

Computational Aspects of Finite Simple Semirings

Andreas Kendziorra

The thesis is submitted to University College Dublin in
fulfilment of the requirements for the degree of
Doctor of Philosophy.

School of Mathematical Sciences

Head of School: Dr. Patrick Murphy

Principal Supervisor: Dr. Marcus Greferath

Doctoral Studies Panel:

Prof. Gary McGuire

Dr. Eimear Byrne

May 2012

Contents

| | |
|--|-----------|
| Summary | v |
| Acknowledgements | ix |
| 1 Introduction | 1 |
| 1.1 Notations and universal algebra | 2 |
| 1.2 Basics of order and lattice theory | 4 |
| 1.3 Semirings | 10 |
| 1.3.1 Proper finite simple semirings with zero | 12 |
| 1.4 Cryptography | 13 |
| 1.4.1 Cryptography based on semigroup actions | 15 |
| 1.5 Overview | 18 |
| 2 Analysis of a cryptosystem using residuated mappings | 21 |
| 2.1 The protocol | 21 |
| 2.2 The analysis | 23 |
| 3 Representation and cardinalities of finite simple semirings | 25 |
| 3.1 Representation of semirings | 26 |
| 3.1.1 The semiring of tight residuated mappings | 26 |
| 3.1.2 Formal Concept Analysis | 28 |
| 3.1.3 The semiring of bonds | 30 |
| 3.2 Cardinalities of semirings | 36 |
| 3.2.1 Cardinality of $E(\mathbf{L})$ | 38 |
| 3.2.2 A characterisation of adjunctions | 41 |
| 3.2.3 Number of adjunctions between two ordered sets | 44 |
| 3.2.4 Number of regular dual bonds | 47 |
| 3.2.5 Tight adjunctions between horizontal sums of chains | 50 |
| 4 Invertible matrices over finite additively idempotent semirings | 53 |
| 4.1 Matrices over additively idempotent semirings | 54 |
| 4.2 Direct decompositions | 56 |
| 4.3 Invertible matrices | 59 |
| 4.4 Remarks | 64 |

| | | |
|----------|--|-----------|
| 5 | Finite simple additively idempotent semirings | 67 |
| 5.1 | Semimodules | 70 |
| 5.1.1 | Existence of idempotent irreducible semimodules | 72 |
| 5.1.2 | Properties of idempotent sub-irreducible semimodules | 76 |
| 5.1.3 | Density results for idempotent irreducible semimodules | 80 |
| 5.2 | Embedding of $(R, +, \cdot)$ into $(\mathbf{JM}(\mathbf{L}), \vee, \circ)$ | 83 |
| 5.3 | Subsemirings of $(\mathbf{JM}(\mathbf{L}), \vee, \circ)$ | 90 |
| 5.4 | Characterisation theorems | 91 |
| 5.5 | Isomorphic semirings | 93 |
| 5.6 | Neutral elements | 95 |
| 5.7 | The remaining case | 97 |
| | Bibliography | 107 |
| | Symbols | 111 |
| | Index | 113 |

Summary

During the last decade, Maze, Monico, and Rosenthal suggested new ideas for public key cryptography based on semigroup actions. Some concrete cryptosystems involve matrices over finite simple semirings. In 2008, Zumbrägel came up with a classification result, which characterises all proper finite simple semirings with zero. This characterisation can be expressed in terms of residuated mappings between finite lattices. The result was a big theoretical step in the study of the proposed cryptosystems.

This thesis is meant to continue this investigation. We will focus on foundational and computational problems that are relevant for cryptographic applications. To be more precise, we will deal with the following problems:

- We investigate how to represent simple semirings in a computational device. Such a representation should require little space, admit efficient operations, and it should allow to generate arbitrary semirings elements. The solutions we propose suggest to store a semiring implicitly by storing a lattice or by storing a *formal context*. Furthermore, we investigate the cardinalities of these semirings depending on the generating lattice or formal context.
- One chapter of this thesis will deal with invertible matrices over finite additively idempotent semirings. As all semirings considered in the other chapters of this dissertation have these properties, our results will cover these semirings. In particular, we will derive an invertibility criterion for such matrices, and we will give a computation of the inverse matrix. Moreover, we will present a formula for the number of invertible matrices.
- In the largest chapter, we will extend the classification of finite simple semirings. Here, we aim to characterise every finite simple additively idempotent semirings as a semiring of join-morphisms of a semilattice. It will turn out that this approach works for a very large class of semirings. Particularly, we will obtain a complete classification of finite simple semirings with an additively neutral element.

Most of the approaches and results in this dissertation are based on the characterisation of proper finite simple semirings as semirings of residuated mappings. Therefore, major parts of this work involve concepts and tools from order theory, lattice theory, and in particular from residuation theory.

I hereby certify that the submitted work is my own work, was completed while registered as a candidate for the degree stated on the Title Page, and I have not obtained a degree elsewhere on the basis of the research presented in this submitted work.

Date:

Signature:

Collaborators:

- Stefan E. Schmidt: contributed ideas and results to Chapter 3 and Chapter 4.
- Jens Zumbrägel: contributed ideas and results to Chapter 4 and Chapter 5.

Acknowledgements

First of all, I would like to thank my advisors and mentors Marcus Greferath and Jens Zumbärgel. Their continuous support, praise, and encouragement were essential for the success of this work. Moreover, their confidence, their friendship, and the freedom that I was allowed to experience during my studies enabled for me the best conditions a student could think of.

I am most grateful to Stefan Schmidt for teaching me so much, for enabling me to obtain this PhD scholarship, for supporting me over a long time, and also for his friendship. Every visit in Dresden during the last three years has been a welcome mental refreshment and many results of this thesis are due to these visits.

I owe my thanks to the examination committee, Joachim Rosenthal, Eimear Byrne, and Gary McGuire for their helpful suggestions.

I would like to thank Oliver Gnilke for being a great teammate and desk neighbour. Working got so much nicer and more efficient since he joined our group.

I owe my thanks to the Science Foundation Ireland for their generous financial support under Grant No. 08/IN.1/I1950 and the Claude Shannon Institute for providing me an excellent research environment.

I would like to thank Anna-Lena, Kay, Martin, Michael, and Robin, who took time to proofread my thesis, in spite of having been very busy themselves.

Chapter 1

Introduction

The work in this dissertation is dedicated to finite algebraic structures with application in cryptography: we will particularly focus on finite simple semirings. Jens Zumbärgel classified finite simple semirings with zero in [61]. These semirings are interesting for new ideas in public key cryptography based on semigroup actions [42]. The work of Zumbärgel contains a characterisation of proper finite simple semirings, which can be expressed in terms of residuated mappings of finite lattices. Based on these results, we continue the study of finite simple semirings, where we mostly restrict to aspects important for cryptographic applications. However, the study of simple (universal) algebras is a topic of independent interest in mathematics. The classification of finite simple groups, for example, received vast attention. Unlike the classification of finite simple groups or the classification of finite simple rings, the classification of finite simple semirings has not yet been completed. Therefore, one important part of this dissertation is about the continuation of the classification of finite simple semirings.

In this introductory chapter we give the most important background information for this dissertation. Firstly, we clarify some notation and recall fundamental concepts from universal algebra in Section 1.1. Since we use order and lattice theoretic concepts throughout this dissertation, we give some background information on order and lattice theory in Section 1.2. In Section 1.3, we introduce semirings. In particular, we will present the characterisation of proper finite simple semiring given in [61]. Section 1.4 is about cryptography, particularly about public-key cryptography based on semigroup actions and hence, about the application of semirings in cryptography. Finally, we give an overview and an outline of this work in Section 1.5.

1.1 Notations and universal algebra

This section will clarify some notation concerning (universal) algebras. Notation introduced for arbitrary algebras will also be used for specific algebras. For example, when we define homomorphisms between two algebras \mathbf{A} and \mathbf{B} , then it should become clear how homomorphisms between two semirings $(R, +, \cdot)$ and $(S, +, \cdot)$, between two monoids $(M, +, 0)$ and $(N, +, 0)$, and so on are defined. Also, if we define, for example, that $\text{Hom}(\mathbf{A}, \mathbf{B})$ denotes the set of all homomorphism from an algebra \mathbf{A} to an algebra \mathbf{B} , then $\text{Hom}(\mathbf{M}, \mathbf{N})$ will correspondingly denote the set of all (monoid) homomorphism from \mathbf{M} to \mathbf{N} for two monoids \mathbf{M} and \mathbf{N} .

In addition to the above notation we will recall some basic concepts from universal algebra, which are important for us. This is basically the concept of congruences. Since we will use congruences for semirings, lattices, and semimodules, we introduce them and explain their role in this general setting. All definitions and notations are mostly stated as in [8] or [24]. Proofs for all stated facts can also be found in those books.

Algebras

An **n -ary operation** on a nonempty set A is a mapping f from A^n to A , and n is the **arity** of f . A **finitary operation** is an n -ary operation for an $n \in \mathbb{N}$. An **algebra \mathbf{A}** is a pair (A, F) , where A is a nonempty set and F a family of finitary operations on A . The set A is called the **base set** of \mathbf{A} , and the elements of F are called the **fundamental operations** of \mathbf{A} .

We will denote algebras by bold capital letters or by pairs as above. If a bold capital letter is assigned to an algebra, then the base set will be denoted by the corresponding italic capital letter. This means if we mention an algebra \mathbf{A} without mentioning the base set explicitly, then it will be clear that A is meant to be the base set of \mathbf{A} . For a finite set of operations $F = \{f_1, \dots, f_n\}$, we will also denote an algebra (A, F) by (A, f_1, \dots, f_n) .

If one wants to talk about two algebras at the same time, the concept of *language* is helpful: A **language** of algebras is a set \mathcal{F} , whose elements are called **operation symbols**, such that for each operation symbol $f \in \mathcal{F}$ a nonnegative n is assigned, which is called the **arity** of f . An **n -ary operation symbol** is an operation symbol of arity n .

If \mathcal{F} is a language of algebras, then an **\mathcal{F} -algebra** is an algebra $\mathbf{A} = (A, F)$ such that F is indexed by \mathcal{F} , i.e. $F = (f^{\mathbf{A}} \mid f \in \mathcal{F})$, and $f^{\mathbf{A}}$ has the same arity as f for

1.1. Notations and universal algebra

every $f \in \mathcal{F}$. If the context is clear, one can also write f instead of $f^{\mathbf{A}}$.

If \mathbf{A} and \mathbf{B} are two \mathcal{F} -algebras for a language \mathcal{F} , then \mathbf{B} is a **subalgebra** of \mathbf{A} if $B \subseteq A$ and $f^{\mathbf{B}} = f^{\mathbf{A}}|_{B^n}$ for every $f \in \mathcal{F}$, where n is the arity of f .

Homomorphisms

Let \mathcal{F} be a language of algebras and let \mathbf{A} and \mathbf{B} be two \mathcal{F} -algebras. A **homomorphism** from \mathbf{A} to \mathbf{B} is a mapping $\varphi : A \rightarrow B$ that satisfies

$$\varphi(f^{\mathbf{A}}(a_1, \dots, a_n)) = f^{\mathbf{B}}(\varphi(a_1), \dots, \varphi(a_n))$$

for every $n \in \mathbb{N}$, every n -ary $f \in \mathcal{F}$, and all $a_1, \dots, a_n \in A$. An **endomorphism** of \mathbf{A} is a homomorphism from \mathbf{A} to \mathbf{A} , and an **epimorphism**¹ from \mathbf{A} to \mathbf{B} is a surjective homomorphism from \mathbf{A} to \mathbf{B} . An **isomorphism** from \mathbf{A} to \mathbf{B} is a bijective homomorphism from \mathbf{A} to \mathbf{B} , and an **automorphism** of \mathbf{A} is an isomorphism from \mathbf{A} to \mathbf{A} . If there exists an isomorphism from \mathbf{A} to \mathbf{B} , then \mathbf{A} and \mathbf{B} are called **isomorphic**, which is denoted by $\mathbf{A} \cong \mathbf{B}$. We will denote the set of homomorphisms from \mathbf{A} to \mathbf{B} by $\text{Hom}(\mathbf{A}, \mathbf{B})$, the set of endomorphism of \mathbf{A} by $\text{End}(\mathbf{A})$, and the set of automorphisms of \mathbf{A} by $\text{Aut}(\mathbf{A})$.

Congruences

For a set S , an equivalence relation \sim on S , and an element $x \in S$ we denote the equivalence class of x with respect to \sim by $[x]_{\sim}$ or if there is no confusion just by $[x]$.

Definition 1.1. Let $\mathbf{A} = (A, F)$ be an algebra. A **congruence** on \mathbf{A} is an equivalence relation \sim on A with the following property: For every $n \in \mathbb{N}$, every n -ary $f \in F$, and all elements $a_i, b_i \in A$ for $i = 1, \dots, n$ the implication

$$(\forall i = 1, \dots, n : a_i \sim b_i) \Rightarrow f(a_1, \dots, a_n) \sim f(b_1, \dots, b_n)$$

holds.

The **equality relation** $\text{id}_A = \{(a, a) \mid a \in A\}$ and the **complete relation** $A \times A$ are examples of congruences on an algebra \mathbf{A} . A congruence is called **non-total** if it is unequal to the complete relation.

¹We will work with the definition of *epimorphism* as it is used in universal algebra. This is different from the definition in category theory

Congruences play the same role for algebras as normal subgroups for groups or ideals for rings as we will see in the next steps:

Let \mathcal{F} be a language of algebras, let \mathbf{A} be an \mathcal{F} -algebra, and let \sim be a congruence on \mathbf{A} . Then the **quotient algebra** of \mathbf{A} by \sim , denoted by \mathbf{A}/\sim , is the algebra with the base set A/\sim and whose fundamental operations $(f^{\mathbf{A}/\sim} \mid f \in \mathcal{F})$ satisfy

$$f^{\mathbf{A}/\sim}([a_1], \dots, [a_n]) = [f^{\mathbf{A}}(a_1, \dots, a_n)]$$

for every $n \in \mathbb{N}$, every n -ary operation symbol $f \in \mathcal{F}$, and all $a_1, \dots, a_n \in A$. In particular, \mathbf{A}/\sim is also an \mathcal{F} -algebra. Moreover, the mapping

$$\varphi_{\sim} : A \rightarrow A/\sim, x \mapsto [x]$$

is an epimorphism from \mathbf{A} to \mathbf{A}/\sim , called the **natural homomorphism** from \mathbf{A} to \mathbf{A}/\sim .

Let \mathbf{A} and \mathbf{B} be two algebras and let $\varphi \in \text{Hom}(\mathbf{A}, \mathbf{B})$. Then the **kernel** $\ker(\varphi) := \{(a, b) \in A \times A \mid \varphi(a) = \varphi(b)\}$ of φ is a congruence on \mathbf{A} .

Theorem 1.2 (Homomorphism Theorem). *Let \mathbf{A} and \mathbf{B} be algebras and α an epimorphism from \mathbf{A} to \mathbf{B} . Then there exists an isomorphism β from $\mathbf{A}/\ker(\alpha)$ to \mathbf{B} defined by $\beta : [x] \mapsto \alpha(x)$.*

The homomorphism theorem shows that every homomorphic image of an algebra \mathbf{A} is isomorphic to a quotient algebra of \mathbf{A} . Since every quotient algebra is determined by a congruence, every homomorphic image is determined by a congruence.

An algebra \mathbf{A} is called **simple** if its only congruences are id_A and $A \times A$. Hence, every quotient algebra and every homomorphic image of a simple algebra \mathbf{A} is isomorphic to \mathbf{A} or has just one element.

1.2 Basics of order and lattice theory

Since the characterisation of proper finite simple semiring with zero in [61] is based on some lattice theoretic background, and since most of the work in this dissertation uses some order theoretic tools, we will give some information on order and lattice theory in this section. Particularly the concept of residuated mappings will be of importance for this dissertation. The reader more interested in lattice theory is referred to the standard monograph [4] by Birkhoff but also to [23] by Grätzer. More information about residuated mappings can be found in [7] and [5]. Beside the

1.2. Basics of order and lattice theory

books already mentioned, the reader may consult [25] or [52] for more background information on general order theory.

Ordered sets

An **ordered set** \mathbf{P} is a pair (P, \leq) , where P is a nonempty set and \leq is a binary, reflexive, antisymmetric, and transitive relation on P . The relation \leq is called an **order** (or **order relation**) on P . Analogously to the convention on the notation of algebras, we will denote an ordered set by a bold capital letter or as a pair consisting of the set and the order on the set. If a bold capital letter is assigned to an ordered set, the corresponding set will be denoted by the corresponding italic capital letter. Also, if not stated differently, we will denote the order by \leq . This means if an ordered set \mathbf{P} is mentioned, then it will be clear that $\mathbf{P} = (P, \leq)$.

Let $\mathbf{P} = (P, \leq)$ be an ordered set. Then we write $x < y$ if $x \leq y$ and $x \neq y$ for $x, y \in P$. Furthermore, we define the order \geq on P by $x \geq y :\Leftrightarrow y \leq x$ for $x, y \in P$. It is called the **dual order** of \leq , and $\mathbf{P}^d := (P, \geq)$ is called the **dual ordered set** of \mathbf{P} . If $x, y \in P$ with $x < y$ and $x \leq z \leq y$ imply $x = z$ or $y = z$ for every $z \in P$, then x is called a **lower neighbour** of y , and y is called an **upper neighbour** of x . If there exists an element $x \in P$ with $x \leq y$ for every $y \in P$, then x is called the **least element** of \mathbf{P} , and it is denoted by $0_{\mathbf{P}}$. A **greatest element** is defined dually and denoted by $1_{\mathbf{P}}$. Let X be a subset of P . An **upper bound** of X is an element $a \in P$ with $x \leq a$ for every $x \in X$. A **lower bound** is defined dually. If there exists a least element in the set of all upper bounds of X , then it is called the **supremum** of X and is denoted by $\bigvee X$ or $\text{sup } X$. Dually, a greatest lower bound is called the **infimum** and is denoted by $\bigwedge X$ or $\text{inf } X$. If $X = \{x, y\}$, then we also write $x \vee y$ for $\bigvee X$ and $x \wedge y$ for $\bigwedge X$. Supremum and infimum are also called **join** and **meet**.

Semilattices

A **join-semilattice** (or **\vee -semilattice**) is an ordered set $\mathbf{L} = (L, \leq)$, in which the supremum $x \vee y$ exists for every two elements $x, y \in L$. **Meet-semilattices** (or **\wedge -semilattices**) are defined dually.

An algebra $(L, +)$ is called a **semilattice** if $+$ is a binary, associative, commutative, idempotent operation on L .

The following theorem states that the definition of (join-)semilattices as ordered sets is equivalent to the definition of semilattices as algebras, what can be found

in [4] or [23].

Theorem 1.3. 1. Let the ordered set $\mathbf{L} = (L, \leq)$ be a join-semilattice and set $x \vee y := \sup\{x, y\}$ for all $x, y \in L$. Then the algebra $\mathbf{L}^a = (L, \vee)$ is a semilattice.

2. Let the algebra $(L, +)$ be a semilattice and define the binary relation \leq on L by

$$x \leq y :\Leftrightarrow x + y = y \quad \text{for all } x, y \in L.$$

Then $\mathbf{L}^p = (L, \leq)$ is an ordered set, and the ordered set is a join-semilattice with $x \vee y = x + y$ for all $x, y \in L$.

3. Let the ordered set $\mathbf{L} = (L, \leq)$ be a join-semilattice. Then $(\mathbf{L}^a)^p = \mathbf{L}$.

4. Let the algebra $(L, +)$ be a semilattice. Then $(\mathbf{L}^p)^a = \mathbf{L}$.

An analogous theorem exists for meet-semilattices. Due to this theorem, we do not have to state explicitly if we consider a join-semilattice \mathbf{L} as an ordered set (L, \leq) or as an algebra (L, \vee) if we mention just \mathbf{L} . However, if a certain situation requires a certain consideration, then we will do so. The same holds for meet-semilattices.

An element a of a join-semilattice \mathbf{L} is called **join-irreducible** if it is not a least element and $a = b \vee c$ implies $b = a$ or $c = a$ for all $b, c \in L$. Otherwise it is called **join-reducible**. The set of join-irreducible elements of \mathbf{L} is denoted by $J(\mathbf{L})$. If \mathbf{L} is finite, then the element a is join-irreducible iff it has exactly one lower neighbour. **Meet-irreducible** and **meet-reducible** are defined dually for elements in meet-semilattices. The set of meet-irreducible elements of a meet-semilattice \mathbf{L} is denoted by $M(\mathbf{L})$.

Lattices

The ordered set $\mathbf{L} = (L, \leq)$ is a **lattice** if the supremum $x \vee y$ and the infimum $x \wedge y$ exist for any two elements $x, y \in L$. Furthermore, it is called a **complete lattice** if the supremum $\bigvee X$ and the infimum $\bigwedge X$ exist for every subset X of L . A complete lattice \mathbf{L} has a greatest element, $1_{\mathbf{L}} = \bigvee L$, and a least element, $0_{\mathbf{L}} = \bigwedge L$. From the definition there follows that the supremum and the infimum also exist for $X = \emptyset$. We have $\bigvee \emptyset = 0_{\mathbf{L}}$ and $\bigwedge \emptyset = 1_{\mathbf{L}}$.

There also exists a definition of *lattices* as algebras: An algebra (L, \vee, \wedge) is called a **lattice** if \vee and \wedge are binary, associative, commutative operations on L satisfying

1.2. Basics of order and lattice theory

the **absorption laws**

$$x \vee (x \wedge y) = x \quad \text{and} \quad x \wedge (x \vee y) = x$$

for all $x, y \in L$.

In analogy to Theorem 1.3, the following theorem shows that the two definitions of lattices are equivalent. For a proof see e.g. [23].

Theorem 1.4. 1. Let the ordered set $\mathbf{L} = (L, \leq)$ be a lattice and set

$$x \vee y := \sup\{x, y\} \quad \text{and} \quad x \wedge y := \inf\{x, y\}$$

for all $x, y \in L$. Then the algebra $\mathbf{L}^a = (L, \vee, \wedge)$ is a lattice.

2. Let the algebra $\mathbf{L} = (L, \vee, \wedge)$ be a lattice and define the binary relation \leq on L by

$$x \leq y \quad :\Leftrightarrow \quad x \vee y = y \quad \text{for all } x, y \in L.$$

Then $\mathbf{L}^p = (L, \leq)$ is an ordered set, and the ordered set \mathbf{L}^p is a lattice.

3. Let the ordered set $\mathbf{L} = (L, \leq)$ be a lattice. Then $(\mathbf{L}^a)^p = \mathbf{L}$.

4. Let the algebra $\mathbf{L} = (L, \vee, \wedge)$ be a lattice. Then $(\mathbf{L}^p)^a = \mathbf{L}$.

Because of this theorem, we also do not have to state explicitly if we consider a lattice \mathbf{L} as an ordered set (L, \leq) or as an algebra (L, \vee, \wedge) if we mention just \mathbf{L} , unless a certain situation requires a certain consideration.

A lattice \mathbf{K} is a **sublattice** of a lattice \mathbf{L} if the algebra (K, \vee, \wedge) is a subalgebra of (L, \vee, \wedge) .

A lattice \mathbf{L} is called **distributive** if

$$\begin{aligned} x \vee (y \wedge z) &= (x \vee y) \wedge (x \vee z) \quad \text{and} \\ x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z) \end{aligned}$$

are satisfied for all $x, y, z \in L$.

An element $a \in L$ of a complete lattice $\mathbf{L} = (L, \leq)$ is called **\vee -irreducible** (or **complete join-irreducible**) if $a \neq \vee\{x \in L \mid x < a\}$. Analogously, a is called **\wedge -irreducible** (or **complete meet-irreducible**) if $a \neq \wedge\{x \in L \mid a < x\}$. For finite lattices, \vee -irreducible is equivalent to join-irreducible and \wedge -irreducible is equivalent to meet-irreducible.

Residuated mappings

Let $\mathbf{P} = (P, \leq)$ and $\mathbf{Q} = (Q, \leq)$ be ordered sets and $f : P \rightarrow Q$ a mapping. Then f is called **isotone** if it fulfils $x \leq y \Rightarrow f(x) \leq f(y)$ for all $x, y \in P$. If f is isotone and there exists an isotone mapping $g : Q \rightarrow P$ with $f \circ g \leq \text{id}_Q$ and $g \circ f \geq \text{id}_P$, then f is called **residuated**. If f is residuated, then the mapping $g : Q \rightarrow P$ satisfying $f \circ g \leq \text{id}_Q$ and $g \circ f \geq \text{id}_P$ is uniquely determined. Furthermore, it is called the **residual** of f and denoted by f^+ . One also finds that f is residuated iff the set $\{x \in P \mid f(x) \leq y\}$ is nonempty and admits a greatest element for every $y \in Q$. Moreover, if f is residuated, then f^+ fulfils $f^+(y) = \bigvee \{x \in P \mid f(x) \leq y\}$ for every $y \in Q$ (see [7]). By $\text{Res}(\mathbf{P}, \mathbf{Q})$ we denote the set of all residuated mappings from \mathbf{P} to \mathbf{Q} and we define $\text{Res}(\mathbf{P}) := \text{Res}(\mathbf{P}, \mathbf{P})$.

Morphisms

Let $\mathbf{P} = (P, \leq)$ and $\mathbf{Q} = (Q, \leq)$ be ordered sets and $f : P \rightarrow Q$ a mapping. Then f is an **order embedding** from \mathbf{P} into \mathbf{Q} if it fulfils $x \leq y \Leftrightarrow f(x) \leq f(y)$ for all $x, y \in P$. An order embedding is necessarily injective and isotone. If f is a surjective order embedding, then it is called an **(order) isomorphism** from \mathbf{P} to \mathbf{Q} . Dually, f is called a **dual (order) isomorphism** if it is surjective and satisfies $x \leq y \Leftrightarrow f(x) \geq f(y)$ for all $x, y \in P$. If there exists an order isomorphism from \mathbf{P} to \mathbf{Q} , then \mathbf{P} and \mathbf{Q} are called **isomorphic**, which is denoted by $\mathbf{P} \cong \mathbf{Q}$. An isomorphism from \mathbf{P} to \mathbf{P} is called an **(order) automorphism** of \mathbf{P} . The set of automorphisms of \mathbf{P} is denoted by $\text{Aut}(\mathbf{P})$. Note that if \mathbf{L} and \mathbf{K} are join-semilattices (meet-semilattices), then a mapping $f : L \rightarrow K$ is an order isomorphism between the ordered sets (L, \leq) and (K, \leq) iff it is an isomorphism between the algebras (L, \vee) and (K, \vee) ((L, \wedge) and (K, \wedge)). In particular, if \mathbf{L} and \mathbf{K} are lattices, then f is an order isomorphism between the ordered sets (L, \leq) and (K, \leq) iff it is an isomorphism between the algebras (L, \vee, \wedge) and (K, \vee, \wedge) . The corresponding holds for automorphisms of semilattices and lattices.

Let $\mathbf{L} = (L, \leq)$ and $\mathbf{K} = (K, \leq)$ be two join-semilattices. Then a mapping $f : L \rightarrow K$ is called a **join-morphism** or **\vee -morphism** if it satisfies

$$f(x \vee y) = f(x) \vee f(y)$$

for all $x, y \in L$. By $\text{JM}(\mathbf{L}, \mathbf{K})$ we denote the set of all join-morphisms from \mathbf{L} to \mathbf{K} and we define $\text{JM}(\mathbf{L}) := \text{JM}(\mathbf{L}, \mathbf{L})$. Furthermore, f is said to be a **complete join-**

1.2. Basics of order and lattice theory

morphism or **complete \vee -morphism** if for every subset X of L , such that $\bigvee X$ exists in \mathbf{L} , $\bigvee f(X)$ exists in \mathbf{K} and

$$f(\bigvee X) = \bigvee f(X).$$

(**Complete**) **meet-morphisms** or (**complete**) **\wedge -morphisms** between meet-semilattices are defined dually.

A complete join-morphism $f : L \rightarrow K$ between complete lattices $\mathbf{L} = (L, \leq)$ and $\mathbf{K} = (K, \leq)$ satisfies in particular

$$f(0_{\mathbf{L}}) = f(\bigvee \emptyset) = \bigvee f(\emptyset) = \bigvee \emptyset = 0_{\mathbf{K}}.$$

If \mathbf{L} is finite, then a mapping $g : L \rightarrow K$ is a complete join-morphism iff it is a join-morphism and fulfils $f(0_{\mathbf{L}}) = 0_{\mathbf{K}}$. The following proposition states a connection between complete join-morphisms and residuated mappings between complete lattices [7]:

Proposition 1.5. *Let \mathbf{L} and \mathbf{K} be complete lattices and $f : L \rightarrow K$ a mapping. Then f is residuated iff it is a complete join-morphism.*

Closure operators and closure systems

If \mathbf{P} is an ordered set and $\varphi : P \rightarrow P$ a mapping, then φ is called **idempotent** if it satisfies $\varphi(x) = \varphi(\varphi(x))$, **increasing** if it satisfies $x \leq \varphi(x)$, and **decreasing** if it satisfies $x \geq \varphi(x)$ for every $x \in P$. Furthermore, φ is called a **closure operator** (**kernel operator**) on \mathbf{P} if it is isotone, idempotent, and increasing (decreasing). Clearly, φ is a closure operator on \mathbf{P} iff it is a kernel operator on \mathbf{P}^d . By definition it follows easily that φ is a closure operator on \mathbf{P} iff it satisfies

$$x \leq \varphi(y) \Leftrightarrow \varphi(x) \leq \varphi(y) \tag{1.1}$$

for all $x, y \in P$. Dually, φ is a kernel operator on \mathbf{P} iff it satisfies

$$\varphi(y) \leq x \Leftrightarrow \varphi(x) \leq \varphi(y) \tag{1.2}$$

for all $x, y \in P$. A subset $S \subseteq P$ is called a **closure system** (**kernel system**) of \mathbf{P} if there exists a closure operator (kernel operator) γ on \mathbf{P} satisfying $S = \gamma(P)$. We denote the set of all closure systems of \mathbf{P} by $C(\mathbf{P})$ and the set of all kernel systems of \mathbf{P} by $K(\mathbf{P})$. If $\mathbf{L} = (L, \leq)$ is a complete lattice and S is a subset of L ,

then S is a closure system of \mathbf{L} iff S is closed under \bigwedge . Dually, S is a kernel system of \mathbf{L} iff S is closed under \bigvee . If S is a closure system (kernel system) of \mathbf{L} , then $\mathbf{S} := (S, \leq \cap (S \times S))$ is a complete lattice and the infimum (supremum) in \mathbf{S} corresponds to the infimum (supremum) in \mathbf{L} (see [57]).

1.3 Semirings

Semirings are a natural generalisation of rings, where the additive structure is allowed to be a commutative semigroup instead of an abelian group. A well-known example of a semiring that is not a ring is provided by the set of natural numbers with the usual addition and multiplication. The concept of semirings was introduced by Vandiver [56] in 1934. Semirings are widely used as a tool in mathematics but also have many applications in computer science, e.g. in automata theory. For more detailed information on semirings, the reader is referred to [20, 27, 28]. A large collection of references on semirings can be found in [19]. In order to define semirings, one needs the definition of semigroup:

Definition 1.6. Let S be a nonempty set and \cdot a binary operation on S . Then (S, \cdot) is called a **semigroup** if the operation \cdot is associative.

The reader should note that the notion of *semiring* is not unique in the literature. We will use the following version:

Definition 1.7. Let R be a nonempty set and $+$ and \cdot two binary operations on R , called **addition** and **multiplication**. Then the algebra $(R, +, \cdot)$ is called a **semiring** if

- $(R, +)$ is a commutative semigroup,
- (R, \cdot) is a semigroup,
- the **distributive laws**

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{and} \quad (x + y) \cdot z = x \cdot z + y \cdot z \quad \text{for all } x, y, z \in R$$

hold.

A semiring $(R, +, \cdot)$ is called a **proper semiring** if it is not a ring, i.e. $(R, +)$ is not a group. It is called **commutative** if (R, \cdot) is commutative.

1.3. Semirings

If $(R, +, \cdot)$ is a semiring, then we mostly write for the multiplication $xy := x \cdot y$ for $x, y \in R$.

Definition 1.8. Let $(R, +, \cdot)$ be a semiring. If there exists an additively neutral element 0 in R that fulfils $0r = r0 = 0$ for every $r \in R$, then it is called the **zero** of $(R, +, \cdot)$. If there exists a multiplicatively neutral element 1 in R , then it is called the **one** of $(R, +, \cdot)$.

Matrix semirings

Let $(R, +, \cdot)$ be a semiring and I an index set. An $I \times I$ **matrix** A over R is a mapping $A : I \times I \rightarrow R$. By $\text{Mat}_{I \times I}(R)$ we denote the set of all $I \times I$ matrices over R . If $I = \{1, \dots, n\}$ for an $n \in \mathbb{N}$, then we also call an $I \times I$ matrix an $n \times n$ matrix and we denote $\text{Mat}_{n \times n}(R) := \text{Mat}_{I \times I}(R)$. If $A \in \text{Mat}_{I \times I}(R)$ and $(i, j) \in I \times I$, then we define $a_{i,j} := A(i, j)$. Now let I be finite. For $A, B \in \text{Mat}_{I \times I}(R)$, the **matrix sum** $A + B$ is defined component-wise. The **matrix product** $A \cdot B$ is defined to be the matrix C , where

$$c_{i,j} = \sum_{k \in I} a_{i,k} b_{k,j}.$$

The algebra $(\text{Mat}_{I \times I}(R), +, \cdot)$ equipped with these two operations is also a semiring, called **matrix semiring**.

Simple semirings

By Definition 1.1, a congruence on a semiring $(R, +, \cdot)$ is an equivalence relation \sim on R such that

$$a \sim b \text{ and } c \sim d \Rightarrow a + c \sim b + d \quad \text{for all } a, b, c, d \in R \text{ and} \quad (1.3)$$

$$a \sim b \text{ and } c \sim d \Rightarrow a \cdot c \sim b \cdot d \quad \text{for all } a, b, c, d \in R. \quad (1.4)$$

One can easily see that Equation 1.3 is equivalent to

$$a \sim b \Rightarrow a + c \sim b + c \quad \text{for all } a, b, c \in R \quad (1.5)$$

and Equation 1.4 to

$$a \sim b \Rightarrow a \cdot c \sim b \cdot c \text{ and } c \cdot a \sim c \cdot b \quad \text{for all } a, b, c \in R. \quad (1.6)$$

The notion of simplicity for semirings is not unique in the literature either. We

use the common definition of *simple* from universal algebra:

Definition 1.9. A semiring $(R, +, \cdot)$ is called **simple** if its only congruences are id_R and $R \times R$.

1.3.1 Proper finite simple semirings with zero

Until the end of the last decade, proper finite simple semirings, especially those with zero, had not been comprehensively studied. In 2008, Zumbrägel came up with the classification of finite simple semirings with zero in [61]. The main result of it gives a characterisation of proper finite simple semirings with zero. Originally Zumbrägel characterised these semirings as endomorphism semirings of monoids. In this section we will present this result, and we will reformulate it in terms of residuated mappings of lattices. The representation of semirings as semirings of residuated mappings is helpful, as we can achieve new results concerning simple semirings due to the rich theory of ordered sets, lattices, and residuated mappings.

Let $\mathbf{M} = (M, +, 0)$ be a commutative monoid. Then the algebra $(\text{End}(\mathbf{M}), +, \circ)$ is a semiring with zero, where the addition $+$ is the pointwise sum and the multiplication \circ the composition of two mappings. If \mathbf{M} is idempotent, then $(\text{End}(\mathbf{M}), +)$ is also idempotent and if furthermore $|M| > 1$, then $(\text{End}(\mathbf{M}), +, \circ)$ is in particular a proper semiring.

Now let $\mathbf{M} = (M, +, 0)$ be a commutative idempotent monoid. Then a subsemiring $(R, +, \circ)$ of $(\text{End}(\mathbf{M}), +, \circ)$ is called **dense** in [61] if R contains the endomorphism $e_{a,b} \in \text{End}(\mathbf{M})$ for all $a, b \in M$, which is defined by

$$e_{a,b}(x) := \begin{cases} 0 & \text{if } x + a = a \\ b & \text{else} \end{cases}$$

for all $x \in M$. The main result from [61] is the following:

Theorem 1.10. *Let $(R, +, \cdot)$ be a proper finite semiring with zero. Then the following are equivalent:*

1. $(R, +, \cdot)$ is simple.
2. $|R| \leq 2$ or $(R, +, \cdot)$ is isomorphic to a dense subsemiring of $(\text{End}(\mathbf{M}), +, \circ)$, where $\mathbf{M} = (M, +, 0)$ is a finite idempotent commutative monoid.

If $\mathbf{M} = (M, +, 0)$ is a finite commutative idempotent monoid and one defines the order relation \leq on M by $x \leq y :\Leftrightarrow x + y = y$, then (M, \leq) is a lattice with

1.4. Cryptography

$\sup\{x, y\} = x + y$ for all $x, y \in M$ and least element 0. Furthermore, a mapping $f : M \rightarrow M$ is an endomorphism of \mathbf{M} iff it is a join-morphism of (M, \leq) satisfying $f(0) = 0$, i.e. it is a residuated mapping of (M, \leq) . Hence, one can also formulate Theorem 1.10 by means of residuated mappings of lattices. In fact, we have the following: Let $\mathbf{L} = (L, \leq)$ be a complete lattice. The algebra $(\text{Res}(\mathbf{L}), \vee, \circ)$ is a semiring, where the addition \vee is the pointwise supremum and the multiplication \circ the composition of two mappings. The mapping $\mathbf{0}_{\mathbf{L}} : L \rightarrow L, x \mapsto 0_{\mathbf{L}}$ is a zero and id_L a one of $(\text{Res}(\mathbf{L}), \vee, \circ)$. This semiring is furthermore additively idempotent and if $|L| > 1$, then it is in particular a proper semiring. If $\mathbf{K} = (K, \leq)$ is another complete lattice, then we define for $a \in L$ and $b \in K$ the residuated mapping $e_{a,b} \in \text{Res}(\mathbf{L}, \mathbf{K})$ by

$$e_{a,b}(x) := \begin{cases} 0_{\mathbf{K}} & \text{if } x \leq a \\ b & \text{else} \end{cases}$$

for every $x \in L$. We call a subsemiring (R, \vee, \circ) of $(\text{Res}(\mathbf{L}), \vee, \circ)$ **dense** if $e_{a,b} \in R$ for all $a, b \in L$. Now we can reformulate Theorem 1.10:

Theorem 1.11. *Let \mathbf{L} be a finite lattice and (R, \vee, \circ) a dense subsemiring of $(\text{Res}(\mathbf{L}), \vee, \circ)$. Then (R, \vee, \circ) is a proper finite simple semiring with zero. Conversely, every proper finite simple semiring $(S, +, \cdot)$ with $|S| > 2$ and a zero is isomorphic to such a semiring.*

In [61], it was already pointed out that endomorphisms of finite commutative idempotent monoids correspond to join-morphisms of finite lattices that preserve the least element of the lattice. However, a connection between Theorem 1.10 and residuated mappings did not appear in the literature before (except in [34, 35, 36], which contain results of the thesis). The formulation of the result in Theorem 1.11, despite being a trivial consequence of Theorem 1.10, is novel and enables new approaches for the study of proper finite simple semirings with zero due to the established theory of residuated mappings.

1.4 Cryptography

Cryptography is the science of secret writing. Its purpose is to enable secure communication, an old desire of humankind. The first known use of cryptography leads back to Ancient Egypt. With the expansion of computers and the increasing use of telecommunication, cryptography is now more important than ever before. In

the recent decades it became a much-noticed discipline in mathematics, computer science and electrical engineering.

Modern cryptography deals with more than secrecy. It can be seen as the study of information security, where various aspects are considered. The most important ones are:

- *Confidentiality*: Only authorised parties should get access to the information.
- *Data integrity*: Data manipulation by unauthorised parties should be detected.
- *Authentication*: The author of the information should get identified.

In this section we state the necessary information about cryptography to understand the cryptosystems based on semigroup actions proposed in [42]. For more information, we refer to various textbooks, e.g. [21, 22, 33, 43].

A typical scenario considered in cryptography is the following: Two parties, typically called Alice and Bob, wish to communicate with each other in a secure way. The problem is that there may be an eavesdropper, usually called Eve, present. If Alice wishes to send a message m to Bob such that Eve is not able to read this message, she will apply an encryption function φ on m and will obtain a ciphertext c , which will be sent to Bob. If Bob has the corresponding decryption function ψ , then Bob can recover m from c . To prevent Eve from recovering the message m , it should be hard for Eve to find ψ , and it should be hard to recover m from c without ψ . The functions φ and ψ usually depend on two inputs, namely a message m and a key k_A , or a ciphertext c and a key k_B , respectively. If both parties use the same key, i.e. $k_A = k_B$, then one talks about a *symmetric encryption scheme*. If a symmetric encryption scheme is used, the parties have to agree on a secret key. Until the 1970's it was believed that a completely secure channel is necessary to communicate such a key, which is a strong assumption. However, Whitfield Diffie and Martin Hellman observed that an agreement over an insecure channel is also possible. This led to the *Diffie-Hellman key agreement* [10].

Protocol 1.12. (Diffie-Hellman key agreement)²

- Alice and Bob publicly agree on a finite group (G, \cdot) and an element $g \in G$.
- Alice chooses an integer a and computes $\alpha = g^a$. She sends α to Bob and keeps a secret.

²Diffie and Hellman used originally the group (\mathbb{Z}_p, \cdot) for a prime number p , and the element g was a primitive element in (\mathbb{Z}_p, \cdot) .

1.4. Cryptography

- Bob chooses an integer b and computes $\beta = g^b$. He sends β to Alice and keeps b secret.
- Their common secret key is $k = \alpha^b = \beta^a = g^{ab}$.

If an eavesdropper Eve is present, then the group (G, \cdot) and the elements g, α , and β are known to her. To prevent Eve from knowing the secret key k it should be hard to recover k from the given information. This means the so-called *Diffie-Hellman problem* should be hard.

Problem 1.13. (Diffie-Hellman problem): Given a finite group (G, \cdot) , an element $g \in G$, and elements $\alpha = g^a$ and $\beta = g^b$ for some positive integers a, b , find the element g^{ab} .

Obviously, Eve could compute k if she additionally knew a or b . Hence, it is a necessary condition that the *discrete logarithm problem* is hard.

Problem 1.14. (Discrete logarithm problem): Given a finite group (G, \cdot) , elements $a, b \in G$ such that $b \in \langle a \rangle$, find a positive integer n with $a^n = b$.

