i(a) = \psi_i(b)$ then $g_{i+1}\psi_i(a) = g_{i+1}\psi_i(b)$ giving $\psi_{i+1}(a) = \psi_{i+1}(b)$) and

$$0 = \ker \phi_0 \times \ker \phi_1 \times \ker \phi_2 \times \ldots \ker \phi_n \times \ker \psi_n \tag{7.2}$$

for each $n \in \omega$ and $\phi_n(A) = B$ for each $n \in \omega$. Therefore

$$0 = \theta \cap \ker \phi_0 \cap \ker \phi_1 \cap \ldots$$

where $\theta = \cup_{n \in \omega} \ker \psi_n$. Thus

$$f : A \longrightarrow A/\theta \times B^\omega$$

where $a \mapsto (a/\theta, (\phi_i(a) : i \in \omega))$ is an injective homomorphism.

If $(b_i) \in B^\omega$ and $b_i = \phi_i(a)$ for $i > n$, then Equation 7.2 shows that there is an $a' \in A$ such that $\phi_i(a') = b_i$ for $i \leq n$ and $\psi_n(a') = \psi_n(a)$. So for $i > n$ we have $\phi_i(a') = \phi_i(a) = b_i$ and $a'/\theta = a/\theta$. Thus whenever $x \in A/\theta \times B^\omega$ is the same as $f(a)$ except for finitely many B-coordinates, then $x = f(a')$ for some $a' \in A$.

So far we have shown, up to isomorphism, A is a subalgebra of $C \times B^\omega$ and if $(c, (b_0, b_1, b_2, \ldots)) \in A$ and $b'_i = b_i$ for all $i > n$ then $(c, (b'_0, b'_1, b'_2, \ldots)) \in A$.

Now for any function $\lambda : \omega \longrightarrow \omega$ we can define a homomorphism

$$f_\lambda : C \times B^\omega \longrightarrow B \times (C \times B^\omega)$$

via

$$(c, (b_0, b_1, b_2, \ldots)) \mapsto (b_0, (c, b_{\lambda(0)}, b_{\lambda(1)}, \ldots)).$$

It turns out f_λ is an isomorphism between $C \times B^\omega$ and $B \times (C \times B^\omega))$ iff λ maps ω bijectively to $w - \{0\}$. To finish this proof, we now explicitly construct a bijection λ with the extra property that the resulting isomorphism f_λ maps A onto $B \times A$.

To construct λ, we use the fact that A is countable and B is finite. Let $(a_i : i \in \omega)$ enumerate all the elements of A with element

$$a^i = (c_i, (b^i_0, b^i_1, \ldots))$$

in the above representation of A as a subalgebra of $C \times B^\omega$. Since B is finite, there exists an infinite set $J_0 \subseteq \omega$ such that $b^0_j = b^0_k$ for all $j, k \in J_0$. Proceeding in this manner we see the existence of a nested sequence of infinite sets $J_0 \supseteq J_1 \supseteq J_2 \supseteq \ldots$ such that for every i we have $b^i_j = b^i_k$ for all $j, k \in J_i$.

We now pick natural numbers n_i such that $0 < n_0 < n_1 < n_2 < \ldots$ and such that $n_i \in J_i$ for each i. Now we are ready to define λ. If n does not occur in the sequence $0, n_1, n_2, n_3, \ldots$ then $\lambda(n) = n$, otherwise define $\lambda(0) = n_0$ and $\lambda(n_i) = n_{i+1}$ for $i \in \omega$. It is clear that λ maps ω bijectively to $w - \{0\}$ and hence $f_\lambda : C \times B^\omega \longrightarrow B \times (C \times B^\omega)$ is an isomorphism.

Now we show that $f_\lambda(A) \subseteq B \times A$: Let $a^i = (c_i, (b^i_0, b^i_1, \ldots))$ be an arbitrary element of A. If $n \geq n_i$ then either $\lambda(n) = n$ or $n, \lambda(n)$ are both elements of J_i. This means $b^i_{\lambda(n)} = b^i_n$ for all $n \geq N$. Define $f_\lambda(a^i) = (b, a')$ where a' differs from a^i only in finitely many B-coordinates. From an earlier observation it follows that $f_\lambda(a) \in B \times A$, so f_λ maps A to $B \times A$.

