
Università degli studi di Cagliari
Dipartimento di Pedagogia, Psicologia e Filosofia

Dottorato in Storia, Filosofia e Didattica delle Scienze
Coordinatore: Prof. Marco Giunti
Ciclo XXVIII
S.S.D: M-FIL 02, MAT 01

# Algebraic structures from quantum and fuzzy logics

Candidate:
Stefano Bonzio

Thesis advisor:
Prof. Francesco Paoli

Research supervisor:
Prof. Antonio Ledda

Esame finale anno accademico 2014/2015

# Contents

# Declaration

I declare that to the best of my knowledge the contents of this thesis are original and my work except where indicated otherwise.

# Acknowledgements

In first place I would like to thank my advisor, Francesco Paoli, for accepting me as his student and introducing me to the magical world of the algebras of logic and universal algebra. Despite his busy schedule and his many duties, he always found enough time to dedicate to me and to my work.

I would like to thank my research supervisor, Antonio Ledda, for his continuous support and encouragement. As a result, the major part of this thesis is joint work with him.

I cannot forget to thank Marisa Dalla Chiara, Paola Verrucchi and Roberto Giuntini. Although for different reasons, without their advises and encouragements, I would have, probably, never started a Ph.D program.

I learned much mathematics and life from many persons in the last few years. In particular I want to mention here Giuseppe Sergioli, Hector Freytes, Giuliano Vivanet and the colleagues of the Ph.D. program: Fabio Corpina, Simone Pinna, Daniela Sanna among the others.

A special thank goes to José Gil-Feréz, for being a very patient teacher, other than a brilliant mathematician.

A special mention has to be done also for Andrea Loi, as I found in him a very good master inside the court as well as an unexpected friend outside the court.

I thank all the members of the Department of Algebra and Geometry of the University of Olomouc for making my visit special. In particular, I thank Ivan Chajda who gave me all his trust, shared his experience and many of his own ideas with me.

The most important support I always got is from my parents and grandparents. Despite underlining the risks that every decision involves, Tino and Tiziana always left me the priceless freedom to choose my own path and supported me on my way.

The love of Luisa has been my force during this 'unexpected' journey to

Sardinia and has made my farewell to Tuscany sweeter.

I finally thank Roger Federer, for being still on court proving that perfection exists and, for this reason, we all can do better. As he claimed: “my best tennis is ahead!”.

# Abstract

This thesis concerns the wide research area of logic. In particular, the first part is devoted to analyze different kinds of relational systems (orthogonal and residuated), by investigating the properties of the algebras associated to them. The second part is focused on algebras of logic, in particular, the relationship between prominent quantum and fuzzy structures with certain semirings is proved. The last chapter concerns an application of group theory to some well known mathematical puzzles.

# Introduction

This thesis interests the wide research area of logic. Despite the distinction between philosophical and mathematical logic appears a senseless academical dispute, to most, it's a contrast an academic has to face anyway from time to time; it's proper to specify that this work is mainly focused on the latter, in the sense that most of the problems it deals with arise from the domain of mathematics. During the last few years I learned that working with logics actually means handling with algebras; that's the reason why my work is an attempt to exploit the domain of the algebras of logic. In particular, the thesis deals at least with two different subjects: *algebras associated to relational systems* and *algebras associated to quantum and fuzzy structures*.

Since logicians use algebras mostly as tools, they are always attracted by the study of some "new" algebras, namely algebras arising from settings apparently independent to logic tout court. Being relational systems the overriding concern of this work, we can consider them as the most prominent example of this tendency: relational systems are nothing but sets equipped with a binary relation, so it appears to be useful studying them via association with algebras.

In the first part of the thesis we introduce different notions of relational systems and study the properties of those algebras associated to such systems. In detail, the first chapter is dedicated to recall the mathematical background which is essential to develop the innovative ideas explained further.

In the second chapter we introduce the notions of orthogonal relational system and orthogonal groupoid, called *orthogroupoid*. We study the relation among the two and prove some algebraic properties of orthogroupoids, namely a decomposition theorem and the amalgamation property. The ideas contained in this part are based on [9], coauthored with I. Chajda and A. Ledda.

Chapter 3 deals with the notion of residuation in relational systems. Var-

ious classes of algebras are introduced to handle different kinds of relational systems, all of which share the property of possessing a residuated operation.

Although the algebras we deal with, in the first part, may not appear proper algebras of logic, they still can be seen as algebras originated "from" logic. Indeed the motivations behind the choice of such systems are remotely influenced by some trends of studies in logic. More precisely, orthogonal relational systems, studied in Chapter 2, are founded on a notion of orthogonality resembling orthogonality in quantum structures. On the other hand, residuated relational systems, studied in Chapter 3, are an attempt of generalizing the notion of *residuation*, a privileged and leading concept in some of the most interesting advances in logic over the last decades, a notion bridging the gap between the apparently different domains of algebraic logic and proof theory. So, even though, at first glance, some of the algebraic structures introduced may seem apparently lacking of interesting features, they satisfy properties common to many algebras of logic, as, for example, the amalgamation property, which is, in short, the algebraic counterpart for the logical notion of *interpolation*.

The second part of the thesis is properly focused on algebras of logic, as *quantum logics* and *fuzzy logics* are strictly related to algebras, in particular to orhtomodular lattices and MV algebras, respectively. In Chapter 4 we follows the idea, already exploited for Boolean algebras and MV algebras, of representing quantum structures as special cases of other most studied algebras, called *semirings*. We show, in particular, how to represent basic algebras and orthomodular lattices as *near semirings* and, as a corollary, we get an equivalence between MV algebras and certain semirings, which was already proven in [4]. The contents of this chapter are based on the ideas developed in [10], written with I. Chajda and A. Ledda.

The third and last part of the present work is an Appendix regarding an application of group theory to puzzles. We extend the group theoretical analysis of the Rubik's cube to its extensions, namely the two famous puzzles known as *Rubik's Revenge* and *Professor's cube*, and we establish the so called "first law of cubology" for them, that is, we state necessary and sufficient conditions for a cube to be solvable. These ideas are based on [11], coauthored with A. Loi and L. Peruzzi.

# Chapter 1

# Mathematical Background

## 1.1 Preliminaries

We assume the reader has a basic knowledge of the fundamental notions of set theory and abstract algebra. The approach to set theory is standard, and no particular set of axioms is required.

We use *classes* as well as *sets*. Roughly speaking, a class is a collection so large that subjecting it to the operations admissible for sets would lead to logical contradictions. We often use the term *family* in reference to set whose members are sets.

In dealing with sets we use the following standard notations: *membership* ($\in$), the *empty set* ($\emptyset$), *inclusion* ($\subseteq$), *proper inclusion* ($\subset$), *union* ($\cup$ and $\bigcup$), *intersection* ($\cap$ and $\bigcap$), *complement* ($-$), (*ordered*) *n-tuples* ($\langle x_1, ..., x_n \rangle$), *direct* (*Cartesian*) *products of sets* $\left( A \times B, \prod_{i \in I} A_i \right)$, *direct powers of a set* $\left( A^I \right)$. We shall not distinguish between (ordered) pairs and 2-tuples. We will denote the ordered pair of $x$ and $y$ by $\langle x, y \rangle$, and sometimes by $(x, y)$.

We now list a series of remarks introducing some notations and basic definitions.

1. The *power set* of a set $A$, the set of all subsets of $A$, will be denoted by $\mathcal{P}(A)$.

2. $A^n$ is the set of all $n$-tuples each of whose terms belongs to $A$.

3. As regards relations:

(a) An *n-ary relation* on a set $A$ is a subset of $A^n$.

(b) A 2-*ary relation* on a set $A$ is called a binary relation.

4. As regards functions:

(a) A *function* $f$ from a set $A$ to a set $B$ is a subset of $B \times A$ such that for each $a \in A$ there is exactly one $b \in B$ with $\langle b, a\rangle \in f$. Synonyms for functions are *mappings*, *maps* If $f$ is a function from $A$ to $B$ we write $f : A \to B$, and, instead of $\langle b, a\rangle \in f$, we write $f(a) = b$.

(b) If $f : A \to B$ and $g : B \to C$ are functions on $A \cup B \cup C$, we write $g \circ f$ (sometimes, $gf$) for their product.

(c) If $f : A \to B$, then $\ker(f)$, the *kernel* of $f$, is the binary relation $\{\langle a_0, a_1\rangle \in A^2 : f(a_0) = f(a_1)\}$. $f$ is called *injective*, or *one-to-one*, iff $\langle x, y\rangle \in \ker(f)$ implies $x = y$, for all $x, y \in A$.

(d) If $f : A \to B$, $X \subseteq A$ and $Y \subseteq B$, then $f(X) = \{f(x) : x \in X\}$ (the *f-image* of $X$) and $f^{-1}(Y) = \{x \in A : f(x) \in Y\}$ (the *f-inverse image* of $Y$). $f : A \to B$ is said to be *surjective*, or said that $f$ maps $A$ onto $B$, if $f(A) = B$.

(e) The function $f : A \to B$ is called *bijective* if it is both injective and surjective.

(f) If $f : A \to B$, then we say that the *domain* of $f$ is $A$, the *co-domain* of $f$ is $B$, and the *range* of $f$ is the set $f(A)$.

5. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ denote respectively the set of all the integer numbers, the set of all the rational numbers, the set of all the real number and the set of all complex numbers.

6. The *union* of a family $F$ of sets, $\bigcup F$, is defined by $x \in \bigcup F$ if $x \in B$, for some $B \in F$. The *intersection* of a family $F$ of sets, $\bigcap F$, is defined dually to the union, namely $x \in \bigcap F$ if $x \in B$, for all $B \in F$.

7. A *preorder* over a set $A$ is a binary relation $\preceq$ on $A$ such that:

(a) $\preceq$ is *reflexive* over $A$; i.e. $x \preceq x$, for any $x \in A$

(b) $\preceq$ is *transitive* over $A$; i.e. if $x \preceq y$ and $y \preceq z$ then $x \preceq z$, for all $x, y, z \in A$.

8. A *partial order* over a set $A$ is a binary relation $\leq$ on $A$ such that:

   (a) $\leq$ is a preorder over $A$.

   (b) $\leq$ is *anti-symmetric*; i.e. if $x \leq y$ and $y \leq x$ then $x = y$, for all $x, y \in A$.