It is unknown if these two problems are equivalent. However, it is believed that they are and with some additional assumptions this was proven in [40].

1.4.1 Cryptography based on semigroup actions

The group exponentiation $\mathbb{Z} \times G \rightarrow G$, $(n, g) \mapsto g^n$, where (G, \cdot) is a finite group, used in the Diffie-Hellman key agreement protocol is an example of a semigroup action. More precisely, the commutative semigroup (\mathbb{Z}, \cdot) is acting on the set G . Maze, Monico, and Rosenthal observed that the Diffie-Hellman key agreement protocol can be generalised by using arbitrary semigroup actions, where the semigroup has to be commutative [41, 42, 46].

Definition 1.15. Let (A, \cdot) be a semigroup and X a set. A **semigroup action** of (A, \cdot) on X is a mapping

$$\rho : A \times X \rightarrow X$$

satisfying $\rho(a \cdot b, x) = \rho(a, \rho(b, x))$ for all $a, b \in A$ and $x \in X$.

For a semigroup action ρ of a semigroup (A, \cdot) on a set X , we will mostly write $a.x := \rho(a, x)$. Furthermore, we use the notation $A.x := \{a.x \mid a \in A\}$ for every $x \in X$.

The resulting generalisation of the Diffie-Hellman key agreement protocol by using commutative semigroup actions is the following protocol [42, Protocol 2.1]:

Protocol 1.16. (Extended Diffie-Hellman key agreement)

- Alice and Bob publicly agree on a commutative semigroup (S, \cdot) , a set X , a semigroup action of (S, \cdot) on X , and an element $x \in X$.
- Alice chooses $a \in S$ and computes $\alpha = a.x$. She sends α to Bob and keeps a secret.
- Bob chooses $b \in S$ and computes $\beta = b.x$. He sends β to Alice and keeps b secret.
- Their common secret key is $k = b.\alpha = a.\beta = (a \cdot b).x$.

As the Diffie-Hellman problem has to be hard for the Diffie-Hellman protocol, the so-called *Diffie-Hellman semigroup action problem* has to be hard for Protocol 1.16.

Problem 1.17. (Diffie-Hellman semigroup action problem): Given a commutative semigroup (S, \cdot) acting on a set X , an element $x \in X$, and elements $\alpha = a.x$ and $\beta = b.x$ for some $a, b \in S$, find $(a \cdot b).x$.

The corresponding problem to the discrete logarithm problem is the *semigroup action problem*.

Problem 1.18. (Semigroup action problem): Given a semigroup (S, \cdot) acting on a set X , an element $x \in X$, and an element $\alpha \in S.x$, find $a \in S$ such that $a.x = \alpha$.

Clearly, the semigroup action problem has to be hard if the Diffie-Hellman semigroup action problem is supposed to be hard. However, here it is also unknown if the two problems are equivalent.

A concrete realisation of Protocol 1.16 was also proposed in [42]. The semigroup action used there involves matrices over semirings. We need some preparation to state the protocol in detail.

Definition 1.19. The **centre** of a semiring $(R, +, \cdot)$ is the set

$$\{r \in R \mid \forall s \in R : rs = sr\}.$$

1.4. Cryptography

Let $(R, +, \cdot)$ be a finite semiring with zero, let n be a positive integer, and let C be the center of $(R, +, \cdot)$. Then C is nonempty since it contains the zero of $(R, +, \cdot)$. Let $C[x]$ be the set of polynomials in the indeterminate x with coefficients in C . If

$$p(x) = r_0 + r_1x + \cdots + r_kx^k \in C[x]$$

and $M \in \text{Mat}_{n \times n}(R)$, then let $p(M) := r_0I_n + r_1M + \cdots + r_kM^k$, where r_0I_n is defined to be the $n \times n$ diagonal matrix with entry r_0 in each diagonal element. Furthermore, let $C[M] := \{p(M) \mid p(x) \in C[x]\}$. Then $(C[M], +, \cdot)$ is a commutative subsemiring of $(\text{Mat}_{n \times n}(R), +, \cdot)$. Let $M_1, M_2 \in \text{Mat}_{n \times n}(R)$. Define the operation $*$ on $C[M_1] \times C[M_2]$ by $(A, B) * (C, D) := (A \cdot C, D \cdot B)$ for $(A, B), (C, D) \in C[M_1] \times C[M_2]$. Consider the following semigroup action of the semigroup $(C[M_1] \times C[M_2], *)$ on the set $\text{Mat}_{n \times n}(R)$:

$$\begin{aligned} (C[M_1] \times C[M_2]) \times \text{Mat}_{n \times n}(R) &\rightarrow \text{Mat}_{n \times n}(R) \\ ((p(M_1), q(M_2)), A) &\mapsto p(M_1) \cdot A \cdot q(M_2). \end{aligned}$$

Using this concrete semigroup action in Protocol 1.16 yields the following, which is [42, Protocol 5.1]:

Protocol 1.20. (Diffie-Hellman with two-sided matrix semiring action)

- Alice and Bob publicly agree on a finite semiring $(R, +, \cdot)$ with zero and choose a positive integer n and matrices $M_1, M_2, S \in \text{Mat}_{n \times n}(R)$.
- Alice chooses polynomials $p_a, q_a \in C[x]$ and computes $A = p_a(M_1) \cdot S \cdot q_a(M_2)$. She sends A to Bob and keeps p_a, q_a secret.
- Bob chooses polynomials $p_b, q_b \in C[x]$ and computes $B = p_b(M_1) \cdot S \cdot q_b(M_2)$. He sends B to Alice and keeps p_b, q_b secret.
- Their common secret key is

$$\begin{aligned} k &= p_a(M_1) \cdot B \cdot q_a(M_2) = p_b(M_1) \cdot A \cdot q_b(M_2) \\ &= p_a(M_1) \cdot p_b(M_1) \cdot S \cdot q_b(M_2) \cdot q_a(M_2). \end{aligned}$$

In [42] (also in [41] and [46]), it was argued that the use of simple semirings is advantageous to avoid Pohlig-Hellman type attacks. The Pohlig-Hellman attack allows to compute the discrete logarithm in a cyclic group based on the Chinese

remainder theorem. The complexity of the algorithm depends on the largest prime factor of the order of the group. To prevent a Pohlig-Hellman attack, the group can be chosen to be a cyclic group of large prime order, which means that the group is a simple group. In order to prevent a similar attack on cryptosystems using semirings, the use of simple semirings was suggested. If the used semiring would not be simple, the semigroup action problem could be solved in some quotient semirings from which one may gain some information to solve the semigroup action problem in the original semiring.

Also the use of proper semirings was suggested to minimize the possibilities of attacks based on linear algebra. The classification of finite simple semirings with zero in [61] enabled a huge choice for an appropriate semiring for the use in Protocol 1.20.

In [42], an example of Protocol 1.20 with some specific parameters was presented. The chosen semiring had six elements, the matrices had size 20×20 , and the polynomials have been bounded to degree at most 50. In [54], Steinwandt and Corona presented a heuristic attack for Protocol 1.20, which broke the cryptosystem for the given parameters. Therefore, the parameter sizes of the protocol have to be increased in order keep the protocol relevant for practical purposes. In particular, the choice of the semiring can be improved. In fact, the semiring used in the example is the smallest proper finite simple semiring with zero and more than two elements. Due to Theorem 1.11 (Theorem 1.10) one can easily construct proper finite simple semirings with zero with large cardinalities.

1.5 Overview

Semirings and specifically simple semirings were given a new application in the work of Maze, Monico, and Rosenthal described in Section 1.4.1. After some initial progress in the classification of finite simple semiring by Monico [45], Zumbrägel's complete classification of finite simple semirings with zero in [61] was a step of high importance for the studies on this topic. The goal of this dissertation is to continue these studies based on the results in [61]. More precisely, we investigate proper finite simple semirings with zero regarding cryptographic applications, and we continue the classification of finite simple semirings by using the ideas from [61].

In Chapter 2, we analyse a cryptosystem proposed in [62]. This cryptosystem uses a semigroup action that involves residuated mappings. However, only the composition of residuated mappings is used. Therefore, no semiring is properly involved in this cryptosystem. The conclusion of this chapter is that the private key can

1.5. Overview

be completely recovered by the public information. The proposed cryptosystem is therefore insecure.

Chapter 3 deals with the representation of proper finite simple semirings with zero. The underlying problem is that one needs a representation of semirings as in Theorem 1.11 that requires little space, enables an efficient performance of the operations, and most importantly admits a method to generate arbitrary semiring elements. We find that it is advantageous to store a semiring implicitly by its generating lattice. Therefore, the question arises how many residuated mappings there exist of a finite lattice. This problem is also studied in Chapter 3, where we consider three different approaches.

In Chapter 4, we investigate invertible matrices over finite additively idempotent semirings. The motivation clearly comes from the cryptographic application of matrices over finite simple semirings. Since proper finite simple semirings with zero are additively idempotent, the results of this chapter cover the case of invertible matrices over such semirings. Due to the fact that every finite additively idempotent semiring with zero and one can be represented as a semiring of residuated mappings, we achieve more general results. The outcome of this chapter is a criterion for matrices over such semirings for being invertible, a construction of the inverse matrix of an invertible matrix, and a formula for the number of invertible matrices.

In the last chapter we proceed on the classification of finite simple semirings. Since all finite simple semirings not yet covered by the classification are additively idempotent, we attempt to characterise every such semiring as a semiring of join-morphisms of a finite semilattice. This requires an extensive study of irreducible semimodules and eventually leads to some characterisation theorems, which are presented in Section 5.4. Proving these theorems, we complete the classification of finite simple semirings *with an additively neutral element*, stated in Theorem 5.63. Moreover, we present some constructions of semirings, and conjecture that they complete the classification of finite simple semirings.

Chapter 2

Analysis of a cryptosystem using residuated mappings

In [62] a cryptosystem based on semigroup actions was proposed that uses residuated mappings. We will analyse its security in the current chapter, and we will find out that the key can be completely recovered by the public information.

2.1 The protocol

To present the cryptosystem, we need *vertical sums* of ordered sets.

Let $\mathbf{P} = (P, \leq_{\mathbf{P}})$ be an ordered set with a greatest element $1_{\mathbf{P}}$ and $\mathbf{Q} = (Q, \leq_{\mathbf{Q}})$ an ordered set with a least element $0_{\mathbf{Q}}$. The ordered set (S, \leq) is the **vertical sum** of \mathbf{P} and \mathbf{Q} , denoted by $\mathbf{P} \bar{\oplus} \mathbf{Q}$, if $P \cap Q = \{1_{\mathbf{P}}\} = \{0_{\mathbf{Q}}\}$, $S = P \cup Q$, and \leq satisfies

$$x \leq y \Leftrightarrow x \leq_{\mathbf{P}} y \text{ or } x \leq_{\mathbf{Q}} y \text{ or } (x, y) \in P \times Q$$

for all $x, y \in S$.

Let \mathbf{L} and \mathbf{K} be finite lattices and $\mathbf{M} := \mathbf{L} \bar{\oplus} \mathbf{K}$. Define

$$\begin{aligned} R_{\mathbf{L}} &:= \{f \in \text{Res}(\mathbf{M}) \mid f|_K = \text{id}_K\}, \\ R_{\mathbf{K}} &:= \{f \in \text{Res}(\mathbf{M}) \mid f|_L = \text{id}_L\}. \end{aligned}$$

Since every mapping $f \in R_{\mathbf{L}}$ and every mapping $g \in R_{\mathbf{K}}$ satisfies $f(1_{\mathbf{L}}) = f(0_{\mathbf{K}}) = 0_{\mathbf{K}} = 1_{\mathbf{L}}$ and $g(0_{\mathbf{K}}) = g(1_{\mathbf{L}}) = 1_{\mathbf{L}} = 0_{\mathbf{K}}$, respectively, they also satisfy $f(L) \subseteq L$ and $g(K) \subseteq K$. Therefore, the equality $f \circ g = g \circ f$ holds for all $f \in R_{\mathbf{L}}$ and $g \in R_{\mathbf{K}}$.

The following protocol from [62, Section 4.2.1] is the one that we will analyse.

Protocol 2.1.

- Alice and Bob publicly agree on two finite lattices \mathbf{L} and \mathbf{K} and choose an element $h \in \text{Res}(\mathbf{L} \oplus \mathbf{K})$.
- Alice chooses $f_A \in R_{\mathbf{L}}$ and $g_A \in R_{\mathbf{K}}$. She sends $f_A \circ h \circ g_A$ to Bob and keeps f_A and g_A secret.
- Bob chooses $f_B \in R_{\mathbf{L}}$ and $g_B \in R_{\mathbf{K}}$. He sends $g_B \circ h \circ f_B$ to Alice and keeps f_B and g_B secret.
- Their common secret key is

$$k = f_A \circ (g_B \circ h \circ f_B) \circ g_A = g_B \circ (f_A \circ h \circ g_A) \circ f_B.$$

Note that in this protocol just the multiplication of the semiring $(\text{Res}(\mathbf{L} \oplus \mathbf{K}), \vee, \circ)$ is used. However, the semigroup $(\text{Res}(\mathbf{L} \oplus \mathbf{K}), \circ)$ is not necessarily simple. Therefore, there exists no reason to restrict to the residuated mappings of $\mathbf{L} \oplus \mathbf{K}$. In fact, one could use any mappings that satisfy $f|_K = \text{id}_K$ and $f(L) \subseteq L$ or $f|_L = \text{id}_L$ and $f(K) \subseteq K$, respectively. Moreover, it is not necessary to consider mappings of lattices. Instead one can use mappings of arbitrary sets. To analyse the cryptosystem, we will use this more general viewpoint. More precisely, we will use the following setting:

Let X be a finite set, let U and V be two subsets of X satisfying $U \cup V = X$, let $\mathcal{T}(X) := \{f \mid f : X \rightarrow X\}$, and define

$$\begin{aligned} R_U &:= \{f \in \mathcal{T}(X) \mid f|_V = \text{id}_V, f(U) \subseteq U\}, \\ R_V &:= \{f \in \mathcal{T}(X) \mid f|_U = \text{id}_U, f(V) \subseteq V\}. \end{aligned}$$

Then we have that $f \circ g = g \circ f$ for all $f \in R_U$ and $g \in R_V$.

Now we will reformulate Protocol 2.1 in terms of this more general setting.

Protocol 2.2.

- Alice and Bob publicly agree on two finite sets U and V and a mapping $h \in \mathcal{T}(U \cup V)$.
- Alice chooses $f_A \in R_U$, $g_A \in R_V$, and computes $\alpha = f_A \circ h \circ g_A$. She sends α to Bob and keeps f_A and g_A secret.

2.2. The analysis

- Bob chooses $f_B \in R_U$, $g_B \in R_V$, and computes $\beta = g_B \circ h \circ f_B$. He sends β to Alice and keeps f_B and g_B secret.
- Their common secret key is

$$k = f_A \circ \beta \circ g_A = g_B \circ \alpha \circ f_B.$$

2.2 The analysis

Clearly, if one can break Protocol 2.2, then one can break Protocol 2.1 as well. We presume for both cryptosystems that each mapping is represented by a sequence. This means if $X = \{x_1, \dots, x_n\}$ is a finite set and $f \in \mathcal{T}(X)$, then f is represented by the sequence $(f(x_1), \dots, f(x_n))$. Therefore, the key size of each private and each public key is $|X|$. In particular, the secret key k has the key size $|X|$. If one wants to recover the key k in Protocol 2.2, then one has to determine $k(x)$ for every $x \in U \cup V$.

The following lemma provides some technical statements, which are needed to prove Proposition 2.4. However, since every statement is easy to see, we will omit a proof.

Lemma 2.3. *Let everything as in Protocol 2.2. Furthermore, let $u \in U$ and $v \in V$. Then:*

1. $\beta(u) \in V \Leftrightarrow h \circ f_B(u) \in V$.
2. $\alpha(v) \in U \Leftrightarrow h \circ g_A(v) \in U$.
3. $\alpha(u) = f_A \circ h(u)$.
4. $\beta(v) = g_B \circ h(v)$.

The next proposition shows that the key k in Protocol 2.2 can be completely recovered from α , β , and h .

Proposition 2.4. *Let everything as in Protocol 2.2. Furthermore, let $u \in U$ and $v \in V$. Then:*

1. If $\beta(u) \in V$, then $k(u) = \beta(u)$.
2. If $\beta(u) \notin V$, then $h^{-1}(\beta(u)) \cap U$ is nonempty and $k(u) = \alpha(x)$ for every $x \in h^{-1}(\beta(u)) \cap U$.
3. If $\alpha(v) \in U$, then $k(v) = \alpha(v)$.

4. If $\alpha(v) \notin U$, then $h^{-1}(\alpha(v)) \cap V$ is nonempty and $k(v) = \beta(x)$ for every $x \in h^{-1}(\alpha(v)) \cap V$.

Proof. 1.: For u , we have $k(u) = f_A \circ \beta \circ g_A(u) = f_A \circ \beta(u)$ since $g_A|_U = \text{id}_U$. Because of $f_A|_V = \text{id}_V$ and $\beta(u) \in V$, it follows that $k(u) = \beta(u)$.

2.: Let $\beta(u) \notin V$. By Lemma 2.3, this is equivalent to $h \circ f_B(u) \notin V$. Thus, $h \circ f_B(u) \in U$. Because of $g_B|_U = \text{id}_U$, we find that $h \circ f_B(u) = g_B \circ h \circ f_B(u) = \beta(u)$. Hence, $f_B(u) \in h^{-1}(\beta(u)) \cap U$. Now let $x \in h^{-1}(\beta(u)) \cap U$. It follows that $k(u) = f_A \circ \beta \circ g_A(u) = f_A \circ \beta(u) = f_A \circ h(x)$. By $x \in U$ and Lemma 2.3, we get $k(u) = f_A \circ h(x) = \alpha(x)$.

3. and 4. can be proven analogously to 1. and 2., respectively. \square

Because of this proposition, Protocol 2.1 and Protocol 2.2 can be considered insecure. Indeed, k can be recovered from α , β , and h in Protocol 2.2, which are known. Fix an element $u \in U$. If $\beta(u) \in V$, then $k(u) = \beta(u)$. Therefore, only one look-up is necessary to recover $k(u)$. But also if $\beta(u) \notin V$, then $k(u)$ can be easily recovered. In fact, one only has to find an element $x \in h^{-1}(\beta(u)) \cap U$. Therefore, one can check successively for every element $u' \in U$ if $h(u') = \beta(u)$ is fulfilled until one finds an element $u_0 \in U$ that fulfills $h(u_0) = \beta(u)$. Then $k(u) = \alpha(u_0)$ holds. Hence, at most $|U|$ look-ups are necessary to recover $k(u)$ in this case. Consequently, at most $|U|^2$ look-ups are necessary to recover $k|_U$. Analogously, one can show that at most $|V \setminus U|^2$ look-ups are necessary to recover $k_{V \setminus U}$. Therefore, at most $|U|^2 + |V \setminus U|^2$ look-ups are necessary to recover k , which is upper bounded by $|X|^2$ for $X = U \cup V$. Since each key has the key size $|X|$, the effort to break Protocol 2.2 is at most quadratic in the size of the keys.

In the more specific Protocol 2.1, where the lattice $\mathbf{M} = \mathbf{L} \bar{\oplus} \mathbf{K}$ is used, the key size of the secret key k is $|M|$ and there are at most $|M|^2$ look-ups necessary to recover k .

Chapter 3

Representation and cardinalities of finite simple semirings

In order to use semirings for cryptography, one has to represent their elements in a way that can be handled by a computer. A naive way of doing this could be to store the addition and the multiplication table of a finite semiring. In this case the performance of addition and multiplication is very efficient since every addition and every multiplication can be performed by a simple table look-up. This, however, will be practicable only for semirings of small size, as otherwise the operation tables require by far too much memory resources. For cryptographic applications, obviously semirings with a huge cardinality are required. If one is interested in using proper finite simple semirings with zero, one can make use of Theorem 1.11. The idea is then to store merely a finite lattice \mathbf{L} , which can be done e.g. by storing one of its operation tables (supremum or infimum) or alternatively the order relation represented as a table with binary entries. Since one has to perform pointwise supremum operations, the supremum table seems to be the best choice at first sight. After this, there are two options: The first one is to compute and store every residuated mapping of \mathbf{L} . If one wants to use a dense subsemiring of $(\text{Res}(\mathbf{L}), \vee, \circ)$ instead of $(\text{Res}(\mathbf{L}), \vee, \circ)$, then one can restrict to this subsemiring. The performance of the operations behaves very well, due to the fact that pointwise supremum and composition are inexpensive to compute. However, depending on the lattice, the cardinality of $\text{Res}(\mathbf{L})$ may be huge and storing will require again a lot of memory. Also the computation of all residuated mappings is computationally expensive. For this reason, this option is not practicable.

The second option is to generate a ‘random’ residuated mapping whenever it is

required. The performance of the semiring operations is the same as in the first option, i.e. computationally inexpensive, and there is no memory required to store $\text{Res}(\mathbf{L})$. All that has to be stored is \mathbf{L} . The appearing problem now is to generate ‘random’ residuated mappings. Section 3.1 deals with this problem.

Another problem is to make sure that the cardinality of the used semiring is sufficiently large. Otherwise the security relevant problems of a semiring based cryptosystem such as Protocol 1.20 could be easily solvable. Therefore, lower bounds on the size of these semirings in terms of the lattice size are desirable. This problem is discussed in Section 3.2.

Many results of this chapter are based on a collaboration with Stefan E. Schmidt, which are partly published in [34].

3.1 Representation of semirings

In this section we will present two solutions for the problem of generating ‘random’ residuated mappings. The first one works for the smallest dense subsemiring of $(\text{Res}(\mathbf{L}), \vee, \circ)$ only. It follows almost immediately from the definition of density and will be described in Section 3.1.1. The second solution works for the semiring of all residuated mappings of a finite lattice. Instead of representing semiring elements as residuated mappings, we will do this in terms of so-called *bonds*, which are objects intensively studied in *Formal Concept Analysis* (FCA). To accomplish this, we will give a short introduction into formal concept analysis in Section 3.1.2. Our bond-based solution will be then described in Section 3.1.3.

3.1.1 The semiring of tight residuated mappings

We start this section with introducing *adjunctions* and *Galois connections*, which are strongly connected to residuated mappings. Adjunctions and Galois connections will also be used in Section 3.2.

Adjunctions and Galois connections

Let $\mathbf{P} = (P, \leq)$ and $\mathbf{Q} = (Q, \leq)$ be ordered sets. A pair (f, g) of mappings $f : P \rightarrow Q$ and $g : Q \rightarrow P$ is called an **adjunction** of (\mathbf{P}, \mathbf{Q}) if it satisfies

$$f(x) \leq y \Leftrightarrow x \leq g(y)$$

3.1. Representation of semirings

for all $x \in P$, $y \in Q$. It is called a **Galois connection** if it satisfies

$$f(x) \leq y \Leftrightarrow x \geq g(y)$$

for all $x \in P$, $y \in Q$. By $\text{Adj}(\mathbf{P}, \mathbf{Q})$ we denote the set of all adjunctions of (\mathbf{P}, \mathbf{Q}) and by $\text{Gal}(\mathbf{P}, \mathbf{Q})$ the set of all Galois connections of (\mathbf{P}, \mathbf{Q}) . Obviously, a pair (f, g) is an adjunction of (\mathbf{P}, \mathbf{Q}) iff it is a Galois connection of $(\mathbf{P}, \mathbf{Q}^d)$. The following proposition states the connection between residuated mappings and adjunctions (cf. [7]):

Proposition 3.1. *Let \mathbf{P} and \mathbf{Q} be ordered sets. Then (f, g) is an adjunction of (\mathbf{P}, \mathbf{Q}) iff f is a residuated mapping from \mathbf{P} to \mathbf{Q} with residual g .*

Besides [7] one may also consult [9, 14] for a survey on Galois connections and adjunctions.

Tight residuated mappings

Raney defined *tight Galois connections* between complete lattices in [48] as follows: Let \mathbf{L} and \mathbf{K} be complete lattices. A Galois connection (f, g) of (\mathbf{L}, \mathbf{K}) is called **tight** if $f(x) = \bigwedge_{y \not\leq x} \bigvee_{z \not\leq y} f(z)$ holds for every $x \in L$. We will call an adjunction (f, g) of (\mathbf{L}, \mathbf{K}) **tight** if (f, g) is a tight Galois connection of $(\mathbf{L}, \mathbf{K}^d)$. Furthermore, we call a residuated mapping f from \mathbf{L} to \mathbf{K} **tight** if f is the first part of a tight adjunction of (\mathbf{L}, \mathbf{K}) . Schreiner showed in [51] with reference to Shmuely [53] that a residuated mapping f from \mathbf{L} to \mathbf{K} is tight iff it is the pointwise supremum of a family of mappings of the form $e_{a,b}$ as defined in Section 1.3.1. The following is [1, Lemma 1.3]:

Lemma 3.2. *For complete lattices $\mathbf{K}, \mathbf{L}, \mathbf{M}, \mathbf{N}$, $f \in \text{Res}(\mathbf{K}, \mathbf{L})$, $g \in \text{Res}(\mathbf{L}, \mathbf{M})$, and $h \in \text{Res}(\mathbf{M}, \mathbf{N})$, the residuated mappings $g \circ f$ and $h \circ g$ are tight whenever g is tight. Moreover, the tight residuated mappings in $\text{Res}(\mathbf{L}, \mathbf{M})$ are closed under \vee .*

For a complete lattice \mathbf{L} , let $E(\mathbf{L})$ denote the set of all tight residuated mappings in $\text{Res}(\mathbf{L})$. By Lemma 3.2, $E(\mathbf{L})$ is closed under \vee and \circ . Consequently, $(E(\mathbf{L}), \vee, \circ)$ is a subsemiring of $(\text{Res}(\mathbf{L}), \vee, \circ)$.

In particular, if \mathbf{L} is a finite lattice, then $(E(\mathbf{L}), \vee, \circ)$ is the smallest dense subsemiring of $(\text{Res}(\mathbf{L}), \vee, \circ)$. Raney showed in [48, Theorem 2] that any Galois connection between two finite lattices is tight if one of these lattices is distributive. Therefore, any residuated mapping of a finite distributive lattice \mathbf{L} is tight and

hence, we find that $E(\mathbf{L}) = \text{Res}(\mathbf{L})$. There is an obvious way to generate arbitrary elements in $E(\mathbf{L})$, as every mapping $\varphi \in E(\mathbf{L})$ has a representation

$$\varphi = e_{a_1, b_1} \vee \dots \vee e_{a_n, b_n} \quad (3.1)$$

for an $n \in \mathbb{N}$ and some $a_1, \dots, a_n, b_1, \dots, b_n \in L$. Therefore, in order to generate an element in $E(\mathbf{L})$, one can pick arbitrary elements $a_1, \dots, a_n, b_1, \dots, b_n \in L$ for an $n \in \mathbb{N}$ and then compute $\varphi := e_{a_1, b_1} \vee \dots \vee e_{a_n, b_n}$. It is difficult though to determine the distribution of the mappings φ generated in this manner once random choices of a_i and b_i are underlying. Regardless, this algorithm yields arbitrary φ , and most importantly every element in $E(\mathbf{L})$ can be generated in this fashion.

Obviously however, this procedure works just for the semiring $(E(\mathbf{L}), \vee, \circ)$. If \mathbf{L} is distributive, it works for the semiring $(\text{Res}(\mathbf{L}), \vee, \circ)$ due to the equality $E(\mathbf{L}) = \text{Res}(\mathbf{L})$. In order to generate elements of the semiring $(\text{Res}(\mathbf{L}), \vee, \circ)$ or another dense subsemiring thereof (except $(E(\mathbf{L}), \vee, \circ)$) for a non-distributive lattice \mathbf{L} , a different method is required. A solution for these cases was given by [12], where an algorithm was presented to generate so-called *biclosed relations*. These biclosed relations correspond to *bonds* in Formal Concept Analysis.

3.1.2 Formal Concept Analysis

In this section we give a brief account of formal concept analysis. For more information regarding this topic, one should consult [17] and [16]. The former focuses on the foundations and the latter also covers applications.

A **formal context** is a triple $\mathbb{K} = (G, M, I)$ consisting of two sets G and M and a relation I between G and M . The elements of G are called the **objects** and the elements of M are called the **attributes** of \mathbb{K} . The relation I is called the **incidence relation** of \mathbb{K} . For a subset A of G , one defines

$$A' := A^I := \{m \in M \mid \forall g \in A : gIm\},$$

and for a subset B of M , one defines

$$B' := B^I := \{g \in G \mid \forall m \in B : gIm\}.$$

For singletons, i.e. for $g \in G$ and $m \in M$, one also defines

$$g' := g^I := \{g\}^I \quad \text{and} \quad m' := m^I := \{m\}^I.$$

3.1. Representation of semirings

A **formal concept** of \mathbb{K} is a pair (A, B) with $A \subseteq G$, $B \subseteq M$, $A' = B$, and $B' = A$. One calls A the **extent** and B the **intent** of the concept (A, B) . The set of formal concepts of \mathbb{K} is denoted by $\mathfrak{B}(\mathbb{K})$, the set of extents of \mathbb{K} by $\text{Ext}(\mathbb{K})$, and the set of intents of \mathbb{K} by $\text{Int}(\mathbb{K})$. If $A \subseteq G$ and $B \subseteq M$, then (A'', A') and (B', B'') are formal concepts. For an object $g \in G$, the concept (g'', g') is called an **object concept**, and for an attribute $m \in M$, the concept (m', m'') is called an **attribute concept**. The **hierarchical order** on $\mathfrak{B}(\mathbb{K})$ is the order \leq on $\mathfrak{B}(\mathbb{K})$ defined by $(A_1, B_1) \leq (A_2, B_2) :\Leftrightarrow A_1 \subseteq A_2$ (which is equivalent to $B_2 \subseteq B_1$) for all $(A_1, B_1), (A_2, B_2) \in \mathfrak{B}(\mathbb{K})$. The ordered set $(\mathfrak{B}(\mathbb{K}), \leq)$ is called the **concept lattice** of \mathbb{K} and is denoted by $\underline{\mathfrak{B}}(\mathbb{K})$. Next we will state the *basic theorem on concept lattices* in a shortened form [17, Theorem 3]:

Theorem 3.3 (The Basic Theorem on Concept Lattices). *The concept lattice $\underline{\mathfrak{B}}(\mathbb{K})$ of a formal context \mathbb{K} is a complete lattice. Conversely, every complete lattice is isomorphic to the concept lattice of a suitable formal context. In particular, every complete lattice (L, \leq) is isomorphic to $\underline{\mathfrak{B}}(L, L, \leq)$.*

For a given complete lattice $\mathbf{L} = (L, \leq)$, the formal context (L, L, \leq) is called the **canonical context** of \mathbf{L} .

A formal context (G, M, I) is called **clarified** if $g' = h'$ implies $g = h$ for all $g, h \in G$ and $m' = n'$ implies $m = n$ for all $m, n \in M$. A clarified formal context \mathbb{K} is called **reduced** if every object concept is \vee -irreducible in $\underline{\mathfrak{B}}(\mathbb{K})$ and every attribute concept is \wedge -irreducible in $\underline{\mathfrak{B}}(\mathbb{K})$.

Two formal contexts (G, M, I) and (H, N, J) are called **isomorphic** if there exist bijective mappings $\alpha : G \rightarrow H$ and $\beta : M \rightarrow N$ with $gIm \Leftrightarrow \alpha(g)J\beta(m)$ for all $g \in G, m \in M$.

The following is [17, Proposition 12]:

Proposition 3.4. *For every finite lattice \mathbf{L} , there is up to isomorphism a unique reduced context $\mathbb{K}(\mathbf{L})$ with $\mathbf{L} \cong \underline{\mathfrak{B}}(\mathbb{K}(\mathbf{L}))$, which is*

$$\mathbb{K}(\mathbf{L}) := (J(\mathbf{L}), M(\mathbf{L}), \leq \cap (J(\mathbf{L}) \times M(\mathbf{L}))).$$

The formal context $\mathbb{K}(\mathbf{L})$ for a finite lattice \mathbf{L} is also called the **standard context** of \mathbf{L} . This context is the ‘smallest’ formal context whose concept lattice is isomorphic to \mathbf{L} in the following sense: There is no formal context with fewer objects or attributes such that its concept lattice is isomorphic to \mathbf{L} .

3.1.3 The semiring of bonds

In this section we will introduce *bonds* and show that the semiring $(\text{Res}(\mathbf{L}), \vee, \circ)$ for a finite lattice \mathbf{L} is isomorphic to a semiring of bonds. Further on, we will investigate its operations and present a method to generate arbitrary bonds. Bonds are comprehensively studied in formal concept analysis, but a connection between bonds and finite simple semirings never appeared in the literature before.

For two sets X and Y , a relation $R \subseteq X \times Y$, and subsets $A \subseteq X$, $B \subseteq Y$, we denote $A^R := \{y \in Y \mid \forall x \in A : xRy\}$ and $B^R := \{x \in X \mid \forall y \in B : xRy\}$. As before, we write $x^R := \{x\}^R$ and $y^R := \{y\}^R$ for $x \in X$ and $y \in Y$.

Definition 3.5. A **bond** between formal contexts $\mathbb{K} = (G, M, I)$ and $\mathbb{L} = (H, N, J)$ is a relation $R \subseteq G \times N$ such that

- $\forall g \in G : g^R \in \text{Int}(\mathbb{L})$ and
- $\forall n \in N : n^R \in \text{Ext}(\mathbb{K})$.

By $\text{Bo}(\mathbb{K}, \mathbb{L})$ we denote the set of all bonds between \mathbb{K} and \mathbb{L} and we define $\text{Bo}(\mathbb{K}) := \text{Bo}(\mathbb{K}, \mathbb{K})$.

Example 3.6. Consider the following formal context $\mathbb{L} = (G, M, I)$ with object set $G = \{g_1, g_2\}$, attribute set $M = \{m_1, m_2\}$, and incidence relation $I = \{(g_1, m_2)\}$, which can be expressed by the following table:

| | | |
|--------------|-------|----------|
| \mathbb{L} | m_1 | m_2 |
| g_1 | | \times |
| g_2 | | |

Then the set $\text{Bo}(\mathbb{L})$ consists of the following six bonds:

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------|---|----------|-------|-------|-------|----------|----------|-------|----------|----------|---------|--|--|-------|-------|-------|----------|----------|-------|--|----------|---------|---|--|-------|-------|-------|----------|----------|-------|--|--|
| $R_1 =$ | <table border="1" style="border-collapse: collapse; text-align: center; width: 100px; height: 40px;"> <tr><td style="padding: 2px;"></td><td style="padding: 2px;">m_1</td><td style="padding: 2px;">m_2</td></tr> <tr><td style="padding: 2px;">g_1</td><td style="padding: 2px;">\times</td><td style="padding: 2px;">\times</td></tr> <tr><td style="padding: 2px;">g_2</td><td style="padding: 2px;">\times</td><td style="padding: 2px;">\times</td></tr> </table> | | m_1 | m_2 | g_1 | \times | \times | g_2 | \times | \times | $R_2 =$ | <table border="1" style="border-collapse: collapse; text-align: center; width: 100px; height: 40px;"> <tr><td style="padding: 2px;"></td><td style="padding: 2px;">m_1</td><td style="padding: 2px;">m_2</td></tr> <tr><td style="padding: 2px;">g_1</td><td style="padding: 2px;">\times</td><td style="padding: 2px;">\times</td></tr> <tr><td style="padding: 2px;">g_2</td><td style="padding: 2px;"></td><td style="padding: 2px;">\times</td></tr> </table> | | m_1 | m_2 | g_1 | \times | \times | g_2 | | \times | $R_3 =$ | <table border="1" style="border-collapse: collapse; text-align: center; width: 100px; height: 40px;"> <tr><td style="padding: 2px;"></td><td style="padding: 2px;">m_1</td><td style="padding: 2px;">m_2</td></tr> <tr><td style="padding: 2px;">g_1</td><td style="padding: 2px;">\times</td><td style="padding: 2px;">\times</td></tr> <tr><td style="padding: 2px;">g_2</td><td style="padding: 2px;"></td><td style="padding: 2px;"></td></tr> </table> | | m_1 | m_2 | g_1 | \times | \times | g_2 | | |
| | m_1 | m_2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| g_1 | \times | \times | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| g_2 | \times | \times | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | m_1 | m_2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| g_1 | \times | \times | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| g_2 | | \times | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | m_1 | m_2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| g_1 | \times | \times | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| g_2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| $R_4 =$ | <table border="1" style="border-collapse: collapse; text-align: center; width: 100px; height: 40px;"> <tr><td style="padding: 2px;"></td><td style="padding: 2px;">m_1</td><td style="padding: 2px;">m_2</td></tr> <tr><td style="padding: 2px;">g_1</td><td style="padding: 2px;"></td><td style="padding: 2px;">\times</td></tr> <tr><td style="padding: 2px;">g_2</td><td style="padding: 2px;"></td><td style="padding: 2px;">\times</td></tr> </table> | | m_1 | m_2 | g_1 | | \times | g_2 | | \times | $R_5 =$ | <table border="1" style="border-collapse: collapse; text-align: center; width: 100px; height: 40px;"> <tr><td style="padding: 2px;"></td><td style="padding: 2px;">m_1</td><td style="padding: 2px;">m_2</td></tr> <tr><td style="padding: 2px;">g_1</td><td style="padding: 2px;"></td><td style="padding: 2px;">\times</td></tr> <tr><td style="padding: 2px;">g_2</td><td style="padding: 2px;"></td><td style="padding: 2px;"></td></tr> </table> | | m_1 | m_2 | g_1 | | \times | g_2 | | | $R_6 =$ | <table border="1" style="border-collapse: collapse; text-align: center; width: 100px; height: 40px;"> <tr><td style="padding: 2px;"></td><td style="padding: 2px;">m_1</td><td style="padding: 2px;">m_2</td></tr> <tr><td style="padding: 2px;">g_1</td><td style="padding: 2px;"></td><td style="padding: 2px;"></td></tr> <tr><td style="padding: 2px;">g_2</td><td style="padding: 2px;"></td><td style="padding: 2px;"></td></tr> </table> | | m_1 | m_2 | g_1 | | | g_2 | | |
| | m_1 | m_2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| g_1 | | \times | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| g_2 | | \times | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | m_1 | m_2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| g_1 | | \times | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| g_2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | m_1 | m_2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| g_1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| g_2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

3.1. Representation of semirings

The next proposition is [17, Corollary 112].

Proposition 3.7. *If R is a bond between formal contexts $\mathbb{K} = (G, M, I)$ and $\mathbb{L} = (H, N, J)$, then (φ_R, φ_R^+) with*

$$\begin{aligned} \varphi_R : \mathfrak{B}(\mathbb{K}) &\longrightarrow \mathfrak{B}(\mathbb{L}), & (A, A^I) &\longmapsto (A^{RJ}, A^R) \text{ and} \\ \varphi_R^+ : \mathfrak{B}(\mathbb{L}) &\longrightarrow \mathfrak{B}(\mathbb{K}), & (B^J, B) &\longmapsto (B^R, B^{RI}) \end{aligned}$$

is an adjunction of $(\mathfrak{B}(\mathbb{K}), \mathfrak{B}(\mathbb{L}))$. If (φ, φ^+) is an adjunction of $(\mathfrak{B}(\mathbb{K}), \mathfrak{B}(\mathbb{L}))$, then

$$\begin{aligned} R_\varphi := R_{(\varphi, \varphi^+)} &:= \{(g, n) \in G \times N \mid \varphi(g^{II}, g^I) \leq (n^J, n^{JJ})\} \\ &= \{(g, n) \in G \times N \mid (g^{II}, g^I) \leq \varphi^+(n^J, n^{JJ})\} \end{aligned}$$

is a bond between \mathbb{K} and \mathbb{L} . These constructions are inverse to each other.

Due to this proposition, there is a one-to-one correspondence between bonds and adjunctions, and therefore also between bonds and residuated mappings.

Example 3.8. Let $\mathbf{L} = (\{0, 1, 2\}, \leq)$ be the total order of three elements. Then $\text{Res}(\mathbf{L})$ consists of the following six mappings:

| | | | |
|-------------|---|---|---|
| | 0 | 1 | 2 |
| φ_1 | 0 | 0 | 0 |
| φ_2 | 0 | 0 | 1 |
| φ_3 | 0 | 0 | 2 |
| φ_4 | 0 | 1 | 1 |
| φ_5 | 0 | 1 | 2 |
| φ_6 | 0 | 2 | 2 |

The concept lattice $\mathfrak{B}(\mathbb{L})$ of the context \mathbb{L} from Example 3.6 is isomorphic to \mathbf{L} , and the mapping φ_i corresponds the bond R_i from Example 3.6 for every $i = 1, \dots, 6$.

In the following we denote for two formal contexts \mathbb{K} and \mathbb{L}

$$\begin{aligned} \text{Adj}(\mathbb{K}, \mathbb{L}) &:= \text{Adj}(\mathfrak{B}(\mathbb{K}), \mathfrak{B}(\mathbb{L})), \\ \text{Res}(\mathbb{K}, \mathbb{L}) &:= \text{Res}(\mathfrak{B}(\mathbb{K}), \mathfrak{B}(\mathbb{L})), \\ \text{Res}(\mathbb{K}) &:= \text{Res}(\mathbb{K}, \mathbb{K}), \end{aligned}$$

and we define the order \leq on $\text{Adj}(\mathbb{K}, \mathbb{L})$ by $(\varphi, \varphi^+) \leq (\psi, \psi^+) :\Leftrightarrow \varphi \leq \psi$ for

$(\varphi, \varphi^+), (\psi, \psi^+) \in \text{Adj}(\mathbb{K}, \mathbb{L})$. Hence, we have

$$(\text{Res}(\mathbb{K}, \mathbb{L}), \leq) \cong (\text{Adj}(\mathbb{K}, \mathbb{L}), \leq).$$

Furthermore, for two adjunctions $(\varphi, \varphi^+), (\psi, \psi^+) \in \text{Adj}(\mathbb{K}, \mathbb{L})$, the equivalence

$$\varphi \leq \psi \quad \Leftrightarrow \quad \varphi^+ \geq \psi^+$$

holds (see [7]).