Now we show $f_\lambda(A)$ maps A onto $B \times A$: Take a typical element $(b, a^i) = (b, (c^i, (b^i_0, b^i_1, \ldots,)))$ of $B \times A$ and let N be such that $b^i_{\lambda(n)} = b^i_n$ for $n \geq N$. Now define

$$a' = (c', (b'_0, b'_1, \ldots)) \in C \times B^\omega$$

where $c' = c^i$, $b'_0 = b$, $b^i_{\lambda(n)} = b^i_n$ for $n \leq N$ and $b^i_m = b'_m$ for all other m. Since a^i and a' only differ in finitely many B-coordinates, we have $a' \in A$. Noting $b^i_{\lambda(n)} = b^i_n$ for $n \geq N$, it follows that $f_\lambda(a') = (b, a^i)$ which completes the proof. □

We conclude with two impressive corollaries of this theorem.

Corollary 7.3.4. *Suppose A is countable and either B or C is finite. If $A \simeq A \times B \times C$ then $A \simeq A \times B$.*

Proof. Assume B is finite. Notice

$$\begin{aligned} A &\simeq B \times (A \times C) \\ A \times C &\simeq B \times (A \times C \times C) \\ A \times C \times C &\simeq B \times (A \times C \times C \times C) \\ &\text{etc.} \end{aligned}$$

Thus A is infinitely divisible by B. By Theorem 7.3.3 it follows that $A \simeq A \times B$. Otherwise if C is finite, we get $A \simeq A \times C$. Therefore $A \times B \simeq A \times B \times C \simeq A$. □

Corollary 7.3.5. *Suppose B is countable and C is finite. If $A \simeq B \times C$ and $B \simeq A \times D$ then $A \simeq B$.*

Proof. $A \simeq B \times C \simeq A \times D \times C$. Applying Corollary 7.3.4 we obtain $A \simeq A \times D \simeq B$. □

This result is somewhat reminiscent of the Cantor-Schröder-Bernstein Theorem which states that whenever $A \leftrightarrow B \cup C$ and $B \leftrightarrow A \cup D$ then $A \leftrightarrow B$. Here $A \leftrightarrow B$ is shorthand notation for representing equipotent sets A and B, that is they have the same cardinality.

Do not be misled by Theorem 7.3.3 in thinking that countable structures are well behaved. Examples of countable groups, lattices and Boolean algebras A exist with $A \simeq A^3$ and $A \not\simeq A^2$. A.L.S. Corner [Cor69] published an example of an abelian group with this strange property. Equally interesting, W. Hanf [Han57] explains how to find Boolean algebras such that $A \simeq A^k$ but $A \not\simeq A^i$ for any $1 < i < k$.

7.4 Subdirectly irreducible algebras

In this section we investigate the connections between subdirectly irreducible algebras and directly indecomposable algebras. This may be a strange place to include this, but Corollary 7.1.5 will be invoked. Here we also prove Theorem 7.4.3, the only unique factorization theorem in this chapter, but first we recall what a subdirectly irreducible algebra is.

Definition 7.4.1. An algebra A is said to be a **subdirect product** of a family $(A_i)_{i\in I}$ of indexed algebras if

$$\begin{aligned} A &\leq \prod_{i\in I} A_i, \\ \pi_i(A) &= A_i \quad \text{for each } i \in I. \end{aligned}$$

Furthermore we say the embedding $e : A \longrightarrow \prod_{i\in I} A_i$ is a **subdirect** embedding if $e(A)$ is a subdirect product of the A_i. □

Definition 7.4.2. An algebra A is **subdirectly irreducible** iff for every subdirect embedding

$$e : A \longrightarrow \prod_{i\in I} A_i$$

there is an $i \in I$ such that $A \simeq A_i$. □

Examples of subdirectly irreducible algebras includes any two-element algebras, simple structures, $\mathbf{Z}_{p^\infty}$, etc. It can be shown that any finite abelian group G is subdirectly irreducible if and only if it is cyclic and $|G| = p^n$ for some prime number p. Further interesting properties of subdirectly irreducible algebras can be found in [BS].

It can also be shown that every subdirectly irreducible algebra is directly indecomposable and hence has the unique factorization property. The converse is not true as the three-element chain (as a lattice) is directly indecomposable but not subdirectly irreducible.