   For orders, and pre-orders, we prefer to write $x \leq y$ instead of $\langle x, y\rangle \in \leq$. Given an order over a nonempty set $A$, the pair $\langle A, \leq\rangle$ is called a *partially ordered set*, *poset*, for short.

9. By *a chain in an ordered set* $\langle A, \leq\rangle$ is meant a set $B \subseteq A$ such that for all $x, y \in B$ either $x \leq y$ or $y \leq x$. An *upper bound* of $B$ is an element $u \in A$ for which $c \leq u$, for all $c \in B$.

10. A *linearly ordered set*, sometimes called a *chain*, is an ordered set $\langle A, \leq\rangle$ such that for all $x, y \in A$ either $x \leq y$ or $y \leq x$.

11. As regards equivalence relations:

    (a) An *equivalence relation* over a set $A$ is a binary relation $\sim$ on $A$ that is reflexive over $A$, transitive and *symmetric*; i.e. $x \sim y$ iff $y \sim x$.[1]

    (b) Given an equivalence relation over a set $A$ and for $x \in A$, the *equivalence class of* $x$ *modulo* $\sim$ is the set $x/\sim = \{y \in A : x \sim y\}$.

    (c) Given an equivalence relation $\sim$ over $A$, $A/\sim$ is a *partition* of $A$. That is, $A/\sim$ is a set of nonempty subsets of $A$, $A = \bigcup A/\sim$, and each pair of distinct sets $U$ and $V$ in $A/\sim$ are disjoint.

    (d) The set of all equivalence relations over $A$ is denoted by $Eq(A)$.

    (e) $\langle Eq(A), \subseteq\rangle$ is an ordered set having greatest lower bounds and least upper bounds for any subset of its elements. The greatest lower bound of $S \subseteq Eq(A)$ is $\bigcap S$. The least upper bound is the transitive closure of the $\bigcup S$.

12. The equality symbol $=$ is used in this thesis both to assert that two expressions name the same object and to express formal equations, which are sometimes indicated, in algebraic literature, by the symbol $\approx$.

[1] We adopt this notation instead of $\langle x, y\rangle \in \sim$ iff $\langle y, x\rangle \in \sim$.

## 1.2 Lattice theory and universal algebra

We start with some basic notions of universal algebra.

### 1.2.1 Algebras

First of all we introduce the definition of algebra.

For $A$ a nonempty set and $n$ a natural number, we define $A^0 = \{\emptyset\}$, and for $n > 0$, $A^n$ is the set of $n$-tuples elements from $A$. An *$n$-ary operation* (function) on $A$ is any function $f : A^n \to A$; $n$ is the *arity* (rank) of the function $f$. A finitary operation is an $n$-ary operation, for some $n$. The image of $\langle a_1, ..., a_n \rangle$ under an $n$-ary operation $f$, is denoted by $f(a_1, ..., a_n)$. An operation $f$ is said to be *nullary operation* if its arity is 0; it is completely determined by the image $f(\emptyset)$ in $A$ of the only element $\emptyset$ in $A^0$, and as such it is convenient to identify it with the element $f(\emptyset)$. Thus, a nullary operation is thought of as an element of $A$. An operation $f$ on $A$ is said to be *unary*, *binary*, if its arity is 1or 2, respectively.

A *language* (type) of algebras is a set $\mathcal{F}$ of function symbols such that a nonnegative integer $n$ is assigned to each member of $f$, and $f$ is said to be an *$n$-ary function symbol.*[2] The subset of all $n$-ary function symbols of $\mathcal{F}$ is denoted by $\mathcal{F}_n$.

For $\mathcal{F}$ a given language of algebras, an *algebra* $\mathbf{A}$ of *type* $\mathcal{F}$ is an ordered pair $\langle A, F \rangle$ where $A$ is a nonempty set and $F$ is a family of finitary operations on $A$, indexed by the language $\mathcal{F}$ such that in correspondence with each $n$-ary function symbol $f \in \mathcal{F}$ there is an $n$-ary operation $f^{\mathbf{A}}$ on $A$. The set $A$ is called the *universe* of $\mathbf{A} = \langle A, F \rangle$ and the $f^{\mathbf{A}}$'s are called the *fundamental operations* of $\mathbf{A}$. If $F$ is finite, say $\mathcal{F} = \{f_1, ..., f_n\}$, we often write $\langle A, f_1, ..., f_n \rangle$ for $\langle A, F \rangle$.

An algebra $\mathbf{A}$ is said *finite* if the cardinality of $A$, $|A|$, is finite, and trivial if $|A| = 1$.

Well known examples of algebras are listed below:

**Example 1.1.** A *groupoid* $\mathbf{G}$ is an algebra equipped only with a binary operation, i.e. it is an algebra of type $\langle 2 \rangle$.

[2] In this thesis, where no danger of confusion is impending, we will sometimes denote the type of a given algebra with lowercase greek letters.

**Example 1.2.** A *group* **G** is an algebra $\langle G, \cdot, ^{-1}, 1\rangle$, of type $\langle 2, 1, 0\rangle$ which satisfies the following equations:

(G1) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,

(G2) $x \cdot 1 = 1 \cdot x = x$,

(G3) $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

The element 1 is usually referred to as the neutral element of **G**.
A group is said to be commutative (Abelian) if the following identity holds:

(G4) $x \cdot y = y \cdot x$.

**Example 1.3.** A *semigroup* is a groupoid $\langle G, \cdot\rangle$, where $\cdot$ is an associative operation, i.e. (G1) holds true. Furthermore, a semigroup is commutative if (G4) holds.

**Example 1.4.** A *monoid* is an algebra $\langle M, \cdot, 1\rangle$ of type $\langle 2, 1, 0\rangle$ satisfying (G1) and (G2). A monoid is *commutative* if it satisfies also (G4).

**Example 1.5.** A *ring* **R** is an algebra $\langle R, +, \cdot, -, 0\rangle$ of type $\langle 2, 2, 1, 0\rangle$, which satisfies the following conditions:

(R1) $\langle R, +, -, 0\rangle$ is a commutative group,

(R2) $\langle R, \cdot\rangle$ is a semigroup,

(R3) $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$,

(R4) $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

(R3) and (R4) are usually referred to as right and left-distributivity, respectively.

**Example 1.6.** A *lattice* **L** is an algebra $\langle L, \wedge, \vee\rangle$ of type $\langle 2, 2\rangle$, satisfying the following equations:

(L1) (a) $x \wedge x = x$;
(b) $x \vee x = x$, (idempotency)

(L2) (a) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$;
(b) $x \vee (y \vee z) = (x \vee y) \vee z$, (associativity)

(L3) (a) $x \wedge y = y \wedge x$;
(b) $x \vee y = y \vee x$, (commutativity)

(L4) (a) $x \wedge (x \vee y) = x$;
(b) $x \vee (x \wedge y) = x$. (absorption)

A lattice is said to be *distributive* if the following equations hold:

(L5) (a) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$;
(b) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

Actually only one equations among (L5)-(a), (b) is enough to define a distributive lattice, indeed it is folklore that in a lattice $\mathbf{L}$, (L5)-(a) holds if and only if (L5)-(b) does.
A lattice can be equivalently defined as a partially ordered set $\langle A, \leq \rangle$, in which any two arbitrary elements in $A$ have both a *supremum* (*join*) denoted by sup, and an *infimum* (*meet*) denoted by inf.
More precisely, if $\mathbf{L}$ is a lattice in the sense expressed in Example 1.6, then, by defining $x \leq y$ if and only if $x \wedge y = x$ (or, equivalently, $x \vee y = y$), one has that $\langle L, \leq \rangle$ is a lattice in the sense specified above. The order $\leq$ is called the *induced* order. Conversely, if $\langle L, \leq \rangle$ is a partially ordered set such that, inf and sup exist for any two arbitrary elements, then, defining $x \wedge y = \inf\{x, y\}$ and $x \vee y = \sup\{x, y\}$, one gets that the algebra $\langle L, \wedge, \vee \rangle$ is a lattice in the sense of Example 1.6. Furthermore it is not difficult to show that the maps used to establish the equivalent definitions of lattice are mutually inverse.

**Example 1.7.** A *bounded lattice* $\mathbf{L}$ is an algebra $\langle L, \wedge, \vee, 0, 1 \rangle$ of type $\langle 2, 2, 0, 0 \rangle$, satisfying the following conditions:

(BL1) $\langle L, \wedge, \vee \rangle$ is a lattice,

(BL2) $x \wedge 0 = 0$,

(BL3) $x \vee 1 = 1$.

(BL2) and (BL3) can be equivalently expressed by saying that the constants 1 and 0 are the top and the least element (respectively) with respect to the induced order $\leq$.

**Example 1.8.** A *Boolean algebra* $\mathbf{B}$ is an algebra $\langle B, \wedge, \vee, ', 0, 1 \rangle$ of type $\langle 2, 2, 1, 0, 0 \rangle$, satisfying the following conditions:

(BA1) $\langle B, \wedge, \vee, 0, 1\rangle$ is a bounded distributive lattice,

(BA2) $x \wedge x' = 0$;

(BA3) $x \vee x' = 1$;

(BA4) $(x \wedge y)' = x' \vee y'$, (De Morgan's law),

(BA5) $x'' = x$. (Law of double negation)

Other important kind of lattices are ortholattices and orthomodular lattices.

**Example 1.9.** An *ortholattice* **O** is an algebra $\langle O, \wedge, \vee, ', 0, 1\rangle$ of type $\langle 2, 2, 1, 0, 0\rangle$ satisfying the following conditions:

(O1) $\langle O, \wedge, \vee, 0, 1\rangle$ is a bounded lattice,

(O2) $x \wedge x' = 0$;

(O3) $x \vee x' = 1$;

(O4) $(x \wedge y)' = x' \vee y'$;

(O5) $x'' = x$.

It is easy to notice that every Boolean algebra is also an ortholattice.

**Example 1.10.** A *orthomodular lattice* **T** is an ortholattice which satisfies:

(OML) If $x \leq y$ then $x \vee (x' \wedge y) = y$.