Proposition 3.9. *If $\mathbb{K} = (G, M, I)$ and $\mathbb{L} = (H, N, J)$ are formal contexts, then*

$$(\text{Res}(\mathbb{K}, \mathbb{L}), \leq) \cong (\text{Adj}(\mathbb{K}, \mathbb{L}), \leq) \cong (\text{Bo}(\mathbb{K}, \mathbb{L}), \supseteq).$$

In particular, if $(\varphi, \varphi^+), (\psi, \psi^+) \in \text{Adj}(\mathbb{K}, \mathbb{L})$, then

$$\varphi \leq \psi \quad \Leftrightarrow \quad \varphi^+ \geq \psi^+ \quad \Leftrightarrow \quad R_\varphi \supseteq R_\psi.$$

Proof. Let $(\varphi, \varphi^+), (\psi, \psi^+) \in \text{Adj}(\mathbb{K}, \mathbb{L})$ and $(g, n) \in R_\psi$. If $(\varphi, \varphi^+) \leq (\psi, \psi^+)$, then $\varphi(g^I, g^I) \leq \psi(g^I, g^I) \leq (n^J, n^J)$. Thus, $(g, n) \in R_\varphi$. Consequently, $R_\varphi \supseteq R_\psi$. Now let $R_\psi \subseteq R_\varphi$ and $(A, A^I) \in \mathfrak{B}(\mathbb{K})$. We find that $A^{R_\psi} \subseteq A^{R_\varphi}$. Hence, $\varphi(A, A^I) = (A^{R_\varphi J}, A^{R_\varphi}) \leq (A^{R_\psi J}, A^{R_\psi}) = \psi(A, A^I)$. This however shows $\varphi \leq \psi$. \square

Let $\mathbb{K} = (G, M, I)$ and $\mathbb{L} = (H, N, J)$ be two formal contexts. We denote by $\mathfrak{P}(G \times N)$ the powerset of $G \times N$ and by $\underline{\mathfrak{P}}(G \times N)$ the powerset lattice $(\mathfrak{P}(G \times N), \subseteq)$ of $G \times N$. In [12, Proposition 3.1] it was shown that $\text{Bo}(\mathbb{K}, \mathbb{L})$ is a closure system of $\underline{\mathfrak{P}}(G \times N)$. Hence, $(\text{Bo}(\mathbb{K}, \mathbb{L}), \subseteq)$ is a complete lattice with $\inf\{R, R'\} = R \cap R'$ for all $R, R' \in \text{Bo}(\mathbb{K}, \mathbb{L})$. Consequently, $(\text{Bo}(\mathbb{K}, \mathbb{L}), \supseteq)$ is a complete lattice with $\sup\{R, R'\} = R \cap R'$ for all $R, R' \in \text{Bo}(\mathbb{K}, \mathbb{L})$.

Corollary 3.10. *If \mathbb{K} and \mathbb{L} are formal contexts and $R, S, T \in \text{Bo}(\mathbb{K}, \mathbb{L})$, then*

$$R = S \cap T \quad \Leftrightarrow \quad \varphi_R = \varphi_S \vee \varphi_T \quad \Leftrightarrow \quad \varphi_R^+ = \varphi_S^+ \wedge \varphi_T^+.$$

In particular:

$$(\text{Res}(\mathbb{K}, \mathbb{L}), \vee) \cong (\text{Bo}(\mathbb{K}, \mathbb{L}), \cap).$$

We saw that the pointwise supremum in $\text{Res}(\mathbb{K}, \mathbb{L})$ corresponds to set intersection in $\text{Bo}(\mathbb{K}, \mathbb{L})$. Next, we would like to describe an operation on the set of

3.1. Representation of semirings

bonds that corresponds to the composition of residuated mappings. For that, we need [17, Proposition 84]:

Proposition 3.11. *Let $\mathbb{K}_i = (G_i, M_i, I_i)$ be formal contexts for $i = 1, 2, 3$, $R_{12} \in \text{Bo}(\mathbb{K}_1, \mathbb{K}_2)$, and let $R_{23} \in \text{Bo}(\mathbb{K}_2, \mathbb{K}_3)$. Then*

$$R_{12} \circ R_{23} := \{(g, m) \in G_1 \times M_3 \mid g^{R_{12}I_2} \subseteq m^{R_{23}}\}$$

is a bond from \mathbb{K}_1 to \mathbb{K}_3 .

Proposition 3.12. *Let $\mathbb{K}_i = (G_i, M_i, I_i)$ be formal contexts for $i = 1, 2, 3$, and let $R_{12} \in \text{Bo}(\mathbb{K}_1, \mathbb{K}_2)$, $R_{13} \in \text{Bo}(\mathbb{K}_1, \mathbb{K}_3)$, $R_{23} \in \text{Bo}(\mathbb{K}_2, \mathbb{K}_3)$. Furthermore, let $(\varphi_{12}, \varphi_{12}^+)$, $(\varphi_{13}, \varphi_{13}^+)$, $(\varphi_{23}, \varphi_{23}^+)$ be the corresponding adjunctions as in Proposition 3.7. Then*

$$\varphi_{13} = \varphi_{23} \circ \varphi_{12} \quad \Leftrightarrow \quad \varphi_{13}^+ = \varphi_{12}^+ \circ \varphi_{23}^+ \quad \Leftrightarrow \quad R_{13} = R_{12} \circ R_{23}.$$

In particular

$$(\text{Res}(\mathbb{K}_1), \circ) \cong (\text{Bo}(\mathbb{K}_1), \circ^d),$$

where $R \circ^d R' := R' \circ R$ for all $R, R' \in \text{Bo}(\mathbb{K}_1)$.

Proof. The first equivalence follows by [7, Theorem 2.8]. A proof for the second equivalence can be found in [15, Proposition 13]. \square

The semiring $(\text{Bo}(\mathbb{K}), \cap, \circ)$

A combination of Corollary 3.10 and Proposition 3.12 yields the following theorem.

Theorem 3.13. *Let $\mathbb{K} = (G, M, I)$ be a formal context, where G and M are finite. Then $(\text{Bo}(\mathbb{K}), \cap, \circ)$ is a proper finite simple semiring with zero $0_{\text{Bo}} = G \times M$ and one $1_{\text{Bo}} = \{(g, m) \in G \times M \mid g^I \subseteq m\}$. In particular, if \mathbf{L} is a finite lattice and \mathbb{L} a formal context with $\underline{\mathfrak{B}}(\mathbb{L}) \cong \mathbf{L}$, then*

$$(\text{Bo}(\mathbb{L}), \cap, \circ^d) \cong (\text{Res}(\mathbf{L}), \vee, \circ).$$

In light of Theorem 3.13, one can represent the finite simple semiring $(\text{Res}(\mathbf{L}), \vee, \circ)$ for a finite lattice \mathbf{L} as a semiring of bonds $(\text{Bo}(\mathbb{L}), \cap, \circ^d)$ for a suitable formal context $\mathbb{L} = (G, M, I)$. The additive operation is in this case the set-theoretic intersection of two bonds and the multiplication is the product \circ^d as defined in

Proposition 3.11 and Proposition 3.12. In order to make use of this semiring, it is required to store the formal context \mathbb{L} by storing the incidence relation I as a table of $|G|$ rows and $|M|$ columns. A bond R in $\text{Bo}(\mathbb{L})$ is also a relation between G and M and can be represented and stored in the same way. The intersection of two bonds is obviously inexpensive to compute. To multiply two bonds $R, R' \in \text{Bo}(\mathbb{L})$, i.e. to compute

$$R \circ^d R' = R' \circ R = \{(g, m) \in G \times M \mid g^{R'I} \subseteq m^R\},$$

one has to compute $g^{R'I}$ for every $g \in G$ and then to check if $g^{R'I} \subseteq m^R$ is satisfied for all $g \in G$ and $m \in M$. This check is easy to perform since m^R corresponds to one column in the corresponding table of R and $g^{R'I}$ can be identified as a column in the same way. Therefore, a number of $|G|$ computations of the form $g^{R'I}$ combined with $|G| \cdot |M|$ checks accomplish a single multiplication of two bonds.

As a suitable formal context to a given finite lattice $\mathbf{L} = (L, \leq)$ one could choose for example the canonical context $\mathbb{L} = (L, L, \leq)$. Another choice could be the standard context $\mathbb{K}(\mathbf{L})$ of \mathbf{L} . The advantage of this latter context is that it is the smallest formal context whose concept lattice is isomorphic to \mathbf{L} . This means it is the context that requires the least space of all. The corresponding table of the incidence relation of $\mathbb{K}(\mathbf{L})$, which has to be stored, has exactly $|J(\mathbf{L})| \cdot |M(\mathbf{L})|$ elements. However, to use this formal context it will be required to compute all join- and all meet-irreducible elements of \mathbf{L} . Alternatively, one could take the canonical context $\mathbb{L} = (L, L, \leq)$ and compute its reduced context. The way how this can be done is described in [17], but it is essentially the same as computing all join- and all meet-irreducible elements of \mathbf{L} .

Using a semiring of bonds does not require any knowledge about the lattice structure of the corresponding concept lattice. This means we may start rather with choosing a formal context \mathbb{L} instead of a lattice. Then we know that $(\text{Bo}(\mathbb{L}), \cap, \circ^d)$ and also $(\text{Bo}(\mathbb{L}), \cap, \circ)$ are proper finite simple semirings with zero. Additionally there holds $(\text{Bo}(\mathbb{L}), \cap, \circ^d) \cong (\text{Res}(\underline{\mathfrak{B}}(\mathbb{L})), \vee, \circ)$, which is however not important for the implementation, and it is not required either to know the structure of $\underline{\mathfrak{B}}(\mathbb{L})$. To keep the storage performance most efficient, one can initially choose a reduced formal context.

3.1. Representation of semirings

Generating bonds

Now we come to the advantage of using a semiring of bonds. As mentioned earlier, an algorithm to generate bonds was presented in [12]. In that paper, bonds have been called *biclosed relations* in a slightly different setting. Here, we will state the algorithms in terms of formal concept analysis.

Let $\mathbb{K} = (G, M, I)$ and $\mathbb{L} = (H, N, J)$ be two formal contexts. Since $\text{Bo}(\mathbb{K}, \mathbb{L})$ is a closure system of $\mathfrak{B}(G \times N)$, there exists a corresponding closure operator $\Gamma : \mathfrak{B}(G \times N) \rightarrow \text{Bo}(\mathbb{K}, \mathbb{L})$. Define $\Gamma_1, \Gamma_2 : \mathfrak{B}(G \times N) \rightarrow \mathfrak{B}(G \times N)$ by

$$\begin{aligned}\Gamma_1(R) &:= \{(g, n) \in G \times N \mid n \in g^{RJJ}\} \quad \text{and} \\ \Gamma_2(R) &:= \{(g, n) \in G \times N \mid g \in n^{RII}\}.\end{aligned}$$

The following statement is [12, Proposition 3.3].

Proposition 3.14. *Let $\mathbb{K} = (G, M, I)$ and $\mathbb{L} = (H, N, J)$ be two formal contexts and $R \in \mathfrak{B}(G \times N)$. If G and N are finite, then there exists an integer $k \leq |G \times N|$ such that $(\Gamma_1 \Gamma_2)^k(R) = \Gamma(R)$.*

If one of the concept lattices of the contexts in Proposition 3.14 is distributive, then one can derive a more precise statement (cf. [12, Corollary 7.1]):

Proposition 3.15. *Let $\mathbb{K} = (G, M, I)$ and $\mathbb{L} = (H, N, J)$ be two formal contexts and $R \in \mathfrak{B}(G \times N)$. If G and N are finite and $\mathfrak{B}(\mathbb{K})$ or $\mathfrak{B}(\mathbb{L})$ is distributive, then the equality $\Gamma(R) = \Gamma_1 \Gamma_2 \Gamma_1(R)$ holds.*

Now we will state the algorithms for Γ_1 , Γ_2 , and Γ , which have been presented in [12].

Algorithm 3.16. (Determination of Γ_1)

1. $change1 \leftarrow \text{false}$
2. **for** all $g \in G$ **do**
3. $Y \leftarrow g^R$
4. **if** $Y^{JJ} \neq Y$ **then**
5. $change1 \leftarrow \text{true}$
6. **for** all $n \in Y^{JJ}$
7. $(g, n) \in R$
8. **end for**
9. **end if**
10. **end for**

Algorithm 3.17. (Determination of Γ_2)

1. $change2 \leftarrow \text{false}$
2. **for** all $n \in N$ **do**
3. $X \leftarrow n^R$
4. **if** $X^{II} \neq X$ **then**
5. $change2 \leftarrow \text{true}$
6. **for** all $g \in X^{II}$
7. $(g, n) \in R$
8. **end for**
9. **end if**
10. **end for**

Algorithm 3.18. (Determination of Γ)

1. **repeat**
2. $R \leftarrow \Gamma_1(R)$
3. $R \leftarrow \Gamma_2(R)$
4. **until** ($change1 = \text{false}$) and ($change2 = \text{false}$)
5. **return**

Consequently, in order to generate an arbitrary element of the semiring $(\text{Bo}(\mathbb{L}), \cap, \circ^d)$ for a given formal context $\mathbb{L} = (G, M, I)$, one randomly chooses a subset S of $G \times M$ and computes the bond $R := \Gamma(S)$. It will be again difficult to determine the distribution of the occurring bonds R in general, as particular properties of Γ will have an influence on this distribution. Regardless, every element in $\text{Bo}(\mathbb{L})$ can be generated in this fashion.

Due to Proposition 3.15, one might argue to stick to formal contexts with a distributive concept lattice to increase the efficiency of computing Γ . However, we know that if \mathbb{L} is a formal context such that $\mathfrak{B}(\mathbb{L})$ is finite and distributive, then $(\text{Bo}(\mathbb{L}), \cap, \circ^d) \cong (\text{Res}(\mathfrak{B}(\mathbb{L})), \vee, \circ)$ and $\text{Res}(\mathfrak{B}(\mathbb{L})) = E(\mathfrak{B}(\mathbb{L}))$. This means instead of using bonds we could equally well use the method discussed in Section 3.1.1.

3.2 Cardinalities of semirings

To find the cardinalities of the set $\text{Res}(\mathbf{L})$ of residuated mappings and the set $E(\mathbf{L})$ of tight residuated mappings by exact formulas, which are efficiently computable also for large lattices \mathbf{L} , is a goal that appears to be out of reach. However, we present methods to compute $|\text{Res}(\mathbf{L})|$ and $|E(\mathbf{L})|$ in reasonable time for lattices of

3.2. Cardinalities of semirings

small size. These allow us to compute the cardinalities for each lattice \mathbf{L} up to 14 elements, and in particular to find

$$\begin{aligned}\text{MinR}_n &:= \min\{|\text{Res}(\mathbf{L})| \mid \mathbf{L} \text{ is a lattice, } |L| = n\} \\ \text{MinE}_n &:= \min\{|E(\mathbf{L})| \mid \mathbf{L} \text{ is a lattice, } |L| = n\}\end{aligned}$$

for $n \leq 14$. Our method is still capable to compute $|\text{Res}(\mathbf{L})|$ and $|E(\mathbf{L})|$ for a single lattice of order slightly larger than 14. However, as the number of lattices having cardinality $n > 14$ grows too fast (for example, there are already 152 233 518 lattices of cardinality 15, see [29]) it becomes infeasible to compute MinR_n and MinE_n for larger values of n with these methods. A motivation for computing MinR_n and MinE_n for small $n \in \mathbb{N}$ was to look for a special pattern in the lattices that admit these minimal cardinalities, with the goal to predict these lattices for further values of n . Although some pattern was found for small n , we are unfortunately unable to suggest the desired predictions for larger n . We present our computing method and the results for MinE_n in Section 3.2.1, and for MinR_n in Section 3.2.3. The computation of MinR_n depends on a characterisation of adjunctions, which we explain in Section 3.2.2.

Since we introduced the method to store a lattice by storing a reduced formal context in Section 3.1, it is also interesting to know the cardinality of the set of bonds $\text{Bo}(\mathbb{L})$ for a given reduced formal context \mathbb{L} . Again, to find an exact formula for $|\text{Bo}(\mathbb{L})|$ for contexts \mathbb{L} of arbitrary size appears to be impossible. However, we compute the lower bound $|E(\underline{\mathfrak{B}}(\mathbb{L}))|$ of $|\text{Bo}(\mathbb{L})| = |\text{Res}(\underline{\mathfrak{B}}(\mathbb{L}))|$ with the method we use to compute $E(\mathbf{L})$ for a finite lattice \mathbf{L} . In Section 3.2.1 we see that elements in $E(\underline{\mathfrak{B}}(\mathbb{L}))$ correspond to *regular dual bonds*, and in fact we count these regular dual bonds. This method allows us to find

$$\text{MinB}_n := \min\{|E(\underline{\mathfrak{B}}(\mathbb{L}))| \mid \mathbb{L} = (G, M, I) \text{ is a reduced context, } |G| = |M| = n\}$$

for every $n \leq 7$. In this case, when looking at the concept lattices of the contexts that admit a minimal number of regular dual bonds, there is enough special pattern to state a conjecture predicting these lattices for general $n \in \mathbb{N}$. Although we did not find a proof for this conjecture, we are quite confident that it holds, and we also can provide some evidence. These findings are discussed in Sections 3.2.4 and 3.2.5.

3.2.1 Cardinality of $E(\mathbb{L})$

Essential for this section is the concept of a *regular dual bond*, which belongs to the theory of formal concept analysis. We will see that regular dual bonds correspond to tight Galois connections and hence to tight residuated mappings.

Definition 3.19. A **dual bond** between two formal contexts $\mathbb{K} = (G, M, I)$ and $\mathbb{L} = (H, N, J)$ is a relation $R \subseteq G \times H$ such that

- $\forall g \in G : g^R \in \text{Ext}(\mathbb{L})$, and
- $\forall h \in H : h^R \in \text{Ext}(\mathbb{K})$.

By Proposition 3.7, bonds correspond to adjunctions. There is an analogous statement for dual bonds and Galois connections [17, Theorem 53]:

Proposition 3.20. *If R is a dual bond between formal contexts $\mathbb{K} = (G, M, I)$ and $\mathbb{L} = (H, N, J)$, then (φ_R, ψ_R) , where*

$$\begin{aligned} \varphi_R : \mathfrak{B}(\mathbb{K}) &\longrightarrow \mathfrak{B}(\mathbb{L}), & (X, X^I) &\longmapsto (X^R, X^{RJ}) \\ \psi_R : \mathfrak{B}(\mathbb{L}) &\longrightarrow \mathfrak{B}(\mathbb{K}), & (Y, Y^J) &\longmapsto (Y^R, Y^{RI}), \end{aligned}$$

is a Galois connection of $(\underline{\mathfrak{B}}(\mathbb{K}), \underline{\mathfrak{B}}(\mathbb{L}))$. Conversely, if (φ, ψ) is a Galois connection of $(\underline{\mathfrak{B}}(\mathbb{K}), \underline{\mathfrak{B}}(\mathbb{L}))$, then

$$\begin{aligned} R_{\varphi, \psi} &:= \{(g, h) \in G \times H \mid (g^{II}, g^I) \leq \psi(h^{JJ}, h^J)\} \\ &= \{(g, h) \in G \times H \mid (h^{JJ}, h^J) \leq \varphi(g^{II}, g^I)\} \end{aligned}$$

is a dual bond between \mathbb{K} and \mathbb{L} . These constructions are inverse to each other.

Definition 3.21. Given two formal contexts $\mathbb{K} = (G, M, I)$ and $\mathbb{L} = (H, N, J)$, the **direct product** of \mathbb{K} and \mathbb{L} is the context $\mathbb{K} \times \mathbb{L} := (G \times H, M \times N, \nabla)$, where ∇ is defined by

$$(g, h)\nabla(m, n) \quad :\Leftrightarrow \quad gIm \text{ or } hJn.$$

The next proposition gives a first reason why direct products will be of importance for us [15, Proposition 9]:

Proposition 3.22. *If \mathbb{K} and \mathbb{L} are formal contexts, then every extent of the direct product $\mathbb{K} \times \mathbb{L}$ is a dual bond between \mathbb{K} and \mathbb{L} .*

3.2. Cardinalities of semirings

However, the converse of this proposition is not true in general, i.e. there exist formal contexts and dual bonds between these contexts that are not extents of the direct product (see [15] for an example). The dual bonds that are extents of the direct product are of interest to us.

Definition 3.23. A dual bond between formal contexts \mathbb{K} and \mathbb{L} is called **regular** if it is an extent of $\mathbb{K} \times \mathbb{L}$. A Galois connection (φ, ψ) of (\mathbf{K}, \mathbf{L}) for two complete lattices \mathbf{K} and \mathbf{L} is called **regular** if its associated dual bond $R_{\varphi, \psi}$ between the canonical contexts of \mathbf{K} and \mathbf{L} is regular.

Regular dual bonds and regular Galois connections have been investigated in [37, 38]. It was shown in [38] that the definition of regular Galois connections does not depend on using the canonical contexts. This means if \mathbf{K} and \mathbf{L} are two complete lattices, \mathbb{K} and \mathbb{L} two formal contexts with $\underline{\mathfrak{B}}(\mathbb{K}) \cong \mathbf{K}$ and $\underline{\mathfrak{B}}(\mathbb{L}) \cong \mathbf{L}$, and (φ, ψ) is a Galois connection of (\mathbf{K}, \mathbf{L}) , then (φ, ψ) is regular iff its associated dual bond $R_{\varphi, \psi}$ between \mathbb{K} and \mathbb{L} is regular.

Moreover, regular Galois connections can be characterised by the following proposition [38, Theorem 3]:

Proposition 3.24. *Given complete lattices \mathbf{K} and \mathbf{L} and a mapping $\varphi : K \rightarrow L$, the following are equivalent:*

1. *The mapping φ is the first part of a regular Galois connection of (\mathbf{K}, \mathbf{L}) .*
2. *For all $x \in K$ it holds: $\varphi(x) = \bigwedge_{y \not\leq x} \bigvee_{z \not\leq y} \varphi(z)$.*

The second condition is exactly the definition of tight Galois connections. Therefore, we obtain the following corollary:

Corollary 3.25. *Given complete lattices \mathbf{K} and \mathbf{L} and two mappings $\varphi : K \rightarrow L$ and $\psi : L \rightarrow K$, the following are equivalent:*

1. *The pair (φ, ψ) is a regular Galois connection of (\mathbf{K}, \mathbf{L}) .*
2. *The pair (φ, ψ) is a tight Galois connection of (\mathbf{K}, \mathbf{L}) .*
3. *The mapping φ is a tight residuated mapping from \mathbf{K} to \mathbf{L}^d .*

As a consequence, if one wants to compute the number of tight residuated mappings of a complete lattice \mathbf{L} , it suffices to count the regular dual bonds between two formal contexts \mathbb{L}_1 and \mathbb{L}_2 satisfying $\underline{\mathfrak{B}}(\mathbb{L}_1) \cong \mathbf{L}$ and $\underline{\mathfrak{B}}(\mathbb{L}_2) \cong \mathbf{L}^d$. By definition,

the number of these dual bonds is the same as the number of the extents of the direct product $\mathbb{L}_1 \times \mathbb{L}_2$, which is the same as the number of concepts of $\mathbb{L}_1 \times \mathbb{L}_2$. The **duality principle for concept lattices** says that for a given formal context $\mathbb{K} = (G, M, I)$ also the triple $\mathbb{K}^d := (M, G, I^{-1})$ with $I^{-1} := \{(m, g) \in M \times G \mid gIm\}$ is a formal context and moreover

$$\underline{\mathfrak{B}}(\mathbb{K}) \cong \underline{\mathfrak{B}}(\mathbb{K}^d)^d$$

(cf. [17]). The context \mathbb{K}^d is called the **dual formal context** of \mathbb{K} . Therefore, we can take any formal context \mathbb{K} satisfying $\underline{\mathfrak{B}}(\mathbb{K}) \cong \mathbf{L}$ and count the concepts of the direct product $\mathbb{K} \times \mathbb{K}^d$. In particular, we can reduce the context size, which may increase the efficiency of the counting algorithms. If we pick a suitable reduced formal context \mathbb{K} , then also the direct product $\mathbb{K} \times \mathbb{K}^d$ is reduced [17, Corollary 74]. Hence, for a given finite lattice \mathbf{L} , we may take its standard context $\mathbb{K}(\mathbf{L})$, compute the direct product $\mathbb{K}(\mathbf{L}) \times \mathbb{K}(\mathbf{L})^d$, and count all concepts of the direct product. We applied this method for all lattices up to order 14.

There are several algorithms in the literature for computing all concepts of a formal context. We implemented the *Grail algorithm* from [59]. The results of the computations can be found in Table 3.1 and Table 3.2. In Table 3.1, MinE_n and a corresponding lattice that admits MinE_n tight residuated mappings is presented for every $n \leq 14$. We do not present the results for $n = 1, 2, 3$ since in each case there exists just one lattice. We mention that each lattice in the table that admits the corresponding minimal number MinE_n is essentially unique, in the sense that only the dual lattice admits the same minimal number. It is not known whether this uniqueness property holds for general $n \in \mathbb{N}$.

For $n \leq 14$, let \mathbf{L}_n denote the lattice depicted in Table 3.1, which corresponds to MinE_n . Examining the sequence $(\mathbf{L}_n)_{n=4, \dots, 14}$, one recognises that \mathbf{L}_n is isomorphic to a sublattice of \mathbf{L}_{n+1} , for every $n \leq 11$, whereas this rule breaks up for $n = 12$. Even though there is no order embedding for the cases $n = 12$ and $n = 13$, one can nevertheless observe a similarity of the lattices. However, these findings were not sufficient to state a conjecture for predicting a lattice \mathbf{L}_n with a minimum number of tight residuated mappings for any $n \in \mathbb{N}$, even if we assume that a corresponding lattice \mathbf{L}_{n-1} is given.

In Table 3.2, the minimum, the average, and the maximum value of $|E(\mathbf{L})|$ for lattices with n elements are presented for every $n \leq 14$. The minimum value is exactly the value MinE_n . In these experimental results one finds that the minimum

3.2. Cardinalities of semirings

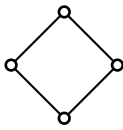
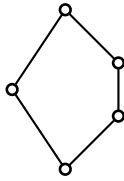
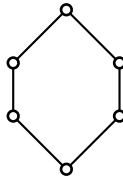
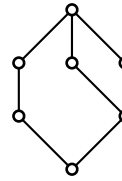
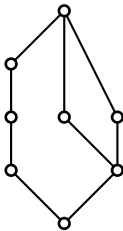
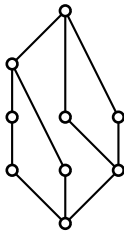
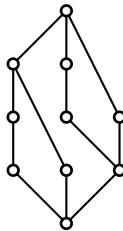
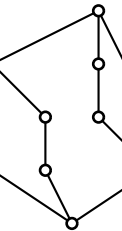
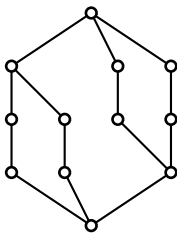
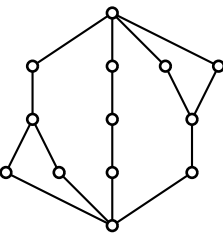
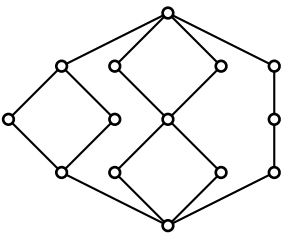
| | | | |
|--|--|---|---|
|  |  |  |  |
| MinE ₄ = 16 | MinE ₅ = 42 | MinE ₆ = 98 | MinE ₇ = 210 |
|  |  |  |  |
| MinE ₈ = 410 | MinE ₉ = 744 | MinE ₁₀ = 1258 | MinE ₁₁ = 2032 |
|  |  |  | |
| MinE ₁₂ = 3120 | MinE ₁₃ = 4618 | MinE ₁₄ = 6618 | |

Table 3.1: For every $n \in \mathbb{N}$ with $4 \leq n \leq 14$, the number MinE_n is presented together with a lattice, which admits exactly MinE_n tight residuated mappings.

and the average value are roughly proportional to 2^n . However, a decreasing of the ratio $\text{MinE}_n / \text{MinE}_{n-1}$ is recognisable. The same holds for the corresponding ratio of average values. One also finds that the average value is very close to the minimum value for small n , but the ratio average/minimum is increasing. In other words, the minimum value tends to get small with respect to the average value for increasing n .

3.2.2 A characterisation of adjunctions

To compute the number of all residuated mappings of a finite lattice, we will use a theorem that characterises adjunctions by triples consisting of a closure operator, a kernel operator, and an isomorphism between the corresponding closure and kernel systems. We call these triples *smart triples*. To prove the theorem we will need the following simple lemma, which can be found in [7].

Lemma 3.26. *If (f, g) is an adjunction of (\mathbf{P}, \mathbf{Q}) for two ordered sets \mathbf{P} and \mathbf{Q} ,*

| n | minimum | average | maximum |
|-----|---------|---------|------------|
| 4 | 16 | 18 | 20 |
| 5 | 42 | 51 | 70 |
| 6 | 98 | 133 | 252 |
| 7 | 210 | 322 | 924 |
| 8 | 410 | 722 | 3 432 |
| 9 | 744 | 1 525 | 12 870 |
| 10 | 1 258 | 3 056 | 48 620 |
| 11 | 2 032 | 5 850 | 184 756 |
| 12 | 3 120 | 10 769 | 705 432 |
| 13 | 4 618 | 19 181 | 2 704 156 |
| 14 | 6 618 | 33 260 | 10 400 600 |

Table 3.2: The minimum, the average, and the maximum value of $|E(\mathbf{L})|$ for lattices with n elements are presented for every $n \leq 14$. The average values have been rounded to integer values.

then

$$f \circ g \circ f = f \quad \text{and} \quad g \circ f \circ g = g.$$

For an ordered set $\mathbf{P} = (P, \leq)$ and a mapping $\varphi : P \rightarrow P$, we will denote in the following $\varphi\mathbf{P} := (\varphi(P), \leq \cap (\varphi(P) \times \varphi(P)))$.

Definition 3.27. Let \mathbf{P} and \mathbf{Q} be ordered sets. A triple $(\gamma, \kappa, \varphi)$ is called a **smart triple** of (\mathbf{P}, \mathbf{Q}) if

- the mapping γ is a closure operator on \mathbf{P} ,
- the mapping κ is a kernel operator on \mathbf{Q} , and
- the mapping φ is an order isomorphism from $\gamma\mathbf{P}$ onto $\kappa\mathbf{Q}$.

By $\text{Sm}(\mathbf{P}, \mathbf{Q})$ we denote the set of all smart triples of (\mathbf{P}, \mathbf{Q}) .

The following theorem states a one-to-one correspondence between $\text{Sm}(\mathbf{P}, \mathbf{Q})$ and $\text{Adj}(\mathbf{P}, \mathbf{Q})$ for given ordered sets \mathbf{P} and \mathbf{Q} . The result is not a novel one. In fact, already Ore presented the corresponding result for Galois connections between complete lattices in [47] in 1944, the paper in which, probably for the first time, the notion of (order theoretic) Galois connections was used. Jürgen Schmidt stated the result for adjunctions between complete lattices in [50]. A version of the general result for adjunctions between arbitrary ordered sets can be found e.g. in [13]. However, we were unable to find a proof for this general result in the literature. Therefore, we will add here a proof of the theorem.

3.2. Cardinalities of semirings

Theorem 3.28. *Let \mathbf{P} and \mathbf{Q} be ordered sets. There is a bijection Φ from $\text{Sm}(\mathbf{P}, \mathbf{Q})$ onto $\text{Adj}(\mathbf{P}, \mathbf{Q})$ via*

$$\Phi : (\gamma, \kappa, \varphi) \mapsto (\varphi \circ \gamma, \varphi^{-1} \circ \kappa).$$

The inverse of Φ is given by the mapping Ψ from $\text{Adj}(\mathbf{P}, \mathbf{Q})$ onto $\text{Sm}(\mathbf{P}, \mathbf{Q})$ via

$$\Psi : (f, g) \mapsto (\gamma, \kappa, \varphi)$$

where

$$\gamma = g \circ f, \quad \kappa = f \circ g, \quad \varphi : \gamma(P) \rightarrow \kappa(Q), \quad x \mapsto f(x).$$

Proof. The proof is given by showing the following properties:

1. The mapping Φ maps into $\text{Adj}(\mathbf{P}, \mathbf{Q})$.
2. The mapping Ψ maps into $\text{Sm}(\mathbf{P}, \mathbf{Q})$.
3. The mapping $\Psi \circ \Phi$ is the identity on $\text{Sm}(\mathbf{P}, \mathbf{Q})$.
4. The mapping $\Phi \circ \Psi$ is the identity on $\text{Adj}(\mathbf{P}, \mathbf{Q})$.

1.: Given a smart triple $(\gamma, \kappa, \varphi)$ of (\mathbf{P}, \mathbf{Q}) , let $(f, g) := \Phi(\gamma, \kappa, \varphi)$ and let $x \in P$, $y \in Q$ such that $\varphi(\gamma(x)) = f(x) \leq y$. By the facts that φ maps onto $\kappa(Q)$ and κ is idempotent, this is equivalent to $\kappa(\varphi(\gamma(x))) = \varphi(\gamma(x)) \leq y$. Applying Equation 1.2, this is equivalent to $\kappa(\varphi(\gamma(x))) = \varphi(\gamma(x)) \leq \kappa(y)$. Since φ^{-1} is an order isomorphism onto $\gamma\mathbf{P}$ and γ is idempotent, this is equivalent to $\gamma(x) \leq \varphi^{-1}(\kappa(y)) = \gamma(\varphi^{-1}(\kappa(y)))$. Finally, by Equation 1.1, this is equivalent to $x \leq \gamma(\varphi^{-1}(\kappa(y))) = \varphi^{-1}(\kappa(y)) = g(y)$.

2.: Given an adjunction (f, g) of (\mathbf{P}, \mathbf{Q}) , let $(\gamma, \kappa, \varphi) := \Psi(f, g)$. We will first show that γ is a closure operator on \mathbf{P} . Let $x, x_1, x_2 \in P$. Because of $f(x) \leq f(x)$, we find $x \leq g(f(x)) = \gamma(x)$. Thus, γ is increasing. Let $x_1 \leq x_2$. Since f and g are isotone, we have that $\gamma(x_1) = g(f(x_1)) \leq g(f(x_2)) = \gamma(x_2)$. Hence, γ is isotone. That γ is idempotent follows from Lemma 3.26 by $\gamma(\gamma(x)) = g(f(g(f(x)))) = g(f(x)) = \gamma(x)$. Analogously, it follows that κ is a kernel operator on \mathbf{Q} . To show that φ is an order isomorphism, we define the isotone mapping $\omega : \kappa(Q) \rightarrow \gamma(P) : y \mapsto g(y)$. That ω maps into $\gamma(P)$ follows from $\kappa(Q) = (f \circ g)(Q)$ and $\gamma(P) = (g \circ f)(P)$. The isotonicity of ω follows from the isotonicity of g . Now let $x \in \gamma(P)$. There exists an element $y \in P$ with $x = \gamma(y) = g(f(y))$ and it follows that $\omega(\varphi(x)) = g(f(g(f(y)))) = g(f(y)) = \gamma(y) = x$. Analogously, we find that

$\varphi(\omega(z)) = z$ holds for $z \in \kappa(Q)$, and it follows that φ is an isotone bijection with isotone inverse mapping ω , i.e. φ is an order isomorphism.

3.: Given a smart triple $(\gamma, \kappa, \varphi)$ of (\mathbf{P}, \mathbf{Q}) , let $(f, g) := \Phi(\gamma, \kappa, \varphi)$ and $(\gamma', \kappa', \varphi') := \Psi(f, g)$. For $x \in P$, the equality $\gamma'(x) = g(f(x)) = \varphi^{-1}(\kappa(\varphi(\gamma(x))))$ holds. Since $\varphi(\gamma(x)) \in \kappa(Q)$, we have $\gamma'(x) = \varphi^{-1}(\varphi(\gamma(x))) = \gamma(x)$. Analogously, it follows that $\kappa' = \kappa$. For $x \in \gamma(P)$, we have $\varphi'(x) = f(x) = \varphi(\gamma(x))$ and because of $x \in \gamma(P)$, we find $\gamma(x) = x$ and so $\varphi'(x) = \varphi(x)$. Thus, $(\gamma, \kappa, \varphi) = (\gamma', \kappa', \varphi')$.

4.: Given an adjunction (f, g) of (\mathbf{P}, \mathbf{Q}) , let $(\gamma, \kappa, \varphi) := \Psi(f, g)$ and $(f', g') := \Phi(\gamma, \kappa, \varphi)$. For $x \in P$, we get $f'(x) = \varphi(\gamma(x)) = f(g(f(x))) = f(x)$. Hence, $f' = f$. Analogously, it follows that $g' = g$. Thus, $(f', g') = (f, g)$. \square

3.2.3 Number of adjunctions between two ordered sets

We will apply Theorem 3.28 to determine the number of adjunctions between two ordered sets. Instead of closure and kernel operators, we will use in this section closure and kernel systems for technical reasons. Since the set of all closure operators (kernel operators) on an ordered set \mathbf{P} corresponds bijectively to the set of all closure systems (kernel systems) of \mathbf{P} (cf. [7, Theorem 4.5]), there is no difference in counting the closure operators (kernel operators) and in counting the closure systems (kernel systems) of \mathbf{P} . For an ordered set $\mathbf{P} = (P, \leq)$ and a subset A of P , we denote in the following $\mathbf{A}_{\mathbf{P}} := (A, \leq \cap (A \times A))$. By Theorem 3.28, we have

$$|\text{Adj}(\mathbf{P}, \mathbf{Q})| = \sum_{A \in C(\mathbf{P})} \sum_{B \in K(\mathbf{Q})} |\{\varphi \mid \varphi \text{ is an isomorphism from } \mathbf{A}_{\mathbf{P}} \text{ to } \mathbf{B}_{\mathbf{Q}}\}|. \quad (3.2)$$

Clearly, it would be sufficient to sum in the second sum over all $B \in K(\mathbf{Q})$ with $\mathbf{A}_{\mathbf{P}} \cong \mathbf{B}_{\mathbf{Q}}$. Now let \sim be the equivalence relation on $C(\mathbf{P})$ that is defined by $A \sim A' :\Leftrightarrow \mathbf{A}_{\mathbf{P}} \cong \mathbf{A}'_{\mathbf{P}}$ for $A, A' \in C(\mathbf{P})$. Analogously, let \equiv be the equivalence relation on $K(\mathbf{Q})$ that is defined by $B \equiv B' :\Leftrightarrow \mathbf{B}_{\mathbf{Q}} \cong \mathbf{B}'_{\mathbf{Q}}$ for $B, B' \in K(\mathbf{Q})$. Furthermore, let

$$\pi : C(\mathbf{P})/\sim \rightarrow K(\mathbf{Q})/\equiv \cup \{\emptyset\}, [A] \sim \mapsto \begin{cases} [B] \equiv & \text{if } \mathbf{A}_{\mathbf{P}} \cong \mathbf{B}_{\mathbf{Q}}, \\ \emptyset & \text{if } \forall B \in K(\mathbf{Q}) : \mathbf{A}_{\mathbf{P}} \not\cong \mathbf{B}_{\mathbf{Q}}, \end{cases}$$

3.2. Cardinalities of semirings

and

$$\sigma : K(\mathbf{Q})/\equiv \rightarrow C(\mathbf{P})/\sim \cup \{\emptyset\}, [B] \equiv \mapsto \begin{cases} [A] \sim & \text{if } \mathbf{A}_\mathbf{P} \cong \mathbf{B}_\mathbf{Q}, \\ \emptyset & \text{if } \forall A \in C(\mathbf{P}) : \mathbf{A}_\mathbf{P} \not\cong \mathbf{B}_\mathbf{Q}. \end{cases}$$

Now we can reformulate Equation 3.2 as

$$|\text{Adj}(\mathbf{P}, \mathbf{Q})| = \sum_{[A] \sim \in C(\mathbf{P})/\sim} |[A] \sim| \cdot |\pi([A] \sim)| \cdot |\text{Aut}(\mathbf{A}_\mathbf{P})| \quad (3.3)$$

$$= \sum_{[B] \equiv \in K(\mathbf{Q})/\equiv} |[B] \equiv| \cdot |\sigma([B] \equiv)| \cdot |\text{Aut}(\mathbf{B}_\mathbf{Q})|. \quad (3.4)$$

With these two equations we determine the number of adjunctions between two ordered sets.

Cardinality of $\text{Res}(\mathbf{L})$

We implemented Equation 3.3 and computed $|\text{Adj}(\mathbf{L}, \mathbf{L})| = |\text{Res}(\mathbf{L})|$ for every lattice \mathbf{L} up to order 14. The results can be found in Table 3.3 and Table 3.4. In Table 3.3, MinR_n and a corresponding lattice that admits MinR_n residuated mappings are presented for every $n \leq 14$. Also here, each lattice is essentially unique, in the sense that only the dual lattice admits the same minimal number, but it is unknown whether this uniqueness property holds for general $n \in \mathbb{N}$.

Examining the sequence $(\mathbf{L}_n)_{n=4, \dots, 14}$, where \mathbf{L}_n is the corresponding lattice to MinR_n in Table 3.3, one recognises again some pattern. In most cases, \mathbf{L}_n is not isomorphic to a sublattice of \mathbf{L}_{n+1} , but often there is an order embedding from \mathbf{L}_n into \mathbf{L}_{n+1} ; more precisely, these order embeddings exist for $n = 4, \dots, 8$ and for $n = 10, 11, 12$. For $n = 9$, such an embedding does not exist and it is even hard to spot a similarity between \mathbf{L}_9 and \mathbf{L}_{10} . For $n = 13$, such an embedding does not exist either, however, in this case one recognises a similarity between \mathbf{L}_{13} and \mathbf{L}_{14} . All in all, the recognised structure in the sequence $(\mathbf{L}_n)_{n=4, \dots, 14}$ does not suffice to find rules that help to make a prediction for a lattice \mathbf{L}_n with MinR_n residuated mappings for any $n \in \mathbb{N}$, even when \mathbf{L}_{n-1} is known.