Up to now we have seen many proofs of why finite abelian groups have the unique factorization property. Here we will give another one, but first note that in groups the directly indecomposable algebras (the finite cyclic groups of prime order) are subdirectly irreducible. This condition gets exploited in producing Theorem 7.4.3.

Theorem 7.4.3. *Let V be a variety where every directly indecomposable algebra is subdirectly irreducible. If a finite algebra in this variety has an one-element subuniverse then it is uniquely factorable.*

Proof. Suppose A is a finite algebra with an one-element subuniverse. We proceed proving the claim on induction on the size of A. Suppose

$$A \simeq \prod_{i \in I} A_i \simeq \prod_{j \in J} B_j,$$

where A_i and B_j are directly indecomposable algebras. Without loss of generality assume A_1 is the largest algebra of the set $\{A_i : i \in I\} \cup \{B_j : j \in J\}$. Observe A_1 can be embedded into A (if M and N are algebras of the same type and B has a one-element subalgebra, say $\{0\}$, then the injective map $a \mapsto (a, 0)$ becomes a homomorphism from A to $A \times B$). Thus a subdirect embedding

$$A_1 \longrightarrow \prod_{j \in J} \overline{B}_j,$$

exists where $\overline{B}_j$ is a subalgebra of B_j for all $j \in J$. However, A_1 is subdirectly irreducible. Thus $A_1 \simeq \overline{B}_k$ for some $k \in J$. Hence $A_1 \simeq B_k$ as $|A_1| = |\overline{B}_k| \leq |B_k| \leq |A_1|$. Therefore $A_1 \simeq B_k$. Applying Corollary 7.1.5 we get

$$\prod_{i \in I - \{1\}} A_i \simeq \prod_{j \in J - \{k\}} B_j.$$

Invoking the induction hypothesis on $|A|$, finishes the proof. □

7.5 Conclusion

This chapter studied other fascinating factorization problems. This is still mostly unexplored terrority and there are more results to be unearthed. For example it would be interesting to find sufficient conditions when these implications holds.

Furthermore, we showcased other interesting techniques for tackling these problems: Category theory, equational theory and set theory. Category theory is still an untapped resource to study these kinds of problems and hopefully it will be a powerful tool in the future to assist in studying and understanding these problems. Also, equational theory is intrinsically part of algebraic structures and may have the keys to unlock some of their mysteries.

Overall progress has been slow, due to the small number of minds actively engaged in this area. In Chapter 2 we illustrated techniques using congruence theory and lattice theory. Although these methods have been fruitful to produce numerous UFP theorems, we still need further insight to solve the following important open problem :

If $Con\, A$ is a modular lattice of finite height and A has an one-element subalgebra, must A be uniquely factorable?

In Chapter 3 we modernized the idea of endomorphisms and subalgebras to assist us in proving a UFP result for zero-algebras. Although these methods were different, we also demonstarted why they cannot be extended to other algebraic classes.

It is possible to program a simple brute-force algorithm that would allow us to verify whether

a finite structure has the UFP or not, but with infinite algebras this is no longer possible. This was our focus in Chapters 4 and 5, to find infinite structures whose factorization behaves like the factorization of integers. Here we utilised and demonstrated that the idea of decomposition functions are far more useful than endomorphisms. We applied these methods to establish and showcase the possibility of reconstructing many UFP results by requiring certain identities to hold.

Another important class of algebras is idempotent algebras. In Chapter 6 we mainly focussed on idempotent semigroups. Using some structure theory of semigroups and new techniques developed by R. Mckenzie we showed that every finite idempotent semigroup has the UFP, but the following important problem still remains unsolved :

Does every finite idempotent structure possess the unique factorization property?

Although these techniques have served us well, fresh techniques are still needed (like those proposed in this chapter) to rekindle this branch of mathematics which allows us to give interesting structural results about universal algebras.

Bibliography

[Bir48] G. Birkhoff, "Lattice Theory", Revised Edition, Colloquium Publications, Vol. **25**, Americ. Math. Soc., Providence, 1948.

[BK47] G. Birkhoff and S.A. Kiss, "A ternary operation in distributive lattices", *Bull. Amer. Math. Soc.* **53**, Number 8 (1947), p. 749-752.

[Bru47] N.G. de Bruijn, "Gemeenschappelijke representantensystemen van twee klassenindelingen van een verzameling", *Niew Archief voor Wiskunde* **22** (1947), p. 48-52.