The equation above is usually referred to as *orthomodular law* and can be equivalently expressed by the following identity

$$(x \vee y) \wedge (x \vee (x \vee y)') = x,$$

which, in turn, is equivalent to the dual form:

$$(x \wedge y) \vee (y \wedge (x \wedge y)') = y.$$

### 1.2.2 Fundamentals of lattice theory

Recalling the definition from Example 1.6, a lattice $\mathbf{L}$ may be approached as an algebra of type $\langle 2, 2\rangle$ or, equivalently, as a partial ordered set $\langle L, \leq\rangle$ admitting inf and sup for any pair of elements. Posets and lattices have the very useful characteristic that the can be drawn in pictures. Indeed, any (finite) poset can be associated univically to the so-called Hasse diagram, see [14] for details.

If a lattice is distributive, it also satisfies the *modular* law, i.e.

$$\text{If } \; x \leq y \; \text{ then } \; x \vee (y \wedge z) = y \wedge (x \vee z)\,.$$

We now list three useful criteria which allowing to characterize distributive, modular and orthomodular lattices.
It is easy to check that the lattice $\mathbf{N}_5$ depicted in Fig.1.1 is non-modular. Moreover it is the most typical example of non-modular lattice.

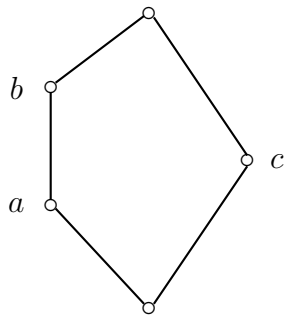



Figure 1.1: The Hasse diagram of the non-modular lattice $\mathbf{N}_5$.

**Theorem 1.1** (Dedekind)**.** *A lattice* $\mathbf{L}$ *is a non-modular lattice if and only if* $\mathbf{N}_5$ *can be embedded into* $\mathbf{L}$*.*

Exactly as $\mathbf{N}_5$ is the most prominent example of non-modular lattice, $\mathbf{M}_5$ (Fig. 1.2) plays the same role witnessing non-distributivity.

**Theorem 1.2** (Birkhoff)**.** *A lattice* $\mathbf{L}$ *is a non-distributive lattice if and only if* $\mathbf{M}_5$ *or* $\mathbf{N}_5$ *can be embedded into* $\mathbf{L}$*.*

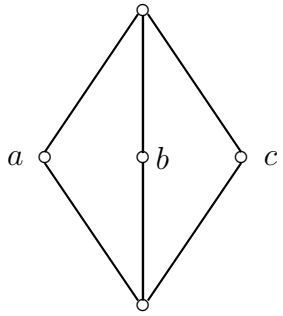



Figure 1.2: The Hasse diagram of the non-distributive lattice $\mathbf{M}_5$.

The disjunctive statement in Theorem 1.2 above is justified by the fact that every non-modular lattice is also non-distributive.

The property of an ortholattice to be non-orthomodular is established by the so-called "Benzene ring" (Fig. 1.3), whose name is taken from the chemical structure of Benzene.

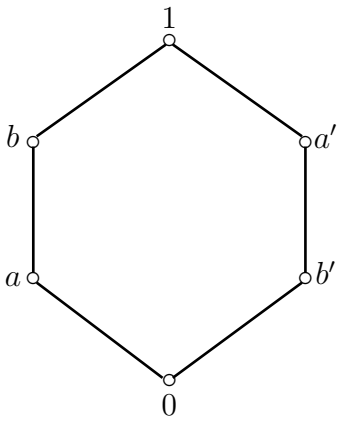



Figure 1.3: The Benzene ring, a typical example of non-orthomodular lattice.

**Theorem 1.3.** *An ortholattice* **OL** *is an orthomodular lattice if and only if it does not contain the "Benzene ring".*

Let us now introduce the notion of complete lattice.

A lattice $\mathbf{L}$ is *complete* if for every subset $A$ of $L$ both the *infimum* and the *supremum* element of $A$ exist in $L$. We will denote by $\bigwedge A$ and $\bigvee A$ the inf of $A$ and the sup of $A$, respectively. The following result states that it is enough to have only one among $\bigwedge A$ and $\bigvee A$ in order to get a complete lattice.

**Proposition 1.1.** *Let $P$ be a poset such that $\bigwedge A$ exists for every subset $A$, or such that $\bigvee A$ exists for every subset $A$. Then $P$ is a complete lattice.*

An example of complete lattice is the lattice of equivalence relations $Eq(A)$ on a given set $A$.

Let us now mention a key class of lattices: the class of algebraic lattices.

For a lattice $\mathbf{L}$, an element $a \in L$ is *compact* if whenever $\bigvee A$ exists and $a \leq \bigvee A$ for $A \subseteq L$, then $a \leq \bigvee B$ for some finite $B \subseteq A$. $\mathbf{L}$ is *compactly generated* iff every element in $L$ is the sup of compact elements. A lattice is *algebraic* if it is complete and compactly generated.

### 1.2.3 Subalgebras, quotients, direct and subdirect products

There are various ways to construct new algebras from given ones. Three of the very basic constructions are the formation of subalgebras, homomorphic images and direct products.

As a first step we provide the notion of subalgebra.

Let $\mathbf{A}$ and $\mathbf{B}$ be algebras of the same type. We say that $\mathbf{B}$ is a *subalgebra* of $\mathbf{A}$ if $B \subseteq A$ and every fundamental operation of $\mathbf{B}$ is the restriction of the corresponding operation of $\mathbf{A}$, i.e. for any function symbol $f$, $f^{\mathbf{B}}$ is $f^{\mathbf{A}}$ restricted to $B$. We will write $\mathbf{B} \leq \mathbf{A}$ if $\mathbf{B}$ is a subalgebra of $\mathbf{A}$. A subuniverse of $\mathbf{A}$ is a subset $B$ of $A$ closed under the fundamental operations of $\mathbf{A}$, that is: if $f$ is a fundamental $n$-ary operation of $\mathbf{A}$ and $a_1, ..., a_n \in B$, then we demand $f(a_1, ..., a_n) \in B$.

Clearly, if $\mathbf{B} \leq \mathbf{A}$ then $B$ is a subuniverse of $A$. Moreover note that if $\mathbf{A}$ has nullary operations, any of its subalgebras contains them as well.

We now introduce the notion of homomorphism.

Let $\mathbf{A}$ and $\mathbf{B}$ be algebras of the same type. A function $\alpha : \mathbf{A} \to \mathbf{B}$ is said to be an *homomorphism* if for any $n$-ary function symbol $f$ of $\mathcal{F}_{\mathbf{A}}$ and $a_1, ..., a_n \in \mathbf{A}$

$$\alpha(f(a_1, ..., a_n)) = f(\alpha(a_1), ..., \alpha(a_n)).$$

If, in addition, the mapping $\alpha$ is onto then $\mathbf{B}$ is said to be a *homomorphic image* of $\mathbf{A}$. $\alpha$ is called an *embedding* if is one-one ($\alpha$ is also called a monomorphism). Alternatively, we can often say that $\mathbf{A}$ can be embedded in $\mathbf{B}$. Futhermore $\alpha$ is an *isomorphism* if is an embedding and is onto. It is not difficult to check that the composition of homomorphisms is a homomorphism.

**Theorem 1.4.** *If $\alpha : \mathbf{A} \to \mathbf{B}$ is an embedding, then $\alpha(A)$ is a subuniverse of $\mathbf{B}$.*

The idea of homomorphism is strictly tied with the concepts of congruence and quotient algebra. As it is well known the notion of congruence provide an important meeting point between lattice theory and universal algebra.

Let $\mathbf{A}$ be an algebra of type $\mathcal{F}$ and $\theta$ an equivalence relation on $A$. We say that $\theta$ is a *congruence* if it satisfies the following *compatibility property*: for every $n$-ary function symbol $f \in \mathcal{F}$ and elements $a_i, b_i \in A$, if $(a_i, b_i) \in \theta$ for $1 \leq i \leq n$, then $(f(a_1, ..., a_n), f(b_1, ..., b_n)) \in \theta$.

In order to introduce an algebraic structure inherited from the algebra $\mathbf{A}$ on the set of equivalence classes $A/\theta$ the compatibility property is strictly needed. Henceforth the set of congruence relations of a given algebra $\mathbf{A}$ will be denoted by $Con(\mathbf{A})$.

Let $\mathbf{A}$ be an algebra of type $\mathcal{F}$ and $\theta$ a conguence relation on $A$. The quotient algebra of $\mathbf{A}$ by $\theta$, written $\mathbf{A}/\theta$, is the algebra whose universe is $A/\theta$ and whose fundamental operations satisfy:

$$f^{A/\theta}(a_1/\theta, ..., a_n/\theta) = f^A(a_1, ..., a_n)/\theta$$

where $a_1, ..., a_n \in A$ and $f$ is an $n$-ary function symbol in $\mathcal{F}$.

Clearly, the type of the quotient algebra $\mathbf{A}/\theta$ is the same of the algebra $\mathbf{A}$.

In what follows we will denote $\{(x, x) : x \in A\}$, the identity congruence, by $\Delta$, and the universal relation by $\nabla$.

If $\theta_1, \theta_2 \in Con(\mathbf{A})$ and $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$, we say that $\theta_1, \theta_2$ permute. $\mathbf{A}$ is *congruence-permutable* if for any $\theta_i, \theta_j \in Con(\mathbf{A})$ $\theta_i \circ \theta_j = \theta_j \circ \theta_i$.

A congruence $\theta \in Con(\mathbf{A})$ is a *factor congruence* if there exists a congruence $\theta^* \in Con(\mathbf{A})$ such that

$$\begin{aligned} \theta \cap \theta^* &= \Delta, \\ \theta \vee \theta^* &= \nabla, \\ \theta \circ \theta^* = \theta^* \circ \theta. & \end{aligned}$$

We call the pair $\theta$, $\theta^*$ a *pair of complementary factor congruences.*

Let us now recall some basic results regarding $Con(\mathbf{A})$.

**Theorem 1.5.** $\mathbf{Con}(\mathbf{A}) = \langle Con(\mathbf{A}), \subseteq \rangle$ *is a complete sublattice of* $\mathrm{Eq}(\mathbf{A}) = \langle Eq(\mathbf{A}), \subseteq \rangle$*, the lattice of equivalence relations on* $\mathbf{A}$*.*

The congruence lattice of $\mathbf{A}$, denoted by $\mathbf{Con}(\mathbf{A})$, is the lattice whose universe is $Con\,(\mathbf{A})$ and meets consist of intersections of congruences and joins of the generated congruences, namely the smallest congruences containing the given ones.