In Table 3.4, the minimum, the average, and the maximum value of $|\text{Res}(\mathbf{L})|$ for lattices with n elements are presented for every $n \leq 14$. The minimum value is exactly the value MinR_n . Similar to the results for $|E(\mathbf{L})|$, one can recognise that the minimum and the average value are roughly proportional to 2^n and that the ratio $\text{MinE}_n / \text{MinE}_{n-1}$ is decreasing. One also finds that the average value is very close

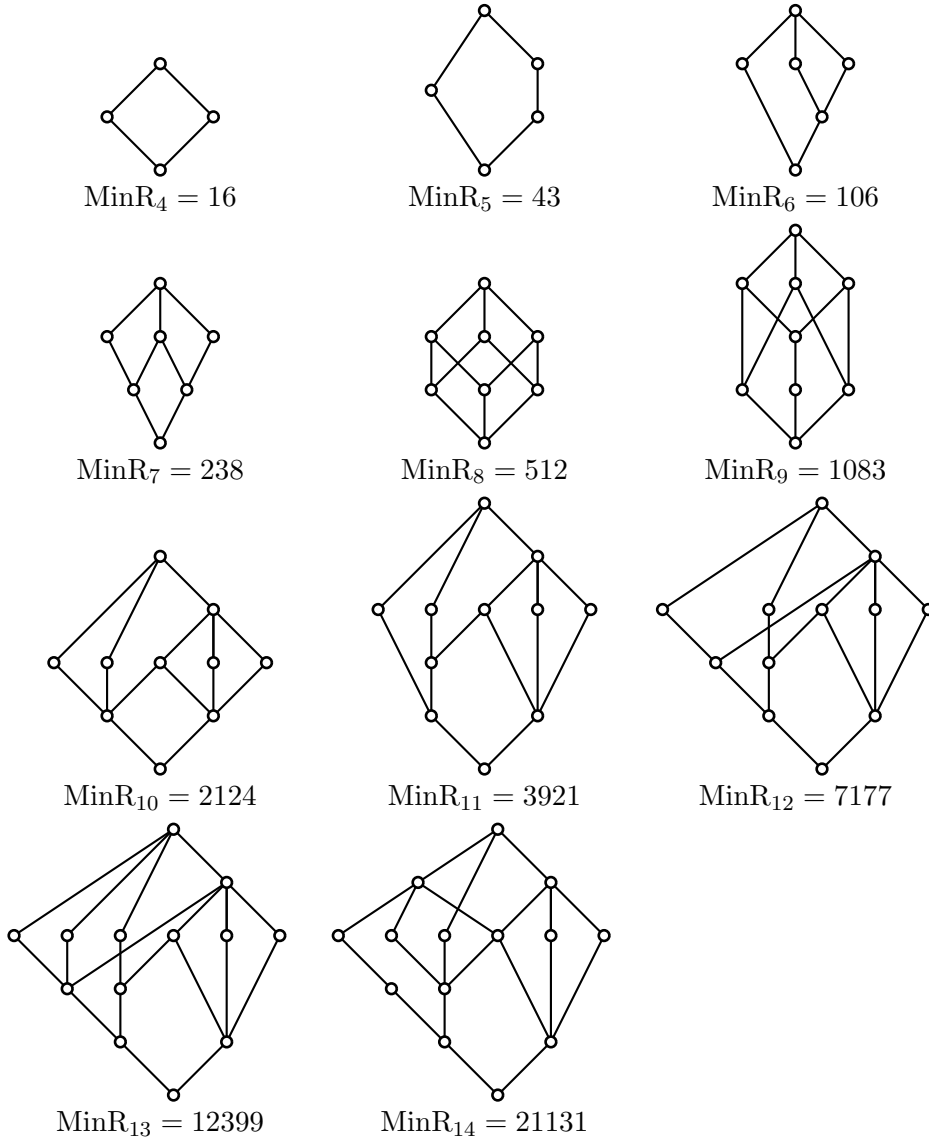


Table 3.3: For every $n \in \mathbb{N}$ with $4 \leq n \leq 14$, the number MinR_n is presented together with a lattice, which admits exactly MinR_n residuated mappings.

3.2. Cardinalities of semirings

| n | minimum | average | maximum |
|-----|---------|---------|----------------|
| 4 | 16 | 18 | 20 |
| 5 | 43 | 53 | 70 |
| 6 | 106 | 148 | 252 |
| 7 | 238 | 395 | 1 582 |
| 8 | 512 | 992 | 13 376 |
| 9 | 1 083 | 2 344 | 130 986 |
| 10 | 2 124 | 5 013 | 1 441 810 |
| 11 | 3 921 | 10 761 | 17 572 214 |
| 12 | 7 177 | 22 201 | 234 662 352 |
| 13 | 12 399 | 46 039 | 3 405 357 826 |
| 14 | 21 131 | 89 517 | 53 334 454 586 |

Table 3.4: The minimum, the average, and the maximum value of $|\text{Res}(\mathbb{L})|$ for lattices with n elements are presented for every $n \leq 14$. The average values have been rounded to integer values.

to the minimum value for small n , but the ratio average/minimum is increasing. In other words, the minimum value tends to get small with respect to the average value for increasing n .

3.2.4 Number of regular dual bonds

In this section we consider the number of bonds for a given reduced formal context \mathbb{L} . This is relevant when using the semiring of bonds $(\text{Bo}(\mathbb{L}), \cap, \circ)$ for cryptographic purposes. However, we encountered some difficulties when computing the number of all bonds to a given reduced context. Indeed, if we compute the concept lattice $\underline{\mathfrak{B}}(\mathbb{L})$ and apply the results from Section 3.2.3 to compute $|\text{Res}(\underline{\mathfrak{B}}(\mathbb{L}))| = |\text{Bo}(\mathbb{L})|$, the size of the concept lattice gets rather large compared to the number of objects and attributes of a reduced context. Therefore, this method works efficiently only for very small reduced contexts. Instead, we apply the method from Section 3.2.1 to compute a lower bound for the number of bonds. This works because of the obvious fact that R is a bond between formal contexts \mathbb{K} and \mathbb{L} iff R is a dual bond between \mathbb{K} and \mathbb{L}^d . Hence, if a reduced formal context \mathbb{L} is given, we compute the regular dual bonds between \mathbb{L} and \mathbb{L}^d , by which we obtain the number $|E(\underline{\mathfrak{B}}(\mathbb{L}))|$, which is a lower bound of $|\text{Res}(\underline{\mathfrak{B}}(\mathbb{L}))| = |\text{Bo}(\mathbb{L})|$.

We restrict the study to the case that the number of objects in a reduced context equals the number of attributes. More precisely, we compute the number of regular dual bonds between \mathbb{L} and \mathbb{L}^d for every reduced context with n objects and

n attributes for every $n \leq 7$. The results can be found in Table 3.5, where MinB_n , a corresponding reduced context that admits MinB_n regular dual bonds, and the concept lattice of the context are presented for every $n \leq 7$.

If one looks at the lattices in Table 3.5, then one recognises a similarity of all lattices. Namely, each lattice is a *horizontal sum of chains*: A **chain** (or **totally ordered set**) is an ordered set \mathbf{P} with $x \leq y$ or $x \geq y$ for all $x, y \in P$. An ordered set is called **bounded** if it has a least and a greatest element. The ordered set $\mathbf{P} = (P, \leq)$ is the **horizontal sum** of the bounded ordered sets $(P_i, \leq_i)_{i \in I}$ if $P = \bigcup_{i \in I} P_i$ with $P_i \cap P_j = \{0_{\mathbf{P}}, 1_{\mathbf{P}}\}$ whenever $i \neq j$, and $x \leq y$ iff there exists an $i \in I$ such that $\{x, y\} \subseteq P_i$ and $x \leq_i y$. If each bounded ordered set (P_i, \leq_i) is a chain, then \mathbf{P} is a **horizontal sum of chains**.

Due to this observation and also for reasons that are explained in Remark 3.30 and in Remark 3.34 below, we have the following conjecture.

Conjecture 3.29. *Let RC_n denote the set of all reduced contexts with n objects and n attributes for an $n \in \mathbb{N}$. Then there exists a context $\mathbb{L} \in \text{RC}_n$ such that $\underline{\mathfrak{B}}(\mathbb{L})$ is a horizontal sum of chains and $|E(\underline{\mathfrak{B}}(\mathbb{L}))| = \text{MinB}_n$.*

Remark 3.30. Let \mathbb{L} be a reduced formal context with n objects and n attributes for an $n \in \mathbb{N}$. Then the concept lattice of \mathbb{L} has at least $n + 1$ elements because it has n join-irreducible elements and additionally it has a least element, which is not join-irreducible. In particular, $\underline{\mathfrak{B}}(\mathbb{L})$ has $n + 1$ elements iff it is a chain. Moreover, $\underline{\mathfrak{B}}(\mathbb{L})$ has $n + 2$ elements iff it is a horizontal sum of chains but not a chain. In other words, if $\underline{\mathfrak{B}}(\mathbb{L})$ is a horizontal sum of chains, then it has very few elements compared to the size of the context. One should note that the concept lattice of \mathbb{L} can have up to 2^n elements; this is the case iff \mathbb{L} is of the form (G, G, \neq) , which is equivalent to $\underline{\mathfrak{B}}(\mathbb{L})$ being isomorphic to the boolean lattice with 2^n elements. The fact that horizontal sums of chains have very few elements with respect to the context size suggests that they also admit very few residuated mappings. This is one evidence for Conjecture 3.29. In Section 3.2.5 it will get clear why they admit in particular very few tight residuated mappings.

We point out that Conjecture 3.29 is equivalent to the following formulation stated in terms of lattice theory instead of formal concept analysis.

Conjecture 3.31. *Let \mathcal{L}_n denote the set of all lattices with n join- and n meet-irreducible elements for an $n \in \mathbb{N}$. Then there exists a lattice $\mathbf{L} \in \mathcal{L}_n$ such that \mathbf{L} is a horizontal sum of chains and $|E(\mathbf{L})| = \min\{|E(\mathbf{K})| \mid \mathbf{K} \in \mathcal{L}_n\}$.*

3.2. Cardinalities of semirings




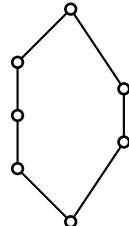
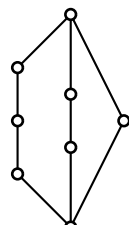
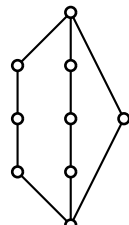
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|---|---|---|---|---|---------------------|---|---|---|---|----------------------|---|---|--|---|--|---|----------------------|---|---|--|---|---|--|---|--|-----------------------|--|---|--|--|--|---|---|--|---|---|-----------------------|--|--|---|--|--|--|--|--|--|--|---|---|-----------------------|
| <table border="1" style="display: inline-table; vertical-align: middle;"><tr><td></td><td>x</td></tr><tr><td></td><td></td></tr></table> | | x | | |  | $\text{MinB}_2 = 6$ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1" style="display: inline-table; vertical-align: middle;"><tr><td></td><td>x</td><td>x</td></tr><tr><td></td><td></td><td>x</td></tr><tr><td></td><td></td><td></td></tr></table> | | x | x | | | x | | | |  | $\text{MinB}_3 = 20$ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | x | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1" style="display: inline-table; vertical-align: middle;"><tr><td></td><td>x</td><td>x</td><td>x</td></tr><tr><td></td><td></td><td>x</td><td>x</td></tr><tr><td></td><td></td><td></td><td>x</td></tr><tr><td></td><td></td><td></td><td></td></tr></table> | | x | x | x | | | x | x | | | | x | | | | |  | $\text{MinB}_4 = 70$ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | x | x | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | x | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1" style="display: inline-table; vertical-align: middle;"><tr><td>x</td><td>x</td><td>x</td><td></td><td></td></tr><tr><td></td><td>x</td><td>x</td><td></td><td></td></tr><tr><td></td><td></td><td>x</td><td></td><td></td></tr><tr><td></td><td></td><td></td><td>x</td><td>x</td></tr><tr><td></td><td></td><td></td><td></td><td>x</td></tr></table> | x | x | x | | | | x | x | | | | | x | | | | | | x | x | | | | | x |  | $\text{MinB}_5 = 216$ | | | | | | | | | | | | | | | | | | | | | | | | |
| x | x | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | x | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | x | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1" style="display: inline-table; vertical-align: middle;"><tr><td>x</td><td>x</td><td>x</td><td></td><td></td><td></td></tr><tr><td></td><td>x</td><td>x</td><td></td><td></td><td></td></tr><tr><td></td><td></td><td>x</td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td>x</td><td>x</td><td></td></tr><tr><td></td><td></td><td></td><td></td><td>x</td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td>x</td></tr></table> | x | x | x | | | | | x | x | | | | | | x | | | | | | | x | x | | | | | | x | | | | | | | x |  | $\text{MinB}_6 = 418$ | | | | | | | | | | | | | |
| x | x | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | x | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | x | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1" style="display: inline-table; vertical-align: middle;"><tr><td>x</td><td>x</td><td>x</td><td></td><td></td><td></td><td></td></tr><tr><td></td><td>x</td><td>x</td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td>x</td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td>x</td><td>x</td><td>x</td><td></td></tr><tr><td></td><td></td><td></td><td></td><td>x</td><td>x</td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td>x</td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td>x</td></tr></table> | x | x | x | | | | | | x | x | | | | | | | x | | | | | | | | x | x | x | | | | | | x | x | | | | | | | x | | | | | | | | x |  | $\text{MinB}_7 = 752$ |
| x | x | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | x | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | x | x | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | x | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Table 3.5: For every $n \in \mathbb{N}$ with $2 \leq n \leq 7$, the number MinB_n is presented together with a reduced formal context, which admits exactly MinB_n regular dual bonds, and the concept lattice of the context.

3.2.5 Tight adjunctions between horizontal sums of chains

Here we want to determine the number of tight adjunctions between two lattices that are both horizontal sums of finite chains. In the following let $(\mathbf{C}_i = (C_i, \leq_i))_{i \in I}$ be a collection of finite chains for a finite index set I and let $\mathbf{L} = (L, \leq)$ be the horizontal sum of $(\mathbf{C}_i)_{i \in I}$. Analogously, let $(\mathbf{C}'_i = (C'_i, \leq_i))_{i \in I'}$ be a collection of finite chains for a finite index set I' and let $\mathbf{K} = (K, \leq)$ be the horizontal sum of $(\mathbf{C}'_i)_{i \in I'}$. First we need a lemma.

Lemma 3.32. *Let (f, g) be a tight adjunction of (\mathbf{L}, \mathbf{K}) . Then $f(L)$ has at most one incomparable pair with respect to the order in \mathbf{K} .*

Proof. Let $(a_j)_{j \in J}$ be a sequence in L and $(b_j)_{j \in J}$ a sequence in K for an index set J such that $f = \bigvee_{j \in J} e_{a_j, b_j}$. Assume that there are two incomparable pairs (y_1, y_2) and (y_3, y_4) in $f(L)$ with $\{y_1, y_2\} \neq \{y_3, y_4\}$. So $y_i \notin \{0_{\mathbf{K}}, 1_{\mathbf{K}}\}$ for $i = 1, \dots, 4$, and since every element in $K \setminus \{0_{\mathbf{K}}, 1_{\mathbf{K}}\}$ is join-irreducible, we have $y_1, \dots, y_4 \in B := \{b_j \mid j \in J\}$. Furthermore, for each $i = 1, \dots, 4$ there exists an $x_i \in L$ with $f(x_i) = y_i$ and there is a $j_i \in J$ with $x_i \not\leq a_{j_i}$ and $y_i = f(x_i) = b_{j_i}$. Hence, the pairs (b_{j_1}, b_{j_2}) and (b_{j_3}, b_{j_4}) are incomparable. We have that $a_{j_1} \leq a_{j_2}$ implies $x_2 \not\leq a_{j_1}, a_{j_2}$ and therefore $y_2 = f(x_2) = b_{j_1} \vee b_{j_2} = 1_{\mathbf{K}}$, a contradiction. A similar argument exists for $a_{j_2} \leq a_{j_1}, a_{j_3} \leq a_{j_4}, a_{j_4} \leq a_{j_3}$, so we know that (a_{j_1}, a_{j_2}) and (a_{j_3}, a_{j_4}) are incomparable pairs in \mathbf{L} . W.l.o.g. say that $b_{j_1}, b_{j_2}, b_{j_3}$ are pairwise distinct, so $a_{j_1}, a_{j_2}, a_{j_3}$ are pairwise distinct, too. Moreover, a_{j_3} must be incomparable with a_{j_1} or a_{j_2} . W.l.o.g. say a_{j_1} and a_{j_3} are incomparable. From $x_1 \not\leq a_{j_1}$ it follows that $x_1 \leq a_{j_2}$ (otherwise, $y_1 = f(x_1) = b_{j_1} \vee b_{j_2} = 1_{\mathbf{K}}$). From $x_2 \not\leq a_{j_2}$ it follows that $x_2 \leq a_{j_1}$. Hence, $x_2 \not\leq a_{j_3}$. Consequently, $b_{j_2} = f(x_2) = b_{j_2} \vee b_{j_3}$. Now we consider two cases:

Case 1: a_{j_2}, a_{j_3} are incomparable. From $x_1 \leq a_{j_2}$ it follows that $x_1 \not\leq a_{j_3}$, and therefore $b_{j_1} = f(x_1) = b_{j_1} \vee b_{j_3}$. So we have $b_{j_1}, b_{j_2} \geq b_{j_3}$ and it follows that $b_{j_3} = 0_{\mathbf{K}}$, which is a contradiction.

Case 2: $a_{j_2} \leq a_{j_3}$. From $x_3 \not\leq a_{j_3}$ it follows that $x_3 \not\leq a_{j_2}$, and therefore $b_{j_3} = b_{j_2} \vee b_{j_3}$. We find $b_{j_2} = b_{j_3}$, a contradiction. The case $a_{j_2} \geq a_{j_3}$ works analogously.

Since we arrive at a contradiction in both cases, the lemma is proved. \square

In the following we denote by \mathbf{M}_2 the boolean lattice with 4 elements, i.e. the lattice consisting of a least element 0, a greatest element 1, and two further elements a and b , which are incomparable (see Figure 3.1).

3.2. Cardinalities of semirings

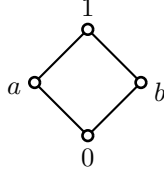


Figure 3.1: The lattice \mathbf{M}_2 .

Proposition 3.33. *Let $(f, g) \in \text{Adj}(\mathbf{L}, \mathbf{K})$. Then (f, g) is tight iff $(f \circ g)\mathbf{K}$ is a chain or isomorphic to \mathbf{M}_2 .*

Proof. The “only if” direction follows by $(f \circ g)(K) = f(L)$ and Lemma 3.32. The “if” direction follows from the fact that (f, g) is an adjunction of $(\mathbf{L}, (f \circ g)\mathbf{K})$. Since $(f \circ g)\mathbf{K}$ is distributive, (f, g) must be a tight adjunction of $(\mathbf{L}, (f \circ g)\mathbf{K})$ (see [38, Theorem 4]). So there exist $a_1, \dots, a_k \in L, b_1, \dots, b_k \in f(g(K)) \subseteq K$ with $f = \bigvee_{i=1}^k e_{a_i, b_i}$. Thus, f is also a tight residuated mapping from \mathbf{L} to \mathbf{K} , and so (f, g) is a tight adjunction of (\mathbf{L}, \mathbf{K}) . \square

Since $(f \circ g)\mathbf{K}$ is isomorphic to $(g \circ f)\mathbf{L}$ for every $(f, g) \in \text{Adj}(\mathbf{L}, \mathbf{K})$, we just have to consider closure and kernel systems that are chains or isomorphic to \mathbf{M}_2 . Let c_j be the number of closure systems of \mathbf{L} that are chains with j elements and let k_j the number of kernel systems of \mathbf{K} that are chains with j elements. Furthermore, let l_j be the number of chains in $(\mathbf{C}_i)_{i \in I}$ with $|C_i| = j$ and l'_j the number of chains in $(\mathbf{C}'_i)_{i \in I'}$ with $|C'_i| = j$. Then we have

$$c_1 = 1, \quad c_2 = |L| - 1, \quad c_j = \sum_{i \geq j} l_i \binom{i-1}{j-1} \text{ for } j \geq 3, \quad (3.5)$$

$$k_1 = 1, \quad k_2 = |K| - 1, \quad k_j = \sum_{i \geq j} l'_i \binom{i-1}{j-1} \text{ for } j \geq 3. \quad (3.6)$$

Let m denote the number of incomparable pairs in \mathbf{L} and m' the number of incomparable pairs in \mathbf{K} . So the number of closure systems of \mathbf{L} isomorphic to \mathbf{M}_2 equals m and the number of kernel systems of \mathbf{K} isomorphic to \mathbf{M}_2 equals m' . We have

$$m = \frac{1}{2} \sum_{i \in I} (|C_i| - 2)(|L| - |C_i|) = \frac{1}{2} \sum_{j \geq 1} l_j (j - 2)(|L| - j), \quad (3.7)$$

$$m' = \frac{1}{2} \sum_{i \in I'} (|C'_i| - 2)(|K| - |C'_i|) = \frac{1}{2} \sum_{j \geq 1} l'_j (j - 2)(|K| - j). \quad (3.8)$$

Since $|\text{Aut}(\mathbf{M}_2)| = 2$ and $|\text{Aut}(\mathbf{C})| = 1$ for any chain \mathbf{C} , we find with Equations 3.3, 3.4, and Proposition 3.33 that the number of tight adjunctions between \mathbf{L} and \mathbf{K} equals

$$2mm' + \sum_{i \geq 1} c_i k_i. \quad (3.9)$$

With Equations 3.5 - 3.8 this number can be easily computed. In particular we get

$$|E(\mathbf{L})| = 2m^2 + \sum_{i \geq 1} c_i^2. \quad (3.10)$$

Remark 3.34. For a finite lattice \mathbf{L} , every chain $\mathbf{C} = (C, \leq)$ in \mathbf{L} with $1_{\mathbf{L}} \in C$ ($0_{\mathbf{L}} \in C$) is a closure system (kernel system) of \mathbf{L} and admits therefore tight residuated mappings of \mathbf{L} . Also each incomparable pair (a, b) in \mathbf{L} yields the closure system $\{a \wedge b, a, b, 1_{\mathbf{L}}\}$ and the kernel system $\{0_{\mathbf{L}}, a, b, a \vee b\}$ of \mathbf{L} , which are both isomorphic to \mathbf{M}_2 . Therefore, each incomparable pair also admits tight residuated mappings of \mathbf{L} . Of course, there might also be closure and kernel systems of \mathbf{L} that are not isomorphic to a chain or \mathbf{M}_2 admitting further tight residuated mappings of \mathbf{L} . The fact that a horizontal sum of chains possesses closure and kernel systems isomorphic to a chain or \mathbf{M}_2 only gives rise to the conjecture that they admit very few tight residuated mappings. This is another evidence for Conjecture 3.29.

If Conjecture 3.29 is true, then it is easy to compute MinB_n . Indeed, for $n \in \mathbb{N}$, one has to consider every partition (d_1, \dots, d_k) of n with at least two nonzero parts d_i, d_j and one has to compute $|E(\mathbf{L})|$ by Equation 3.10 for the horizontal sum \mathbf{L} of the chains $\mathbf{C}_1, \dots, \mathbf{C}_k$, where \mathbf{C}_i has $d_i + 2$ elements for every $i = 1, \dots, k$. Then one knows the number $|E(\mathbf{L})|$ for every horizontal sum of chains \mathbf{L} , where \mathbf{L} is not a chain and has n join- and n meet-irreducible elements. Additionally, one has to compute $|E(\mathbf{C})|$ by Equation 3.10 for the chain with $n + 1$ elements \mathbf{C} . Finally MinB_n is given as the minimum of all these cardinalities.

Chapter 4

Invertible matrices over finite additively idempotent semirings

When matrices over semirings are used for cryptographic purposes, as for example in Protocol 1.20, the principal questions arise how to easily decide whether a matrix is invertible and, if so, how to compute the inverse matrix. For matrices over fields the answers to these questions are well-known: A matrix over a field is invertible iff its determinant is nonzero, and the inverse of an invertible matrix can be computed e.g. with the help of Gauss-Jordan elimination. A similar useful criterion for invertibility of matrices over arbitrary semirings is not known in general. There are results for invertible matrices over boolean algebras [39, 49, 58]. Furthermore, there exist generalisations to matrices over certain ordered algebraic structures [6], and there are findings for matrices over Brouwerian lattices [60] and distributive lattices [18]. Also for matrices over certain commutative semirings some results are known [11, 55]. In this chapter we present a criterion for invertible matrices over finite additively idempotent semirings with zero and one. Moreover, we give a construction for the inverse of an invertible matrix and a formula for the number of invertible matrices of a given size over a given semiring. For this, we represent a finite additively idempotent semiring with zero and one as a semiring of residuated mappings of a finite lattice. Our results cover the case of invertible matrices over proper finite simple semirings with zero.

This chapter is based on a collaboration with Stefan E. Schmidt and Jens Zumbrägel [35].

4.1 Matrices over additively idempotent semirings

Let $(R, +, \cdot)$ be a finite additively idempotent semiring. Then the additive semigroup $(R, +)$ is a semilattice (see Theorem 1.3). In particular, the ordered set (R, \leq) with the order \leq defined by $x \leq y :\Leftrightarrow x + y = y$ for all $x, y \in R$ is a join-semilattice with $\sup\{x, y\} = x + y$ for all $x, y \in R$. Moreover, if $(R, +)$ has a neutral element 0 , then (R, \leq) is a lattice with the least element 0 . In particular, if $(R, +, \cdot)$ is a finite additively idempotent semiring with zero, then (R, \leq) is a lattice. The next proposition shows that one can embed such a semiring into a semiring of residuated mappings if it has additionally a one.

Proposition 4.1. *Let $(R, +, \cdot)$ be a finite additively idempotent semiring with zero and one, $\mathbf{R} := (R, \leq)$, and*

$$T : R \rightarrow \text{Res}(\mathbf{R}), \quad r \mapsto T_r \quad \text{with} \quad T_r : x \mapsto rx.$$

Then $(R, +, \cdot)$ is isomorphic to the subsemiring $(T(R), \vee, \circ)$ of $(\text{Res}(\mathbf{R}), \vee, \circ)$.

Proof. Clearly, $T_r \in \text{Res}(\mathbf{R})$ for every $r \in R$ and T is a semiring homomorphism between $(R, +, \cdot)$ and $(\text{Res}(\mathbf{R}), \vee, \circ)$. Since $(R, +, \cdot)$ has a one 1 , we have that $T_r = T_s$ implies $r = T_r(1) = T_s(1) = s$ for all $r, s \in R$, i.e. T is injective. Hence, $(R, +, \cdot)$ is isomorphic to the subsemiring $(T(R), \vee, \circ)$ of $(\text{Res}(\mathbf{R}), \vee, \circ)$. \square

Let I be a finite index set and \mathbf{M}_i commutative monoids for every $i \in I$. It is easy to see that the mapping

$$\Omega : \prod_{(i,j) \in I \times I} \text{Hom}(\mathbf{M}_j, \mathbf{M}_i) \rightarrow \text{End} \left(\prod_{i \in I} \mathbf{M}_i \right), \quad (f_{i,j}) \mapsto \left(\sum_{j \in I} f_{i,j} \right)_{i \in I}$$

with

$$\left(\sum_{j \in I} f_{i,j} \right)_{i \in I} ((m_j)_{j \in I}) = \left(\sum_{j \in I} f_{i,j}(m_j) \right)_{i \in I}$$

for every $(m_j)_{j \in I} \in \text{End}(\prod_{j \in I} \mathbf{M}_j)$ is an isomorphism between the semirings

$$\left(\prod_{(i,j) \in I \times I} \text{Hom}(\mathbf{M}_j, \mathbf{M}_i), +, \circ \right) \quad \text{and} \quad \left(\text{End} \left(\prod_{i \in I} \mathbf{M}_i \right), +, \circ \right),$$

where $+$ denotes in each case the pointwise sum, \circ on $\text{End}(\prod_{i \in I} \mathbf{M}_i)$ the composition, and \circ is defined on $\prod_{(i,j) \in I \times I} \text{Hom}(\mathbf{M}_j, \mathbf{M}_i)$ by $(f_{i,j}) \circ (g_{i,j}) =: (h_{i,j})$ with

4.1. Matrices over additively idempotent semirings

$h_{i,j} = \sum_{k \in I} f_{i,k} \circ g_{k,j}$. In particular, it holds that

$$(\text{Mat}_{I \times I}(\text{End}(\mathbf{M})), +, \cdot) \cong \left(\prod_{(i,j) \in I \times I} \text{End}(\mathbf{M}), +, \circ \right) \cong (\text{End}(\mathbf{M}^I), +, \circ),$$

where $\mathbf{M}^I := \prod_{i \in I} \mathbf{M}$.

If \mathbf{L} and \mathbf{K} are finite lattices and $f : L \rightarrow K$ is a mapping, then f is residuated iff f is a homomorphism between the monoids $(L, \vee, 0_{\mathbf{L}})$ and $(K, \vee, 0_{\mathbf{K}})$. Therefore, for a finite index set S and some finite lattices \mathbf{L}_s , we get the following isomorphism for residuated mappings:

$$\left(\prod_{(s,t) \in S \times S} \text{Res}(\mathbf{L}_t, \mathbf{L}_s), \vee, \circ \right) \cong \left(\text{Res}\left(\prod_{s \in S} \mathbf{L}_s\right), \vee, \circ \right).$$

Example 4.2. Consider the direct product $\mathbf{L} = \mathbf{L}_1 \times \mathbf{L}_2$ of two finite lattices \mathbf{L}_1 and \mathbf{L}_2 . Then a mapping φ in $\text{Res}(\mathbf{L})$ corresponds to an element

$$\begin{pmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{pmatrix} \in \prod_{i,j=1,2} \text{Res}(\mathbf{L}_j, \mathbf{L}_i),$$

where $\varphi_{i,j} \in \text{Res}(\mathbf{L}_j, \mathbf{L}_i)$.

For matrices over $\text{Res}(\mathbf{L})$, we get the following corresponding isomorphism:

$$(\text{Mat}_{I \times I}(\text{Res}(\mathbf{L})), +, \cdot) \cong (\text{Res}(\mathbf{L}^I), \vee, \circ).$$

Therefore, a matrix $M \in \text{Mat}_{I \times I}(\text{Res}(\mathbf{L}))$ is invertible iff the corresponding residuated mapping

$$\varphi_M := \left(\bigvee_{j \in I} m_{i,j} \right)_{i \in I} \in \text{Res}(\mathbf{L}^I)$$

is invertible, which is equivalent to φ_M being bijective.

Lemma 4.3. *Let \mathbf{L} be a complete lattice and $f \in \text{Res}(\mathbf{L})$. Then f is an automorphism of \mathbf{L} iff f is bijective.*

Proof. Let f be bijective. For $x, y \in L$, the equivalence $x \leq y \Leftrightarrow y = x \vee y \Leftrightarrow f(y) = f(x \vee y) = f(x) \vee f(y) \Leftrightarrow f(x) \leq f(y)$ holds, i.e. f is an automorphism. The other direction is clear. \square

Corollary 4.4. *Let \mathbf{L} be a finite lattice, I a finite index set, and $M \in \text{Mat}_{I \times I}(\text{Res}(\mathbf{L}))$. Then M is invertible iff the corresponding mapping $\varphi_M \in \text{Res}(\mathbf{L}^I)$ is an automorphism of \mathbf{L}^I .*

Hence, we aim to give a characterisation for when a mapping of the direct product \mathbf{L}^I is an automorphism of \mathbf{L}^I . If \mathbf{L} is a direct product $\times_{t \in T} \mathbf{L}_t$ of irreducible lattices \mathbf{L}_t , $t \in T$, for a finite index set T , our task is then to determine when a mapping of the direct product $(\times_{t \in T} \mathbf{L}_t)^I$ is an automorphism. Consequently, it suffices to find a criterion for mappings of direct products of irreducible lattices. We present such a criterion (Theorem 4.10) and we translate it so that we can answer the question when a matrix in $\text{Mat}_{I \times I}(\text{Res}(\mathbf{L}))$ is invertible (Corollary 4.11). We also explain how our results apply to subsemirings of $(\text{Res}(\mathbf{L}), \vee, \circ)$, so that, by Proposition 4.1, they can be applied to every finite additively idempotent semiring with zero and one.

4.2 Direct decompositions

In this section we investigate maximal direct decompositions of lattices, on which our criterion for matrix invertibility will crucially depend.

An algebra \mathbf{A} is called **trivial** if $|A| = 1$, otherwise it is called **nontrivial**. We call an algebra \mathbf{A} **irreducible** if it is nontrivial and not isomorphic to a direct product of two nontrivial algebras. Analogously, an ordered set \mathbf{P} is called **trivial** if $|P| = 1$, otherwise it is called **nontrivial**. We also call an ordered set \mathbf{P} **irreducible** if it is nontrivial and not isomorphic to a direct product of two nontrivial ordered sets. Clearly, the direct product of lattices as ordered sets is the same as the direct product of lattices as algebras. Consequently, a lattice is irreducible as an ordered set iff it is irreducible as an algebra.

Definition 4.5. A **subdirect decomposition** of an algebra \mathbf{A} is a family $(\Theta_t)_{t \in T}$ of congruences of \mathbf{A} with

$$\bigcap_{t \in T} \Theta_t = \text{id}_A .$$

We call a subdirect decomposition $(\Theta_t)_{t \in T}$ of \mathbf{A} a **direct decomposition** of \mathbf{A} if the mapping

$$\iota : A \rightarrow \times_{t \in T} A/\Theta_t, \quad a \mapsto ([a]\Theta_t)_{t \in T}$$

is surjective. Moreover, we call a direct decomposition $(\Theta_t)_{t \in T}$ of \mathbf{A} **maximal** if

4.2. Direct decompositions

Θ_t is non-total for every $t \in T$ and if for every direct decomposition $(\Theta_s)_{s \in S}$ of \mathbf{A} , where Θ_s is non-total for every $s \in S$, the inequality $|S| \leq |T|$ holds.

For every algebra \mathbf{A} and every subdirect decomposition $(\Theta_t)_{t \in T}$ of \mathbf{A} the mapping ι is an injective homomorphism, and hence \mathbf{A} is isomorphic to $\iota(\mathbf{A})$. If ι is even surjective, then \mathbf{A} is isomorphic to the direct product $\times_{t \in T} \mathbf{A}/\Theta_t$. If Θ_t is non-total for a $t \in T$, then the factor \mathbf{A}/Θ_t is nontrivial.

Let \mathcal{F} be a language of algebras, I an index set, \mathbf{A}_i a nontrivial \mathcal{F} -algebra for every $i \in I$, and let $\mathbf{A} := \times_{i \in I} \mathbf{A}_i$. For an element $a \in A$, we denote the i -th coordinate of a by a_i . Define the congruence $\Phi_i := \{(a, b) \in A \times A \mid a_i = b_i\}$ for every $i \in I$. Then $(\Phi_i)_{i \in I}$ is clearly a direct decomposition of \mathbf{A} and Φ_i is non-total for every $i \in I$. Thus for a maximal direct decomposition $(\Theta_t)_{t \in T}$ of \mathbf{A} , the inequality $|T| \geq |I|$ holds.

An ordered set (P, \leq) is called the **sum** of the ordered sets $(P_i, \leq_i)_{i \in I}$, for an index set I , if $P = \bigcup_{i \in I} P_i$, where $P_i \cap P_j = \emptyset$ for all $i, j \in I$ with $i \neq j$, and

$$x \leq y \quad \Leftrightarrow \quad \exists i \in I : x, y \in P_i \text{ and } x \leq_i y$$

for all $x, y \in P$. An ordered set \mathbf{P} is called **connected** if it cannot be decomposed into the sum of any two ordered sets.

The next proposition is stated in [26].

Proposition 4.6. *The representation of a connected ordered set as the direct product of irreducible ordered sets is unique up to pairwise isomorphism of the factors.*

Since a lattice is a connected ordered set, we get the following.

Corollary 4.7. *Let S and T be index sets, \mathbf{L}_t an irreducible lattice for every $t \in T$, $\mathbf{L} := \times_{t \in T} \mathbf{L}_t$, and $(\Theta_s)_{s \in S}$ a maximal direct decomposition of \mathbf{L} . Then there exists a bijection $\sigma : S \rightarrow T$ with $\mathbf{L}/\Theta_s \cong \mathbf{L}_{\sigma(s)}$.*

For this reason, we may assume that if \mathbf{L} is the direct product of the irreducible lattices \mathbf{L}_t , $t \in T$, then a maximal direct decomposition of \mathbf{L} is of the form $(\Theta_t)_{t \in T}$ with $\mathbf{L}/\Theta_t \cong \mathbf{L}_t$ for all $t \in T$.

In [23, Chapter 1.3, Theorem 13] the following result is proven.

Theorem 4.8. *Let \mathbf{L} and \mathbf{K} be lattices, let Θ_L be a congruence on \mathbf{L} , and let Θ_K be a congruence on \mathbf{K} . Define the relation $\Theta_L \times \Theta_K$ on $\mathbf{L} \times \mathbf{K}$ by*

$$(a, b)(\Theta_L \times \Theta_K)(c, d) \quad \text{iff} \quad a\Theta_L c \text{ and } b\Theta_K d.$$

Then $\Theta_L \times \Theta_K$ is a congruence on $\mathbf{L} \times \mathbf{K}$. Conversely, every congruence on $\mathbf{L} \times \mathbf{K}$ is of this form.

Note that ‘ $\Theta_L \times \Theta_K$ ’ is a slight abuse of notation since it is not identical to the Cartesian product of the two sets Θ_L and Θ_K .

It furthermore holds that

$$[a]\Theta_L \times [b]\Theta_K = \{(c, d) \in L \times K \mid a\Theta_L c \text{ and } b\Theta_K d\} = [(a, b)](\Theta_L \times \Theta_K) \quad (4.1)$$

and so

$$\mathbf{L}/\Theta_L \times \mathbf{K}/\Theta_K = (\mathbf{L} \times \mathbf{K})/(\Theta_L \times \Theta_K) \quad (4.2)$$

for two lattices \mathbf{L}, \mathbf{K} and congruences Θ_L on \mathbf{L} and Θ_K on \mathbf{K} .

The following result is a strengthening of Corollary 4.7.

Lemma 4.9. *Let T be a finite index set, \mathbf{L}_t an irreducible lattice for every $t \in T$, $\mathbf{L} := \times_{t \in T} \mathbf{L}_t$, and $(\Theta_t)_{t \in T}$ a maximal direct decomposition of \mathbf{L} . Then there exists a permutation σ of T with $\mathbf{L}_t \cong \mathbf{L}_{\sigma(t)}$ and*

$$(x_s)_{s \in T} \Theta_{\sigma(t)} (y_s)_{s \in T} \Leftrightarrow x_t = y_t$$

for all $(x_s)_{s \in T}, (y_s)_{s \in T} \in L$ and $t \in T$.

Proof. By Corollary 4.7, we may assume that $\mathbf{L}/\Theta_t \cong \mathbf{L}_t$ holds for all $t \in T$. We fix $t_0 \in T$ and define $\mathbf{L}' := \times_{t \in T \setminus \{t_0\}} \mathbf{L}_t$. Thus, $\mathbf{L} = \mathbf{L}_{t_0} \times \mathbf{L}'$. By Theorem 4.8, there exist for every $t \in T$ some congruences $\Theta_t^{t_0} \in \text{Con}(\mathbf{L}_{t_0})$, $\Theta'_t \in \text{Con}(\mathbf{L}')$ with $\Theta_t = \Theta_t^{t_0} \times \Theta'_t$. We will show that $(\Theta_t^{t_0})_{t \in T}$ is a direct decomposition of \mathbf{L}_{t_0} . Let $(x, x') \in \bigcap_{t \in T} \Theta_t^{t_0}$. We have to show that $x = x'$ holds. Let $\bar{y} \in L'$. Thus, $(\bar{y}, \bar{y}) \in \bigcap_{t \in T} \Theta'_t$ and consequently $((x, \bar{y}), (x', \bar{y})) \in \bigcap_{t \in T} \Theta_t = \text{id}_L$. So, we have $(x, \bar{y}) = (x', \bar{y})$ and therefore $x = x'$. Hence, $(\Theta_t^{t_0})_{t \in T}$ is a subdirect decomposition of \mathbf{L}_{t_0} . Now let $x_t \in \mathbf{L}_{t_0}$ for every $t \in T$. We will show that there exists an element $z \in \mathbf{L}_{t_0}$ with $[z]\Theta_t^{t_0} = [x_t]\Theta_t^{t_0}$ for every $t \in T$. Choose an element $(y_t)_{t \in T \setminus \{t_0\}} \in \mathbf{L}'$. For every $s \in T$, we will regard $(x_s, (y_t)_{t \in T \setminus \{t_0\}}) \in L$ as the element in L , where the t_0 -th coordinate is x_s . Since $(\Theta_t)_{t \in T}$ is a direct decomposition of \mathbf{L} , there exists an element $(\hat{x}_t)_{t \in T} \in L$ with $[(\hat{x}_t)_{t \in T}]\Theta_s = [(x_s, (y_t)_{t \in T \setminus \{t_0\}})]\Theta_s$ for every $s \in T$. By Equation 4.1, for every $s \in T$,

$$\begin{aligned} [\hat{x}_{t_0}]\Theta_s^{t_0} \times [(\hat{x}_t)_{t \in T \setminus \{t_0\}}]\Theta'_s &= [(\hat{x}_t)_{t \in T}]\Theta_s = [(x_s, (y_t)_{t \in T \setminus \{t_0\}})]\Theta_s \\ &= [x_s]\Theta_s^{t_0} \times [(y_t)_{t \in T \setminus \{t_0\}}]\Theta'_s \end{aligned}$$

4.3. Invertible matrices

holds and it follows that $[\hat{x}_{t_0}]_{\Theta_s^{t_0}} = [x_s]_{\Theta_s^{t_0}}$. Hence, \hat{x}_{t_0} is the desired element z and it follows that $(\Theta_t^{t_0})_{t \in T}$ is a direct decomposition of \mathbf{L}_{t_0} . Consequently, $\mathbf{L}_{t_0} \cong \times_{t \in T} (\mathbf{L}_{t_0} / \Theta_t^{t_0})$ and since \mathbf{L}_{t_0} is irreducible, there exists a unique $t_1 \in T$ with $\mathbf{L}_{t_0} \cong \mathbf{L}_{t_0} / \Theta_{t_1}^{t_0}$. Thus, $\Theta_{t_1}^{t_0} = \text{id}_{L_{t_0}}$. By this and Equation 4.2, it follows that

$$\mathbf{L}_{t_0} \times \mathbf{L}' / \Theta_{t_1}' \cong \mathbf{L}_{t_0} / \Theta_{t_1}^{t_0} \times \mathbf{L}' / \Theta_{t_1}' = (\mathbf{L}_{t_0} \times \mathbf{L}') / (\Theta_{t_1}^{t_0} \times \Theta_{t_1}') = \mathbf{L} / \Theta_{t_1} \cong \mathbf{L}_{t_1} .$$

Since \mathbf{L}_{t_1} is irreducible and \mathbf{L}_{t_0} nontrivial, we have $\mathbf{L}_{t_0} \cong \mathbf{L}_{t_1}$ and $|\mathbf{L}' / \Theta_{t_1}'| = 1$. Hence, $\Theta_{t_1}' = L' \times L'$. We derive $(x_t)_{t \in T} \Theta_{t_1} (y_t)_{t \in T} \Leftrightarrow x_{t_0} = y_{t_0}$ for all $(x_t)_{t \in T}, (y_t)_{t \in T} \in L$.