[BS] S. Burris and H.P. Sankappanavar, "A course in universal algebra", Graduate Texts in Mathematics, Springer-Verlag, New York, 1981.

[CD] P. Crawley & R.P. Dilworth, "Algebraic theory of lattices", Prentice-Hall, (1973).

[Cha61] C.C. Chang, "Cardinal and ordinal factorization of relation types", *Proceed. of Symposia in Pure Mathematics* **Vol. 2**, (1961), p. 48-52.

[Cha67] C.C. Chang, "Cardinal factorization of finite relational structures", *Fund. Math* **60**, (1967), p. 251-269.

[Cha76] I. Chajda, "On the unique factorization problem", *Math. Slovaca* **Vol. 26**, (1976), p. 201-205.

[CJT] C.C. Chang, B. Jónsson and A. Tarski, "Refinement properties for relational structures", *Fund. Math.* **55**, (1964) p. 249-281.

[Cli61] A.H. Clifford and G.B. Preston, "The algebraic theory of semigroups", *Mathematical Surveys* **No. 7**, Amer. Math. Soc., (1961).

[Cor69] A.L.S. Corner, "Additive categories and a theorem of Leavitt", *Bull. Amer. Math. Soc.* **Vol. 75** (1969), p. 78-82.

[CP61] A.H. Clifford and G.B. Preston, "The algebraic theory of semigroups", *Mathematical Surveys* **No. 7**, Amer. Math. Soc., (1961).

[Day69] A. Day, "A characterization of modularity for congruence lattices of algebras", *Canad. Math. Bull.* **Vol. 12** (1969), p. 167-173.

[Ded00] R. Dedekind, "Uber die von drei Moduln erzeugte Dualgruppe", *Math. Ann.* **53** (1900), p. 371-403.

[EF99] H.D. Ebbinghaus and J. Flum, "Finite Model Theory", *Springer-Verlag Berlin Heidelberg New York.* **Second edition** (1999).

[Fit34] H. Fitting, "Über die direkten Produktzerlegungen einer Gruppe in direkt unzerlegbar Faktoren", *Mathematische Zeitschrift* **Vol. 39** (1934), p. 16-30.

[FT52] J.M.G. Fell and A. Tarski, "On algebras whose factor algebras are Boolean", *Pac. J. of Math.* **2** (1952), p. 297-318.

[Fre1] R. Freese, "Notes on direct decompositions", http://www.math.hawaii.edu/ ralph/Notes/dirprod.pdf accessed 15 November 2009.

[Fre2] R. Freese, "On Extending Lemma 4", http://www.math.hawaii.edu/ ralph/Notes/lemma4.pdf accessed 15 November 2009.

[Fuc67] L. Fuchs, "Abelian groups", *Pergamon Press* **New York**, 1967.

[Gra] G. Grätzer, "General Lattice Theory", *Second Edition* **Birkhäuser Verlag, Basel**, (1998).

[Gum81] H. Gumm, "Congruence modularity is permutability composed with distributivity", *Arch. Math. (Basel)* **36** (1981), p. 569-576.

[Han57] W. Hanf, "On some fundamental problems concerning isomorphisms of Boolean algebras", *Math. Scand.* **5** (1957), p. 205-217.

[Has51] J. Hashimoto, "On Direct Product Decomposition of Partially Ordered Set", *The Annals of Mathematics.* **Vol. 54**, No. 2 (1951).

[Jac43] N. Jacobson, "The theory of rings", *Mathematical surveys* **Vol. 2** (1943), New York VI + p. 150.

[Jon57] B. Jónsson, "On direct decompositions of torsion-free abelian groups", *Math. Scand* **Vol. 5** (1957), p. 230-235.

[Jon66] B. Jónsson, "The unique factorization problem for finite relational structures", *Colloq. Math.* **Vol. 14**, (1966), p. 1-32.

[Jon67] B. Jónsson, "Algebras whose congruence lattices are distributive", *Math. Scand.* **Vol. 21**, (1967), p. 110-121.

[JT47] B. Jónsson and A. Tarski, "Direct decompositions of finite algebraic systems", *Notre Dame Mathematical Lectures.* **No. 5**, South Bend, (1947).