**Theorem 1.6.** *For an algebra* $\mathbf{A}$*,* $\mathbf{Con}(\mathbf{A})$ *is an algebraic lattice.*

An algebra $\mathbf{A}$ is *congruence-distributive* (congruence-modular) if $\mathbf{Con}(\mathbf{A})$ is a distributive (modular) lattice.

**Theorem 1.7.** *If* $\mathbf{A}$ *is congruence-permutable, then* $\mathbf{A}$ *is congruence-modular.*

An important example of congruence on a given algebra $\mathbf{A}$ is the kernel of a homomorphism, as stated in the next theorem.

**Theorem 1.8.** *Let* $\alpha : \mathbf{A} \to \mathbf{B}$ *be a homomorphism. Then* $\ker(\alpha)$ *is a congruence on* $\mathbf{A}$*.*

Let $\mathbf{A}$ be an algebra and $\theta \in Con(\mathbf{A})$. Then the map $\eta_\theta : \mathbf{A} \to \mathbf{A}/\theta$, defined by $\eta_\theta(a) = a/\theta$ is called the *natural map.* When there is no ambiguity we write simply $\eta$ instead of $\eta_\theta$.

**Theorem 1.9.** *Let* $\mathbf{A}$ *be an algebra and* $\theta \in \mathbf{Con}(\mathbf{A})$*. Then the natural map* $\eta : \mathbf{A} \to \mathbf{A}/\theta$ *is an onto homomorphism.*

Due to the Theorem 1.9, the natural map is usually referred to as the *natural homomorphism.* The following result establishes a connection between homomorphic images and quotient algebras and it is usually referred to as "First Isomorphism Theorem".

**Theorem 1.10.** *Let* $\alpha : \mathbf{A} \to \mathbf{B}$ *be a homomorphism onto* $\mathbf{B}$*. Then there exists an isomorphism* $\beta$ *from* $A/\ker(\alpha)$ *to* $\mathbf{B}$ *defined by* $\alpha = \beta \circ \eta$*, where* $\eta$ *is the natural homomorphism from* $\mathbf{A}$ *to* $\mathbf{A}/\ker(\alpha)$*.*

The constructions we have met hereto, subalgebras and quotient algebras, allow to construct algebras of smaller (or at least equal) cardinality. On the other hand, the direct product permits to obtain algebras of larger cardinality.

Let $\mathbf{A}_1$ and $\mathbf{A}_2$ be algebras of the same type $\mathcal{F}$. The *direct product* $\mathbf{A}_1 \times \mathbf{A}_2$ is the algebra whose universe is the set $A_1 \times A_2$, and for $f \in \mathcal{F}_n$ and $a_i \in A_1$, $a_i^* \in A_2$, $1 \leq i \leq n$,

$$f^{A_1 \times A_2}\left((a_1, a_1^*), ..., (a_n, a_n^*)\right) = \left(f^{A_1}(a_1, ..., a_n), f^{A_2}(a_1^*, ..., a_n^*)\right).$$

The mapping

$$\pi_i : \mathbf{A}_1 \times \mathbf{A}_2 \to \mathbf{A}_i$$

for $i \in \{1, 2\}$, is the projection function from $\mathbf{A}_1 \times \mathbf{A}_2$ on the $i$th coordinate $\mathbf{A}_i$.It is easily seen that $\mathbf{A}_1$ and $\mathbf{A}_2$ are homomorphic images of $\mathbf{A}_1 \times \mathbf{A}_2$ via the map $\pi_i$.

The idea of direct product of $\mathbf{A}_1$ and $\mathbf{A}_2$ can be confortably extended to an arbitrary number of factors (see [14]). The direct product of a family $\{\mathbf{A}_i\}_{i \in I}$ of algebras of the same similarity type will be denoted by $\Pi_{i \in I}\mathbf{A}_i$. The importance of the notion of complementary factor congruence is given in the following result.

**Theorem 1.11.** *If $\theta$, $\theta^*$ is a pair of complementary factor congruences on $\mathbf{A}$, then $\mathbf{A}$ is isomorphic to $\mathbf{A}/\theta \times \mathbf{A}/\theta^*$.*

We say that an algebra $\mathbf{A}$ is *directly indecomposable* if $\mathbf{A}$ is not isomorphic to a direct product of two non-trivial algebras.

**Lemma 1.1.** *$\mathbf{A}$ is directly indecomposable if the only pair of factor congruences on $\mathbf{A}$ is $\Delta, \nabla$.*

**Theorem 1.12** (Birkhoff)**.** *Every finite algebra is isomorphic to a direct product of directly indecomposable algebras.*

An analogous of Theorem 1.12 in general does not hold for infinite algebras. The pursuit of furnishing a general building block construction for any algebra led Birkhoff to consider the notions of subdirect product and subdirectly irreducible algebras.

An algebra $\mathbf{A}$ is a *subdirect product* of an indexed family $\{\mathbf{A}_i\}_{i \in I}$ of algebras if

1. $\mathbf{A} \leq \Pi_{i \in I} \mathbf{A}_i$,

2. $\pi_i(\mathbf{A}) = \mathbf{A}_i$, for each $i \in I$.

An embedding $\alpha : \mathbf{A} \to \Pi_{i \in I} \mathbf{A}_i$ is subdirect if $\alpha(\mathbf{A})$ is a subdirect product of the $\mathbf{A}_i$.

**Definition 1.1.** An algebra $\mathbf{A}$ is *subdirectly irreducible* if for every subdirect embedding $\alpha : \mathbf{A} \to \prod_{i \in I} \mathbf{A}_i$, there exists an $i \in I$ such that

$$\pi_i \circ \alpha : \mathbf{A} \to \mathbf{A}_i$$

is an isomorphism.

Subdirectly irreducible algebras are characterized by a property of their lattice of congruences.

**Theorem 1.13.** *An algebra* $\mathbf{A}$ *is* subdirectly irreducible *if* $\mathbf{A}$ *is trivial or there is a minimum congruence in* $\mathbf{Con}(\mathbf{A}) - \Delta$.

**Corollary 1.1.** *A subdirectly irreducible algebra is directly indecomposable.*

As prime numbers are the building blocks of the integers, the next Theorem states that subdirectly irreducible algebras are the real building blocks in universal algebra.

**Theorem 1.14** (Birkhoff)**.** *Every algebra* $\mathbf{A}$ *is isomorphic to a subdirect product of subdirectly irreducible algebras.*

We now point out a special class of subdirectly irreducible algebras: the class of simple algebras.

An algebra $\mathbf{A}$ is *simple* if $\mathbf{Con}(\mathbf{A}) = \{\Delta, \nabla\}$. Clearly, if an algebra $\mathbf{A}$ is simple then it is also subdirectly irreducible. A congruence $\theta$ on $\mathbf{A}$ is *maximal* if the interval $[\theta, \nabla]$ of $\mathbf{Con}(\mathbf{A})$ has exactly two elements.

**Theorem 1.15.** *Let* $\theta \in C(\mathbf{A})$. $\mathbf{A}/\theta$ *is simple if* $\theta$ *is a maximal congruence on* $\mathbf{A}$ *or* $\theta = \nabla$.

Another important construction, introduced by Łos in 1955 [57] is the ultraproduct.

First of all we have to introduce the notion of ultrafilter.

Let $X$ be a set. An *ultrafilter* on $X$ is a set $U$ consisting of subsets of $X$ such that:

1. $\emptyset \notin U$;
2. If $A, B \subseteq X, A \subseteq B$, and $A \in U$, then $B \in U$;
3. If $A, B \in U$, then $A \cap B \in U$;
4. If $A \subseteq X$, then either $A \in U$ or $-A \in U$.

Now, let $\{\mathbf{A}_i\}_i \in I$ be a family of algebras of a given type and let $U$ be an ultrafilter on $I$. Define $\theta_U$ on $\Pi_{i\in I}\mathbf{A}_i$

$$\langle a, b\rangle \in \theta_U \text{ iff } \{i \in I : a_i = b_i\} \in U$$

We have that

**Lemma 1.2.** *With $\mathbf{A}_i$, $i \in I$ and $U$ as above, $\theta_U$ is a congruence on $\Pi_{i\in I}\mathbf{A}_i$.*

We have now all the ingredients required to define the notion of ultraproduct:

**Definition 1.2.** With $\mathbf{A}_i$, $i \in I$ and $U$ an ultrafilter over $I$, we define the *ultraproduct*

$$\Pi_{i\in I}\mathbf{A}_i/U$$

to be

$$\Pi_{i\in I}\mathbf{A}_i/\theta_U.$$

### 1.2.4 Class operators, varieties and congruence properties.

A fundamental topic in universal algebra (see e.g. [14]) is the investigation of classes of algebras of the same type closed under one or more constructions.

As in current literature, we will write for an algebra $\mathbf{A}$ and a class of algebras $\mathcal{K}$

$\mathbf{A} \in \mathbf{H}(\mathcal{K})$ if $\mathbf{A}$ is a homomorphic image of some member of $\mathcal{K}$,

$\mathbf{A} \in \mathbf{I}(\mathcal{K})$ if $\mathbf{A}$ is an isomorphic image of some member of $\mathcal{K}$,

$\mathbf{A} \in \mathbf{S}(\mathcal{K})$ if $\mathbf{A}$ is a subalgebra of some member of $\mathcal{K}$,

$\mathbf{A} \in \mathbf{P}(\mathcal{K})$ if $\mathbf{A}$ is a direct product of a family of members of $\mathcal{K}$,

$\mathbf{A} \in \mathbf{P}_s(\mathcal{K})$ if $\mathbf{A}$ is a subdirect product of a nonempty family of members of $\mathcal{K}$.

$\mathbf{A} \in \mathbf{P}_U(\mathcal{K})$ if $\mathbf{A}$ is an ultraproduct of a nonempty family of members of $\mathcal{K}$.