We have shown that there exists a mapping $\sigma : T \rightarrow T$ with $\mathbf{L}_t \cong \mathbf{L}_{\sigma(t)}$ and $(x_s)_{s \in T} \Theta_{\sigma(t)} (y_s)_{s \in T} \Leftrightarrow x_t = y_t$ for all $(x_s)_{s \in T}, (y_s)_{s \in T} \in L, t \in T$. Indeed, with the notation above, we have $t_1 = \sigma(t_0)$. It remains to show that σ is injective. Let $t_2, t_3 \in T$ with $\sigma(t_2) = \sigma(t_3)$. It follows the equivalence $x_{t_2} = y_{t_2} \Leftrightarrow (x_t)_{t \in T} \Theta_{\sigma(t_2)} (y_t)_{t \in T} \Leftrightarrow (x_t)_{t \in T} \Theta_{\sigma(t_3)} (y_t)_{t \in T} \Leftrightarrow x_{t_3} = y_{t_3}$ for all $(x_t)_{t \in T}, (y_t)_{t \in T} \in L$ and we find that $t_2 = t_3$. \square

4.3 Invertible matrices

A criterion

The following theorem states for a mapping of a direct product of irreducible lattices a criterion for being an automorphism. It is basically a consequence of Lemma 4.9. We will see the corresponding result for matrices in Corollary 4.11.

Theorem 4.10. *Let T be a finite index set, \mathbf{L}_t an irreducible lattice for every $t \in T$, $\mathbf{L} := \times_{t \in T} \mathbf{L}_t$, and $\varphi : L \rightarrow L$ a mapping. Then $\varphi \in \text{Aut}(\mathbf{L})$ iff there exists a permutation σ of T and an isomorphism $\varphi_t : L_t \rightarrow L_{\sigma^{-1}(t)}$ for every $t \in T$ such that*

$$\varphi = (\varphi_{\sigma(t)} \circ \pi_{\sigma(t)})_{t \in T} ,$$

where π_t is the t -th projection, i.e. $\varphi((x_t)_{t \in T}) = (\varphi_{\sigma(t)}(x_{\sigma(t)}))_{t \in T}$ for all $(x_t)_{t \in T} \in L$.

Proof. Let $\varphi \in \text{Aut}(\mathbf{L})$, $\varphi^t := \pi_t \circ \varphi$ for every $t \in T$, and $\Theta_t := \ker(\varphi^t)$ for every $t \in T$. We will show that $(\Theta_t)_{t \in T}$ is a maximal direct decomposition of \mathbf{L} . We have

$$\begin{aligned} (x, y) \in \bigcap_{t \in T} \Theta_t &\Leftrightarrow \forall t \in T : (x, y) \in \Theta_t \\ &\Leftrightarrow \forall t \in T : \varphi^t(x) = \varphi^t(y) \Leftrightarrow \varphi(x) = \varphi(y) \Leftrightarrow x = y \end{aligned}$$

for all $x, y \in L$, i.e. $\bigcap_{t \in T} \Theta_t = \text{id}_L$. Therefore, $(\Theta_t)_{t \in T}$ is a subdirect decomposition of \mathbf{L} . Let $y^t \in L$ for every $t \in T$. We will show that there exists a $z \in L$ satisfying $[z]\Theta_t = [y^t]\Theta_t$ for every $t \in T$. Let $x_t := \varphi^t(y^t)$ for every $t \in T$, let $x := (x_t)_{t \in T}$, and let $z := \varphi^{-1}(x)$. It follows that $\varphi^t(z) = x_t = \varphi^t(y^t)$ and therefore that $z\Theta_t y^t$ for every $t \in T$. Hence, $[z]\Theta_t = [y^t]\Theta_t$ for every $t \in T$ and $(\Theta_t)_{t \in T}$ is consequently a direct decomposition. Since φ is bijective, $\Theta_t \neq L \times L$ holds for every $t \in T$. Because a maximal direct decomposition of \mathbf{L} has exactly $|T|$ elements by Corollary 4.7, $(\Theta_t)_{t \in T}$ is a maximal direct decomposition.

By Lemma 4.9, there exists a permutation σ of T with $\mathbf{L}_t \cong \mathbf{L}_{\sigma(t)}$ and $x\Theta_t y \Leftrightarrow x_{\sigma(t)} = y_{\sigma(t)}$ for every $t \in T$ and $x, y \in L$. It follows that $\varphi^t(x) = \varphi^t(y) \Leftrightarrow x\Theta_t y \Leftrightarrow x_{\sigma(t)} = y_{\sigma(t)}$, i.e. $\varphi^t(x)$ depends only on $x_{\sigma(t)}$ for every $t \in T$. Thus the first direction of the statement follows by $\varphi_{\sigma(t)} := \varphi^t \circ \epsilon_{\sigma(t)}$, where $\epsilon_s : L_s \rightarrow L$ is the s -th canonical injection. The second direction is trivial. \square

Let T, I be finite index sets, \mathbf{L}_t an irreducible finite lattice for every $t \in T$, and $\mathbf{L} := \times_{t \in T} \mathbf{L}_t$. Then $\mathbf{L}^I = \times_{(t,i) \in T \times I} \mathbf{L}_{t,i}$, where $\mathbf{L}_{t,i} = \mathbf{L}_t$ for every $(t,i) \in T \times I$. With this notation, we derive in the following the corresponding result for invertible matrices. For a matrix $A \in \text{Mat}_{I \times I}(\text{Res}(\mathbf{L}))$, we will denote the i -th row by A_i and we will regard A_i as mapping from L^I to L .

Corollary 4.11. *Let T, I be finite index sets, \mathbf{L}_t an irreducible finite lattice for every $t \in T$, $\mathbf{L} := \times_{t \in T} \mathbf{L}_t$, and $A \in \text{Mat}_{I \times I}(\text{Res}(\mathbf{L}))$. Then A is invertible iff there exists a permutation σ of $T \times I$ and an isomorphism $\varphi_{t,i} : L_{t,i} \rightarrow L_{\sigma^{-1}(t,i)}$ for every $(t,i) \in T \times I$ such that*

$$\pi_t \circ A_i = \varphi_{\sigma(t,i)} \circ \pi_{\sigma(t,i)},$$

where π_t is the projection from \mathbf{L} to \mathbf{L}_t and $\pi_{t,i}$ the projection from \mathbf{L}^I to $\mathbf{L}_{t,i}$.

Example 4.12. Let \mathbf{L}_1 and \mathbf{L}_2 be two finite lattices, let $\mathbf{L} = \mathbf{L}_1 \times \mathbf{L}_2$, and

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_{2 \times 2}(\text{Res}(\mathbf{L})).$$

We can consider each entry of M as an element in $\times_{i,j=1,2} \text{Res}(\mathbf{L}_j, \mathbf{L}_i)$ as in Ex-

4.3. Invertible matrices

ample 4.2. Then we have the following representation:

$$M = \left(\begin{array}{cc|cc} a_{11} & a_{12} & b_{11} & b_{12} \\ a_{21} & a_{22} & b_{21} & b_{22} \\ \hline c_{11} & c_{12} & d_{11} & d_{12} \\ c_{21} & c_{22} & d_{21} & d_{22} \end{array} \right)$$

Corollary 4.11 states that M is invertible iff each column and each row in this representation has exactly one nonzero entry and this nonzero entry is an isomorphism.

E.g. if M has the representation

$$\left(\begin{array}{cc|cc} 0 & 0 & b_{11} & 0 \\ 0 & a_{22} & 0 & 0 \\ \hline c_{11} & 0 & 0 & 0 \\ 0 & 0 & 0 & d_{22} \end{array} \right),$$

where a_{22}, b_{11}, c_{11} , and d_{22} are isomorphisms, then M is invertible.

If A is invertible, then

$$\varphi_A = (\varphi_{\sigma(t,i)} \circ \pi_{\sigma(t,i)})_{(t,i) \in T \times I}$$

is the corresponding mapping to A in $\text{Res}(\mathbf{L}^J)$ and $a_{i,j}$ is of the form $a_{i,j} = (\hat{\varphi}_{i,j,t})_{t \in T}$ with

$$\hat{\varphi}_{i,j,t} = \begin{cases} \varphi_{\sigma(t,i)} & \text{if } \exists s \in T : \sigma(t,i) = (s,j), \\ \bar{0}_{\mathbf{L}_t} & \text{else,} \end{cases}$$

where $\bar{0}_{\mathbf{L}_t}$ is the mapping that maps constantly to $0_{\mathbf{L}_t}$.

In the special case that \mathbf{L} is irreducible we do not have to consider the index set T since it has just one element. Then the equation in Corollary 4.11 is of the form $A_i = \varphi_{\sigma(i)} \circ \pi_{\sigma(i)}$ for every $i \in I$, i.e. $a_{i,\sigma(i)}$ is the only nonzero entry in the i -th row and $a_{i,\sigma(i)} = \varphi_{\sigma(i)}$ holds. We call a matrix a **generalised permutation matrix** (or **monomial matrix**) if each row and each column has exactly one nonzero entry and this nonzero entry is invertible.

Corollary 4.13. *Let \mathbf{L} be a finite irreducible lattice, I a finite index set, and $A \in \text{Mat}_{I \times I}(\text{Res}(\mathbf{L}))$. Then A is invertible iff A is a generalised permutation matrix.*

Number of invertible matrices

As another consequence of Theorem 4.10, we find the following.

Corollary 4.14. *Let T be a finite index set, \mathbf{L}_t , $t \in T$, pairwise distinct irreducible lattices, $e_t \in \mathbb{N}$ for every $t \in T$, and $\mathbf{L} := \times_{t \in T} \mathbf{L}_t^{e_t}$. Then*

$$|\text{Aut}(\mathbf{L})| = \prod_{t \in T} e_t! \cdot |\text{Aut}(\mathbf{L}_t)|^{e_t}.$$

In particular, for a finite index set I , we have

$$|\text{Aut}(\mathbf{L}^I)| = \prod_{t \in T} (e_t \cdot |I|)! \cdot |\text{Aut}(\mathbf{L}_t)|^{e_t \cdot |I|},$$

which is exactly the number of invertible matrices in $\text{Mat}_{I \times I}(\text{Res}(\mathbf{L}))$.

Example 4.15. Let \mathbf{L} be a finite irreducible lattice and $n \in \mathbb{N}$. Then there exist exactly

$$n! \cdot |\text{Aut}(\mathbf{L})|^n$$

invertible matrices in $\text{Mat}_{n \times n}(\text{Res}(\mathbf{L}))$. If the lattice \mathbf{L} has just one automorphism (e.g. if \mathbf{L} is a chain), namely id_L , then there are $n!$ invertible matrices in $\text{Mat}_{n \times n}(\text{Res}(\mathbf{L}))$, which is exactly the number of $n \times n$ permutation matrices.

There tend to be very few invertible matrices over finite additively idempotent semirings compared to matrices over fields. Consider the following example.

Example 4.16. Let \mathbf{L} be the lattice, whose Hasse-diagram is the one in Figure 4.1. This lattice is irreducible and there exist 50 residuated mappings and two automorphisms of this lattice, which means $|\text{Res}(\mathbf{L})| = 50$ and $|\text{Aut}(\mathbf{L})| = 2$. Therefore, there exist $n! \cdot 2^n$ invertible matrices in $\text{Mat}_{n \times n}(\text{Res}(\mathbf{L}))$. For example, for $n = 3$ there exist approximately $1.95 \cdot 10^{15}$ matrices in $\text{Mat}_{3 \times 3}(\text{Res}(\mathbf{L}))$ and 48 of them are invertible. For comparison, if one considers the 3×3 matrices over the finite field \mathbb{F}_{49} , then there exist approximately $1.63 \cdot 10^{15}$ such matrices and approximately $1.59 \cdot 10^{15}$ of them are invertible.

The inverse matrix

The next proposition provides a construction for the inverse matrix of an invertible matrix.

4.3. Invertible matrices

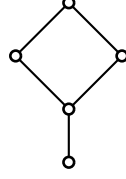


Figure 4.1: The lattice of Example 4.16.

Proposition 4.17. *Let T, I be finite index sets, \mathbf{L}_t an irreducible finite lattice for every $t \in T$, $\mathbf{L} := \times_{t \in T} \mathbf{L}_t$, let $A \in \text{Mat}_{I \times I}(\text{Res}(\mathbf{L}))$ be invertible, and σ and $\varphi_{t,i}$ for every $(t, i) \in T \times I$ as in Corollary 4.11. Then for the inverse matrix B of A , the entry $b_{i,j}$ for $i, j \in I$ is of the form $b_{i,j} = (\check{\varphi}_{i,j,t})_{t \in T}$ with*

$$\check{\varphi}_{i,j,t} = \begin{cases} \varphi_{t,i}^{-1} & \text{if } \exists s \in T : \sigma^{-1}(t, i) = (s, j), \\ \bar{0}_{\mathbf{L}_t} & \text{else.} \end{cases}$$

Proof. As stated before, $\varphi_A = (\varphi_{\sigma(t,i)} \circ \pi_{\sigma(t,i)})_{(t,i) \in T \times I}$ is the corresponding mapping to A in $\text{Res}(\mathbf{L}^I)$. The inverse of φ_A , i.e. the corresponding mapping to the matrix B , is the mapping $\varphi_B = \varphi_A^{-1} = (\varphi_{t,i}^{-1} \circ \pi_{\sigma^{-1}(t,i)})_{(t,i) \in T \times I}$. It follows that $b_{i,j}$ is of the form $b_{i,j} = (\check{\varphi}_{i,j,t})_{t \in T}$ with $\check{\varphi}_{i,j,t}$ as given in the proposition. \square

Example 4.18. Consider the invertible matrix M with the representation

$$\left(\begin{array}{cc|cc} 0 & 0 & b_{11} & 0 \\ 0 & a_{22} & 0 & 0 \\ \hline c_{11} & 0 & 0 & 0 \\ 0 & 0 & 0 & d_{22} \end{array} \right)$$

from Example 4.12. Then the inverse matrix has the representation

$$\left(\begin{array}{cc|cc} 0 & 0 & c_{11}^{-1} & 0 \\ 0 & a_{22}^{-1} & 0 & 0 \\ \hline b_{11}^{-1} & 0 & 0 & 0 \\ 0 & 0 & 0 & d_{22}^{-1} \end{array} \right).$$

Invertible matrices over subsemirings of $(\text{Res}(\mathbf{L}), \vee, \circ)$

Lemma 4.19. *Let \mathbf{L} be a finite lattice, (R, \vee, \circ) a subsemiring of $(\text{Res}(\mathbf{L}), \vee, \circ)$, and $\varphi \in R$ such that φ is invertible in $(\text{Res}(\mathbf{L}), \circ)$. Then $\varphi^{-1} \in R$.*

Proof. Since φ is invertible and \mathbf{L} is finite, we find that $\varphi^{-1} \in \langle \varphi \rangle \subseteq R$, where $\langle \varphi \rangle$ is the span of φ with respect to \circ . \square

If (R, \vee, \circ) is a subsemiring of $(\text{Res}(\mathbf{L}), \vee, \circ)$, then $(\text{Mat}_{I \times I}(R), +, \cdot)$ is also a subsemiring of $(\text{Mat}_{I \times I}(\text{Res}(\mathbf{L})), +, \cdot)$. The next corollary states the corresponding result.

Corollary 4.20. *Let \mathbf{L} be a finite lattice, (R, \vee, \circ) a subsemiring of $(\text{Res}(\mathbf{L}), \vee, \circ)$, I a finite index set, and $A \in \text{Mat}_{I \times I}(R)$ such that A is invertible in $\text{Mat}_{I \times I}(\text{Res}(\mathbf{L}))$. Then $A^{-1} \in \text{Mat}_{I \times I}(R)$.*

This means that for matrices over a subsemiring of $(\text{Res}(\mathbf{L}), \vee, \circ)$, one can also apply Corollary 4.11 to decide whether a matrix is invertible and Proposition 4.17 to construct the inverse of an invertible matrix. Consequently, one can do this for every finite additively idempotent semiring with zero and one by Proposition 4.1. In particular, these results apply to every proper finite simple semiring with zero by Theorem 1.11.

4.4 Remarks

In the following let $(R, +, \cdot)$ be a finite additively idempotent semiring with zero and one. To apply Corollary 4.11 and Proposition 4.17 for matrices over R , it is necessary to represent the semiring as a semiring of residuated mappings of a finite lattice \mathbf{L} . Additionally, it is required to know the representation of the lattice as a direct product $\mathbf{L} = \times_{t \in T} \mathbf{L}_t$ of irreducible lattices \mathbf{L}_t and to represent every residuated mapping (semiring element) as a mapping of $\times_{t \in T} \mathbf{L}_t$. For example, one can represent $(R, +, \cdot)$ as the subsemiring $(T(R), \vee, \circ)$ of $(\text{Res}(\mathbf{R}), \vee, \circ)$, where $\mathbf{R} = (R, \leq)$ (see Proposition 4.1). Also in this case one has to represent \mathbf{R} as a direct product $\mathbf{R} = \times_{t \in T} \mathbf{R}_t$ of irreducible lattices \mathbf{R}_t , and one has to represent every mapping in $T(R)$ as a mapping of $\times_{t \in T} \mathbf{R}_t$.

If the lattice \mathbf{L} is irreducible, then we know by Corollary 4.13 that a matrix is invertible iff it is a generalised permutation matrix, so in this case determining whether a matrix is invertible as well as inverting is very easy. In particular, if the lattice \mathbf{R} is irreducible, then a matrix is invertible iff it is a generalised permutation matrix. Furthermore, the lattice \mathbf{R} is irreducible iff the semigroup $(R, +)$ is irreducible. Hence, we get the following corollary.

Corollary 4.21. *Let $(R, +)$ be irreducible and $A \in \text{Mat}_{I \times I}(R)$. Then A is invertible iff A is a generalised permutation matrix.*

4.4. Remarks

Consequences on cryptosystems

The ability to determine whether a matrix is invertible or not and to compute the inverse of an invertible matrix does not seem to have immediate consequences on Protocol 1.20 due to the two-sided semigroup action. However, it would have an effect on a similar protocol using only a one-sided semigroup action. Consider the following protocol:

Protocol 4.22. (Diffie-Hellman with one-sided matrix semiring action)

- Alice and Bob publicly agree on a finite semiring $(R, +, \cdot)$ with zero and choose a positive integer n and matrices $M, S \in \text{Mat}_{n \times n}(R)$.
- Alice chooses a polynomial $p_a \in C[x]$ and computes $A = p_a(M) \cdot S$. She sends A to Bob and keeps p_a secret.
- Bob chooses polynomial $p_b \in C[x]$ and computes $B = p_b(M) \cdot S$. He sends B to Alice and keeps p_b secret.
- Their common secret key is

$$k = p_a(M) \cdot B = p_b(M) \cdot A = p_a(M) \cdot p_b(M) \cdot S.$$

If the matrix S in this protocol would be invertible, one could easily solve the corresponding semigroup action problem. More precisely, given the matrices A and S (or B and S), one can compute $p_a(M) = A \cdot S^{-1}$ (or $p_b(M) = B \cdot S^{-1}$). On the other hand, since it is possible to determine whether a matrix is invertible or not, it is also possible to avoid an invertible matrix S in the set-up phase of the protocol.

Chapter 5

Finite simple additively idempotent semirings

There have been several studies on simple semirings, e.g. in [2, 3, 31, 32, 44, 45, 61]. Amongst other things a complete classification of finite commutative simple semirings was presented in [2]. But there exists so far no classification of all finite simple semirings. Monico showed in [45] that every proper finite simple semiring with more than two elements and nontrivial addition is additively idempotent. Thereupon additively idempotent semirings have been studied in [31, 32, 61]. In this chapter we aim to describe all finite simple additively idempotent semirings. We did not succeed to characterise all these semirings, but our approach covers many cases. This work was done in collaboration with Jens Zumbärgel [36].

Besides the natural interest in simple objects, there is also a motivation to proceed on the classification of finite simple semirings in the context of this dissertation. As shown in Section 1.4.1, semigroup actions involving commutative matrix semirings have been proposed in [42]. These constructions use semirings with zero only, but this is not a necessary requirement. Let $(R, +, \cdot)$ be a semiring with nonempty centre C . Then we define

$$\mathcal{C} := \{(c_i)_{i \in I} \mid I \subseteq \mathbb{N}_{>0} \text{ is finite, } \forall i \in I : c_i \in C\}.$$

For a positive integer n , a matrix $M \in \text{Mat}_{n \times n}(R)$, and $c = (c_i)_{i \in I} \in \mathcal{C}$, we define

$$c(M) := \sum_{i \in I} c_i M^i.$$

Furthermore, let $C[M] := \{c(M) \mid c \in \mathcal{C}\}$. Then it is easy to see that $(C[M], +, \cdot)$ is a commutative subsemiring of $(\text{Mat}_{n \times n}(R), +, \cdot)$. Therefore, also semirings without zero can be used in Protocol 1.20.

To present the main result from [45], we need the following theorem about simple semigroups, which can be found in [30, Theorem 3.7.1].

Theorem 5.1. *Let $I = \{1, 2, \dots, m\}$, $J = \{1, 2, \dots, n\}$, and P an $n \times m$ matrix with $p_{i,j} \in \{0, 1\}$ for all i, j such that no row or column is identically zero, no two rows are identical, and no two columns are identical. Let $S = (I \times J) \cup \{\infty\}$ and define a binary operation on S by*

$$(i, j) \cdot (k, l) := \begin{cases} (i, l) & \text{if } p_{j,k} = 1, \\ \infty & \text{else,} \end{cases} \quad (i, j) \cdot \infty := \infty \cdot (i, j) := \infty \cdot \infty := \infty.$$

Then (S, \cdot) is a simple semigroup of order $mn + 1$. Conversely, every finite simple semigroup with an absorbing element is isomorphic to one of this kind.

The main result in [45] is the following:

Theorem 5.2. *Let $(R, +, \cdot)$ be a finite simple semiring. Then one of the following holds:*

1. $|R| \leq 2$.
2. $(R, +, \cdot) \cong (\text{Mat}_n(\mathbb{F}_q), +, \cdot)$ for some finite field \mathbb{F}_q and some $n \geq 1$.
3. $(R, +, \cdot)$ is a zero multiplication ring of prime order.
4. (R, \cdot) is a semigroup as in Theorem 5.1 with absorbing element $\infty \in R$ and $R + R = \{\infty\}$.
5. $(R, +)$ is idempotent.

Of course every semiring in the first four cases is simple, but not every additively idempotent semiring is simple. Hence, if one wants to classify all finite simple semirings, then it remains to describe all finite simple additively idempotent semirings. The case, where such a semiring has a zero, was already described by Theorem 1.11.

We use here the same approach as in [61], i.e. we try to characterise every finite simple additively idempotent semiring as a semiring of join-morphisms of a semilattice. For this we have to distinguish between several cases, as we explain now. We call an element r in a semiring $(R, +, \cdot)$ **right (left) absorbing** if it is

multiplicatively right (left) absorbing, i.e. $sr = r$ ($rs = r$) holds for every $s \in R$. If r is left and right absorbing, then it is called **absorbing**. Whenever $(R, +, \cdot)$ is additively idempotent, we consider the order \leq on R defined by $x \leq y :\Leftrightarrow x + y = y$ for $x, y \in R$. Then (R, \leq) is a join-semilattice with $\sup\{x, y\} = x + y$ for all $x, y \in R$. If R is moreover finite, then by the **greatest element** of $(R, +, \cdot)$ we mean the greatest element of (R, \leq) , which is $\sum_{r \in R} r$. We consider the cases where the greatest element of a finite simple additively idempotent semiring is

1. neither right nor left absorbing,
2. right but not left absorbing,
3. left but not right absorbing,
4. absorbing and the semiring possesses a finite idempotent irreducible semimodule (see Section 5.1 for definitions), whose greatest element is
 - (a) join-irreducible,
 - (b) join-reducible.

We succeed with this approach for every case, except Case 4b, for which we have a conjecture.

As we will see in Section 5.6, semirings in Case 4b have no additively neutral element. For this reason, we complete the classification of finite simple semirings with an additively neutral element by our characterisation theorems. This classification is summarised in Theorem 5.63.

The chapter is structured as follows. Section 5.1 contains a comprehensive study of semimodules, especially idempotent irreducible semimodules. These semimodules are necessary to describe the embedding of a finite simple additively idempotent semiring into the semiring of join-morphisms of a semilattice, which is done in Section 5.2. In Section 5.3, we study simple subsemirings of a semiring of join-morphisms of a semilattice. The main results are stated in Section 5.4, which are the characterisation theorems that characterise a finite simple additively idempotent semiring as a semiring of join-morphisms of a semilattice. Section 5.5 clarifies that if two semirings considered in the main results are isomorphic, then also the corresponding semilattices have to be isomorphic. The question when a semiring has an additively or multiplicatively neutral element is answered in Section 5.6, where we also state the complete classification of finite simple semirings with an additively neutral element. In Section 5.7, we discuss the remaining Case 4b.

5.1 Semimodules

In the following let $(R, +, \cdot)$ be a semiring.

Definition 5.3. A **semimodule** over $(R, +, \cdot)$ (or just **R -semimodule**) is a commutative semigroup $(M, +)$ together with an R -multiplication

$$R \times M \rightarrow M, \quad (r, x) \mapsto rx,$$

such that

$$r(sx) = (rs)x, \quad (r + s)x = rx + sx, \quad \text{and} \quad r(x + y) = rx + ry$$

for all $r, s \in R$ and $x, y \in M$.

For an R -semimodule $(M, +)$, we define $RN := \{rn \mid r \in R, n \in N\}$ for every subset N of M and $Ra := \{ra \mid r \in R\}$ for every $a \in M$.

An R -semimodule $(M, +)$ can be understood as the algebra $(M, F \cup \{+\})$, where

$$F := \{T_r : M \rightarrow M, x \mapsto rx \mid r \in R\}.$$

By an **R -subsemimodule** of $(M, +)$ we mean a subalgebra of this algebra, i.e. a subsemigroup $(N, +)$ of $(M, +)$ with $RN \subseteq N$. Clearly, $(Ra, +)$ is an R -subsemimodule of $(M, +)$, for $a \in M$. By a **(semimodule) congruence** on $(M, +)$ we mean a congruence on $(M, F \cup \{+\})$, i.e. an equivalence relation \sim on M satisfying

$$a \sim b \text{ and } c \sim d \quad \Rightarrow \quad a + c \sim b + d \text{ and } ra \sim rb$$

for all $a, b, c, d \in M$ and $r \in R$. One can easily see that this is equivalent to

$$a \sim b \quad \Rightarrow \quad a + c \sim b + c \text{ and } ra \sim rb$$

for all $a, b, c \in M$ and $r \in R$. If \sim is a semimodule congruence on $(M, +)$, then $(M/\sim, +)$ with $[x] + [y] := [x + y]$ and $r[x] := [rx]$ is again an R -semimodule, called **quotient semimodule**.

If $(M, +)$ is an R -semimodule, then we mean by $\text{End}(M, +)$ the set of all semigroup endomorphisms of the semigroup $(M, +)$.

5.1. Semimodules

Definition 5.4. An R -semimodule $(M, +)$ is called **faithful** if the semiring homomorphism

$$T : R \rightarrow \text{End}(M, +), \quad r \mapsto T_r \quad \text{with} \quad T_r : x \mapsto rx,$$

is injective, and $(M, +)$ is called **constant** if T is constant. Moreover, $(M, +)$ is said to be **faithful of smallest cardinality** if $(M, +)$ is faithful and any R -semimodule $(N, +)$ with cardinality $|N| < |M|$ is not faithful.

If $(M, +)$ is a finite faithful R -semimodule of smallest cardinality, then in particular all proper subsemimodules and quotient semimodules of $(M, +)$ are not faithful. When the semiring $(R, +, \cdot)$ is simple, this furthermore implies that all proper subsemimodules and quotient semimodules of $(M, +)$ are constant.

Definition 5.5. Let $(M, +)$ be an R -semimodule. Then $(M, +)$ is called an **R -identity-semimodule** if $rx = x$ holds for all $r \in R$ and $x \in M$. Otherwise, $(M, +)$ is called an **R -nonidentity-semimodule**. For an R -subsemimodule $(N, +)$ of $(M, +)$, we also say **R -identity-subsemimodule** and **R -nonidentity-subsemimodule**.

By this definition, it follows trivially that an R -semimodule $(M, +)$ with $|M| = 1$ is an R -identity-semimodule. R -identity-semimodules are clearly constant.

Definition 5.6. Let $(M, +)$ be an R -nonidentity-semimodule with $|RM| > 1$. We call $(M, +)$ **sub-irreducible** if it has no proper R -nonidentity-subsemimodules, and we call $(M, +)$ **quotient-irreducible** if its only semimodule congruences are id_M and $M \times M$. The semimodule $(M, +)$ is called **irreducible** if it is both sub- and quotient-irreducible.

At this point we want to state a conjecture.

Conjecture 5.7. *Let $(R, +, \cdot)$ be finite, simple, and additively idempotent and let $(M, +)$ be a finite idempotent R -semimodule. Then $(M, +)$ is sub-irreducible iff it is quotient-irreducible.*

Evidence for this conjecture is given by the fact that all semimodules considered in experiments satisfy this equivalence.

Let $(M, +)$ be an R -semimodule and $a, b \in M$. It is easy to see that $Ra = \{b\}$ implies $Rb = \{b\}$. We show that some additional conditions even imply $a = b$.

Lemma 5.8. *Let $(M, +)$ be an idempotent sub-irreducible R -semimodule, and let $a, b \in M$ such that $Ra = \{b\}$. Then $a = b$.*

Proof. Consider the set $N := \{m \in M \mid Rm = \{b\}\}$, which contains the element a . We show that $(N, +)$ is an R -subsemimodule of $(M, +)$. Let $m, n \in N$ and let $s \in R$. For every $r \in R$, we have $r(m + n) = rm + rn = b + b = b$ and $r(sm) = (rs)m = b$. Hence, $m + n \in N$ and $sm \in N$. So the claim follows.

Since $|RM| > 1$, we have $N \neq M$, and by the sub-irreducibility of $(M, +)$, it follows that $(N, +)$ is an R -identity-subsemimodule of $(M, +)$. In particular, for $a \in N$ we have $Ra = \{a\}$, which implies $a = b$. \square

Lemma 5.9. *Let $(M, +)$ be an idempotent sub-irreducible R -semimodule. Then $(M, +)$ is not constant. In particular, if $(R, +, \cdot)$ is simple, then $(M, +)$ is faithful and $(R, +, \cdot)$ is isomorphic to the subsemiring $(T(R), +, \circ)$ of $(\text{End}(M, +), +, \circ)$.*

Proof. Suppose that $(M, +)$ is constant. Then for all $x \in M$, we have $rx = sx$ for all $r, s \in R$, i.e. $|Rx| = 1$. By Lemma 5.8, $Rx = \{x\}$ follows. Hence, M is an R -identity-semimodule, which contradicts a requirement for sub-irreducibility.

If $(R, +, \cdot)$ is simple, then $(R, +, \cdot)$ is clearly isomorphic to $(T(R), +, \circ)$. \square

Whenever $(M, +)$ is an idempotent semimodule, we consider the order \leq on M defined by $x \leq y :\Leftrightarrow x + y = y$ for $x, y \in M$. Then (M, \leq) is a join-semilattice with $\sup\{x, y\} = x + y$ for all $x, y \in M$. If M is moreover finite, then we mean by the **greatest element** of $(M, +)$ the greatest element of (M, \leq) . To avoid confusion with multiplicatively neutral elements, we denote the greatest element of a semilattice $(S, +)$ that is a finite idempotent semimodule or the idempotent additive semigroup of a finite semiring by ∞_S or just by ∞ if the semilattice is clear from the context.

The following two corollaries are consequences of Lemma 5.9.

Corollary 5.10. *Let $(M, +)$ be a finite idempotent sub-irreducible R -semimodule with neutral element 0_M , let $(R, +, \cdot)$ be simple, and let $r \in R$. If $rx = 0_M$ for every $x \in M$, then r is a neutral element in $(R, +)$. If $R\infty_M = \{\infty_M\}$ and $rx = 0_M$ for every $x \in M \setminus \{\infty_M\}$, then r is a neutral element in $(R, +)$.*

Corollary 5.11. *Let $(M, +)$ be an idempotent sub-irreducible R -semimodule, let $(R, +, \cdot)$ be simple, and let $r \in R$. If $(rs)x = rx$ (resp. $(sr)x = rx$) for every $s \in R$ and $x \in M$, then r is left (resp. right) absorbing.*

5.1.1 Existence of idempotent irreducible semimodules

Let $(R, +, \cdot)$ be in this section a finite simple semiring. The main result of this section is Proposition 5.21, which states that $(R, +, \cdot)$ admits a finite idempotent irreducible

5.1. Semimodules

semimodule if $(R, +, \cdot)$ is additively idempotent and fulfils $|R| > 2$. This will be done by showing the existence of an idempotent faithful R -semimodule (and therefore the existence of an idempotent faithful R -semimodule of smallest cardinality) and by showing that faithful R -semimodules of smallest cardinality are irreducible.

The following result is [45, Lemma 6].

Lemma 5.12. *If the multiplication table of $(R, +, \cdot)$ has two identical rows or two identical columns, then $|RR| = 1$ or $|R| = 2$.*

Lemma 5.13. *Let $(M, +)$ be an idempotent sub-irreducible R -semimodule, let $|R| > 2$, and $|RR| > 1$. Then there exists an $a \in M$ with $Ra = M$.*

Proof. Assume that $(Ra, +)$ is for every $a \in M$ an R -identity-semimodule, i.e. for all $r, s \in R$ and every $a \in M$, we have $(rs)a = r(sa) = sa$. By Corollary 5.11, it follows that s is right absorbing for every $s \in R$. Hence, any two rows in the multiplication table are identical and by Lemma 5.12, $|RR| = 1$ or $|R| = 2$ follows. This is a contradiction and it follows that there exists an $a \in M$ such that $(Ra, +)$ is an R -nonidentity-semimodule. By the sub-irreducibility of $(M, +)$, it follows that $Ra = M$. \square

Lemma 5.14. *Let $(M, +)$ be an R -semimodule and $a \in M$ such that $(Ra, +)$ is a constant R -semimodule. Then the relation \sim_a on R , defined by*

$$r \sim_a s \quad :\Leftrightarrow \quad ra = sa$$

for all $r, s \in R$, is a congruence on $(R, +, \cdot)$.

Proof. Let $r, s, t \in R$ with $r \sim_a s$. It holds that $(r+t)a = ra+ta = sa+ta = (s+t)a$, i.e. $r+t \sim_a s+t$. We also find that $(tr)a = t(ra) = t(sa) = (ts)a$, i.e. $tr \sim_a ts$. Since $(Ra, +)$ is constant, it follows that $u(wa) = v(wa)$ for all $u, v, w \in R$. Hence, we have $(rt)a = r(ta) = s(ta) = (st)a$, i.e. $rt \sim_a st$. Thus, \sim_a is a congruence. \square

Lemma 5.15. *Let $|RR| > 1$ and $|R| > 2$. Then $(R, +)$ is a faithful R -semimodule.*

Proof. $(R, +)$ is clearly an R -semimodule. Assume that $(R, +)$ is not faithful. Then $sr = tr$ holds for all $r, s, t \in R$. Thus, any two rows in the multiplication table of $(R, +, \cdot)$ are identical and that is a contradiction to Lemma 5.12. \square

Lemma 5.16. *Let $|RR| > 1$, $|R| > 2$, and let $(M, +)$ be a faithful R -semimodule of smallest cardinality. Then there exists an $a \in M$ with $Ra = M$.*

Proof. Let $a \in M$ with $Ra \subsetneq M$. Then $(Ra, +)$ is not faithful and by simplicity of $(R, +, \cdot)$ it has to be constant. By Lemma 5.14, \sim_a is a congruence on $(R, +, \cdot)$. Consequently, $\sim_a = \text{id}_R$ or $\sim_a = R \times R$. If $\sim_a = \text{id}_R$, then $ra = sa \Leftrightarrow r = s$ for all $r, s \in R$. Hence, $|Ra| = |R|$. But by Lemma 5.15 we have $|Ra| < |M| \leq |R|$, a contradiction. Therefore, $\sim_a = R \times R$, so that $ra = sa$ for all $r, s \in R$, i.e. $|Ra| = 1$.

Now assume that $Ra \subsetneq M$ for every $a \in M$. Hence, for every $a \in M$ we have $|Ra| = 1$, i.e. $Ra = \{b_a\}$ for some $b_a \in M$. It follows that $(rs)a = b_a = sa$ for all $r, s \in R$ and $a \in M$. Since $(M, +)$ is faithful, this implies that s is right absorbing for every $s \in R$. Consequently, any two rows in the multiplication table of $(R, +, \cdot)$ are identical, in contradiction to Lemma 5.12. Thus, there must exist an $a \in M$ with $Ra = M$. \square

Lemma 5.17. *Let $|RR| > 1$, $|R| > 2$, and let $(M, +)$ be a faithful R -semimodule of smallest cardinality. Then $(M, +)$ is quotient-irreducible.*

Proof. Let \sim be a semimodule congruence on $(M, +)$ distinct from id_M and let $N := M/\sim$. Consequently, $(N, +)$ is not faithful and $[rm] = r[m] = s[m] = [sm]$ must hold for all $r, s \in R$ and $m \in M$. By Lemma 5.16, there exists an $a \in M$ with $Ra = M$. Choose $b, c \in M$ arbitrarily. There exist $r_b, r_c \in R$ with $r_b a = b$ and $r_c a = c$. It follows that $[b] = [r_b a] = [r_c a] = [c]$, i.e. $b \sim c$. Hence, $\sim = M \times M$ and the statement follows. \square

Proposition 5.18. *Let $|RR| > 1$, $|R| > 2$, and let $(M, +)$ be a faithful R -semimodule of smallest cardinality. Then $(M, +)$ is irreducible.*

Proof. Since $(M, +)$ is faithful, it must be an R -nonidentity-semimodule and it must fulfil $|RM| > 1$. Let $(N, +)$ be a proper R -subsemimodule of $(M, +)$. $(N, +)$ has to be non-faithful and it follows that $rn = sn$ for all $r, s \in R$ and $n \in N$. Thus, $|Rn| = 1$ for every $n \in N$. Define the equivalence relation \sim on M by

$$m \sim n \quad :\Leftrightarrow \quad \forall r \in R : rm = rn$$

for all $m, n \in M$. Let $a, b, c \in M$ with $a \sim b$ and let $r, s \in R$. We have $r(a + c) = ra + rc = rb + rc = r(b + c)$, i.e. $a + c \sim b + c$. We also find that $r(sa) = (rs)a = (rs)b = r(sb)$, i.e. $sa \sim sb$. Thus, \sim is a semimodule congruence on $(M, +)$. Lemma 5.17 implies that $\sim = M \times M$ or $\sim = \text{id}_M$. Assume $\sim = M \times M$. Then $rm = rn$ holds for all $m, n \in M$ and $r \in R$. So, $Rm = Rn$ for all $m, n \in M$. By Lemma 5.16, there exists an $a \in M$ with $Ra = M$. Then $M = Ra = Rn$ for every $n \in M$, and in particular $|M| = |Rn| = 1$ when choosing $n \in N$; this is a contradiction.

5.1. Semimodules

It must hold that $\sim = \text{id}_M$. For every $n \in N$, there is $f(n) \in N$ such that $Rn = \{f(n)\}$. Hence, if $f(n_1) = f(n_2)$ for some $n_1, n_2 \in N$, then $rn_1 = rn_2$ for all $r \in R$, so that $n_1 \sim n_2$ and thus $n_1 = n_2$. Now for any $n \in N$ and $r, s \in R$ the equality $f(f(n)) = r(f(n)) = r(sn) = (rs)n = f(n)$ holds, so that $f(n) = n$ follows. Thus, for every $n \in N$ we have $Rn = \{n\}$, which means that $(N, +)$ is an R -identity-semimodule. We have proven that $(M, +)$ is sub-irreducible. With Lemma 5.17, it is irreducible. \square

For an ordered set (P, \leq) and an element $x \in P$, we denote $x_\downarrow := \{y \in P \mid y \leq x\}$ and $x^\uparrow := \{y \in P \mid y \geq x\}$.

Lemma 5.19. *Let $(R, +, \cdot)$ be additively idempotent and $|R| > 2$. Then $|RR| > 1$.*

Proof. Let $x \in R \setminus \{\infty\}$ and let \sim be the equivalence relation on R with the equivalence classes x_\downarrow and $R \setminus x_\downarrow$. It is easy to check that \sim is a nontrivial congruence of the semigroup $(R, +)$. If $|RR| = 1$ would hold, then every equivalence relation on R would be a congruence of (R, \cdot) . Consequently, \sim would be a nontrivial congruence of $(R, +, \cdot)$ and that would be a contradiction to $(R, +, \cdot)$ being simple. \square

In the following we will consider semirings that fulfil $|R| > 2$ and $|RR| > 1$. When we consider additively idempotent semirings, then we do not have to mention anymore the condition $|RR| > 1$ because of the last lemma.

Lemma 5.20. *Let $(R, +, \cdot)$ be additively idempotent, $|R| > 2$, and let $(M, +)$ be a faithful R -semimodule of smallest cardinality. Then $(M, +)$ is idempotent.*

Proof. Proposition 5.16 yields the existence of an element $a \in M$ with $Ra = M$. Let $b \in M$. Then there exists an $r \in R$ with $ra = b$ and it follows that $b + b = ra + ra = (r + r)a = ra = b$. Thus, $(M, +)$ is idempotent. \square

Proposition 5.21. *Let $(R, +, \cdot)$ be additively idempotent and let $|R| > 2$. Then there exists a finite idempotent irreducible R -semimodule.*

Proof. By Lemma 5.15, there exists a faithful R -semimodule and therefore also a faithful R -semimodule $(M, +)$ of smallest cardinality, which is by Proposition 5.18 irreducible. By Lemma 5.20, it is idempotent. \square

5.1.2 Properties of idempotent sub-irreducible semimodules

Throughout this section let $(R, +, \cdot)$ be a finite simple additively idempotent semiring with $|R| > 2$ and let $(M, +)$ be a finite idempotent sub-irreducible R -semimodule. We will study the properties of the R -semimodule $(M, +)$, depending on the properties of $(R, +, \cdot)$ (∞_R is absorbing, 0_M exists and is left absorbing etc.). These properties are needed to describe the embedding of $(R, +, \cdot)$ into $(\mathbf{JM}(\mathbf{L}), \vee, \circ)$ for a suitable semilattice \mathbf{L} , what will be done in Section 5.2.