[Kap54] I. Kaplanski, "Infinite Abelian groups", *University of Michigan Publications in Mathematics* **2**, (1954), Ann Arbor.

[Kin53] S. Kinoshita, "A solution of a problem of R. Sikorski", *Fund. Math.* **40** (1953), p. 39-41.

[Kor37] V. Kořinek, "Sur la décomposition d'un groupe en produit direct des sousgroupes", *Časopis pro pěstování matematiky a fysiky.* **Vol. 66**, (1937), p. 261-286.

[Kro70] L. Kronecker, "Auseinandersetzung einiger Eigenschaften der Klassenzahl idealer komplexer Zahlen", *Monatsh. Preuss. Akad. Wiss.*, Berlin, (1870), p. 881-889.

[Kur32] A. Kurosh, "Zur Zerlegung unendlicher Gruppen", *Mathematische Zeitschrift.*, **Vol. 23**, (1932), p. 161-196.

[Lov67] L. Lovász, "Operations with structures", *Acta Math. Acad. Sci. Hung.* **18** (1967), p. 321-328.

[Lov71] L. Lovász, "On the cancellation law among finite relation structures", *Periodica Mathematica Hungarica* **Vol. 1** (1971), p. 145-156.

[Mac] S. Mac Lane, "Categories for the Working Mathematician", *Springer-Verlag* **Second edition** (2000).

[Mal54] A.I. Mal' cev, "On the general theory of algebraic system", *Mat. Sb. N.S.* **35(77)** (1954), p. 3-20.

[Mck68] R. Mckenzie, "On finite groupoids and K-prime algebras", *Trans. Amer. Math. Soc.* **133**, (1968), p. 115-129.

[Mck71] R. Mckenzie, "Cardinal multiplication of structures with a reflexive relation", *Fund. Math.* **70** (1971), p. 59-101.

[Mck72] R. Mckenzie, "A method for obtaining refinement theorems, with an application to direct products of semigroups", *Algebra Universalis* **Vol 2**, (1972), p. 324-338.

[Mck72b] R. Mckenzie,"Equational bases and non-modular lattice varieties", *Trans. Amer. Math. Soc.* **174** (1972), p. 1-43.

[MMT] R. Mckenzie, G.F. McNulty, W.F. Taylor, "Algebras, Lattices, Varieties - Volume 1", Brooks/Cole Publishing Company, 1987.

[MW09] J.H. Maclagen and E.M. Wedderburn, "On the direct product in the theory of finite groups", *The Annals of Mathematics.* **Vol. 10** (1909), p. 173-176.

[Ore35] O. Ore, "On the Foundation of Abstract Algebra I", *The Annals of Mathematics.* **Vol. 36** (1935), No. 2, p. 406-437.

[Ore36a] O. Ore, "On the Foundation of Abstract Algebra II", *The Annals of Mathematics.* **Vol. 37** (1936), No. 2, p. 265-292.

[Ore36b] O. Ore, "Direct decompositions", *Duke Math. Journal* **Vol. 58** (1936), p. 581-596.

[Rem11] R. Remak, "Über die Zerlgegung der endliche Gruppen in direkte unzerlegbare Faktoren", *J. reine angew. Math* **139** (1911), p. 293-308.

[Sch28] D. Schmidt, ""Uber unendliche Gruppen mit endlicher Kette", *Mathematische Zeitschrift* **29** (1928), p. 34-41.

[Sik48] R. Sikorski, "On a generalization of theorems of Banach and Cantor-Bernstein", *Colloq. Math.* **1** (1948), p. 140-144 and 242.

[Smi76] J.D.H. Smith, "Mal'cev varieties", *Lecture Notes in Math.* **554**, (1976), Springer, Berlin-Heidelberg-New York.

[Spe27] A. Speiser, "Die Theorie der Gruppen von endlicher Ordnung", *Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen* **Vol. 5** (1927), 2nd edition Berlin.

[Tar48] A. Tarski, "Axiomatic and algebraic aspects of two theorems on sums of cardinals", *Fund. Math* **35** (1948), p. 79-104.

[Tar49] A. Tarski, "Cardinal algebras", With an appendix by B. Jónsson and A. Tarski, *Cardinal products of isomorphism types*, New York, (1949).

[Wed09] J.H.M. Wedderburn, "On the direct product in the theory of finite groups", *Ann. Math.* **10** (1909), p. 173-176.