$\mathbf{H}$, $\mathbf{I}$, $\mathbf{S}$, $\mathbf{P}$, $\mathbf{P}_s$, $\mathbf{P}_U$ are called *class operators*. We say that a class of algebras $\mathcal{K}$ is closed under a class operator $\mathbf{O}$ if $\mathbf{O}(\mathcal{K}) \subseteq \mathcal{K}$, and that $\mathbf{O}$ is idempotent if $\mathbf{OO}(\mathcal{K}) = \mathbf{O}(\mathcal{K})$. Relevant relations between class operators are presented in the next Lemma:

**Lemma 1.3.** *The following inequalities hold:* $\mathbf{SH} \leq \mathbf{HS}$, $\mathbf{PS} \leq \mathbf{SP}$, $\mathbf{PH} \leq \mathbf{HP}$. *Also* $\mathbf{H}$,$\mathbf{S}$ *and* $\mathbf{IP}$ *are idempotent.*

A nonempty class $\mathcal{K}$ of algebras of type $\mathcal{F}$ is called a *variety* if it is closed under homomorphic images, subalgebras and direct products.

If $\mathcal{K}$ is a class of algebras, we will write $\mathbf{V}(\mathcal{K})$ the smallest variety containing $\mathcal{K}$, and we call $\mathbf{V}(\mathcal{K})$ the variety generated by $\mathcal{K}$.

**Theorem 1.16** (Tarski)**.** *Let $\mathcal{K}$ be a class of algebras. Then $\mathbf{V}(\mathcal{K}) = \mathbf{HSP}(\mathcal{K})$.*

**Theorem 1.17** (Birkhoff)**.** *If $\mathcal{K}$ is a variety, then every member of $\mathcal{K}$ is isomorphic to a subdirect product of subdirectly irreducible members of $\mathcal{K}$.*

One of the most relevant results in universal algebra states the connection between varieties and equational classes. An equational class is a class of algebras that is defined by means of equations. For example, all the classes introduced in the previous section are equational.

**Theorem 1.18** (Birkhoff)**.** *$\mathcal{K}$ is an equational class if and only if it is a variety.*

By the previous theorem a variety coincides with an equational class, i.e. a class axiomatized by a list of equations that may be possibly infinite. If this list is *finite* that we speak of a *finitely based variety.*

One of the most fruitful directions of research in universal algebra was initiated by Mal'cev in the 1950's when he showed the connection between permutability of congruences for all algebras in a variety $\mathcal{V}$ and the existence of a ternary term $p$ such that $\mathcal{V}$ satisfies certain identities involving $p$. For this reason, the characterization of properties in varieties by the existence of certain terms involved in certain identities is referred to as Mal'cev conditions, see [19].

**Theorem 1.19** (Mal'cev)**.** *Let $\mathcal{V}$ be a variety. $\mathcal{V}$ is congruence-permutable iff there exists a term $p(x, y, z)$ such that $\mathcal{V}$ satisfies the equations*

$$p(x, x, y) = y,$$

$$p(x, y, y) = x.$$

Examples of congruence-permutable varieties include groups (Example 1.2) and rings (Example 1.5), for which the witness Mal'cev terms are $p(x, y, z) = (x \cdot y^{-1}) \cdot z$ and $p(x, y, z) = (x - y) + z$, respectively.

**Theorem 1.20.** *Let $\mathcal{V}$ be a variety for which there is a ternary term $M(x, y, z)$ such that $\mathcal{V}$ satisfies*

$$M(x, x, y) = M(x, y, x) = M(y, x, x) = x.$$

*Then $\mathcal{V}$ is congruence-distributive.*

The ternary term $M(x, y, z)$ is usually called a *majority term* for $\mathcal{V}$. An example of a congruence-distributive variety is represented by the variety of lattices.

A variety $\mathcal{V}$ that is both congruence-distributive and congruence-permutable is called *arithmetical*. Being arithmetical is also witnessed by the existence of a ternary term.

**Theorem 1.21** (Pixley)**.** *A variety $\mathcal{V}$ is arithmetical iff there is a term $m(x, y, z)$ such that $\mathcal{V}$ satisfies*

$$m(x, y, x) = m(x, y, y) = m(y, y, x) = x.$$

The variety of Boolean algebras (Example 1.8) is an example of an arithmetical variety, with witness term $m(x, y, z) = (x \wedge z) \vee (x \wedge y' \wedge z') \vee (x' \wedge y' \wedge z)$. The reader will have noticed that Theorem 1.20 establishes an implication rather than an equivalence. However, Jónsson proved the following equivalence.

**Theorem 1.22** (Jónsson)**.** *A variety $\mathcal{V}$ is congruence-distributive iff there is a finite $n$ and terms $p_0(x, y, z), ..., p_n(x, y, z)$ such that $\mathcal{V}$ satisfies the following:*

$$p_i(x, y, x) = x \qquad 0 \leq i \leq n$$

$$p_0(x, y, z) = x,$$

$$p_n(x,y,z) = z$$
$$p_i(x,x,y) = p_{i+1}(x,x,y), \qquad \textit{for } i \textit{ even},$$
$$p_i(x,y,y) = p_{i+1}(x,y,y), \qquad \textit{for } i \textit{ odd}.$$

The importance of being congruence-distributive for a variety is shown in the following result, which goes under the name of Jónsson's Lemma [46].

**Theorem 1.23** (Jónsson)**.** *Let $\mathcal{V}(K)$ be a congruence-distributive variety. If $\mathbf{A}$ is a subdirectly irreducible algebra in $\mathcal{V}(K)$, then $\mathbf{A} \in \mathbf{HSP_U}(K)$.*

## 1.3 Basic of Group theory

We recall here some notions relative to the special class of *groups*, which have been introduced in Example 1.2. The basic textbooks on the topic are uncountably many, but we remand the interested reader for example to [40], [42], [67].

**Definition 1.3.** A *group* is an algebra $\mathbf{G} = \langle G, \cdot, ^{-1}, 1\rangle$ of type $\langle 2,1,0\rangle$ which satisfies the following equations:

(G1) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,

(G2) $x \cdot 1 = 1 \cdot x = x$,

(G3) $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

Many algebraic textbooks prefer to introduce groups as algebras equipped with a binary associative operation, a neutral element and satisfying the property that any element possesses an inverse, i.e. for each $x$ there exists $x^{-1}$ s.t. $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

A very natural example is the group of permutations over a set, i.e. all the bijective maps from a set $X$ into itself. Given a set $X$, the set $S_X$ of all permutations inherits the structure of a group, with composition as binary operation and the identical permutation as neutral element. It is also clear that any permutation admits an inverse. $\mathbf{S}_X$ is usually referred to as the *symmetric group*. Whenever $X$ is a finite set of cardinality $n$, we write $\mathbf{S}_n$ instead of $\mathbf{S}_X$. Groups of permutations are examples of non-commutative groups, in particular:

**Remark 1.1.** $\mathbf{S}_3$ is the smallest non Abelian group.

Let $X$ be a set with $|X| = n$ and $a, b \in X$. The *transposition* of the two elements $a, b$, is the permutation defined by $\tau(a) = b$, $\tau(b) = a$, and $\tau(x) = x$ for all $x \in X$, with $x \neq a$, $x \neq b$.

**Proposition 1.2.** *Every permutation is a product of transpositions.*

The following result strengthen the content of Proposition 1.2 and allows to classify permutations as even or odd.

**Theorem 1.24.** *If a permutation* $\sigma = \tau_1\tau_2...\tau_n = v_1v_2...v_s$ *is a product of transpositions* $\tau_1\tau_2...\tau_n$ *and* $v_1v_2...v_s$*, then* $n \equiv s(\text{mod}2)$.

Theorem 1.24 can be equivalently expressed by saying that a product of an even number of transpositions cannot equal a product of an odd number of transpositions. For this reason, it makes sense to introduce the following, important distinction

**Definition 1.4.** A permutation is *even* when it is the product of an even number of transpositions, *odd* when it is the product of an odd number of transpositions.

The definition of even and odd permutation readily leads to the definition of the sign of a permutation.

**Definition 1.5.** The *sign* of a permutation $\sigma$ is a function defined as follows:

$$sgn(\sigma) = \begin{cases} +1, & \text{if } \sigma \text{ is even,} \\ -1, & \text{if } \sigma \text{ is odd.} \end{cases}$$

In the terms of universal algebra, given a group $\mathbf{G}$, a subgroup $\mathbf{H}$ of $\mathbf{G}$ is simply a subalgebra of $\mathbf{G}$. This fact is equivalently expressed by saying that a subset $H$ of $G$ is a subgroup if and only if:

1. $1 \in H$,
2. if $x \in H$ then $x^{-1} \in H$,
3. if $x, y \in H$ then $x \cdot y \in H$,

where $\cdot$, $^{-1}$ and 1 are the very same operations of $\mathbf{G}$.

**Definition 1.6.** A subgroup $\mathbf{N}$ of a group $\mathbf{G}$ is *normal* when $xN = Nx$ for all $x \in G$, where $xN = \{x \cdot n : n \in N\}$.

Normal subgroups can be equivalently described as closed under conjugation.

**Proposition 1.3.** *A subgroup* $\mathbf{N}$ *of a group* $\mathbf{G}$ *is normal if and only if* $xNx^{-1} \subseteq N$ *for all* $x \in G$.

It is not difficult to check that normal subgroups (as well as subgroups) are closed under arbitrary intersections, so they form a complete lattice.

The importance of normal subgroup derives from the fact that they allow to construct quotient groups. Indeed the set of normal subgroups of a given group is in bijective correspondence with set of congruences; more precisely, given a group $\mathbf{G}$, the (complete) lattice of congruences, $\mathbf{Con}(\mathbf{G})$, is isomorphic to the lattice of normal subgroups.

The notion of kernel of a homomorphism admits an elegant description for groups. Let $\mathbf{A}$ and $\mathbf{B}$ be two groups and $\varphi : \mathbf{A} \to \mathbf{B}$ an homomorphism, then $\ker(\varphi) = \{x \in A : \varphi(x) = 1_B\}$.

The symmetric group $\mathbf{S}_n$ has always a normal subgroup, that consists of all even permutations and is referred to as the *alternating group*, $\mathcal{A}_n$.

A useful type of permutation is established by cycles. Given a number $k$, $2 \leq k \leq n$ and distinct elements $a_1, a_2, ..., a_k$ of a set $X$, the *k-cycle* $(a_1 a_2 ... a_k)$ is the permutation $\gamma$ defined by

$$\gamma(a_i) = a_{i+1} \quad \text{for all } 1 \leq i < k,$$

$$\gamma(a_k) = a_1, \text{ and}$$

$$\gamma(x) = x \quad \text{for all } x \neq a_1, ..., a_k.$$

A permutation is a *cycle* when it is a $k$-cycle for some $2 \leq k \leq n$. Clearly a cycle of two elements is a transposition (2-cycle).