Lemma 5.22. *Let $(N, +)$ be an idempotent R -semimodule. Then for all $x, y \in N$ and $r, s \in R$:*

1. $x \leq y$ implies $rx \leq ry$.

2. $r \leq s$ implies $rx \leq sx$.

Proof. 1. $x \leq y \Leftrightarrow x + y = y \Rightarrow rx + ry = r(x + y) = ry \Leftrightarrow rx \leq ry$.

2. $r \leq s \Leftrightarrow r + s = s \Rightarrow sx = (r + s)x = rx + sx \Leftrightarrow rx \leq sx$. □

The order compatibilities stated in Lemma 5.22 are quite essential for us. In the following we will use them frequently, without referring to this lemma explicitly.

Lemma 5.23. *Let $a, b \in M$ such that $Ra = \{b\}$. Then $a = b$, and a is either an absorbing or a neutral element of $(M, +)$.*

Proof. We have $a = b$ from Lemma 5.8. Consider the sets a_\downarrow and a^\uparrow , which form R -subsemimodules $(a_\downarrow, +)$ and $(a^\uparrow, +)$ of $(M, +)$. We have to show that either $a_\downarrow = M$, in which case a is an absorbing element, or $a^\uparrow = M$, in which case a is a neutral element.

Suppose then that $a_\downarrow \neq M$ and $a^\uparrow \neq M$. Consider $N := a_\downarrow \cup a^\uparrow$, which forms an R -subsemimodule $(N, +)$ of $(M, +)$. Since $(M, +)$ is sub-irreducible we have that $(a_\downarrow, +)$ and $(a^\uparrow, +)$ are R -identity-semimodules, and hence N is also an R -identity-semimodule.

Now we claim that $(M \setminus a_\downarrow, +)$ is an R -subsemimodule of $(M, +)$ as well. Let $x, y \in M$, $x, y \notin a_\downarrow$ and let $r \in R$; then clearly $x + y \notin a_\downarrow$. Suppose that $rx \in a_\downarrow$, i.e. $rx \leq a$. Then $x + a = r(x + a) = rx + ra = rx + a = a$, so that $x \leq a$, contradicting $x \notin a_\downarrow$. Hence, $(M \setminus a_\downarrow, +)$ is an R -subsemimodule of $(M, +)$, which is proper, and thus an R -identity-subsemimodule. From this and because of $M = a_\downarrow \cup (M \setminus a_\downarrow)$ it follows that $(M, +)$ is an R -identity-semimodule, which contradicts a requirement for sub-irreducibility. □

5.1. Semimodules

Corollary 5.24. *Let $(N, +)$ be an R -identity-subsemimodule of $(M, +)$. If $(M, +)$ has no neutral element, then $N = \{\infty\}$. If $(M, +)$ has a neutral element 0 , then $N \subseteq \{0, \infty\}$.*

Proposition 5.25. *If $(M, +)$ has no neutral element, then $Ra = M$ for every $a \in M \setminus \{\infty\}$. If $(M, +)$ has a neutral element 0 , then $Ra = M$ for every $a \in M \setminus \{0, \infty\}$.*

Proof. First consider the case that $(M, +)$ has no neutral element and let $a \in M \setminus \{\infty\}$. Assume that $(Ra, +)$ is an R -identity-semimodule. By Corollary 5.24, $Ra = \{\infty\}$ holds, and by Lemma 5.23, we have $a = \infty$, what is a contradiction. Hence, $(Ra, +)$ is an R -nonidentity-semimodule, and by the sub-irreducibility of $(M, +)$, it follows that $Ra = M$.

Now let $(M, +)$ have a neutral element 0 and let $a \in M \setminus \{0, \infty\}$. Assume that the R -semimodule $(Ra, +)$ is an R -identity-semimodule. It cannot hold that $|Ra| = 1$, otherwise we would have $a = 0$ or $a = \infty$ by Lemma 5.23. By Corollary 5.24, $Ra = \{0, \infty\}$ follows. Thus, the congruence \sim_a on $(R, +, \cdot)$ (see Lemma 5.14) has two nonempty equivalence classes and is therefore a nontrivial congruence on $(R, +, \cdot)$. But that is a contradiction to $(R, +, \cdot)$ being simple. Consequently, $(Ra, +)$ is not an R -identity-semimodule and by the sub-irreducibility of $(M, +)$ it follows that $Ra = M$. \square

Proposition 5.26. *The following statements hold:*

1. *If $(M, +)$ has no neutral element, then $\infty_R x = \infty_M$ for every $x \in M$.*
2. *If $(M, +)$ has a neutral element 0_M , then $\infty_R x = \infty_M$ for every $x \in M \setminus \{0_M\}$.*
3. *If ∞_R is not left absorbing, then $(M, +)$ has a neutral element 0_M and it satisfies $R0_M = \{0_M\}$.*
4. *If ∞_R is right absorbing, then $R\infty_M = \{\infty_M\}$.*

Proof. 1.: By Proposition 5.25, there exists for every $x \in M \setminus \{\infty_M\}$ an $r_x \in R$ with $r_x x = \infty_M$. By $r_x x \leq \infty_R x \leq \infty_R \infty_M$, the statement follows.

2.: If $|M| = 2$, i.e. $M = \{0_M, \infty_M\}$, then there exists an $a \in M$ and an $r \in R$ with $ra = \infty_M$ by Lemma 5.13. It follows that $ra \leq \infty_R a \leq \infty_R \infty_M$, i.e. $\infty_R \infty_M = \infty_M$. If $|M| > 2$, then the statement follows analogously as in 1.

3.: Assume that $(M, +)$ has no neutral element. By 1. we get $(\infty_R r)x = \infty_R(rx) = \infty_M = \infty_R x$ for every $r \in R$ and $x \in M$, i.e. ∞_R is left absorbing

by Corollary 5.11, which contradicts the precondition. Hence, $(M, +)$ has a neutral element 0_M . Now assume that $\infty_M \in R0_M$ holds. Then there exists an $r_0 \in R$ with $r_0 0_M = \infty_M$. With $r_0 0_M \leq \infty_{R0_M} \leq \infty_{Rx}$ we find $\infty_{Rx} = \infty_M$ for every $x \in M$. Analogously, the same contradiction as in the previous assumption follows. Thus, $\infty_M \notin R0_M$ and the proper R -subsemimodule $(R0_M, +)$ of $(M, +)$ must fulfil $R0_M = \{0_M\}$ by Corollary 5.24.

4.: By Lemma 5.13, there exists an $x \in M$ and an $r \in R$ with $rx = \infty_M$ and it follows that $\infty_{R\infty_M} = \infty_M$ by $rx \leq r\infty_M \leq \infty_{R\infty_M}$. If ∞_R is right absorbing, then $r\infty_M = r(\infty_{R\infty_M}) = (r\infty_R)\infty_M = \infty_{R\infty_M} = \infty_M$ for every $r \in R$. \square

Proposition 5.27. *Let $(R, +)$ have a neutral element 0_R . Then $(M, +)$ has a neutral element.*

Proof. By Lemma 5.13, there exists an $x \in M$ with $Rx = M$. Thus, for every $y \in M$ there exists an $r_y \in R$ with $r_y x = y$. It follows that $0_{Rx} \leq r_y x = y$ for every $y \in M$. Hence, 0_{Rx} is a least element in (M, \leq) and therefore a neutral element in $(M, +)$. \square

In the following we denote by 0_M the neutral element of $(M, +)$.

Lemma 5.28. *Let $(R, +)$ have a neutral element 0_R . Then:*

1. $0_{Rx} = 0_M$ for every $x \in M \setminus \{\infty_M\}$.
2. If 0_R is left absorbing, then $0_{R\infty_M} = 0_M$.
3. If 0_R is not left absorbing, then $R\infty_M = \{\infty_M\}$ (in particular $0_{R\infty_M} = \infty_M$).
4. If 0_R is not right absorbing, then $R0_M = M$.

Proof. 1.: If $|M| = 2$, i.e. $M \setminus \{\infty_M\} = \{0_M\}$, then there exists an $r \in R$ and an $x \in M$ with $rx = 0_M$ by Lemma 5.13. It follows that $0_{R0_M} \leq 0_{Rx} \leq rx = 0_M$. If $|M| > 2$, then there exists for every $x \in M \setminus \{0_M, \infty_M\}$ an $r \in R$ with $rx = 0_M$ by Proposition 5.25. It follows that $0_{R0_M} \leq 0_{Rx} \leq rx = 0_M$, i.e. $0_{Rx} = 0_M$ for every $x \in M \setminus \{\infty_M\}$.

2.: By Lemma 5.13, there exists an $a \in M$ with $Ra = M$. If $a = \infty_M$, then there exists an $r \in R$ with $r\infty_M = 0_M$ and it follows that $0_{R\infty_M} \leq r\infty_M = 0_M$. If $a \neq \infty_M$, then there exists an $s \in R$ with $sa = \infty_M$. By 1. it follows that $0_{R\infty_M} = 0_R(sa) = (0_{Rs})a = 0_{Ra} = 0_M$.

3.: Now let 0_R be not left absorbing and assume that $0_{R\infty_M} = 0_M$ holds. For every $r \in R$ and every $y \in M$ we find $(0_{Rr})y = 0_R(ry) = 0_M = 0_{Ry}$. This means

5.1. Semimodules

0_R is left absorbing by Corollary 5.11, which is a contradiction. Now assume that $0_R \infty_M \neq \infty_M$ holds. By 1. we have $0_M = 0_R(0_R \infty_M) = (0_R 0_R) \infty_M \geq 0_R \infty_M$. This means $0_R \infty_M = 0_M$, which is again a contradiction. We conclude that $0_R \infty_M = \infty_M$ must hold. With $0_R \infty_M \leq r \infty_M$ we find that $r \infty_M = \infty_M$ for every $r \in R$.

4.: Now let 0_R be not right absorbing and assume that $(R0_M, +)$ is an R -identity-semimodule. By $0_R 0_M = 0_M$ and Corollary 5.24, we know that $0_M \in R0_M \subseteq \{0_M, \infty_M\}$ holds. If $R0_M = \{0_M, \infty_M\}$ would hold, then \sim_{0_M} (see Lemma 5.14) would be a nontrivial congruence on $(R, +, \cdot)$. Hence, $R0_M = \{0_M\}$. If 0_R is left absorbing, then $(r0_R)x = r(0_Rx) = r0_M = 0_M = 0_Rx$ follows for every $r \in R$ and $x \in M$ because of $0_Rx = 0_M$ for every $x \in M$. If 0_R is not left absorbing, then we also have

$$(r0_R)x = r(0_Rx) = \begin{cases} r0_M = 0_M = 0_Rx & \text{if } x \neq \infty_M, \\ r \infty_M = \infty_M = 0_Rx & \text{else} \end{cases}$$

for every $r \in R$ and $x \in M$. By Corollary 5.11, 0_R is right absorbing and that is a contradiction. Consequently, $(R0_M, +)$ cannot be an R -identity-semimodule. By the sub-irreducibility of $(M, +)$, we find $R0_M = M$. \square

Lemma 5.29. *Let $(R, +)$ have no neutral element. Then:*

1. *If $(M, +)$ has a neutral element 0_M , then $R \infty_M = \{\infty_M\}$.*
2. *If ∞_R is not right absorbing, then $(M, +)$ has no neutral element.*

Proof. 1.: Assume there exists an $r \in R$ with $r \infty_M = 0_M$. Because of $rx \leq r \infty_M$, we have $rx = 0_M$ for every $x \in M$. By Corollary 5.10, r is a neutral element in $(R, +)$ and that contradicts the precondition. Hence, $0_M \notin R \infty_M$. By the sub-irreducibility of $(M, +)$ and Corollary 5.24, it follows that $R \infty_M = \{\infty_M\}$.

2.: Assume that $(M, +)$ has a neutral element 0_M . By Proposition 5.26 and 1. the equality $(r \infty_R)x = r(\infty_Rx) = r \infty_M = \infty_M = \infty_Rx$ holds for every $r \in R$ and $x \in M \setminus \{0_M\}$. Since ∞_R is not right absorbing, there must exist an $r_0 \in R$ with $(r_0 \infty_R)0_M \neq \infty_R 0_M$ by Corollary 5.11. Hence, it clearly must hold that $\infty_R 0_M \neq \infty_M$ and it follows that $r0_M \leq \infty_R 0_M < \infty_M$ for every $r \in R$, i.e. $\infty_M \notin R0_M$. By the sub-irreducibility of $(M, +)$ and Corollary 5.24, it follows that $R0_M = \{0_M\}$. This yields a contradiction by $(r_0 \infty_R)0_M = r_0(\infty_R 0_M) = r_0 0_M = 0_M = \infty_R 0_M$. Thus, $(M, +)$ has no neutral element. \square

Proposition 5.30. *Let ∞_R be neither left nor right absorbing. Then $(R, +, \cdot)$ has a zero.*

Proof. Since ∞_R is not left absorbing, $(M, +)$ has a neutral element 0_M and $R0_M = \{0_M\}$ holds by Proposition 5.26. It also follows by Proposition 5.26 that $\infty_R x = \infty_M$ for every $x \in M \setminus \{0_M\}$. If $(R, +)$ would have no neutral element, then Lemma 5.29 would imply that $(M, +)$ has no neutral element, which would be a contradiction. Hence, $(R, +)$ has a neutral element 0_R . This neutral element has to be right absorbing, otherwise Lemma 5.28 implies that $R0_M = M$, which would be a contradiction. Assume that 0_R is not left absorbing. Then $R\infty_M = \{\infty_M\}$ by Lemma 5.28. Let $r \in R$ and $x \in M$. It follows that

$$(r\infty_R)x = r(\infty_R x) = \begin{cases} r0_M = 0_M = \infty_R x & \text{if } x = 0_M, \\ r\infty_M = \infty_M = \infty_R x & \text{if } x \neq 0_M. \end{cases}$$

By Corollary 5.11, ∞_R is right absorbing and that is a contradiction. Hence, 0_R is left and right absorbing and therefore a zero. \square

5.1.3 Density results for idempotent irreducible semimodules

Let again $(R, +, \cdot)$ be a finite simple additively idempotent semiring with $|R| > 2$, and let now $(M, +)$ be a finite idempotent irreducible R -semimodule. The following two propositions are density results akin to [61, Proposition 3.13].

Let $a, b \in M$. If there exists an element $r \in R$, with

$$rx = \begin{cases} b & \text{if } x \leq a, \\ \infty_M & \text{else,} \end{cases}$$

then it is unique since $(M, +)$ is faithful, and we denote it by $r_{a,b}$.

Proposition 5.31. *Let ∞_R be not left absorbing. Then $r_{a,0_M} \in R$ for every $a \in M \setminus \{\infty_M\}$.*

Proof. By Proposition 5.26, $(M, +)$ has a neutral element 0_M , which satisfies $R0_M = \{0_M\}$. Define $I_x := \{r \in R \mid rx = 0_M\}$ for every $x \in M$ and the equivalence relation \sim on M by $x \sim y \Leftrightarrow I_x = I_y$ for $x, y \in M$. For every $r \in R$ and $x, y \in M$, the equivalence

$$r \in I_{x+y} \Leftrightarrow 0_M = r(x+y) = rx + ry \Leftrightarrow 0_M = rx = ry \Leftrightarrow r \in I_x \cap I_y$$

5.1. Semimodules

holds, i.e. $I_{x+y} = I_x \cap I_y$. Now let $x, y, z \in M$ with $x \sim y$ and $r, s \in R$. We find that $I_{x+z} = I_x \cap I_z = I_y \cap I_z = I_{y+z}$, i.e. $x + z \sim y + z$. Furthermore, the equivalence

$$s \in I_{rx} \Leftrightarrow 0_M = s(rx) = (sr)x \Leftrightarrow sr \in I_x = I_y \Leftrightarrow 0_M = (sr)y = s(ry) \Leftrightarrow s \in I_{ry}$$

holds, i.e. $I_{rx} = I_{ry}$. Hence, $rx \sim ry$. Consequently, \sim is a semimodule congruence on $(M, +)$. If $\sim = M \times M$, then $I_x = I_{0_M} = R$ would hold for every $x \in M$, i.e. $RM = \{0_M\}$. But this is a contradiction to the irreducibility of $(M, +)$. Thus, $\sim = \text{id}_M$ follows by quotient-irreducibility and we get the equivalence $x \leq y \Leftrightarrow I_y \subseteq I_x$ for all $x, y \in M$. One can easily show that $(I_x, +)$ is an R -semimodule for every $x \in M$. It follows that $(I_x y, +)$ is an R -subsemimodule of $(M, +)$ for all $x, y \in M$. Fix an $a \in M \setminus \{\infty_M\}$ and let $b \in M$ with $b \not\leq a$. Hence, $I_a \not\subseteq I_b$ and therefore $I_a \setminus I_b \neq \emptyset$. If $(I_a b, +)$ is an R -identity-semimodule, then $I_a b \subseteq \{0_M, \infty_M\}$ by Corollary 5.24. Hence, $rb = \infty_M$ for every $r \in I_a \setminus I_b$. This means there exists an $r_b \in I_a$ with $r_b b = \infty_M$. If $(I_a b, +)$ is an R -nonidentity-semimodule, i.e. $I_a b = M$, then there also exists an $r_b \in I_a$ with $r_b b = \infty_M$. Now define $s := \sum_{b \in M, b \not\leq a} r_b \in R$ and let $x \in M$. If $x \leq a$, then $r_b x \leq r_b a = 0_M$ for every b with $b \not\leq a$, i.e. $sx = 0_M$. If $x \not\leq a$, then $sx = \sum_{b \in M, b \not\leq a} r_b x \geq r_x x = \infty_M$, i.e. $sx = \infty_M$. Thus, $s = r_{a, 0_M}$. \square

For the proof of the following proposition we need the notion of *minimal* elements in ordered sets: An element m in an ordered set (P, \leq) is called **minimal** if there exists no element $n \in P$ with $n < m$. By $\text{Min}(P, \leq)$ we denote the set of minimal elements in (P, \leq) .

Proposition 5.32. *Let ∞_M be join-irreducible and $R\infty_M = \{\infty_M\}$. If $(M, +)$ has a neutral element 0_M , then $r_{a, 0_M} \in R$ for every $a \in M \setminus \{\infty_M\}$. If $(M, +)$ has no neutral element, then $r_{a, b} \in R$ for every $a \in M \setminus \{\infty_M\}$ and every $b \in M$.*

Proof. Define $K_x := \{r \in R \mid rx = \infty_M\}$ for every $x \in M$. It is easy to verify that K_x is for every $x \in M \setminus \{0_M\}$ an R -semimodule. By the join-irreducibility of ∞_M , we have

$$s \in K_{x+y} \Leftrightarrow \infty_M = s(x+y) = sx + sy \Leftrightarrow sx = \infty_M \text{ or } sy = \infty_M \Leftrightarrow s \in K_x \cup K_y$$

for $x, y \in M$ and $s \in R$. Hence, $K_{x+y} = K_x \cup K_y$. Define the equivalence relation \sim on M by $x \sim y \iff K_x = K_y$ for all $x, y \in M$. We will show that \sim is a semimodule congruence on $(M, +)$. Let $x, y, z \in M$ with $x \sim y$ and $r, s \in R$. We find $K_{x+z} = K_x \cup K_z = K_y \cup K_z = K_{y+z}$, i.e. $x + z \sim y + z$. Furthermore, we have

the equivalence

$$\begin{aligned} s \in K_{rx} &\Leftrightarrow \infty_M = s(rx) = (sr)x \Leftrightarrow sr \in K_x = K_y \\ &\Leftrightarrow \infty_M = (sr)y = s(ry) \Leftrightarrow s \in K_{ry}, \end{aligned}$$

i.e. $rx \sim ry$. Hence, \sim is a semimodule congruence on $(M, +)$. Assume $\sim = M \times M$. Then $K_x = K_{\infty_M} = R$ for every $x \in M$ and it follows that $RM = \{\infty_M\}$. But this is a contradiction to the irreducibility of $(M, +)$. By the quotient-irreducibility of $(M, +)$, we get $\sim = \text{id}_M$. Because of $K_{x+y} = K_x \cup K_y$, the equivalence $x \leq y \Leftrightarrow K_x \subseteq K_y$ follows for all $x, y \in M$. Let 0_M be the possibly existing neutral element of $(M, +)$. It is easy to verify that $(K_{xy}, +)$ is an R -subsemimodule of $(M, +)$ for all $x, y \in M$ with $x \neq 0_M$. Now fix an element $a \in M \setminus \{\infty_M\}$ and let $x \in M$ with $x \not\leq a$. It follows that $K_x \not\subseteq K_a$ and therefore $K_x \setminus K_a \neq \emptyset$. If $(K_x a, +)$ is an R -nonidentity-semimodule, then $K_x a = M$ and it follows that there exists an $s_{x,b} \in K_x$ with $s_{x,b} a = b$ for every $b \in M$.

Consider the case that 0_M exists, i.e. $\text{Min}(M, \leq) = \{0_M\}$. If $(K_x a, +)$ is an R -identity-semimodule, then $K_x a \subseteq \{0_M, \infty_M\}$ by Corollary 5.24. Then clearly $ra = 0_M$ for every $r \in K_x \setminus K_a$, i.e. there exists an $s_{x,0_M} \in K_x$ with $s_{x,0_M} a = 0_M$. This means for every $b \in \text{Min}(M, \leq) = \{0_M\}$ and every $x \in M$ with $x \not\leq a$ there exists an $s_{x,b} \in K_x$ with $s_{x,b} a = b$.

Now consider the case that $(M, +)$ has no neutral element. If $(K_x a, +)$ is an R -identity-semimodule, then $K_x a = \{\infty_M\}$ by Corollary 5.24, what yields the contradiction $K_x \subseteq K_a$. Hence, $(K_x a, +)$ cannot be an R -identity-semimodule. Again we conclude that there exists an $s_{x,b} \in K_x$ with $s_{x,b} a = b$ for every $b \in \text{Min}(M, \leq)$ and every $x \in M$ with $x \not\leq a$.

Now fix an element $b \in \text{Min}(M, \leq)$, define $s := \sum_{x \in M, x \not\leq a} s_{x,b}$ and let $z \in M$. If $z \leq a$, then $s_{x,b} z \leq s_{x,b} a = b$ for every $x \in M$ with $x \not\leq a$, i.e. $sz = b$. If $z \not\leq a$, then $s_{z,b} z = \infty$ because of $s_{z,b} \in K_z$. It follows that $sz = \sum_{x \in M, x \not\leq a} s_{x,b} z \geq s_{z,b} z = \infty$, i.e. $sz = \infty$. Thus, $r_{a,b} = s \in R$. In particular, if $(M, +)$ has a neutral element 0_M , then $b = 0_M$ and therefore $r_{a,0_M} \in R$. Now consider again the case that $(M, +)$ has no neutral element and choose $c \in M$ arbitrarily. Then by Proposition 5.25 there exists a $t \in R$ with $tb = c$ and it follows that $r_{a,c} = ts \in R$. \square

5.2. Embedding of $(R, +, \cdot)$ into $(\text{JM}(\mathbf{L}), \vee, \circ)$

5.2 Embedding of $(R, +, \cdot)$ into $(\text{JM}(\mathbf{L}), \vee, \circ)$

In this section let $(R, +, \cdot)$ be again a finite simple additively idempotent semiring with $|R| > 2$. From now on, by a semilattice we will always mean a join-semilattice. If \mathbf{L} is a semilattice, then the algebra $(\text{JM}(\mathbf{L}), \vee, \circ)$ is a semiring, where the addition \vee is the pointwise supremum and the multiplication \circ the composition of two mappings. We are going to embed $(R, +, \cdot)$ into the semiring $(\text{JM}(\mathbf{L}), \vee, \circ)$ for a suitable finite semilattice \mathbf{L} . The subsemiring (S, \vee, \circ) of $(\text{JM}(\mathbf{L}), \vee, \circ)$ corresponding to $(R, +, \cdot)$ fulfils then certain conditions, depending on the properties of $(R, +, \cdot)$. In the beginning of this section we list all conditions that may arise for (S, \vee, \circ) and that may be necessary for the characterisation of $(R, +, \cdot)$. First, we need two notations. For $a, b \in L$, let k_a be the mapping from L to L that maps constantly to a , and let $f_{a,b}$ be the mapping defined by

$$f_{a,b} : L \rightarrow L, \quad x \mapsto \begin{cases} b & \text{if } x \leq a, \\ 1_{\mathbf{L}} & \text{else.} \end{cases}$$

The semiring (S, \vee, \circ) may fulfil some of the following conditions:

$$\forall a \in L \setminus \{1\} \forall b \in L : f_{a,b} \in S, \quad (5.1)$$

$$\forall f \in S \exists a \in L \setminus \{1\} \exists b \in L : f_{a,b} \leq f, \quad (5.2)$$

$$\forall a \in L : k_a \in S, \quad (5.3)$$

$$\forall f \in S \exists a \in L : k_a \leq f, \quad (5.4)$$

$$\forall a \in L \forall b \in L \setminus \{1\} \exists f \in S : f(x) = b \text{ if } x \leq a, \text{ and } f(x) > b \text{ else.} \quad (5.5)$$

If \mathbf{L} is a lattice, then (S, \vee, \circ) may also fulfil:

$$\forall a \in L \setminus \{1\} : f_{a,0} \in S, \quad (5.6)$$

$$\forall f \in S \exists a \in L \setminus \{1\} : f_{a,0} \leq f, \quad (5.7)$$

$$\forall a \in L \setminus \{0, 1\} \forall b \in L \exists f \in S : f(a) = b. \quad (5.8)$$

We also need the following notations. Let \mathbf{L} be a finite semilattice and \mathbf{K} a finite

lattice. Then we denote:

$$\begin{aligned} \text{JM}_1(\mathbf{L}) &:= \{f \in \text{JM}(\mathbf{L}) \mid f(1) = 1\}, \\ \text{Res}_1(\mathbf{K}) &:= \{f \in \text{Res}(\mathbf{K}) \mid f(1) = 1\}, \\ \text{Res}_0(\mathbf{K}) &:= \{f \in \text{Res}(\mathbf{K}) \mid \forall x \in K : f(x) = 0 \Rightarrow x = 0\}, \\ \text{Res}_{0,1}(\mathbf{K}) &:= \text{Res}_0(\mathbf{K}) \cap \text{Res}_1(\mathbf{K}). \end{aligned}$$

As explained in the introduction to this chapter, we distinguish between the properties of ∞_R when describing the embedding. More precisely, we consider the cases that ∞_R is right but not left absorbing, ∞_R is left but not right absorbing, and ∞_R is absorbing.

∞_R is right but not left absorbing

Lemma 5.33. *Let $\mathbf{L} = (L, \leq)$ be a finite lattice, $a \in L \setminus \{1\}$, and $f \in \text{Res}_1(\mathbf{L})$. Then there exists an element $b \in L \setminus \{1\}$ such that $f_{b,0} = f_{a,0} \circ f$.*

Proof. Define $b := \bigvee \{x \in L \mid f(x) \leq a\}$. Then $f(x) \leq a \Leftrightarrow x \leq b$ holds for every $x \in L$ and it follows that $f_{b,0} = f_{a,0} \circ f$. Because of $f(1) = 1$ and $a < 1$, it cannot hold that $b = 1$. \square

Lemma 5.34. *Let $\mathbf{L} = (L, \leq)$ be a finite lattice and (S, \vee, \circ) a simple subsemiring of $(\text{Res}_1(\mathbf{L}), \vee, \circ)$ that fulfils (5.6). Then it also fulfils (5.7).*

Proof. Define the set $Z := \{f \in S \mid \forall a \in L \setminus \{1\} : f_{a,0} \not\leq f\}$ and the equivalence relation \sim on S with the equivalence classes $S \setminus Z$ and $\{z\}$ for every $z \in Z$. Let $f, g, h \in S$ with $f \sim g$ and $f \neq g$. Consequently, f and g must be contained in $S \setminus Z$ and hence there exist $a, b \in L \setminus \{1\}$ with $f_{a,0} \leq f$ and $f_{b,0} \leq g$. One can easily show that $f_{a,0} \leq f \vee h$, $f_{a,0} \leq h \circ f$, and $f_{c,0} \leq f \circ h$ for some $c \in L \setminus \{1\}$ holds for every $h \in S$, what yields $f \vee h, f \circ h, h \circ f \in S \setminus Z$. Analogously, one can show $g \vee h, g \circ h, h \circ g \in S \setminus Z$ and it follows that $f \vee h \sim g \vee h, f \circ h \sim g \circ h$, and $h \circ f \sim h \circ g$. Thus, \sim is a congruence. Since \sim must be trivial and $S \setminus Z$ is a class with more than one element, $\sim = S \times S$ follows. Hence, $Z = \emptyset$. \square

Note in the following that $\text{End}(M, +) = \text{JM}(M, \leq)$ holds for a finite idempotent semimodule $(M, +)$.

Proposition 5.35. *Let ∞_R be right but not left absorbing. Then there exists a finite lattice \mathbf{L} with more than two elements such that $(R, +, \cdot)$ is isomorphic to a subsemiring of $(\text{Res}_1(\mathbf{L}), \vee, \circ)$ that fulfils (5.6), (5.7), and (5.8).*

5.2. Embedding of $(R, +, \cdot)$ into $(\text{JM}(\mathbf{L}), \vee, \circ)$

Proof. By Proposition 5.21, there exists a finite idempotent irreducible R -semi-module $(M, +)$. By Lemma 5.9, $(R, +, \cdot)$ is isomorphic to the subsemiring $(T(R), +, \circ)$ of $(\text{JM}(M, \leq), +, \circ)$. By Proposition 5.26, $(M, +)$ has a neutral element 0_M , i.e. (M, \leq) is a lattice, and $R0_M = \{0_M\}$ holds. Proposition 5.26 furthermore yields $R\infty_M = \{\infty_M\}$. Thus, $(T(R), +, \circ)$ is even a subsemiring of $(\text{Res}_1(M, \leq), +, \circ)$. The lattice (M, \leq) must have more than two elements because of $|R| > 2$. Now, (5.6) follows by Proposition 5.31, (5.7) by Lemma 5.34, and (5.8) by Proposition 5.25. \square

Example 5.36. Consider the finite simple additively idempotent semiring $(R, +, \cdot)$ with the following operation tables:

| | | | | | | | |
|-----|-----|-----|-----|---------|-----|-----|-----|
| $+$ | a | b | c | \cdot | a | b | c |
| a | a | b | c | a | a | a | c |
| b | b | b | c | b | a | b | c |
| c | c | c | c | c | a | c | c |

The greatest element c of this semiring is right but not left absorbing. Let $\mathbf{L} = (\{0, 1, 2\}, \leq)$ be the total order of three elements and consider the semiring $(\text{Res}_1(\mathbf{L}), \vee, \circ)$. This semiring consists of the mappings α, β , and γ , which are of the following form and fulfil the following operation tables:

| | | | | | | | | | | | |
|-------------|-----|-----|-----|----------|----------|----------|----------|----------|----------|----------|----------|
| x | 0 | 1 | 2 | \vee | α | β | γ | \circ | α | β | γ |
| $\alpha(x)$ | 0 | 0 | 2 | α | α | β | γ | α | α | α | γ |
| $\beta(x)$ | 0 | 1 | 2 | β | β | β | γ | β | α | β | γ |
| $\gamma(x)$ | 0 | 2 | 2 | γ | γ | γ | γ | γ | α | γ | γ |

Clearly, $(\text{Res}_1(\mathbf{L}), \vee, \circ)$ fulfils (5.6), (5.7), and (5.8) and the semiring $(R, +, \cdot)$ is isomorphic to $(\text{Res}_1(\mathbf{L}), \vee, \circ)$.

∞_R is left but not right absorbing

To achieve a similar result for the case that ∞_R is left but not right absorbing, we need some preparation.

Let $\mathbf{L} = (L, \leq)$ be a finite lattice with supremum \vee and infimum \wedge . Then the dual lattice $\mathbf{L}^d = (L, \geq)$ of \mathbf{L} has the supremum $\vee^d := \wedge$, the infimum $\wedge^d := \vee$, the least element $0_{\mathbf{L}^d} = 1_{\mathbf{L}}$, and the greatest element $1_{\mathbf{L}^d} = 0_{\mathbf{L}}$.

For two mappings $f, g : S \rightarrow S$ on a set S , we define $f \circ^d g := g \circ f$.

For a lattice \mathbf{L} , we define $\text{Rd}(\mathbf{L}) := \{f^+ \mid f \in \text{Res}(\mathbf{L})\}$, i.e. $\text{Rd}(\mathbf{L})$ is the set of residuals. For a subset S of $\text{Res}(\mathbf{L})$ we define $S^+ := \{f^+ \mid f \in S\}$. It holds that $\text{Rd}(\mathbf{L}) = \text{Res}(\mathbf{L}^d)$ and in particular

$$(\text{Res}(\mathbf{L}), \vee, \circ) \cong (\text{Rd}(\mathbf{L}), \wedge, \circ^d) = (\text{Res}(\mathbf{L}^d), \vee^d, \circ^d),$$

where $\Omega : f \mapsto f^+$ is an isomorphism between $(\text{Res}(\mathbf{L}), \vee, \circ)$ and $(\text{Rd}(\mathbf{L}), \wedge, \circ^d)$ (see [7]).

Lemma 5.37. *Let $\mathbf{L} = (L, \leq)$ be a lattice. Then*

$$(\text{Res}_1(\mathbf{L}), \vee, \circ) \cong (\text{Res}_0(\mathbf{L}^d), \vee^d, \circ^d).$$

Moreover, if (S, \vee, \circ) is a subsemiring of $(\text{Res}_1(\mathbf{L}), \vee, \circ)$, then (S^+, \vee^d, \circ^d) is a subsemiring of $(\text{Res}_0(\mathbf{L}^d), \vee^d, \circ^d)$ and $(S, \vee, \circ) \cong (S^+, \vee^d, \circ^d)$ holds.

Proof. Let $f \in \text{Res}_1(\mathbf{L})$ and $y \in L$. Since the set $\{x \in L \mid f(x) \leq y\}$ is closed under \vee , we have that $f^+(y) = \vee\{x \in L \mid f(x) \leq y\} = \mathbf{1}_{\mathbf{L}}$ implies $\mathbf{1}_{\mathbf{L}} = f(\mathbf{1}_{\mathbf{L}}) \leq y$, i.e. $y = \mathbf{1}_{\mathbf{L}}$. Because of $\mathbf{1}_{\mathbf{L}} = \mathbf{0}_{\mathbf{L}^d}$, we have $f^+ \in \text{Res}_0(\mathbf{L}^d)$. Now let $g \in \text{Res}(\mathbf{L})$ such that $g^+ \in \text{Res}_0(\mathbf{L}^d)$, i.e. $g^+(y) = \mathbf{0}_{\mathbf{L}^d} = \mathbf{1}_{\mathbf{L}}$ implies $y = \mathbf{0}_{\mathbf{L}^d} = \mathbf{1}_{\mathbf{L}}$. It follows that $g(\mathbf{1}_{\mathbf{L}}) = g^{++}(\mathbf{1}_{\mathbf{L}}) = \wedge\{y \in L \mid g^+(y) \geq \mathbf{1}_{\mathbf{L}}\} = \wedge\{\mathbf{1}_{\mathbf{L}}\} = \mathbf{1}_{\mathbf{L}}$. Thus, $g \in \text{Res}_1(\mathbf{L})$. Hence, $\Omega|_{\text{Res}_1(\mathbf{L})}$ is an isomorphism between $(\text{Res}_1(\mathbf{L}), \vee, \circ)$ and $(\text{Res}_0(\mathbf{L}^d), \vee^d, \circ^d)$, and for every subsemiring (S, \vee, \circ) of $(\text{Res}_1(\mathbf{L}), \vee, \circ)$, we have $(S, \vee, \circ) \cong (\Omega(S), \vee^d, \circ^d)$ and $S^+ = \Omega(S) \subseteq \text{Res}_0(\mathbf{L}^d)$. \square

Let $\mathbf{L} = (L, \leq)$ be a finite nontrivial lattice and define $L_- := L \setminus \{0_{\mathbf{L}}\}$ and $\mathbf{L}_- := (L_-, \leq \cap (L_- \times L_-))$. Then let $\Psi_{\mathbf{L}}$ be the mapping defined by

$$\Psi_{\mathbf{L}} : \text{Res}_0(\mathbf{L}) \rightarrow \text{JM}(\mathbf{L}_-), \quad f \mapsto f|_{L_-}.$$

The following lemma is easy to prove.

Lemma 5.38. *Let $\mathbf{L} = (L, \leq)$ be a finite nontrivial lattice. Then $\Psi_{\mathbf{L}}$ is an isomorphism between $(\text{Res}_0(\mathbf{L}), \vee, \circ)$ and $(\text{JM}(\mathbf{L}_-), \vee, \circ)$. In particular, $(\Psi_{\mathbf{L}}(S), \vee, \circ)$ is a subsemiring of $(\text{JM}(\mathbf{L}_-), \vee, \circ)$ and $(S, \vee, \circ) \cong (\Psi_{\mathbf{L}}(S), \vee, \circ)$ holds for every subsemiring (S, \vee, \circ) of $(\text{Res}_0(\mathbf{L}), \vee, \circ)$.*

5.2. Embedding of $(R, +, \cdot)$ into $(\text{JM}(\mathbf{L}), \vee, \circ)$

Lemma 5.39. *Let $\mathbf{K} = (K, \leq)$ be a finite lattice and $\mathbf{L} := \mathbf{K}^d$. Moreover, let (S, \vee, \circ) be a subsemiring of $(\text{Res}_1(\mathbf{K}), \vee, \circ)$ that fulfils (5.6), (5.7), and (5.8). Then $(\Psi_{\mathbf{L}}(S^+), \vee^d, \circ)$ is a subsemiring of $(\text{JM}(\mathbf{L}_-), \vee^d, \circ)$ (where \vee^d refers to the supremum in $\mathbf{L} = \mathbf{K}^d$), which fulfils (5.3), (5.4), and (5.5).*

Proof. (S^+, \vee^d, \circ^d) is by Lemma 5.37 a subsemiring of $(\text{Res}_0(\mathbf{L}), \vee^d, \circ^d)$ and therefore (S^+, \vee^d, \circ) is a subsemiring of $(\text{Res}_0(\mathbf{L}), \vee^d, \circ)$. By Lemma 5.38, $(\Psi_{\mathbf{L}}(S^+), \vee^d, \circ)$ is a subsemiring of $(\text{JM}(\mathbf{L}_-), \vee^d, \circ)$. By (5.6), we have $f_{a,0_{\mathbf{K}}} \in S$ for every $a \in K \setminus \{1_{\mathbf{K}}\}$ and therefore $f_{a,0_{\mathbf{K}}}^+ \in S^+$ for every $a \in K \setminus \{1_{\mathbf{K}}\}$, where

$$f_{a,0_{\mathbf{K}}}^+(y) = \bigvee \{x \in K \mid f_{a,0_{\mathbf{K}}}(x) \leq y\} = \begin{cases} 1_{\mathbf{K}} & \text{if } y = 1_{\mathbf{K}}, \\ a & \text{else.} \end{cases}$$

Because of $L_- = L \setminus \{0_{\mathbf{L}}\} = K \setminus \{1_{\mathbf{K}}\}$, we get $\Psi_{\mathbf{L}}(f_{a,0_{\mathbf{K}}}^+) = f_{a,0_{\mathbf{K}}}^+|_{K \setminus \{1_{\mathbf{K}}\}} = k_a$. Consequently, condition (5.3) is fulfilled. Now let $a \in K$ and $b \in K \setminus \{0_{\mathbf{K}}, 1_{\mathbf{K}}\}$. Then by (5.8), there exists an $f \in S$ with $f(b) = a$ and $f^+(a) = \bigvee \{x \in K \mid f(x) \leq a\} \geq b$ holds. Hence, $a \leq x$ implies $b \leq f^+(a) \leq f^+(x)$ for every $x \in K$. Let $x \in K$ with $a \not\leq x$ and assume $b \leq f^+(x)$. It follows that $a = f(b) \leq f(f^+(x)) \leq \text{id}(x) = x$, what is a contradiction, and we derive the equivalence $a \leq x \Leftrightarrow b \leq f^+(x)$ for every $x \in K$. If we use the order \leq^d of $\mathbf{L} = \mathbf{K}^d$, then we have $f^+(x) \leq^d b$ if $x \leq^d a$ and $f^+(x) \not\leq^d b$ else. Hence, $k_b \vee^d f^+(x) = b$ if $x \leq^d a$ and $k_b \vee^d f^+(x) >^d b$ else. The mapping $\Psi_{\mathbf{L}}(k_b \vee^d f^+)$ is then the required mapping for a and b in condition (5.5). Condition (5.4) is satisfied by $(\Psi_{\mathbf{L}}(S^+), \vee^d, \circ)$ because (S, \vee, \circ) fulfils (5.7) and (S, \vee) is isomorphic to $(\Psi_{\mathbf{L}}(S^+), \vee^d)$. \square

Proposition 5.40. *Let ∞_R be left but not right absorbing. Then there exists a finite nontrivial semilattice \mathbf{L} such that $(R, +, \cdot)$ is isomorphic to a subsemiring of $(\text{JM}(\mathbf{L}), \vee, \circ)$ that fulfils (5.3), (5.4), and (5.5).*

Proof. Define $r \star s := s \cdot r$ for all $r, s \in R$. Then $(R, +, \star)$ is a finite simple additively idempotent semiring such that ∞_R is right but not left absorbing. By Proposition 5.35, there exists a finite lattice $\mathbf{K} = (K, \leq)$ with $|K| \geq 3$ such that $(R, +, \star)$ is isomorphic to a subsemiring (S, \vee, \circ) of $(\text{Res}_1(\mathbf{K}), \vee, \circ)$ that fulfils conditions (5.6), (5.7), and (5.8). Let $\mathbf{L} := \mathbf{K}^d$. By Lemma 5.39, $(\Psi_{\mathbf{L}}(S^+), \vee^d, \circ)$ is a subsemiring of $(\text{JM}(\mathbf{L}_-), \vee^d, \circ)$, which fulfils (5.3), (5.4), and (5.5). \mathbf{L}_- is clearly nontrivial. Because of $(R, +, \star) \cong (S, \vee, \circ) \cong (S^+, \vee^d, \circ^d)$ by Lemma 5.37, we furthermore find $(R, +, \cdot) \cong (S^+, \vee^d, \circ) \cong (\Psi_{\mathbf{L}}(S^+), \vee^d, \circ)$ by Lemma 5.38. \square

Example 5.41. Consider the finite simple additively idempotent semiring $(R, +, \cdot)$ with the following operation tables:

| | | | | | | | |
|-----|-----|-----|-----|---------|-----|-----|-----|
| $+$ | a | b | c | \cdot | a | b | c |
| a | a | b | c | a | a | a | a |
| b | b | b | c | b | a | b | c |
| c | c | c | c | c | c | c | c |

The greatest element c of this semiring is left but not right absorbing. Let $\mathbf{L} = (\{0, 1\}, \leq)$ be the total order of two elements and consider the semiring $(\text{JM}(\mathbf{L}), \vee, \circ)$. This semiring consists of the mappings α, β , and γ , which are of the following form and fulfil the following operation tables:

| | | | | | | | | | | |
|-------------|-----|-----|----------|----------|----------|----------|----------|----------|----------|----------|
| x | 0 | 1 | \vee | α | β | γ | \circ | α | β | γ |
| $\alpha(x)$ | 0 | 0 | α | α | β | γ | α | α | α | α |
| $\beta(x)$ | 0 | 1 | β | β | β | γ | β | α | β | γ |
| $\gamma(x)$ | 1 | 1 | γ | γ | γ | γ | γ | γ | γ | γ |

Clearly, $(\text{JM}(\mathbf{L}), \vee, \circ)$ fulfils (5.3), (5.4), and (5.5) and the semiring $(R, +, \cdot)$ is isomorphic to $(\text{JM}(\mathbf{L}), \vee, \circ)$.