**Proposition 1.4.** *The alternating group* $\mathbf{A}_n$ *is generated by all* 3*-cycles.*

**Definition 1.7.** The support of a permutation $\sigma$ is the set $\{x : \sigma(x) \neq x\}$. Two permutations are *disjoint* when their supports are disjoint.

Even though groups of permutation are the typical examples of non commutative groups, it is easy to check that disjoint permutations commute. This fact allows to prove the following.

**Theorem 1.25.** *Every permutation is a product of pairwise disjoint cycles, and this decomposition is unique up to the order of the terms.*

### 1.3.1 Group actions

An important application of group theory regards the action of groups on sets.

**Definition 1.8.** A *left group action* of a group $\mathbf{G}$ on a set $X$ is a mapping: $\mathbf{G} \times X \to X$, $(g, x) \to g \cdot x$, such that:

(i) $1 \cdot x = x$,

(ii) $g \cdot (h \cdot x) = (g \cdot h) \cdot x$, for all $g, h \in G$ and $x \in X$.

Then $\mathbf{G}$ *acts on the left* on $X$.

Analogously one defines right action of $\mathbf{G}$ on a set $X$.

For example, the symmetric group $\mathbf{S}_X$ of all permutations of a set $X$ acts on $X$ by: $\sigma \cdot x = \sigma(x)$, where $\sigma \in S_X$ and $x \in X$. Actually, every group $\mathbf{G}$ acts on itself (more precisely on $G$) by left multiplication. Also every subgroup of $\mathbf{G}$ acts on $G$ by left multiplication.

The following states the connection between action of groups and groups of permutation, leading to Cayley's theorem, which gives reason to the importance of groups of permutations to the abstract study of group theory.

**Proposition 1.5.** *In a (left) group action of a group* $\mathbf{G}$ *on a set* $X$*, the action* $\sigma_g : x \to g \cdot x$*, where* $g \in G$ *is a permutation of* $X$*; moreover,* $g \to \sigma_g$ *is a homomorphism of* $\mathbf{G}$ *into the symmetric group* $\mathbf{S}_X$*.*

**Theorem 1.26** (Cayley)**.** *Every group* $\mathbf{G}$ *is isomorphic to a subgroup of the symmetric group* $S_G$*.*

We recall here a definition that will be frequently used in the Appendix.

**Definition 1.9.** In a left group action of a group $\mathbf{G}$ on a set $X$, the *orbit* of an element $x \in X$ is the set $\{y \in G |\ y = g \cdot x, \text{ for some } g \in G\}$.

## 1.4 Basics of fuzzy and quantum structures

The most prominent example of a fuzzy structure are MV-algebras, the algebraic counterpart of Łukasiewicz infinite-valuled logic.

### 1.4.1 MV-algebras

Following the lines of [33] we introduce MV-algebras through a small number of simple equations.

**Definition 1.10.** An *MV-algebra* is an algebra $\mathbf{A} = \langle A, \oplus, ', 0\rangle$ of type $\langle 2, 1, 0\rangle$ satisfying the following equations:

(MV1) $x \oplus (y \oplus z) = (x \oplus y) \oplus z$,

(MV2) $x \oplus y = y \oplus x$,

(MV3) $x \oplus 0 = x$,

(MV4) $x'' = x$,

(MV5) $x \oplus 1 = 1$,

(MV6) $(x' \oplus y)' \oplus y = (y' \oplus x)' \oplus x$,

where $1 = 0'$.

On every MV-algebra the operations $\otimes$ and $\ominus$ can be defined as follows:

$$x \otimes y = (x' \oplus y')',$$

$$x \ominus y = x \otimes y'.$$

Let us agree to write $x \leq y$ iff $x' \oplus y = 1$ (see [33] Lemma 1.1.2). One can prove that $\leq$ is a *partial order relation* (*the natural order*).

On any MV-algebra $\mathbf{A}$, the natural order determines a lattice structure. The join $\vee$ and the meet $\wedge$ are given by

$$x \vee y = x \oplus (x' \otimes y), \quad x \wedge y = x \otimes (x' \oplus y).$$

The constants 0 and 1 are, respectively, the bottom and top element with respect to the lattice order $\leq$. An MV-algebra whose natural order is a linear order is called an *MV-chain*.

The following two theorems are the famous *Subdirect Representation Theorem* and *Completeness Theorem*, due to Chang [31].

**Theorem 1.27.** *Every MV-algebra is subdirect product of MV-chains.*

**Theorem 1.28.** *An equation holds in* $[0, 1]$ *iff it holds in every MV-algebra.*

### 1.4.2 Quantum structures and Basic algebras

Orthomodular lattices are the most known examples of quantum structures. They were originally introduced in 1936 by Birkhoff and von Neumann [6] as an algebraic counterpart for the logic of quantum mechanics.

We refer to [34] for a detailed account of quantum logics and to [5], [52] for a detailed algebraic discussion on orthomodular lattices.

Recall from Example 1.10 that an orthomodular lattice is an ortholattice $\mathbf{OL} = \langle L, \vee, \wedge, ', 0, 1\rangle$ satisfying the orthomodular law (OML)

$$x \leq y \text{ implies } x \vee (x' \wedge y) = y.$$

Since the quasi-identity above can be equivalently replaced by the identity

$$x \vee (x' \wedge (x \vee y)) = x \vee y,$$

orthomodular lattices form a variety. In general, $x'$ is not the unique complement of $x$. In Fig.1.4 it is indeed given an example of an orthomodular lattice where every element different from the constants 0 and 1 has three complements.

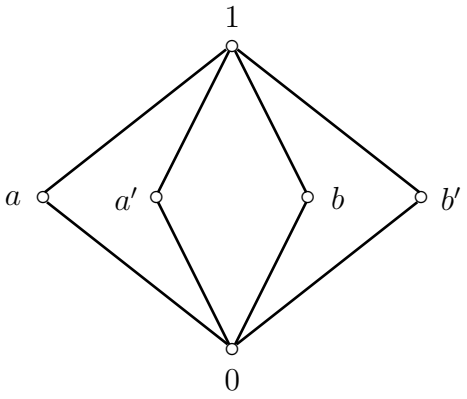



Figure 1.4: An example of orthomodular lattice where the complement of an element is not unique.

Given a bounded lattice $\mathbf{L} = \langle L, \vee, \wedge, 0, 1\rangle$, for every element $a \in L$, the section $[a, 1] = \{x \in L | a \leq x\}$ is often called a *section*, see for example [16]. By an antitone involution on a lattice $\mathbf{L}$, it is meant a mapping $f$ of $\mathbf{L}$ into

itself such that $f(f(x)) = x$ for each $x \in L$, and for $x, y \in L$ with $x \leq y$, then $f(y) \leq f(x)$. We say that $\mathbf{L}$ is endowed by *section antitone involutions* if for every $a \in L$ there exists an antitone involution on the interval $[a, 1]$. It is clear that there exist as many antitone involutions as the elements of $L$. For this reason, normally an antitone involution on the section $[a, 1]$ is usually indicated by a superscript $^a$, i.e. for an element $x \in [a, 1]$ its image is denoted by $x^a$. By defining, for each $a \in L$, $x^a = x' \vee a$, one gets that an orthomodular lattice **OL** has section antitone involutions.

Section antitone involutions can be defined also for MV-algebras. Indeed, if $\mathbf{M}$ is an MV-algebra, then for every $a \in M$, the mapping: $x \to x^a = \neg x \oplus a$ is an antitone involution on the section $[a, 1]$ and in particular, $\neg x = x^0$.

This similarity between a purely quantum (Orthomodular lattices) and a fuzzy structure (MV-algebras) motivated Chajda, Halaš and Kühr to introduce a common abstraction for Orthomodular lattices and MV-algebras, called *basic algebras*. We recall here some basic facts concerning basic algebras, while we remand to [18] for a complete introduction to the subject.

**Definition 1.11.** A basic algebra is an algebra $\mathbf{A} = \langle A, \oplus, \neg, 0\rangle$ satisfying the following identities:

(BA1) $x \oplus 0 = x$;

(BA2) $\neg\neg x = x$;

(BA3) $\neg(\neg x \oplus y) \oplus y = \neg(y \oplus \neg x) \oplus x$;

(BA4) $\neg(\neg(\neg(x \oplus y) \oplus y) \oplus z) \oplus (x \oplus z) = 1$,

where $\neg 0 = 1$.

As an historical remark, basic algebras were first introduced in [21], however the canonical axiomatization presented above first appeared in [24]. A basic algebra is said to be commutative if it satisfies $x \oplus y = y \oplus x$.

In any basic algebras the order defined by $x \leq y$ if and only if $\neg x \oplus y = 1$ is partial lattice order, whose corresponding *join* and *meet* are defined as

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

Furthermore, the algebra $\langle A, \vee, \wedge, 0, 1\rangle$, where operations are defined as above is a bounded lattice and the mapping $f_a : x \to x^a = \neg x \oplus a$ is an antitone involution on the section $[a, 1]$.

**Theorem 1.29** ([18], Theorem 2.5)**.** *Let* $\mathbf{A}$ *be a basic algebra. Then* $\mathbf{L}(A) = \langle A, \vee, \wedge, (f_a)_{a\in A}, 0, 1\rangle$ *is a bounded lattice with section antitone involutions.*

**Theorem 1.30** ([18], Theorem 2.6)**.** *Let* $\mathbf{L} = \langle A, \vee, \wedge, (f_a)_a \in A, 0, 1\rangle$ *be a bounded lattice with section antitone involutions. Then the algebra* $\mathbf{A}(L) = \langle L, \oplus, \neg, 0\rangle$*, where* $x \oplus y := (x^0 \vee y)^y$ *and* $\neg x := x^0$*, is a basic algebra.*

It follows immediately from the definition that every MV-algebra is a basic algebra, in particular, a commutative basic algebra. For the converse, it was shown by Botur and Halaš [13] that any commutative *finite* basic algebras is also an MV-algebra, but this does not hold in general. Indeed there exist examples of infinite commutative basic algebras which are not MV-algebras, [12].