∞_R is absorbing

The following proposition is [31, Theorem 2.2] for finite semilattices. Note that for a finite semilattice \mathbf{L} the mappings $f_{a,b}$ with $a \in L \setminus \{1\}$ and $b \in L$ are exactly the mappings of range at most two in $\text{JM}_1(\mathbf{L})$.

Proposition 5.42. *Let $\mathbf{L} = (L, \leq)$ be a finite nontrivial semilattice and (S, \vee, \circ) a subsemiring of $(\text{JM}_1(\mathbf{L}), \vee, \circ)$ that fulfils (5.1). Then (S, \vee, \circ) is simple iff it fulfils (5.2).*

Proposition 5.43. *Let ∞_R be absorbing. Furthermore, let $(M, +)$ be a finite idempotent irreducible R -semimodule with join-irreducible greatest element. Then $(R, +, \cdot)$ is isomorphic to a subsemiring of $(\text{JM}_1(M, \leq), +, \circ)$ that fulfils (5.1) and (5.2).*

Proof. By Lemma 5.9, $(R, +, \cdot)$ is isomorphic to a subsemiring of $(\text{JM}(M, \leq), +, \circ)$ and because of $R\infty_M = \{\infty_M\}$ by Proposition 5.26 even of $(\text{JM}_1(M, \leq), +, \circ)$. First consider the case that $(R, +)$ has no neutral element. Assume that $(M, +)$ has a neutral element 0_M . Let z be the unique lower neighbour of ∞_M . By Proposition 5.32,

5.2. Embedding of $(R, +, \cdot)$ into $(\mathbf{JM}(\mathbf{L}), \vee, \circ)$

$r_{z,0_M}$ is contained in R and by Corollary 5.10 it is a neutral element in $(R, +)$. This is a contradiction. Hence, $(M, +)$ has no neutral element. Therefore, condition (5.1) is satisfied by Proposition 5.32 and (5.2) holds by Proposition 5.42.

Now let $(R, +)$ have a neutral element 0_R . Then $(M, +)$ has also a neutral element 0_M , by Proposition 5.27. Because of $R\infty_M = \{\infty_M\}$, it follows by Proposition 5.32 that $r_{a,0_M} \in R$ for every $a \in M \setminus \{\infty_M\}$. Since ∞_R is left absorbing, 0_R cannot be right absorbing. By Lemma 5.28, it follows that $R0_M = M$. Let $b \in M$. Then there exists an $s_b \in R$ with $s_b 0_M = b$ and it follows that $r_{a,b} = s_b r_{a,0_M} \in R$. Thus, (5.1) is fulfilled and (5.2) follows by Proposition 5.42. \square

Example 5.44. Consider the finite simple additively idempotent semiring $(R, +, \cdot)$ with the following operation tables:

| | | | | | | | | | | | |
|-----|-----|-----|-----|-----|-----|---------|-----|-----|-----|-----|-----|
| $+$ | a | b | c | d | e | \cdot | a | b | c | d | e |
| a | a | b | c | d | e | a | a | b | a | b | e |
| b | b | b | d | d | e | b | a | b | e | e | e |
| c | c | d | c | d | e | c | c | d | c | d | e |
| d | d | d | d | d | e | d | c | d | e | e | e |
| e | e | e | e | e | e | e | e | e | e | e | e |

The greatest element e of this semiring is absorbing and the subsemigroup $(\{a, c, e\}, +)$ of $(R, +)$ is a finite idempotent irreducible R -semimodule, whose greatest element e is join-irreducible. Consider the subsemiring $(S, +, \circ)$ of $(\mathbf{JM}_1(\{a, c, e\}, \leq), +, \circ)$ consisting of the mappings $\alpha, \beta, \gamma, \delta$, and ϵ , which are of the following form and fulfil the following operation tables:

| | | | | | | | | | | | | | | | |
|---------------|-----|-----|-----|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|
| x | a | c | e | \vee | α | β | γ | δ | ϵ | \circ | α | β | γ | δ | ϵ |
| $\alpha(x)$ | a | a | e | α | α | β | γ | δ | ϵ | α | α | β | α | β | ϵ |
| $\beta(x)$ | a | e | e | β | β | β | δ | δ | ϵ | β | α | β | ϵ | ϵ | ϵ |
| $\gamma(x)$ | c | c | e | γ | γ | δ | γ | δ | ϵ | γ | γ | δ | γ | δ | ϵ |
| $\delta(x)$ | c | e | e | δ | δ | δ | δ | δ | ϵ | δ | γ | δ | ϵ | ϵ | ϵ |
| $\epsilon(x)$ | e | e | e | ϵ | ϵ | ϵ | ϵ | ϵ | ϵ | ϵ | ϵ | ϵ | ϵ | ϵ | ϵ |

The semiring $(S, +, \circ)$ fulfils (5.1) and (5.2) and the semiring $(R, +, \cdot)$ is isomorphic to $(S, +, \circ)$.

5.3 Subsemirings of $(\text{JM}(\mathbf{L}), \vee, \circ)$

In this section we consider the other direction, i.e. we start with a semilattice \mathbf{L} and show that certain subsemirings of $(\text{JM}(\mathbf{L}), \vee, \circ)$ are simple.

Proposition 5.45. *Let \mathbf{L} be a finite lattice with more than two elements and let (R, \vee, \circ) be a subsemiring of $(\text{Res}_1(\mathbf{L}), \vee, \circ)$ that fulfils (5.6), (5.7), and (5.8). Then (R, \vee, \circ) is a finite simple additively idempotent semiring and the greatest element is right but not left absorbing.*

Proof. It is clear that (R, \vee, \circ) is a finite additively idempotent semiring; its greatest element is $\infty_R = f_{0,0}$. It is easy to see that each element $f_{a,0} \in R$, where $a \in L \setminus \{1\}$, is right absorbing, hence in particular $f_{0,0}$ is right and not left absorbing.

To prove the simplicity, let \sim be a congruence on (R, \vee, \circ) , and suppose that $\sim \neq \text{id}_R$, i.e. there are $f, g \in R$ such that $f \neq g$ and $f \sim g$. Hence, there exists an $x \in L$ such that $f(x) \neq g(x)$, and we may assume that $f(x) \not\leq g(x) =: a$. Then we have $f_{a,0} \in R$, so that $f_{a,0} \circ f \sim f_{a,0} \circ g$, and there are $b, c \in L$ such that $f_{a,0} \circ f = f_{b,0}$ and $f_{a,0} \circ g = f_{c,0}$. Furthermore, $f_{b,0}(x) = 1$ and $f_{c,0}(x) = 0$, so that $c \not\leq b$. We have shown that there are some elements $b, c \in L$ with $c \not\leq b$ such that $f_{b,0} \sim f_{c,0}$.

Now we show that for all $z \in L \setminus \{0, 1\}$ there exists a $y \in L$, $y < z$ such that $f_{z,0} \sim f_{y,0}$. So let $z \in L \setminus \{0, 1\}$ and let $h \in R$ such that $h(z) = c$. Considering $k := h \vee f_{z,0}$ it is easy to see that $f_{c,0} \circ k = f_{z,0}$. On the other hand there exists a $y \in L$ such that $f_{b,0} \circ k = f_{y,0}$, and it holds that $f_{y,0}(z) = 1$. From this and since $f_{z,0} \leq f_{y,0}$, it follows that $y < z$. Furthermore, we have $f_{z,0} = f_{c,0} \circ k \sim f_{b,0} \circ k = f_{y,0}$, as desired.

By applying the last paragraph repeatedly, we see that $f_{z,0} \sim f_{0,0}$ for all $z \in L \setminus \{1\}$. Now let $f \in R$ be arbitrary and let $z \in L \setminus \{1\}$ such that $f_{z,0} \leq f$. Then we get $f = f_{z,0} \vee f \sim f_{0,0} \vee f = f_{0,0}$. Hence, $\sim = R \times R$, as desired. \square

Proposition 5.46. *Let \mathbf{L} be a nontrivial finite semilattice and (R, \vee, \circ) a subsemiring of $(\text{JM}(\mathbf{L}), \vee, \circ)$ that fulfils (5.3), (5.4), and (5.5). Then (R, \vee, \circ) is a finite simple additively idempotent semiring and the greatest element is left but not right absorbing.*

Proof. It is clear that (R, \vee, \circ) is a finite additively idempotent semiring; its greatest element is $\infty_R = k_1$. Each element $k_a \in R$, where $a \in L$, is left absorbing, hence in particular k_1 is left but not right absorbing.

To prove the simplicity, let \sim be a congruence on (R, \vee, \circ) , and suppose $\sim \neq \text{id}_R$, i.e. there are $f, g \in R$ such that $f \neq g$ and $f \sim g$. There exists an $x \in L$ such

5.4. Characterisation theorems

that $f(x) \neq g(x)$, and we may assume $c := f(x) \not\leq g(x) =: b$. Then we have $k_c = f \circ k_x \sim g \circ k_x = k_b$.

Now for all $z \in L \setminus \{1\}$ there exists a $y \in L$, $y > z$ such that $k_z \sim k_y$. Indeed, let $h \in R$ such that $h(x) = z$ if $x \leq b$, and $h(x) > z$ else. Then in particular $y := h(c) > z$, and $k_y = h \circ k_c \sim h \circ k_b = k_z$.

By applying the last paragraph repeatedly, we see that $k_z \sim k_1$ for all $z \in L$. Now let $f \in R$ be arbitrary and let $z \in L$ such that $k_z \leq f$. Then $f = k_z \vee f \sim k_1 \vee f = k_1$. Consequently, $\sim = R \times R$, as desired. \square

Proposition 5.47. *Let \mathbf{L} be a finite nontrivial semilattice and let (R, \vee, \circ) be a subsemiring of $(\text{JM}_1(\mathbf{L}), \vee, \circ)$ that fulfils (5.1) and (5.2). Then (R, \vee, \circ) is a finite simple additively idempotent semiring with absorbing greatest element.*

Proof. Clearly, (R, \vee, \circ) is finite and additively idempotent. The simplicity holds by Proposition 5.42. The greatest element is $f_{a,1} = k_1$, for arbitrary $a \in L \setminus \{1\}$, which is absorbing. \square

Proposition 5.48. *Let \mathbf{L} be a finite nontrivial semilattice and (R, \vee, \circ) a simple subsemiring of $(\text{JM}_1(\mathbf{L}), \vee, \circ)$ that fulfils (5.1) and $|R| > 2$. Then (L, \vee) is an irreducible R -semimodule.*

Proof. (L, \vee) is clearly an R -semimodule. By (5.1), (L, \vee) is also an R -nonidentity-semimodule with $|RL| > 1$. Let (K, \vee) be an R -subsemimodule of (L, \vee) with $|K| > 1$. Then there exists an $a \in K$ with $a \neq 1_{\mathbf{L}}$ and $b = f_{a,b}(a) \in K$ follows for every $b \in L$. Thus, $K = L$ and (L, \vee) is consequently sub-irreducible.

Now let \sim be a semimodule congruence on (L, \vee) with $\sim \neq \text{id}_L$. There must exist some $a, b \in L$ with $a \neq b$ and $a \sim b$. Without loss of generality we may assume say $b \not\leq a$. It follows that $a \neq 1$. Choose $c \in L$ arbitrarily. Then $c = f_{a,c}(a) \sim f_{a,c}(b) = 1$. Hence, $c \sim 1$ for every $c \in L$. Thus, $\sim = L \times L$. We conclude that (L, \vee) is quotient-irreducible. \square

5.4 Characterisation theorems

Now we are ready to state the characterisation theorems for finite simple additively idempotent semirings of all cases mentioned in the introduction of this chapter, except Case 4b.

The following theorem states that the finite simple additively idempotent semirings with greatest element that is neither left nor right absorbing are exactly the

finite simple additively idempotent semirings with zero. It follows from Proposition 5.30. The second part of the theorem is obvious.

Theorem 5.49. *Let $(R, +, \cdot)$ be a finite simple additively idempotent semiring with $|R| > 2$ and such that ∞_R is neither left nor right absorbing. Then $(R, +, \cdot)$ is isomorphic to a semiring as in Theorem 1.11. Conversely, every semiring in Theorem 1.11 has a greatest element, which is neither left nor right absorbing.*

We get the following theorem from Proposition 5.35 and Proposition 5.45.

Theorem 5.50. *Let \mathbf{L} be a finite lattice with more than two elements and let (R, \vee, \circ) be a subsemiring of $(\text{Res}_1(\mathbf{L}), \vee, \circ)$ that fulfils (5.6), (5.7), and (5.8). Then (R, \vee, \circ) is a finite simple additively idempotent semiring and the greatest element is right but not left absorbing. Conversely, every finite simple additively idempotent semiring $(S, +, \cdot)$ with $|S| > 2$ and with right but not left absorbing greatest element is isomorphic to such a semiring.*

Proposition 5.40 and Proposition 5.46 yield the following result.

Theorem 5.51. *Let \mathbf{L} be a finite nontrivial semilattice and (R, \vee, \circ) a subsemiring of $(\text{JM}(\mathbf{L}), \vee, \circ)$ that fulfils (5.3), (5.4), and (5.5). Then (R, \vee, \circ) is a finite simple additively idempotent semiring and the greatest element is left but not right absorbing. Conversely, every finite simple additively idempotent semiring $(S, +, \cdot)$ with $|S| > 2$ and with left but not right absorbing greatest element is isomorphic to such a semiring.*

The next theorem holds by Proposition 5.43, Proposition 5.47, and Proposition 5.48.

Theorem 5.52. *Let \mathbf{L} be a nontrivial finite semilattice such that $1_{\mathbf{L}}$ is join-irreducible and let (R, \vee, \circ) be a subsemiring of $(\text{JM}_1(\mathbf{L}), \vee, \circ)$ that fulfils (5.1) and (5.2). Then (R, \vee, \circ) is a finite simple additively idempotent semiring with absorbing greatest element and it possesses an idempotent irreducible R -semimodule, whose greatest element is join-irreducible. Conversely, every finite simple additively idempotent semiring $(S, +, \cdot)$ with $|S| > 2$, with absorbing greatest element, and that possesses an idempotent irreducible S -semimodule, whose greatest element is join-irreducible, is isomorphic to such a semiring.*

5.5 Isomorphic semirings

In this section we show that if we have two semirings as in Theorem 5.50, Theorem 5.51, or Theorem 5.52 that are isomorphic, then the corresponding semilattices have to be isomorphic as well. In [61], the same was done for semirings as in Theorem 1.11 (Theorem 5.49).

Lemma 5.53. *Let \mathbf{L} be a finite lattice and (R, \vee, \circ) a subsemiring of $(\text{Res}_1(\mathbf{L}), \vee, \circ)$ that fulfils (5.6). Then*

$$\Gamma : L \setminus \{1\} \rightarrow f_{0,0} \circ R := \{f_{0,0} \circ f \mid f \in R\}, \quad a \mapsto f_{a,0}$$

is a dual order isomorphism between $(L \setminus \{1\}, \leq)$ and $(f_{0,0} \circ R, \leq)$.

Proof. First we verify $f_{0,0} \circ R = \{f_{a,0} \mid a \in L \setminus \{1\}\}$. The inclusion “ \subseteq ” holds by Lemma 5.33. Now let $a \in L \setminus \{1\}$. Then $f_{a,0} = f_{0,0} \circ f_{a,0} \in f_{0,0} \circ R$. This proves the equality and it follows that Γ is well-defined and surjective. Because of $a \leq b \Leftrightarrow f_{a,0} \geq f_{b,0}$ for all $a, b \in L \setminus \{1\}$, we find that Γ is a dual order isomorphism. \square

Lemma 5.54. *Let \mathbf{L} be a finite semilattice and (R, \vee, \circ) a subsemiring of $(\text{JM}(\mathbf{L}), \vee, \circ)$ that fulfils (5.3). Then*

$$\Lambda : L \rightarrow R \circ k_1 := \{f \circ k_1 \mid f \in R\}, \quad a \mapsto k_a$$

is an order isomorphism between \mathbf{L} and $(R \circ k_1, \leq)$.

Proof. First we verify $R \circ k_1 = \{k_a \mid a \in L\}$. Let $f \in R$. Then $f \circ k_1 = k_{f(1)} \in \{k_a \mid a \in L\}$. Now let $a \in L$. Then $k_a = k_a \circ k_1 \in R \circ k_1$. This proves the equality and it follows that Λ is well-defined and surjective. Because of $a \leq b \Leftrightarrow k_a \leq k_b$ for all $a, b \in L$, we find that Λ is an order isomorphism. \square

Lemma 5.55. *Let \mathbf{L} be a finite semilattice, (R, \vee, \circ) a subsemiring of $(\text{JM}_1(\mathbf{L}), \vee, \circ)$ that fulfils (5.1) and let $a, b \in L \setminus \{1\}$. Then*

$$\Phi : L \rightarrow R \circ f_{a,b} := \{f \circ f_{a,b} \mid f \in R\}, \quad c \mapsto f_{a,c}$$

is an order isomorphism between \mathbf{L} and $(R \circ f_{a,b}, \leq)$.

Proof. First we verify $R \circ f_{a,b} = \{f_{a,c} \mid c \in L\}$. Let $f \in R$. Then $f \circ f_{a,b} = f_{a,f(b)} \in \{f_{a,c} \mid c \in L\}$. Now let $c \in L$. Then $f_{a,c} = f_{b,c} \circ f_{a,b} \in R \circ f_{a,b}$. This

proves the equality and it follows that Φ is well-defined and surjective. Because of $c \leq d \Leftrightarrow f_{a,c} \leq f_{a,d}$ for all $c, d \in L$, we find that Φ is an order isomorphism. \square

Proposition 5.56. *Let $\mathbf{L}_i = (L_i, \leq)$ be a finite lattice and (R_i, \vee, \circ) a subsemiring of $(\text{Res}_1(\mathbf{L}_i), \vee, \circ)$ as in Theorem 5.50 for $i = 1, 2$. If (R_1, \vee, \circ) and (R_2, \vee, \circ) are isomorphic, then \mathbf{L}_1 and \mathbf{L}_2 are also isomorphic.*

Proof. Let (R_1, \vee, \circ) and (R_2, \vee, \circ) be isomorphic and let $\Omega : R_1 \rightarrow R_2$ be an isomorphism. Let $0_i := 0_{\mathbf{L}_i}$ for $i = 1, 2$. Since $f_{0_i, 0_i}$ is the greatest element in (R_i, \leq) , we have $\Omega(f_{0_1, 0_1}) = f_{0_2, 0_2}$. It follows that $\Omega(f_{0_1, 0_1} \circ R_1) = \Omega(f_{0_1, 0_1}) \circ \Omega(R_1) = f_{0_2, 0_2} \circ R_2$. Hence, $(f_{0_1, 0_1} \circ R_1, \leq) \cong (f_{0_2, 0_2} \circ R_2, \leq)$. With Lemma 5.53, we find $(L_1 \setminus \{1_{\mathbf{L}_1}\}, \leq) \cong (f_{0_1, 0_1} \circ R_1, \geq) \cong (f_{0_2, 0_2} \circ R_2, \geq) \cong (L_2 \setminus \{1_{\mathbf{L}_2}\}, \leq)$. It trivially follows that $\mathbf{L}_1 \cong \mathbf{L}_2$. \square

Proposition 5.57. *Let $\mathbf{L}_i = (L_i, \leq)$ be a finite semilattice and (R_i, \vee, \circ) a subsemiring of $(\text{JM}(\mathbf{L}_i), \vee, \circ)$ as in Theorem 5.51 for $i = 1, 2$. If (R_1, \vee, \circ) and (R_2, \vee, \circ) are isomorphic, then \mathbf{L}_1 and \mathbf{L}_2 are also isomorphic.*

Proof. Let (R_1, \vee, \circ) and (R_2, \vee, \circ) be isomorphic and let $\Omega : R_1 \rightarrow R_2$ be an isomorphism. Let here $1_i := 1_{\mathbf{L}_i}$ for $i = 1, 2$. Since k_{1_i} is the greatest element in (R_i, \leq) , we have $\Omega(k_{1_1}) = k_{1_2}$. It follows that $\Omega(R_1 \circ k_{1_1}) = \Omega(R_1) \circ \Omega(k_{1_1}) = R_2 \circ k_{1_2}$. Hence, $(R_1 \circ k_{1_1}, \leq) \cong (R_2 \circ k_{1_2}, \leq)$. By Lemma 5.54, $\mathbf{L}_1 \cong (R_1 \circ k_{1_1}, \leq) \cong (R_2 \circ k_{1_2}, \leq) \cong \mathbf{L}_2$ follows. \square

Proposition 5.58. *Let $\mathbf{L}_i = (L_i, \leq)$ be a finite semilattice and (R_i, \vee, \circ) a subsemiring of $(\text{JM}_1(\mathbf{L}_i), \vee, \circ)$ as in Theorem 5.52 for $i = 1, 2$. If (R_1, \vee, \circ) and (R_2, \vee, \circ) are isomorphic, then \mathbf{L}_1 and \mathbf{L}_2 are also isomorphic.*

An element a in a finite semilattice \mathbf{L} is called a **coatom** of \mathbf{L} if it is a lower neighbour of $1_{\mathbf{L}}$. By $\text{CoAt}(\mathbf{L})$ we denote the set of coatoms in \mathbf{L} .

Proof. Let (R_1, \vee, \circ) and (R_2, \vee, \circ) be isomorphic and let $\Omega : R_1 \rightarrow R_2$ be an isomorphism. One can easily show that

$$\text{CoAt}(\text{JM}_1(\mathbf{L}_i), \leq) = \{f_{a,b} \mid a \in \text{Min}(\mathbf{L}_i), b \in \text{CoAt}(\mathbf{L}_i)\}$$

holds. Thus, for $a \in \text{Min}(\mathbf{L}_1)$ and $b \in \text{CoAt}(\mathbf{L}_1)$ there exist $a' \in \text{Min}(\mathbf{L}_2)$ and $b' \in \text{CoAt}(\mathbf{L}_2)$ with $\Omega(f_{a,b}) = f_{a',b'}$. We find that $\Omega(R_1 \circ f_{a,b}) = \Omega(R_1) \circ \Omega(f_{a,b}) = R_2 \circ f_{a',b'}$. Hence, $(R_1 \circ f_{a,b}, \leq) \cong (R_2 \circ f_{a',b'}, \leq)$. By Lemma 5.55, $\mathbf{L}_1 \cong (R_1 \circ f_{a,b}, \leq) \cong (R_2 \circ f_{a',b'}, \leq) \cong \mathbf{L}_2$ follows. \square

5.6 Neutral elements

Additively neutral element

If the greatest element 1 of a finite semilattice is join-irreducible, then we denote the unique lower neighbour of 1 by 1_* .

Proposition 5.59. *Let \mathbf{L} be a finite lattice and (R, \vee, \circ) a semiring as in Theorem 5.50. Then (R, \vee) has a neutral element iff 1 is join-irreducible. If the neutral element exists, then it is right but not left absorbing.*

Proof. If 1 is join-irreducible, then $f_{1_*,0}$ is clearly a neutral element in (R, \vee) . If (R, \vee) has a neutral element f_0 , then it must fulfil $f_0(a) \leq f_{a,0}(a) = 0$ for every $a \in L \setminus \{1\}$. For all $a, b \in L \setminus \{1\}$, we have $a \vee b \neq 1$ because of $f_0(a \vee b) = f_0(a) \vee f_0(b) = 0$. Hence, $c \vee d = 1$ implies $c = 1$ or $d = 1$ for $c, d \in L$, i.e. 1 is join-irreducible.

The element $f_{1_*,0}$ is right absorbing because of $f(0) = 0$ and $f(1) = 1$ for every $f \in R$. But it is not left absorbing because of $f_{1_*,0} \circ f_{a,0} = f_{a,0}$ for every $a \in L \setminus \{1\}$. \square

Proposition 5.60. *Let \mathbf{L} be a finite semilattice and (R, \vee, \circ) a semiring as in Theorem 5.51. Then (R, \vee) has a neutral element iff \mathbf{L} is a lattice. If the neutral element exists, then it is left but not right absorbing.*

Proof. If \mathbf{L} is a lattice, then k_0 is clearly a neutral element in (R, \vee) . If (R, \vee) has a neutral element f_0 , then it must fulfil $f_0(x) \leq k_a(x) = a$ for all $a, x \in L$. Thus, $f_0(x)$ is a least element in \mathbf{L} for every $x \in L$, i.e. \mathbf{L} is a lattice and $f_0 = k_0$ holds. Clearly, k_0 is left absorbing, but it is not right absorbing because of $k_1 \circ k_0 = k_1$. \square

Proposition 5.61. *Let \mathbf{L} be a finite semilattice and (R, \vee, \circ) a semiring as in Theorem 5.52. Then (R, \vee) has a neutral element iff \mathbf{L} is a lattice. If the neutral element exists, then it is neither left nor right absorbing.*

Proof. If \mathbf{L} is a lattice, then $f_{1_*,0}$ is a neutral element in (R, \vee) . If (R, \vee) has a neutral element f_0 , then it must fulfil $f_0(x) \leq f_{x,a}(x) = a$ for every $a \in L$ and $x \in L \setminus \{1\}$. Thus, for $x \in L \setminus \{1\}$, $f_0(x)$ is a least element in \mathbf{L} , i.e. \mathbf{L} is a lattice and $f_0(x) = 0$ holds. Since $f_{1_*,1} = k_1$ is absorbing, f_0 cannot be left or right absorbing. \square

The next proposition shows that the finite simple additively idempotent semirings with additively neutral element and absorbing greatest element are already characterised by Theorem 5.52.

Proposition 5.62. *Let $(R, +, \cdot)$ be a finite simple additively idempotent semiring with additively neutral element 0_R and let $(M, +)$ be a finite idempotent sub-irreducible R -semimodule. If ∞_R is right absorbing, then ∞_M is join-irreducible.*

Proof. Let $a, b \in M$ with $a + b = \infty_M$. Since ∞_R is right absorbing, 0_R is not left absorbing. By Lemma 5.28-3., $0_R \infty_M = \infty_M$ holds and we find that $\infty_M = 0_R \infty_M = 0_R(a + b) = 0_R a + 0_R b$. By Lemma 5.28-1., $a = \infty_M$ or $b = \infty_M$ follows, i.e. ∞_M is join-irreducible. \square

Therefore, the classification of finite simple semirings with additively neutral element is complete and can be summarised as in the next theorem.

Theorem 5.63. *Let $(R, +, \cdot)$ be a finite semiring with additively neutral element. Then $(R, +, \cdot)$ is simple iff one of the following holds:*

1. $|R| \leq 2$.
2. $(R, +, \cdot) \cong (\text{Mat}_n(\mathbb{F}_q), +, \cdot)$ for some finite field \mathbb{F}_q and some $n \geq 1$.
3. $(R, +, \cdot)$ is a zero multiplication ring of prime order.
4. $(R, +, \cdot)$ is isomorphic to a semiring as in Theorem 1.11.
5. $(R, +, \cdot)$ is isomorphic to a semiring as in Theorem 5.50, where $1_{\mathbf{L}}$ is join-irreducible.
6. $(R, +, \cdot)$ is isomorphic to a semiring as in Theorem 5.51, where \mathbf{L} is a lattice.
7. $(R, +, \cdot)$ is isomorphic to a semiring as in Theorem 5.52, where \mathbf{L} is a lattice.

Multiplicatively neutral element

Proposition 5.64. *Let \mathbf{L} be a lattice and (R, \vee, \circ) a semiring as in Theorem 5.50. Then (R, \circ) has a neutral element iff $\text{id}_L \in R$. If $\text{id}_L \in R$, then $1_{\mathbf{L}}$ is join-irreducible.*

Proof. If $\text{id}_L \in R$, then it is clearly a neutral element in (R, \circ) . Let (R, \circ) have a neutral element e and let $x \in L$. For $a \in L \setminus \{0, 1\}$, there exists an $f \in R$ with $f(a) = x$. It follows that $e(x) = e(f(a)) = (e \circ f)(a) = f(a) = x$, i.e. $\text{id}_L = e \in R$.

If $\text{id}_L \in R$, then there exists an $a \in L \setminus \{1\}$ with $f_{a,0} \leq \text{id}_L$, i.e. $x \not\leq a \Leftrightarrow x = 1$ for every $x \in L$. Hence, a is the unique lower neighbour of 1, i.e. 1 is join-irreducible. \square

5.7. The remaining case

Proposition 5.65. *Let \mathbf{L} be a semilattice and (R, \vee, \circ) a semiring as in Theorem 5.51. Then (R, \circ) has a neutral element iff $\text{id}_L \in R$. If $\text{id}_L \in R$, then \mathbf{L} is a lattice.*

Proof. If $\text{id}_L \in R$, then it is clearly a neutral element in (R, \circ) . If (R, \circ) has a neutral element e , then $e(x) = e(k_x(x)) = (e \circ k_x)(x) = k_x(x) = x$ for every $x \in L$, i.e. $\text{id}_L = e \in R$.

If $\text{id}_L \in R$, then there exists an $a \in L$ with $k_a \leq \text{id}_L$. Thus, $a = k_a(x) \leq \text{id}_L(x) = x$ for every $x \in L$. Hence, a is a least element in \mathbf{L} , i.e. \mathbf{L} is a lattice. \square

Proposition 5.66. *Let \mathbf{L} be a semilattice and (R, \vee, \circ) a semiring as in Theorem 5.52. Then (R, \circ) has a neutral element iff $\text{id}_L \in R$. If $\text{id}_L \in R$, then \mathbf{L} is a lattice.*

Proof. If $\text{id}_L \in R$, then it is clearly a neutral element in (R, \circ) . Let (R, \circ) have a neutral element e and let $x \in L$. For $a \in L \setminus \{1\}$, the equality $e(x) = e(f_{a,x}(a)) = (e \circ f_{a,x})(a) = f_{a,x}(a) = x$ holds, i.e. $\text{id}_L = e \in R$.

If $\text{id}_L \in R$, then there exists $a \in L \setminus \{1\}$ and $b \in L$ with $f_{1*,b} \leq f_{a,b} \leq \text{id}_L$. We find that $x \leq 1_* \Rightarrow b \leq x$ for every $x \in L$ and it follows that $b \leq x$ for every $x \in L \setminus \{1\}$. As $b \leq 1$ holds anyway it follows that b is a least element in \mathbf{L} . Thus, \mathbf{L} is a lattice. \square

From the results in this section it also follows that the existence of a multiplicatively neutral element implies the existence of an additively neutral element for all semirings in Theorem 5.50, Theorem 5.51, and Theorem 5.52.

5.7 The remaining case

The semirings that elude our characterisation theorems are the finite simple additively idempotent semirings with absorbing greatest element, which possess a finite idempotent irreducible semimodule, whose greatest element is join-reducible. In this section we present different conjectures dependent on whether there exists a neutral element for such a semimodule.

Irreducible semimodule with neutral element

If the finite simple additively idempotent semiring with absorbing greatest element possesses a finite idempotent irreducible semimodule with a neutral element, we con-

jecture that the characterisation is similar to Theorem 5.52. In fact, our presumed characterisation in this case is based on the following conjecture.

Conjecture 5.67. *Let $(R, +, \cdot)$ be a finite simple additively idempotent semiring with $|R| > 2$ and let $(M, +)$ be a finite idempotent R -semimodule. Then $(M, +)$ is irreducible iff $(M, +)$ is faithful of smallest cardinality.*

One direction of this conjecture, namely that a faithful semimodule of smallest cardinality is irreducible, is already proven by Proposition 5.18. Concerning the other direction, one can show that, similarly to Proposition 5.48, the semilattices in Theorem 5.49, Theorem 5.50, and Theorem 5.51 are irreducible semimodules. With the results from Section 5.5 it follows that for every semiring characterised in Section 5.4 there exists up to isomorphism a unique idempotent irreducible semimodule. Thus, irreducible semimodules are also faithful semimodules of smallest cardinality in these cases, and we believe that this holds for every idempotent irreducible semimodule over a finite simple additively idempotent semiring with more than two elements.

If the finite simple additively idempotent semiring with absorbing greatest element admits a faithful semimodule of smallest cardinality with a neutral element, we can prove the following result.

Proposition 5.68. *Let $(R, +, \cdot)$ be a finite simple additively idempotent semiring with $|R| > 2$ and let ∞_R be absorbing. Furthermore, let $(M, +)$ be a faithful R -semimodule of smallest cardinality with neutral element 0_M . Then $(R, +, \cdot)$ is isomorphic to a subsemiring of $(\text{JM}_1(M, \leq), +, \circ)$ that fulfils (5.1) and (5.2).*

We need some preparation for the proof. Let $\mathbf{L} = (L, \leq)$ be a finite semilattice and o an element with $o \notin L$. Then define $L_+ := L \cup \{o\}$, $\sqsubseteq := \leq \cup (\{o\} \times L_+)$ and $\mathbf{L}_+ := (L_+, \sqsubseteq)$, i.e. \mathbf{L}_+ is the semilattice \mathbf{L} enriched by a new least element o . \mathbf{L}_+ is therefore a lattice. Moreover, we use the notations $\mathbf{L}^\# := ((\mathbf{L}_+)^d)_-$ and $L^\# := L_+ \setminus \{1_{\mathbf{L}}\}$, i.e. $\mathbf{L}^\# = (L^\#, \sqsupseteq \cap (L^\# \times L^\#))$.

Lemma 5.69. *Let $\mathbf{L} = (L, \leq)$ be a finite semilattice. Then*

$$(\text{JM}_1(\mathbf{L}), \vee, \circ) \cong (\text{JM}_1(\mathbf{L}^\#), \vee^d, \circ^d).$$

Proof. We will prove that

$$(\text{JM}_1(\mathbf{L}), \vee, \circ) \cong (\text{Res}_{0,1}(\mathbf{L}_+), \vee, \circ) \cong (\text{Res}_{0,1}((\mathbf{L}_+)^d), \vee^d, \circ^d) \cong (\text{JM}_1(\mathbf{L}^\#), \vee^d, \circ^d).$$

5.7. The remaining case

We have $(\mathbf{L}_+)_- = \mathbf{L}$. By Lemma 5.38, $(\text{Res}_{0,1}(\mathbf{L}_+), \vee, \circ)$ is isomorphic to $(\Psi_{\mathbf{L}_+}(\text{Res}_{0,1}(\mathbf{L}_+)), \vee, \circ)$ and $\Psi_{\mathbf{L}_+}(\text{Res}_{0,1}(\mathbf{L}_+)) = \text{JM}_1(\mathbf{L})$ holds. The second isomorphism holds because of $\text{Res}_{0,1}(\mathbf{L}_+)^+ = \text{Res}_{0,1}((\mathbf{L}_+)^d)$ and Lemma 5.37. The third isomorphism holds by the same arguments as for the first isomorphism. \square

Denote for the following lemma for a finite lattice $\mathbf{L} = (L, \leq)$:

$$\begin{aligned} \Psi_1 : \text{JM}_1(\mathbf{L}) &\rightarrow \text{Res}_{0,1}(\mathbf{L}_+) \quad \text{with} \quad \Psi_1(f) : x \mapsto \begin{cases} f(x) & \text{if } x \in L, \\ 0_{\mathbf{L}_+} & \text{else,} \end{cases} \\ \Psi_2 : \text{Res}_{0,1}(\mathbf{L}_+) &\rightarrow \text{Res}_{0,1}((\mathbf{L}_+)^d), \quad f \mapsto f^+, \\ \Psi_3 : \text{Res}_{0,1}((\mathbf{L}_+)^d) &\rightarrow \text{JM}_1(\mathbf{L}^\#), \quad f \mapsto f|_{L_+ \setminus \{1_{\mathbf{L}_+}\}}. \end{aligned}$$

This means Ψ_i is an isomorphism for the i -th isomorphism in the proof of Lemma 5.69. Thus, $\Psi_3 \circ \Psi_2 \circ \Psi_1$ is an isomorphism from $(\text{JM}_1(\mathbf{L}), \vee, \circ)$ to $(\text{JM}_1(\mathbf{L}^\#), \vee^d, \circ^d)$.

Lemma 5.70. *Let $\mathbf{L} = (L, \leq)$ be a finite semilattice, $a \in L \setminus \{1_{\mathbf{L}}\}$, $b \in L$, and $g_{a,b} := \Psi_3 \circ \Psi_2 \circ \Psi_1(f_{a,b})$. If $b = 1_{\mathbf{L}}$, then $g_{a,b} = k_{1_{\mathbf{L}^\#}}$. If $b \neq 1_{\mathbf{L}}$, then*

$$g_{a,b} : x \mapsto \begin{cases} a & \text{if } x \leq^d b \\ 1_{\mathbf{L}^\#} & \text{else,} \end{cases}$$

where \leq^d is the order in $\mathbf{L}^\#$.

Proof. Let $h := \Psi_1(f_{a,b})$ and $x \in L_+$. Then for $h^+ = \Psi_2(h)$ we have

$$\begin{aligned} h^+(x) &= \bigvee \{y \in L_+ \mid h(y) \leq x\} \\ &= \begin{cases} \bigvee \{0_{\mathbf{L}_+}\} = 0_{\mathbf{L}_+} = 1_{(\mathbf{L}_+)^d} & \text{if } b \not\leq x \quad (\Leftrightarrow x \not\leq^d b) \\ a & \text{if } b \leq x < 1_{\mathbf{L}_+} \quad (\Leftrightarrow 0_{(\mathbf{L}_+)^d} <^d x \leq^d b) \\ \bigvee L_+ = 1_{\mathbf{L}_+} = 0_{(\mathbf{L}_+)^d} & \text{if } x = 1_{\mathbf{L}_+} \quad (\Leftrightarrow x = 0_{(\mathbf{L}_+)^d}). \end{cases} \end{aligned}$$

With $g_{a,b} = \Psi_3(h^+) = h^+|_{L_+ \setminus \{1_{\mathbf{L}_+}\}}$, the statement follows. \square

Proof of Proposition 5.68. The semimodule $(M, +)$ is irreducible by Lemma 5.18 and idempotent by Lemma 5.20. $\mathbf{M} := (M, \leq)$ is therefore a finite lattice. By Lemma 5.69, $(\text{JM}_1(\mathbf{M}), \vee, \circ) \cong (\text{JM}_1(\mathbf{M}^\#), \vee^d, \circ^d)$ holds, where \vee refers to the supremum in \mathbf{M} . Since $(R, +, \cdot)$ is isomorphic to a subsemiring of $(\text{JM}(\mathbf{M}), \vee, \circ)$ and

because of $R\infty_M = \{\infty_M\}$ by Proposition 5.26, it is isomorphic to a subsemiring of $(\text{JM}_1(\mathbf{M}), \vee, \circ)$. Hence, it is also isomorphic to a subsemiring (S, \vee^d, \circ^d) of $(\text{JM}_1(\mathbf{M}^\#), \vee^d, \circ^d)$. Clearly, (S, \vee^d, \circ) is a subsemiring of $(\text{JM}_1(\mathbf{M}^\#), \vee^d, \circ)$ and it is simple. $(M^\#, \vee^d)$ is therefore a faithful semimodule over (S, \vee^d, \circ) . We will show that it is of smallest cardinality. Let $(N, +)$ be a faithful semimodule of smallest cardinality over (S, \vee^d, \circ) . By Lemma 5.20, it is idempotent and therefore a semilattice. We denote the corresponding ordered set by $\mathbf{N} := (N, \leq)$ and the supremum by γ . Consequently, (S, \vee^d, \circ) is isomorphic to a subsemiring of $(\text{JM}_1(\mathbf{N}), \gamma, \circ)$ and because of $(\text{JM}_1(\mathbf{N}), \gamma, \circ) \cong (\text{JM}_1(\mathbf{N}^\#), \gamma^d, \circ^d)$ by Lemma 5.69 also to a subsemiring (T, γ^d, \circ^d) of $(\text{JM}_1(\mathbf{N}^\#), \gamma^d, \circ^d)$. (T, γ^d, \circ) is a subsemiring of $(\text{JM}_1(\mathbf{N}^\#), \gamma^d, \circ)$ and $(N^\#, \gamma^d)$ is therefore a faithful semimodule over (T, γ^d, \circ) and also over (R, \vee, \circ) since (R, \vee, \circ) and (T, γ^d, \circ) are isomorphic. It follows that $|N| = |N^\#| \geq |M| = |M^\#|$. Thus, $(M^\#, \vee^d)$ is a faithful semimodule of smallest cardinality over (S, \vee^d, \circ) .