**Theorem 1.31** ([16], Theorem 5)**.** *A basic algebra is an MV-algebra if and only if it is associative, i.e. it satisfies:*

$$x \oplus (y \oplus z) = (x \oplus y) \oplus z.$$

On the other hand, it is not difficult to check that also orthomodular lattices are a subvariety of the variety of basic algebras. More properly

**Theorem 1.32** ([16], Theorem 6)**.** *Orthomodular lattices form a subvariety of the variety of basic algebras determined by the identity*

$$y \oplus (x \wedge y) = y.$$

Theorems 1.31 and 1.32 states that basic algebras represent a common abstraction of MV-algebras and orthomodular lattices. However, they are not the variery generated by the two, which has been recently studied in [22].

## 1.5 Residuated Lattices

The notion of *residuation* goes back to Dedekind's work on the theory of rings. In that context residuation was introduced to capture the concept of division, in a ring with unit, in terms of its ideals. A development of this idea allowed to recover many results concerning Noetherian rings in the more abstract theory of lattices equipped with a suitable multiplication and residuation, see [54] and [72] for details.

More recently, the interest for residuated structures, in particular for residuated lattices, has involved logicians, due to the fact that they represent an algebraic counterpart of the so called 'substructural logics', see for example [38], [60].

Let us start by introducing the concept of residuated operation. A binary operation $\cdot : P \times P \to P$ on a poset, $\langle P, \leq \rangle$ is said to be *residuated* provided there exists two binary operations $\backslash, / : P \times P \to P$ s.t.

$$x \cdot y \leq z \quad \text{iff} \quad y \leq x \backslash z \quad \text{iff} \quad x \leq z / y.$$

In this case the poset $\langle P, \leq \rangle$ is a *residuated* poset (under the operation $\cdot$) and the operations $\backslash$, $/$ are the left and right *residuals*, respectively, of multiplication.

In case $\langle P, \cdot, 1 \rangle$ is a monoid then the structure $\langle P, \cdot, 1, \backslash, /, \leq \rangle$ is referred to as a partially ordered monoid. A partially ordered monoid is called *commutative* if the monoidal operation is commutative. In case multiplication is commutative, it is easy to check that the two residuals, $\backslash$, $/$, reduce to the same operation, usually indicated by $\to$. A partially ordered monoid is called *integral*, if the neutral element 1 is the top element with respect to the partial ordering $\leq$, i.e. $x \leq 1$ for every $x \in P$. It has been proven by Iséki [44] that partially ordered commutative residuated integral monoid, briefly Pocrims, can be defined as an algebra $\langle P, \cdot, \to, 1 \rangle$ of type $\langle 2, 2, 0 \rangle$ satisfying the following axioms:

1. $\langle P, \cdot, 1 \rangle$ is an abelian monoid,
2. $x \to 1 = 1$,
3. $1 \to x = x$,
4. $(x \to y) \to ((z \to x) \to (z \to y)) = 1$,
5. $x \to (y \to z) = (x \cdot y) \to z$,
6. If $x \to y = 1$ and $y \to x = 1$ then $x = y$.

Due to a result by Higgs [43], Pocrims form a proper quasi-variety, i.e. a quasi-variety which is not a variety. This means, by Birkhoff theorem, that the quasi-identity (6) in the above definition cannot be equivalently replaced by an identity, or, in other words, that the condition expressing residuation cannot be captured by an identity.

Instead of considering a partially ordered set as basic structure to endow with a residuated operation, one can start from a lattice. This gives rise to a residuated lattice.

**Definition 1.12.** A *residuated lattice* $\mathbf{RL} = \langle L, \wedge, \vee, \cdot, \backslash, / 1\rangle$ is an algebra of type $\langle 2, 2, 2, 2, 0\rangle$ such that:

i) $\langle L, \wedge, \vee\rangle$ is a lattice;

ii) $\langle L, \cdot, 1\rangle$ is a monoid;

iii) $\cdot$ is residuated with $\backslash$ and $/$ as left and right residuals, respectively.

In the case where $\cdot$ is commutative then **RL** is a commutative residuated lattice (see [8] for a general introduction to residuated lattices and [41] for the commutative version) and, again the two residuals $\backslash, /$ reduce to a unique one, $\rightarrow$.

**Proposition 1.6** (Tsinakis)**.** *The classes of residuated lattices and commutative residuated lattices form a variety.*

Residuated lattices, as well as other algebras (for example, groups, rings, Boolean algebras, etc.) admits a particularly pleasant description of the lattice of congruences. Indeed congruences correspond to certain kind of subalgebras, namely *convex normal subalgebras*. In the commutative case, the correspondence reduces to *convex subalgebras*.

Let **L** be a residuated lattice. For each element $a \in L$, define the right conjugation by $a$ as $\rho_a(x) = ((a \cdot x)/a) \wedge 1$ and the left conjugation as $\lambda_a(x) = (a\backslash(x \cdot a)) \wedge 1$.

**Definition 1.13.** A subset $X \subseteq L$ is called *convex* if, for any $x, y \in X$ and $a \in L$, if $x \leq a \leq y$ then $a \in X$. Furthermore, $X$ is called *normal* if it is closed under right and left conjugation.

A convex (normal) subalgebra **H** is a convex (normal) set which is also a subalgebra of **L**.

It is not difficult to check that the family of convex (normal) subalgebras of a **L** is closed under arbitrary intersection, therefore it forms a complete lattice.

**Theorem 1.33** (Blount, Tsinakis)**.** *The lattice of congruences of a residuated lattice is isomorphic to the lattice of convex normal subalgebras.*

**Theorem 1.34** (Hart, Rafter, Tsinakis)**.** *The lattice of congruences of a commutative residuated lattice is isomorphic to the lattice of convex subalgebras.*

## 1.6 Directoids

The concept of *directoid*, more properly of join-directoid, has been introduced by Jažek and Quackenbush [45] as a generalization of the theory of partially ordered sets, see [26] for an explanatory and complete textbook on the topic.

A partially ordered set $\mathbf{P} = \langle P, \leq \rangle$ is said to be *up-directed* in case any two elements $a, b \in P$ have a common upper bound. Similarly, $\mathbf{P}$ is *down-directed* if any two elements $a, b \in P$ posses a common lower bound. Of course, if $\mathbf{P}$ has a greatest element (lowest element), then it is up-directed (down-directed). Furthermore, if $\mathbf{P}$ is a lattice order then it is both up and down-directed. As lattice ordered sets can be treated as algebras, namely as lattices, so directed sets do.

**Definition 1.14.** A *join-directoid* is an algebra $\langle A, \sqcup \rangle$ of type $\langle 2 \rangle$, satisfying the following axioms:

(D1) $x \sqcup x = x$;

(D2) $(x \sqcup y) \sqcup x = x \sqcup y$;

(D3) $y \sqcup (x \sqcup y) = x \sqcup y$;

(D4) $x \sqcup ((x \sqcup y) \sqcup z) = (x \sqcup y) \sqcup z$.

It can be proved [26, Theorem 2.3] that if $\mathbf{P} = \langle P, \leq \rangle$ is an up-directed poset where to any pair of elements $(x, y)$ the common upper bound $x \sqcup y$ is assigned in such a way that $x \sqcup y = \max(x, y)$ if $x$ and $y$ are comparable with each other, then the algebra $\langle P, \sqcup \rangle$ is a join-directoid. Conversely, if $\langle P, \sqcup \rangle$ is a join-directoid in the sense of Definition 1.14 then, by defining $x \leq y$ if and only if $x \sqcup y = y$, for any $x, y \in P$, $\langle P, \leq \rangle$ is an up-directed poset.

Similarly one defines meet-directoids as an algebra $\langle A, \sqcap \rangle$ of type $\langle 2 \rangle$ satysfying the identities:

(D1') $x \sqcap x = x$;

(D2') $(x \sqcap y) \sqcap x = x \sqcap y$;

(D3') $y \sqcap (x \sqcap y) = x \sqcap y$;

(D4') $x \sqcap ((x \sqcap y) \sqcap z) = (x \sqcap y) \sqcap z$.

The correspondence between down-directed posets and meet-directoids can be established analogously, provided that the operation $x \sqcap y$ coincides with $\min(x, y)$ for comparable elements, see [26].

A join-directoid (meet-directoid, resp.) is called *commutative* if it satisfies the further identity $x \sqcup y = y \sqcup x$ ($x \sqcap y = y \sqcap x$).

An *antitone involution* on a poset $\mathbf{P} = \langle P, \leq \rangle$ is a unary operation $'$ s.t., for any $a \in P$, $(a')' = a$, and if $a \leq b$ in $\mathbf{A}$, then $b' \leq a'$. It is evident that, whenever a poset with antitone involution $\mathbf{D}$ has a greatest element 1, then it contains a smallest element too, namely, $1'$.

An *involutive directoid* is an algebra $\mathbf{D} = \langle D, \sqcap, ' \rangle$ of type $(2, 1)$ s.t. $\langle D, \sqcap \rangle$ is a directoid and $'$ is an antitone involution on the induced poset of $\mathbf{D}$. For an involutive directoid $\mathbf{D}$ the operation $\sqcup$ can be defined as $x \sqcup y = (x' \sqcap y')'$ and it is not difficult to check that $\langle D, \sqcup \rangle$ is a (join) directoid. Furthermore, in such case the orders induced by $\sqcup$ and $\sqcap$ coincide. It is not difficult to prove that the class of involutive directoids is a variety [20].

We will call *bounded involutive directoid* the algebra $\mathbf{D} = \langle D, \sqcap, ', 0, 1 \rangle$ of type $\langle 2, 1, 0, 0 \rangle$, where $\langle D, \sqcap, ' \rangle$ is an involutive directoid and the constants 0 and 1 are the least and the top element, respectively, with respect to the induced order.

# Chapter 2

# Orthogonal relational systems

It is superfluous to recall how important binary relational systems are for the whole of mathematics. The origins of the study of binary relation trace back to De Morgan [61], and was elaborated later on by Peirce [62]. For a brief chronology of the development of the study of binary relations see [64]. The modern approach to the study of binary relations goes back to the work of J. Riguet [66], and a first attempt to provide an algebraic theory of relational systems is due to Mal'cev [58]. A general investigation of quotients and homomorphisms of relational systems can be found in [25], where seminal notions from [15] are developed. A leading motivation for our discussion stems from the theory of *semilattices*. In fact, semilattices can be equivalently presented as ordered sets as well as groupoids, see [21]. This approach was extended to ordered sets whose ordering is directed. In this case the resulting groupoid needs not be, in general, a semilattice, but a *directoid*. We will see that many features of a relational system $\mathbf{A} = \langle A, R\rangle$ can be captured by means of the associated groupoid. Reflexivity, symmetry, transitivity or antisymmetry of $R$ can be equationally or quasi-equationally characterized in the groupoid [27, 30].