The greatest element of $(M^\#, \vee^d)$ is by construction join-irreducible. By Proposition 5.43, $f_{a,b} \in S$ holds for every $a \in M^\# \setminus \{1_{\mathbf{M}^\#}\} = M \setminus \{1_{\mathbf{M}}\}$ and every $b \in M^\# \supseteq M \setminus \{1_{\mathbf{M}}\}$. By Lemma 5.70, we find $f_{b,a} \in R$ for all $a, b \in M \setminus \{1_{\mathbf{M}}\}$ and $f_{c,1_{\mathbf{M}}} = k_{1_{\mathbf{M}}} \in R$ for every $c \in M \setminus \{1_{\mathbf{M}}\}$. Hence, (5.1) is fulfilled and (5.2) follows by Proposition 5.42. \square

If Conjecture 5.67 holds we can prove the following conjecture, which constitutes another characterisation theorem.

Conjecture 5.71. *Let \mathbf{L} be a nontrivial finite lattice and let (R, \vee, \circ) be a subsemiring of $(\text{JM}_1(\mathbf{L}), \vee, \circ)$ that fulfils (5.1) and (5.2). Then (R, \vee, \circ) is a finite simple additively idempotent semiring with absorbing greatest element and it possesses an idempotent irreducible R -semimodule with neutral element. Conversely, every finite simple additively idempotent semiring $(S, +, \cdot)$ with $|S| > 2$, with absorbing greatest element, and that possesses an idempotent irreducible S -semimodule with neutral element is isomorphic to such a semiring.*

The first part holds by Proposition 5.47 and Proposition 5.48. The second part would be implied by Conjecture 5.67 and Proposition 5.68.

Irreducible semimodule without neutral element

For the case that the finite simple additively idempotent semiring with absorbing greatest element possesses a finite idempotent irreducible semimodule without neu-

5.7. The remaining case

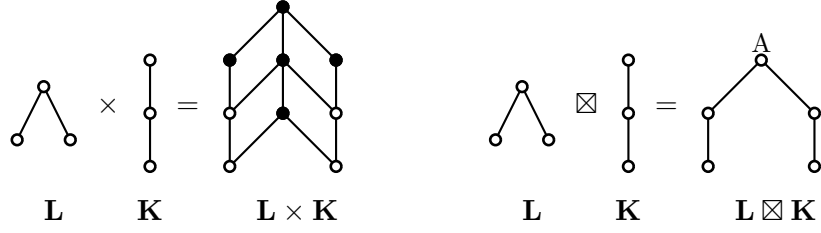


Figure 5.1: Left: The direct product of two semilattices. The black elements are the elements of the set A . Right: The product $\mathbf{L} \boxtimes \mathbf{K}$ of the same semilattices.

tral element and with join-reducible greatest element, we have a construction of semirings of join-morphisms of semilattices. In fact, we conjecture that this construction covers these semirings. We need some preparation for it.

Definition 5.72. Let $\mathbf{L} = (L, \leq)$ and $\mathbf{K} = (K, \leq)$ be finite semilattices and let $A := \{(x, y) \in L \times K \mid x = 1_{\mathbf{L}} \text{ or } y = 1_{\mathbf{K}}\}$. Then define

$$L \boxtimes K := L \times K / (\text{id}_{L \times K} \cup A \times A) \quad \text{and} \quad \mathbf{L} \boxtimes \mathbf{K} := (L \boxtimes K, \leq),$$

where $\{(a, b)\} \leq A$ and $\{(a, b)\} \leq \{(c, d)\}$ iff $a \leq c$ and $b \leq d$, for all $\{(a, b)\}, \{(c, d)\} \in L \boxtimes K \setminus \{A\}$.

Note that every equivalence class in $L \boxtimes K$, except A , has just one element, i.e. $L \boxtimes K = \{A\} \cup \{\{(a, b)\} \mid a \in L \setminus \{1_{\mathbf{L}}\}, b \in K \setminus \{1_{\mathbf{K}}\}\}$. See Figure 5.1 for an example.

Definition 5.73. Let $\mathbf{L} = (L, \leq)$ and $\mathbf{K} = (K, \leq)$ be finite semilattices and let $f \in \text{JM}_1(\mathbf{L})$ and $g \in \text{JM}_1(\mathbf{K})$. Then let $f \boxtimes g$ be the mapping in $\text{JM}_1(\mathbf{L} \boxtimes \mathbf{K})$ defined by

$$(f \boxtimes g)([x, y]) = [f(x), g(y)]$$

for every $(x, y) \in L \times K$, where $[x, y]$ denotes the class of (x, y) in $L \boxtimes K$.

Since $f \in \text{JM}_1(\mathbf{L})$ and $g \in \text{JM}_1(\mathbf{K})$, the mapping $f \boxtimes g$ is clearly well-defined. Note that for $f_1, f_2 \in \text{JM}_1(\mathbf{L})$ and $g_1, g_2 \in \text{JM}_1(\mathbf{K})$ the rules

$$\begin{aligned} (f_1 \boxtimes g_1) \vee (f_2 \boxtimes g_2) &= (f_1 \vee f_2) \boxtimes (g_1 \vee g_2) \quad \text{and} \\ (f_1 \boxtimes g_1) \circ (f_2 \boxtimes g_2) &= (f_1 \circ f_2) \boxtimes (g_1 \circ g_2) \end{aligned}$$

apply.

Let $\mathbf{K} = (K, \leq)$ be the semilattice with

$$K := \{1, \dots, n\} \cup \{\infty\} \quad \text{and} \quad \leq := \text{id}_K \cup (K \times \{\infty\}),$$

for some $n \in \mathbb{N}$; that is, different elements are comparable only if one equals ∞ . In this case, $\text{Aut}(\mathbf{K})$ consists of all bijective mappings $f : L \rightarrow L$ such that $f(\infty) = \infty$, and thus the group $(\text{Aut}(\mathbf{K}), \circ)$ is isomorphic to the symmetric group $\mathbf{S}(K \setminus \{\infty\})$. Any subgroup (S, \circ) of $(\text{Aut}(\mathbf{K}), \circ)$ acts in this sense faithfully on the set $K \setminus \{\infty\} = \{1, \dots, n\}$.

Construction 5.74. *Let $\mathbf{L} = (L, \leq)$ be a semilattice and let $\mathbf{K} := (K, \leq)$ be the semilattice, where $K = \{1, \dots, n\} \cup \{\infty\}$, $n \in \mathbb{N}$ and $\leq := \text{id}_K \cup (K \times \{\infty\})$. Furthermore, let (S, \circ) be a subgroup of $(\text{Aut}(\mathbf{K}), \circ)$ with $f \vee g = k_1$ for all $f, g \in S$ with $f \neq g$, let $\bar{S} := S \cup \{k_1\}$, and let (R, \vee, \circ) be a subsemiring of $(\text{JM}_1(\mathbf{L} \boxtimes \mathbf{K}), \vee, \circ)$ with*

$$\forall \varphi \in R \exists f \in \text{JM}_1(\mathbf{L}) \exists g \in \bar{S} : \varphi = f \boxtimes g, \quad (5.9)$$

$$\forall a \in L \setminus \{1_{\mathbf{L}}\} \forall b \in L \forall g \in \bar{S} : f_{a,b} \boxtimes g \in R, \quad (5.10)$$

$$\forall \varphi \in R \exists a \in L \setminus \{1_{\mathbf{L}}\} \exists b \in L \exists g \in \bar{S} : f_{a,b} \boxtimes g \leq \varphi. \quad (5.11)$$

If $|K| = 2$, then $\mathbf{L} \boxtimes \mathbf{K} \cong \mathbf{L}$ and (R, \vee, \circ) corresponds to a subsemiring (S, \vee, \circ) of $(\text{JM}_1(\mathbf{L}), \vee, \circ)$ that fulfils (5.1) and (5.2). If \mathbf{L} is no lattice and $1_{\mathbf{L}}$ is join-reducible, then (R, \vee, \circ) also possesses a finite idempotent irreducible R -semimodule that has no neutral element and whose greatest element is join-reducible. In fact, (L, \vee) is such a semimodule (see Proposition 5.48).

If $|L| = 2$, then $\mathbf{L} \boxtimes \mathbf{K} \cong \mathbf{K}$ and (R, \vee, \circ) belongs to a class of finite simple semirings with absorbing greatest element, which are also known. These semirings have been presented in the case of commutative semirings in [2] and for not necessarily commutative semirings in [45]: Let (G, \cdot) be a finite group and define $V(G) := G \cup \{\infty\}$. Extend the multiplication of G to $V(G)$ by the rule $x\infty = \infty x = \infty$ for every $x \in V(G)$ and define the addition on $V(G)$ by $x + x = x$ and $x + y = \infty$ for all $x, y \in V(G)$ with $x \neq y$. Then $(V(G), +, \cdot)$ is a finite simple additively idempotent semiring with absorbing greatest element and $(V(G), +)$ is a finite irreducible idempotent semimodule, which has no neutral element and its greatest element is join-reducible if $|G| > 1$.

Construction 5.74 is a new combination of those two types of semirings; it did not

5.7. The remaining case

appear in the literature before. As shown in the next proposition, these semirings are also simple.

Proposition 5.75. *Let everything as in Construction 5.74. Then (R, \vee, \circ) is a finite simple additively idempotent semiring with absorbing greatest element.*

Proof. (R, \vee, \circ) is clearly a finite additively idempotent semiring. Its greatest element is $k_{1_{\mathbf{L} \boxtimes \mathbf{K}}}$, which is obviously absorbing. Let \sim be a congruence on (R, \vee, \circ) with $\sim \neq \text{id}_R$, i.e. there exist $\varphi, \gamma \in R$ with $\varphi \neq \gamma$ and $\varphi \sim \gamma$. By (5.9), there exist $\varphi_1, \gamma_1 \in \text{JM}_1(\mathbf{L})$, $\varphi_2, \gamma_2 \in \bar{S}$ with $\varphi = \varphi_1 \boxtimes \varphi_2$ and $\gamma = \gamma_1 \boxtimes \gamma_2$. Without loss of generality we can assume $\varphi \not\sim \gamma$. It follows that $\varphi \neq k_{1_{\mathbf{L} \boxtimes \mathbf{K}}}$. Choose $\lambda \in R \setminus \{k_{1_{\mathbf{L} \boxtimes \mathbf{K}}}\}$ arbitrarily. We will show that $\lambda \sim k_{1_{\mathbf{L} \boxtimes \mathbf{K}}}$ holds. From this it follows that $\sim = R \times R$ and therefore the simplicity.

Again there exist $\lambda_1 \in \text{JM}_1(\mathbf{L})$, $\lambda_2 \in \bar{S}$ with $\lambda = \lambda_1 \boxtimes \lambda_2$. By (5.11), there exists $a \in L \setminus \{1_{\mathbf{L}}\}$, $b \in L$ and $g \in \bar{S}$ such that $f_{a,b} \boxtimes g \leq \lambda_1 \boxtimes \lambda_2$. We have $\lambda_2 \neq k_{1_{\mathbf{K}}}$ and thus $\lambda_2(y) \neq 1_{\mathbf{K}}$ for some $y \in K$. For all $x \in L$, $[f_{a,b}(x), g(y)] \leq [\lambda_1(x), \lambda_2(y)]$ follows, so that $f_{a,b}(x) \leq \lambda_1(x)$; hence $f_{a,b} \leq \lambda_1$. Because of $\varphi \neq k_{1_{\mathbf{L} \boxtimes \mathbf{K}}}$, it holds that $\varphi_1 \neq k_{1_{\mathbf{L}}}$ and thus there exists an $x \in L$ with $c := \varphi_1(x) \neq 1_{\mathbf{L}}$. It follows that $f_{c,b} \circ \varphi_1 \circ f_{a,x} \vee \lambda_1 = f_{a,b} \vee \lambda_1 = \lambda_1$. It also must hold that $\varphi_2, \lambda_2 \neq k_{1_{\mathbf{K}}}$, i.e. $\varphi_2, \lambda_2 \in S$. Since (S, \circ) is a group, there exists a $v \in S$ with $\varphi_2 \circ v = \lambda_2$. We make a distinction of cases.

Case 1: $\gamma = k_{1_{\mathbf{L} \boxtimes \mathbf{K}}}$. We have

$$\begin{aligned} & (f_{c,b} \boxtimes \text{id}_K) \circ (\varphi_1 \boxtimes \varphi_2) \circ (f_{a,x} \boxtimes v) \vee (\lambda_1 \boxtimes \lambda_2) \\ &= (f_{c,b} \circ \varphi_1 \circ f_{a,x} \vee \lambda_1) \boxtimes (\text{id}_K \circ \varphi_2 \circ v \vee \lambda_2) = (\lambda_1 \boxtimes \lambda_2) = \lambda \end{aligned}$$

and

$$(f_{c,b} \boxtimes \text{id}_K) \circ (\gamma_1 \boxtimes \gamma_2) \circ (f_{a,x} \boxtimes v) \vee (\lambda_1 \boxtimes \lambda_2) = k_{1_{\mathbf{L} \boxtimes \mathbf{K}}} \vee (\lambda_1 \boxtimes \lambda_2) = k_{1_{\mathbf{L} \boxtimes \mathbf{K}}}$$

and because of $\varphi \sim \gamma$ it follows that $\lambda \sim k_{1_{\mathbf{L} \boxtimes \mathbf{K}}}$.

Case 2: $\gamma \neq k_{1_{\mathbf{L} \boxtimes \mathbf{K}}}$ and $\varphi_1 = \gamma_1$. It must hold that $\varphi_2 \neq \gamma_2$ and it follows that $\lambda_2 = \varphi_2 \circ v \neq \gamma_2 \circ v$, i.e. $\lambda_2 \vee \gamma_2 \circ v = k_{1_{\mathbf{K}}}$. As in the previous case one can show the equality $(f_{c,b} \boxtimes \text{id}_K) \circ (\varphi_1 \boxtimes \varphi_2) \circ (f_{a,x} \boxtimes v) \vee (\lambda_1 \boxtimes \lambda_2) = \lambda$. Additionally it holds in

this case that

$$\begin{aligned}
 & (f_{c,b} \boxtimes \text{id}_K) \circ (\gamma_1 \boxtimes \gamma_2) \circ (f_{a,x} \boxtimes v) \vee (\lambda_1 \boxtimes \lambda_2) \\
 &= (f_{c,b} \circ \gamma_1 \circ f_{a,x} \vee \lambda_1) \boxtimes (\text{id}_K \circ \gamma_2 \circ v \vee \lambda_2) \\
 &= (f_{c,b} \circ \gamma_1 \circ f_{a,x} \vee \lambda_1) \boxtimes k_{1_K} = k_{1_{L \boxtimes K}}
 \end{aligned}$$

and we find again that $\lambda \sim k_{1_{L \boxtimes K}}$.

Case 3: $\gamma \neq k_{1_{L \boxtimes K}}$ and $\varphi_1 \not\leq \gamma_1$. There exists a $y \in L$ with $\varphi_1(y) \not\leq \gamma_1(y) =: d$. Furthermore, $\gamma_2 \neq k_{1_K}$ holds, i.e. $\gamma_2 \in S$. Consequently, there exists a $w \in S$ with $\gamma_2 \circ w = \lambda_2$. It follows that

$$\begin{aligned}
 & (f_{d,b} \boxtimes \text{id}_K) \circ (\varphi_1 \boxtimes \varphi_2) \circ (f_{a,y} \boxtimes w) \vee (\lambda_1 \boxtimes \lambda_2) \\
 &= (f_{d,b} \circ \varphi_1 \circ f_{a,y} \vee \lambda_1) \boxtimes (\text{id}_K \circ \varphi_2 \circ w \vee \lambda_2) \\
 &= (k_{1_L} \vee \lambda_1) \boxtimes (\varphi_2 \circ w \vee \lambda_2) = k_{1_{L \boxtimes K}}.
 \end{aligned}$$

Moreover, we have

$$\begin{aligned}
 & (f_{d,b} \boxtimes \text{id}_K) \circ (\gamma_1 \boxtimes \gamma_2) \circ (f_{a,y} \boxtimes w) \vee (\lambda_1 \boxtimes \lambda_2) \\
 &= (f_{d,b} \circ \gamma_1 \circ f_{a,y} \vee \lambda_1) \boxtimes (\text{id}_K \circ \gamma_2 \circ w \vee \lambda_2) \\
 &= (f_{a,b} \vee \lambda_1) \boxtimes (\lambda_2 \vee \lambda_2) = \lambda
 \end{aligned}$$

and we find again that $\lambda \sim k_{1_{L \boxtimes K}}$.

Case 4: $\gamma \neq k_{1_{L \boxtimes K}}$ and $\varphi_1 \not\leq \gamma_1$. In this case there exists a $z \in L$ with $e := \varphi_1(z) \not\leq \gamma_1(z)$. Analogously to the previous case, one can show that $(f_{e,b} \boxtimes \text{id}_K) \circ (\varphi_1 \boxtimes \varphi_2) \circ (f_{a,z} \boxtimes v) \vee (\lambda_1 \boxtimes \lambda_2) = \lambda$ and $(f_{e,b} \boxtimes \text{id}_K) \circ (\gamma_1 \boxtimes \gamma_2) \circ (f_{a,z} \boxtimes v) \vee (\lambda_1 \boxtimes \lambda_2) = k_{1_{L \boxtimes K}}$ holds, and we find again $\lambda \sim k_{1_{L \boxtimes K}}$. \square

Proposition 5.76. *Let everything as in Construction 5.74. Additionally, let $|S| = n > 1$ or let \mathbf{L} be no lattice and $1_{\mathbf{L}}$ join-reducible. Then $(L \boxtimes K, \vee)$ is a finite idempotent irreducible R -semimodule without neutral element and its greatest element is join-reducible.*

Proof. $(L \boxtimes K, \vee)$ is clearly a finite idempotent R -semimodule without neutral element and its greatest element is join-reducible. Moreover, it is an R -nonidentity semimodule and it fulfils $|R(L \boxtimes K)| > 1$.

Considering the action of the group (S, \circ) on the set $K \setminus \{\infty\} = \{1, \dots, n\}$, it follows from the conditions in Construction 5.74 that for every $x \in \{1, \dots, n\}$ the

5.7. The remaining case

orbit map $S \rightarrow \{1, \dots, n\}$, $g \mapsto g(x)$ is injective; now, since $|S| = n$, this map is even bijective.

Let (M, \vee) be an R -subsemimodule of $(L \boxtimes K, \vee)$ with $|M| > 1$, i.e. there exist $[a, b] \in M$ with $[a, b] \neq A$. Hence, $a \neq 1_{\mathbf{L}}$ and $b \neq 1_{\mathbf{K}}$. Choose $[c, d] \in L \boxtimes K$ arbitrarily. Since the orbit map $g \mapsto g(b)$ is bijective, it follows that there exists a $g \in S$ with $g(b) = d$. It follows that $(f_{a,c} \boxtimes g)([a, b]) = [c, d]$. Thus, $M = R[a, b] = L \boxtimes K$ and $(L \boxtimes K, \vee)$ is consequently sub-irreducible.

Let \sim be a semimodule congruence on $(L \boxtimes K, \vee)$ with $\sim \neq \text{id}$, i.e. there exist $[a, b], [c, d] \in L \boxtimes K$ with $[a, b] \sim [c, d]$ and $[a, b] \neq [c, d]$. Let $e \in L$, $f \in K$. We will show that $[e, f] \sim A$ holds. From this it follows that $\sim = L \boxtimes K \times L \boxtimes K$, i.e. $(L \boxtimes K, \vee)$ is quotient-irreducible.

If $[a, b] = A$, then $[c, d] \neq A$, i.e. $d \neq 1_{\mathbf{K}}$. Hence, there exists a $g \in S$ with $g(d) = f$ and it follows that $A = (f_{c,e} \boxtimes g)(A) \sim (f_{c,e} \boxtimes g)([c, d]) = [e, f]$. The case $[c, d] = A$ works analogously. So from now on we can consider the case that $[a, b], [c, d] \neq A$. If $a = c$, then $b \neq d$ holds and it follows that $[a, b] = [a, b] \vee [a, b] \sim [c, d] \vee [a, b] = [a, 1_{\mathbf{K}}] = A$. We find $A \sim [e, f]$ as before. Now consider the case $a \not\leq c$. There exists an $h \in S$ with $h(b) = f$ and it follows that $[e, f] = (f_{a,e} \boxtimes h)([a, b]) \sim (f_{a,e} \boxtimes h)([c, d]) = [1_{\mathbf{L}}, h(d)] = A$. The case $a \not\leq c$ works analogously. Hence, $(L \boxtimes K, \vee)$ is irreducible. \square

Corollary 5.77. *Let everything as in Construction 5.74. Additionally, let $|S| > 1$ or let \mathbf{L} be no lattice and $1_{\mathbf{L}}$ join-reducible. Then (R, \vee, \circ) is a finite simple additively idempotent semiring with absorbing greatest element, which possesses a finite idempotent irreducible semimodule without neutral element and whose greatest element is join-reducible.*

We computed all finite simple additively idempotent semirings with cardinality at most 10. Among these semirings, every finite simple additively idempotent semiring with absorbing greatest element that possesses a finite idempotent irreducible semimodule that has no neutral element and whose greatest element is join-reducible is isomorphic to a semiring in Corollary 5.77. For this reason, we state the following conjecture.

Conjecture 5.78. *Let (R, \vee, \circ) be a finite simple additively idempotent semiring with absorbing greatest element that possesses a finite idempotent irreducible semimodule without neutral element and whose greatest element is join-reducible. Then (R, \vee, \circ) is isomorphic to a semiring in Corollary 5.77.*

Despite that we could not complete the classification of finite simple semirings, we believe that it is still possible to complete the classification by characterising finite simple additively idempotent semirings in terms of join-morphisms of semilattices. Indeed, it does not seem to be out of reach to prove Conjecture 5.71 by proving Conjecture 5.67. Also a proof of Conjecture 5.78 may be attainable. Nevertheless, other approaches that we did not consider yet might be more promising.

Bibliography

- [1] H.-J. Bandelt: *Tight Residuated Mappings and d -Extensions*, 29. Universal Algebra, Esztergom (Hungary), Coll. Math. Soc. János Bolyai, 1977, pp. 61–72
- [2] R. El Bashir, J. Hurt, A. Jančařík, T. Kepka: *Simple Commutative Semirings*, Journal of Algebra, Vol. 236, No. 1, 2001, pp. 277–306
- [3] R. El Bashir, T. Kepka: *Congruence-Simple Semirings*, Semigroup Forum, Vol. 75, No. 3, 2007, pp. 588–608
- [4] G. Birkhoff: *Lattice Theory*, 3rd ed., Amer. Math. Soc., Providence, 1967
- [5] T. S. Blyth: *Lattices and Ordered Algebraic Structures*, Springer, London, 2005
- [6] T. S. Blyth: *Matrices Over Ordered Algebraic Structures*, Journal London Math. Soc., Vol. 39, No. 1, 1964, pp. 427–432
- [7] T. S. Blyth, M. F. Janowitz: *Residuation theory*, Pergamon Press, Oxford, 1972
- [8] S. Burris, H. P. Sankappanavar: *A Course in Universal Algebra*, Springer, New York, 1981
- [9] K. Denecke, M. Erné, S. L. Wismath: *Galois Connections and Applications*, Kluwer, Dordrecht, 2004
- [10] W. Diffie, M. E. Hellman: *New Directions in Cryptography*, IEEE Trans. Inform. Theory, Vol. 22, No. 6, 1976, pp. 644–654
- [11] D. Dolžan, P. Oblak: *Invertible and nilpotent matrices over antirings*, Linear Algebra Appl., Vol. 430, 2009, pp. 271–278
- [12] F. Domenach, B. Leclerc: *Biclosed Binary Relations and Galois Connections*, Order, Vol. 18, No. 1, 2001, pp. 89–104
- [13] M. Erné: *Adjunctions and Galois Connections: Origins, History and Development*, In: Galois Connections and Applications, Kluwer, Dordrecht, 2004, pp. 1–138
- [14] M. Erné, J. Kosłowski, A. Melton, G. E. Strecker: *A Primer on Galois Connections*, Annals of the New York Academy of Sciences, Vol. 704, 1993, pp. 103–125

BIBLIOGRAPHY

- [15] B. Ganter: *Relational Galois Connections*, Lecture Notes in Computer Science, Springer, Berlin, Vol. 4390, 2007, pp. 1–17
- [16] B. Ganter, G. Stumme, R. Wille: *Formal Concept Analysis - Foundations and Applications*, Lecture Notes in Computer Science 3626, Springer, 2005
- [17] B. Ganter, R. Wille: *Formal Concept Analysis - Mathematical Foundations*, Springer, Berlin, 1999
- [18] Y. Give'on: *Lattice Matrices*, Information and Control, Vol. 7, No. 4, 1964, pp. 477–484
- [19] K. Głazek: *A Guide to the Literature on Semirings and their Applications in Mathematics and Information Sciences*, Kluwer Academic Publishers, Dordrecht, 2002
- [20] J. S. Golan: *Semirings and their Applications*, Kluwer Academic Publishers, Dordrecht, 1999
- [21] O. Goldreich: *Foundations of Cryptography I - Basis Tools*, Cambridge University Press, 2001
- [22] O. Goldreich: *Foundations of Cryptography II - Basis Applications*, Cambridge University Press, 2004
- [23] G. Grätzer: *General Lattice Theory*, Birkhäuser Verlag, Basel, Boston, Berlin, 1998
- [24] G. Grätzer: *Universal Algebra*, 2nd ed., Springer, New York, 2008
- [25] E. Harzheim: *Ordered Sets*, Springer, 2005
- [26] J. Hashimoto: *On Direct Product Decomposition of Partially Ordered Sets*, Ann. of Math., Vol. 54, No. 2, 1951, pp. 315–318
- [27] U. Hebisch, H. J. Weinert: *Semirings - algebraic theory and applications in computer science*, World Scientific, Singapore, 1998
- [28] U. Hebisch, H. J. Weinert: *Semirings and Semifields*, In: Handbook of Algebra, Vol. 1, Elsevier, Amsterdam, 1996, pp. 425–462
- [29] J. Heitzig, J. Reinhold: *Counting Finite Lattices*, Algebra univers., Vol. 48, No. 1, 2002, pp. 43–53
- [30] J. Howie: *Fundamentals of Semigroup Theory*, Oxford Univ. Press, Oxford, 1995
- [31] J. Ježek, T. Kepka: *The Semiring of 1-Preserving Endomorphisms of a Semilattice*, Czechoslovak Mathematical Journal, Vol. 59, No. 2, 2009, pp. 999–1003

BIBLIOGRAPHY

- [32] J. Ježek, T. Kepka, M. Maróti: *The endomorphism semiring of a semilattice*, Semigroup Forum, Vol. 78, No. 1, 2009, pp. 21–26
- [33] J. Katz, Y. Lindell: *Introduction to Modern Cryptography*, Chapman & Hall/CRC, 2007
- [34] A. Kendziorra, S. E. Schmidt: *The Application of a Characterization of Adjunctions*, accepted for J. Algebra Appl., 2012
- [35] A. Kendziorra, S. E. Schmidt, J. Zumbrägel: *Invertible matrices over finite additively idempotent semirings*, Preprint, [arXiv:1112.5990v1](https://arxiv.org/abs/1112.5990v1), 2011
- [36] A. Kendziorra, J. Zumbrägel: *Finite simple additively idempotent semirings*, Preprint, [arXiv:1201.0272v1](https://arxiv.org/abs/1201.0272v1), 2011
- [37] M. Krötzsch, P. Hitzler, G.-Q. Zhang: *Morphisms in Context*, Proceedings of the 13th International Conference on Conceptual Structures (ICCS-05), 2005, pp. 223–237
- [38] M. Krötzsch, G. Malik: *The Tensor Product as a Lattice of Regular Galois Connections*, Lecture Notes in Computer Science, Springer, Berlin, Vol. 3874, 2006, pp. 89–104
- [39] R. D. Luce: *A Note on Boolean Matrix Theory*, Proc. Amer. Math. Soc., Vol. 3, No. 3, 1952, pp. 382–388
- [40] U. M. Maurer: *Towards the Equivalence of Breaking the Diffie-Hellman Protocol and Computing Discrete Logarithms*, Advances in cryptology - Crypto '94, Vol. 839, 1994, pp. 271–281
- [41] G. Maze: *Algebraic methods for constructing one-way trapdoor functions*, Ph.D. thesis, University of Notre Dame, 2003, available at <http://user.math.uzh.ch/maze/>
- [42] G. Maze, C. Monico, J. Rosenthal: *Public key cryptography based on semigroup actions*, Adv. Math. Commun., Vol. 1, No. 4, 2007, pp. 489–507
- [43] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone: *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1997
- [44] S. S. Mitchell, P. B. Fenoglio: *Congruence-free commutative semirings*, Semigroup Forum, Vol. 37, No. 1, 1988, pp. 79–91
- [45] C. Monico: *On finite congruence-simple semirings*, J. Algebra, Vol. 271, No. 2, 2004, pp. 846–854
- [46] C. Monico: *Semirings and Semigroup Actions in Public-Key Cryptography*, Ph.D. thesis, University of Notre Dame, 2002, available at <http://user.math.uzh.ch/rosenthal/>

BIBLIOGRAPHY

- [47] O. Ore: *Galois Connexions*, Trans. Amer. Math. Soc., Vol. 55, No. 3, 1944, pp. 493–513
- [48] G. N. Raney: *Tight Galois Connections and Complete Distributivity*, Trans. Amer. Math. Soc., Vol. 97, No. 3, 1960, pp. 418–426
- [49] D. E. Rutherford: *Inverses of Boolean Matrices*, Proc. Glasgow Math. Assoc., Vol. 6, No. 1, 1963, pp. 49–53
- [50] J. Schmidt: *Beiträge zur Filtertheorie. II*, Mathematische Nachrichten, Vol. 10, 1953, pp. 197–232
- [51] E. A. Schreiner: *Tight Residuated Mappings*, Proc. Univ. of Houston Lattice Theory Conf., Houston, 1973, pp. 519–530
- [52] B. S. W. Schröder: *Ordered Sets - An Introduction*, Birkhäuser, Boston, 2003
- [53] Z. Shmueli: *The Structure of Galois Connections*, Pacific Journal of Mathematics, Vol. 54, No. 2, 1974, pp. 209–225
- [54] R. Steinwandt, A. S. Corona: *Cryptanalysis of a 2-Party Key Establishment Based on a Semigroup Action Problem*, Adv. Math. Commun., Vol. 5, No. 1, 2011, pp. 87–92
- [55] Y. Tan: *On invertible matrices over antirings*, Linear Algebra Appl., Vol. 423, 2007, pp. 428–444
- [56] H. S. Vandiver: *Note on a simple type of algebra in which the cancellation law of addition does not hold*, Bull. Amer. Math. Soc., Vol 40, No. 4, 1934, pp. 914–920
- [57] M. Ward: *The Closure Operators of a Lattice*, Ann. of Math., Vol. 43, No. 2, 1942, pp. 191–196
- [58] J. H. M. Wedderburn: *Boolean Linear Associative Algebra*, Ann. of Math., Vol. 35, No. 1, 1934, pp. 185–194
- [59] S. Yevtushenko: *Computing and Visualizing Concept Lattices*, Ph.D thesis, Technische Universität Darmstadt, 2004, available at <http://tuprints.ulb.tu-darmstadt.de/>
- [60] C.-K. Zhao: *Inverses of L-Fuzzy Matrices*, Fuzzy Sets and Systems, Vol. 34, No. 1, 1990, pp. 103–116
- [61] J. Zumbrägel: *Classification of finite congruence-simple semirings with zero*, J. Algebra Appl., Vol. 7, No. 3, 2008, pp. 363–377
- [62] J. Zumbrägel: *Public-Key Cryptography Based on Simple Semirings*, Ph.D. thesis, Universität Zürich, 2008, available at <http://shannoninstitute.ucd.ie/~jzumbr/>

Symbols

| | |
|---|--|
| $0_{\mathbf{P}}$, 5 | $\text{Bo}(\mathbb{K}, \mathbb{L}), \text{Bo}(\mathbb{K}), 30$ |
| 1_* , 95 | $\text{CoAt}(\mathbf{L}), 94$ |
| $1_{\mathbf{P}}$, 5 | $\text{End}(\mathbf{A}), 3$ |
| $<$, 5 | $\text{Ext}(\mathbb{K}), 29$ |
| A', A^I , 28 | $\text{Gal}(\mathbf{P}, \mathbf{Q}), 27$ |
| A^R , 30 | $\text{Hom}(\mathbf{A}, \mathbf{B}), 3$ |
| $C(\mathbf{P}), 9$ | $\text{Int}(\mathbb{K}), 29$ |
| $C[M]$, 17, 68 | $\text{JM}_1(\mathbf{L}), 84$ |
| $C[x]$, 17 | $\text{JM}(\mathbf{L}, \mathbf{K}), \text{JM}(\mathbf{L}), 8$ |
| $E(\mathbf{L}), 27$ | $\text{Mat}_{I \times I}(R), 11$ |
| $J(\mathbf{L}), 6$ | $\text{Mat}_{n \times n}(R), 11$ |
| $K(\mathbf{P}), 9$ | $\text{Min}(P, \leq), 81$ |
| $L \boxtimes K, \mathbf{L} \boxtimes \mathbf{K}, 101$ | $\text{MinB}_n, 37$ |
| $L^\#, \mathbf{L}^\#, 98$ | $\text{MinE}_n, 37$ |
| $L_+, \mathbf{L}_+, 98$ | $\text{MinR}_n, 37$ |
| $L_-, \mathbf{L}_-, 86$ | $\text{Rd}(\mathbf{L}), 86$ |
| $M(\mathbf{L}), 6$ | $\text{Res}_0(\mathbf{L}), 84$ |
| RN , 70 | $\text{Res}_1(\mathbf{L}), 84$ |
| R_φ , 31 | $\text{Res}_{0,1}(\mathbf{L}), 84$ |
| Ra , 70 | $\text{Res}(\mathbf{P}, \mathbf{Q}), \text{Res}(\mathbf{P}), 8$ |
| S^+ , 86 | $\text{Res}(\mathbb{K}, \mathbb{L}), \text{Res}(\mathbb{K}), 31$ |
| $\text{Adj}(\mathbf{P}, \mathbf{Q}), 27$ | $\text{Sm}(\mathbf{P}, \mathbf{Q}), 42$ |
| $\text{Adj}(\mathbb{K}, \mathbb{L}), 31$ | $\Theta_L \times \Theta_K, 57$ |
| $\text{Aut}(\mathbf{A}), 3$ | $\mathbf{A}/\sim, 4$ |
| $\text{Aut}(\mathbf{P}), 8$ | $\mathbf{A}_{\mathbf{P}}, 44$ |

| | |
|---|-------------------------------------|
| \mathbf{L}^d , 85 | $f \circ^d g$, 85 |
| \mathbf{M}_2 , 50 | f^+ , 8 |
| \mathbf{P}^d , 5 | $f^{\mathbf{A}}$, 2 |
| \vee, \wedge , 5 | $f_{a,b}$, 83 |
| \circ^d , 33 | g', g^I , 29 |
| $[x]$, 3 | k_a , 83 |
| $[x] \sim$, 3 | $p(m)$, 17 |
| $\mathbb{K}(\mathbf{L})$, 29 | $r_{a,b}$, 80 |
| $\mathbb{K} \times \mathbb{L}$, 38 | x^R , 30 |
| \mathbb{K}^d , 40 | $x_{\downarrow}, x^{\uparrow}$, 75 |
| $\mathfrak{B}(\mathbb{K})$, 29 | |
| $\mathfrak{P}(G \times N), \underline{\mathfrak{P}}(G \times N)$, 32 | |
| \geq , 5 | |
| inf, 5 | |
| $\infty, \infty_M, \infty_R$, 72 | |
| ker(φ), 4 | |
| \leq , 5 | |
| ∇ , 38 | |
| \sim_a , 73 | |
| sup, 5 | |
| $\underline{\mathfrak{B}}(\mathbb{K})$, 29 | |
| $\varphi_{\mathbf{P}}$, 42 | |
| φ_R, φ_R^+ , 31 | |
| \vee, \wedge , 5 | |
| $a.x$, 15 | |
| $e_{a,b}$, 12, 13 | |
| $f \boxtimes g$, 101 | |

Index

- \vee -irreducible, 7
- \wedge -irreducible, 7
- \mathcal{F} -algebra, 2
- \vee -morphism, 8
 - complete, 9
- \vee -semilattice, 5
- \wedge -morphism, 9
 - complete, 9
- \wedge -semilattice, 5
- n -ary, 2
- n -ary operation, 2

- absorbing, 69
 - left, 68
 - right, 68
- absorption laws, 7
- addition, 10
- adjunction, 26
 - tight, 27
- algebra, 2
 - irreducible, 56
 - nontrivial, 56
 - quotient, 4
 - simple, 4
 - trivial, 56
- arity, 2
- attribute concept, 29
- authentication, 14
- automorphism
 - algebra, 3
 - order, 8

- base set, 2
- basic theorem on concept lattices, 29
- biclosed relations, 35
- bond, 30
 - dual, 38
- bound
 - lower, 5
 - upper, 5
- bounded, 48

- canonical context, 29
- centre, 16
- chain, 48
- clarified, 29
- closure operator, 9
- closure system, 9
- coatom, 94
- commutative, 10
- complete \vee -morphism, 9
- complete \wedge -morphism, 9
- complete join-irreducible, 7
- complete join-morphism, 9
- complete lattice, 6
- complete meet-irreducible, 7
- complete meet-morphism, 9
- complete relation, 3
- concept
 - attribute, 29
 - object, 29
- concept lattice, 29
 - basic theorem, 29
- confidentiality, 14
- congruence, 3
 - non-total, 3
 - semimodule, 70
 - semiring, 11
- connected, 57
- constant, 71

- data integrity, 14
- decreasing, 9
- dense, 12, 13
- Diffie-Hellman key agreement, 14
 - extended, 16
- Diffie-Hellman problem, 15
- Diffie-Hellman semigroup action problem, 16
- Diffie-Hellman with two sided matrix semiring action, 17
- direct decomposition, 56
 - maximal, 56

- direct product of formal contexts, 38
- discrete logarithm problem, 15
- distributive lattice, 7
- distributive laws, 10
- dual bond
 - regular, 39
- dual bond, 38
- dual formal context, 40
- dual order, 5
- dual order isomorphism, 8
- dual ordered set, 5
- duality principle for concept lattices, 40

- embedding, 8
- endomorphism, 3
- epimorphism, 3
- equality relation, 3
- equivalence class, 3
- extended Diffie-Hellman key agreement, 16
- extent, 29

- faithful, 71
 - of smallest cardinality, 71
- FCA, 28
- finitary, 2
- formal concept, 29
- formal concept analysis, 28
- formal context, 28
 - canonical, 29
 - clarified, 29
 - dual, 40
 - reduced, 29
- fundamental operation, 2

- Galois connection, 27
 - regular, 39
 - tight, 27
- generalised permutation matrix, 61
- Grail algorithm, 40
- greatest element
 - ordered set, 5
 - semimodule, 72
 - semiring, 69
- homomorphism, 3
 - natural, 4
- homomorphism theorem, 4
- horizontal sum, 48
- horizontal sum
 - of chains, 48

- idempotent, 9
- identity-semimodule, 71
- identity-subsemimodule, 71
- incidence relation, 28
- increasing, 9
- infimum, 5
- intent, 29
- irreducible
 - \bigvee -, 7
 - \bigwedge -, 7
 - algebra, 56
 - complete join, 7
 - complete meet, 7
 - join, 6
 - meet, 6
 - ordered set, 56
 - semimodule, 71
- isomorphic
 - algebras, 3
 - formal contexts, 29
 - ordered sets, 8
- isomorphism
 - algebra, 3
 - order, 8
- isotone, 8

- join, 5
- join-irreducible, 6
- join-morphism, 8
 - complete, 9
- join-reducible, 6
- join-semilattice, 5

- kernel, 4
- kernel operator, 9
- kernel system, 9

INDEX

- language, 2
- lattice, 6
 - complete, 6
 - distributive, 7
- least element, 5
- left absorbing, 68
- lower bound, 5
- lower neighbour, 5
- mapping
 - decreasing, 9
 - idempotent, 9
 - increasing, 9
 - isotone, 8
 - residuated, 8
- matrix, 11
 - generalised permutation, 61
 - monomial, 61
 - product, 11
 - semiring, 11
 - sum, 11
- maximal direct decomposition, 56
- meet, 5
- meet-irreducible, 6
- meet-morphism, 9
 - complete, 9
- meet-reducible, 6
- meet-semilattice, 5
- minimal, 81
- monomial matrix, 61
- morphism
 - \vee -, 8
 - \wedge -, 9
 - join, 8
 - meet, 9
- multiplication, 10
- natural homomorphism, 4
- neighbour
 - lower, 5
 - upper, 5
- non-total congruence, 3
- nonidentity-semimodule, 71
- nonidentity-subsemimodule, 71
- nontrivial
 - algebra, 56
 - ordered set, 56
- object concept, 29
- objects, 28
- one, 11
- operation, 2
- operation symbols, 2
- order, 5
 - dual, 5
- order automorphism, 8
- order embedding, 8
- order isomorphism, 8
 - dual, 8
- order relation, 5
- ordered set, 5
 - bounded, 48
 - connected, 57
 - irreducible, 56
 - nontrivial, 56
 - totally, 48
 - trivial, 56
- proper semiring, 10
- quotient algebra, 4
- quotient semimodule, 70
- quotient-irreducible, 71
- reduced, 29
- regular dual bond, 39
- regular Galois connection, 39
- residual, 8
- residuated, 8
 - tight, 27
- right absorbing, 68
- semigroup, 10
- semigroup action, 15
- semigroup action problem, 16
- semilattice, 5
 - \vee -, 5
 - \wedge -, 5
 - join, 5

- meet, 5
- semimodule, 70
 - congruence, 70
 - constant, 71
 - faithful, 71
 - identity, 71
 - irreducible, 71
 - nonidentity, 71
 - quotient, 70
 - quotient-irreducible, 71
 - sub-irreducible, 71
- semiring, 10
 - commutative, 10
 - proper, 10
 - simple, 12
- simple, 4
 - algebra, 4
 - semiring, 12
- smart triple, 42
- standard context, 29
- sub-irreducible, 71
- subalgebra, 3
- subdirect decomposition, 56
- sublattice, 7
- subsemimodule, 70
 - identity, 71
 - nonidentity, 71
- sum, 57
- supremum, 5
- symmetric encryption scheme, 14
- tight, 27
 - adjunction, 27
 - Galois connection, 27
 - residuated mapping, 27
- totally ordered set, 48
- trivial
 - algebra, 56
 - ordered set, 56
- upper bound, 5
- upper neighbour, 5
- vertical sum, 21
- zero, 11