The concept of orthogonal poset was first considered in [17], where an algebraic characterization of the system through the associated groupoid with involution is presented. In [20] this method was generalized to cover the case of ordered sets with antitone involution. These ideas motivated us to extend the approach to general algebraic systems with involution and distinguished elements. In what follows, we develop this theory.

The chapter is structured as follows: in §2.1 the notions of orthogonal relational system and orthogonal groupoids are introduced and we show how

the two concepts are mutually related. In §2.2 we present a decomposition theorem for a variety of orthogonal groupoids. Finally in §2.3 we show that the class of orthogonal groupoids enjoys the strong amalgamation property.

## 2.1 Relational systems with involution

By a *relational system* is meant a pair $\mathbf{A} = \langle A, R\rangle$, where $A$ is a non-empty set and $R$ is a binary relation on $A$, i.e. $R \subseteq A^2$. If $a, b \in A$, the *upper cone of* $a, b$ is the set

$$U_R(a, b) = \{c \in A : (a, c) \in R \text{ and } (b, c) \in R\}.$$

In case $a = b$ we write $U_R(a)$ for $U_R(a, a)$.

A *relational system with involution* is a triple $\mathbf{A} = \langle A, R, ' \rangle$ such that $\langle A, R\rangle$ is a relational system and $' : A \to A$ is a map such that, for all $a, b \in A$, $(a')' = a$, and if $(a, b) \in R$ then $(b', a') \in R$. For brevity sake, we will write $a''$ for $(a')'$.
A *relational system with 1 and involution* is a quadruple $\mathbf{A} = \langle A, R, ', 1\rangle$, such that the structure $\langle A, R, ' \rangle$ is a relational system with involution and 1 is a distinguished element in $A$ such that $(x, 1) \in R$ for each $x \in A$.

As customary, we indicate $1'$ by 0. It is clear that $(0, x) \in R$ for all $x \in A$. One can easily see that, for any $a, b \in A$, $U_R(a, b) \neq \emptyset$, as $1 \in U_R(a, b)$.

Let $\mathbf{A}$ be a relational system with 1 and involution and let $a, b \in A$. Two elements $a, b$ are called *orthogonal* (in symbols $a \perp b$) when $(a, b') \in R$ (or, equivalently, $(b, a') \in R$). We say that an element $w \in U_R(a, b)$ is a *supremal element* for $a, b$ if for each $z \in U_R(a, b)$, with $z \neq w$, then $(w, z) \in R$. Obviously, if $R$ is an order relation on $A$, then there is at most one supremal element for $a, b \in A$, which coincides with $\sup(a, b)$.

The following notion will be central in our discussion:

**Definition 2.1.** A relational system $\mathbf{A} = \langle A, R, ', 1\rangle$ is *orthogonal* if:

(a) $U_R(x, x') = \{1\}$ for each $x \in A$;

(b) for all non-zero orthogonal elements $x, y$ $(x \perp y)$ there exists a supremal element.

Let us recall a useful notion from [27] and [30].

**Definition 2.2.** Let $\mathbf{A} = \langle A, R\rangle$ be a relational system. A binary operation $+$ on $A$ can be associated to $R$ as follows:

(i) if $(x, y) \in R$ then $x + y = y$;

(ii) if $(x, y) \notin R$ and $(y, x) \in R$ then $x + y = x$;

(iii) if $(x, y) \notin R$ and $(y, x) \notin R$ then $x + y = y + x = z$, where $z$ is an arbitrarily chosen element in $U_R(x, y)$.

We say that the groupoid $\mathbf{G}(A) = \langle A, +\rangle$ is *induced* by the relational system $\mathbf{A} = \langle A, R\rangle$.

Let us remark that, in general, for a relational system $\mathbf{A} = \langle A, R\rangle$, an induced groupoid $\mathbf{G}(A)$ is not univocally determined. This happens whenever there are elements $a, b$ in $A$ s.t. $(a, b), (b, a) \notin R$ and $U_R(a, b)$ contains more than one element. In this case indeed, $a + b$ will be arbitrarily chosen in $U_R(a, b)$.

The strategy adopted in Definition 2.2 for associating an algebra to a relational system is based on the ideas developed in [27] and [30]. This is not, of course, the only possibility to proceed. A different way to do it, consist of introducing the so called *graph algebras*, see [63].

Conversely, if an induced groupoid $\mathbf{G}(A)$ is given, then a relation $R$ on $A$ is uniquely determined by the binary operation $+$ as follows:

$$(x, y) \in R \text{ if and only if } x + y = y.$$

In other words, any induced groupoid $\mathbf{G}(A)$ stores all the information relative to the relational system $\mathbf{A} = \langle A, R\rangle$. Furthermore, whenever $R$ is reflexive, the following obtains:

**Lemma 2.1.** *Let $\mathbf{A} = \langle A, R\rangle$ be a relational system and $R$ be a reflexive relation. Then $x + y \in U_R(x, y)$ for all $x, y \in A$.*

*Proof.* We consider all possible cases. If $(x, y) \in R$ then, by Definition 2.2-(i), $x + y = y$. Therefore, $(x, x + y) \in R$. Moreover, since $R$ is reflexive $(y, y) = (y, x + y) \in R$. If $(x, y) \notin R$ and $(y, x) \in R$ then, by Definition 2.2-(ii), $x + y = x$. Therefore, $(y, x) = (y, x + y) \in R$. Moreover, by reflexivity, $(x, x) = (x, x + y) \in R$. Finally, if $(x, y) \notin R$ and $(y, x) \notin R$, the claim follows from Definition 2.2-(iii). ■

Given a groupoid $\mathbf{G} = \langle G, + \rangle$ it is possible to define a binary relation $R_G$ on $G$ as follows, for any $a, b \in G$:

$$(a, b) \in R_G \text{ if and only if } a + b = b.$$

We call the relational system $\mathbf{A}(G) = \langle G, R_G \rangle$ the *induced relational system* by $\mathbf{G}$ and $R_G$ the relation *induced* by the groupoid $\mathbf{G}$. For simplicity sake, whenever no danger of confusion is impending we drop subscripts from our notation.
By Definition 2.2, it is possible to associate an algebra (in particular a groupoid) to any relational system. However, since our aim is to obtain an algebra out of an *orthogonal* relational system, we need to integrate this definition with a further condition, that takes into account the notion of orthogonality.

**Definition 2.3.** Let $\mathbf{A} = \langle A, R, ', 1 \rangle$ be an orthogonal relational system. Then a binary operation $+$ on $A$ can be associated to $R$ following conditions (i), (ii), (iii) of Definition 2.2 and the following further condition:

(iv) if $x \perp y$ with $x \neq 0 \neq y$, then $x + y = y + x = w$,

where $w$ is a supremal element in $U_R(x, y)$.We call any such structure $\mathbf{G}(A) = \langle A, +, ', 1 \rangle$ *a groupoid induced* by the orthogonal relational system $\mathbf{A} = \langle A, R, ', 1 \rangle$.

Let us remark that the existence of a supremal element for a pair of orthogonal elements is guaranteed by Definition 2.1.

We can now propose an algebraic counterpart of the notion of orthogonal relational system.

**Definition 2.4.** An *orthogonal groupoid*, for short *orthogroupoid*, is an algebra $\mathbf{D} = \langle D, +, ', 1 \rangle$ of type $(2, 1, 0)$ such that $\langle D, + \rangle$ is a groupoid and the following equations hold:

(a) $x'' = x$;

(b) $0 + x = x$ and $x + 1 = 1$, where $0 = 1'$;

(c) $x + x' = 1$;

(d) if $x + z = z$ and $x' + z = z$ then $z = 1$;

(e) $(((z+y)'+(z+x))'+(z+y)')+z'=z'$;

(f) $x+(x+y)=x+y$ and $y+(x+y)=x+y$.

Some basic properties of orthogroupoids are subsumed in the following lemmas.

**Lemma 2.2.** *Let* $\mathbf{D}=\langle D,+,',1\rangle$ *be an algebra in the type* $\langle 2,1,0\rangle$ *satisfying conditions (a), (b), (c) and (e) of* Definition 2.4 *and* $R$ *its induced relation. Then*

*(i)* $0'=1$.

*(ii)* $(x'+y)'+x=x$.

*(iii)* $(0,x)\in R$ *and* $(x,1)\in R$ *for any* $x\in D$.

*(iv) If* $(x,y)\in R$ *then* $(y',x')\in R$.

*Proof.* (i) $0=1'$, thus $0'=1''=1$.
(ii) Replacing $x$ by $y$ and $z$ by $x'$ in Definition 2.4-(e), we get $(((x'+y)'+(x'+y))'+(x'+y)')+x=x$. By (c) and (a) $(x'+y)'+(x'+y)=1$, thus $((x'+y)'+(x'+y))'=0$. Then by (b) $(0+(x'+y)')+x=(x'+y)'+x=x$.
(iii) Straightforward from the definition of induced relation.
(iv) Let $(x,y)\in R$. Then, by definition of $R$, $x+y=y$. By Definition 2.4-(a) and item (ii) $y'+x'=(x+y)'+x'=x'$. Therefore $(y',x')\in R$. ■

**Lemma 2.3.** *Let* $\mathbf{D}=\langle D,+,',1\rangle$ *be a non-trivial orthogroupoid, then the following properties hold:*

*1)* $x+x=x$, *for any* $x\in D$;

*2)* $x\neq x'$ *for any* $x\in D$.

*Proof.* 1) By axiom (f), $x+(y+x)=y+x$. Setting $y=0$, $x+x=x+(0+x)=0+x=x$.
2) Suppose by contradiction that $a=a'$ for some $a\in D$. Then, by 1), $a+a=a$ and also $a'+a=a+a=a$. Then, by (d), $a=1$, hence $0=1'=1$. By (b) $0+c=c$, for any $c\in D$, and $0'+c=1+c=0+c=c$, thus $c=1$ by (d). So, if $a=a'$ then $\mathbf{D}$ is trivial, against the assumption. ■

Although in Definition 2.4 orthogroupoids have a quasi-equational presentation (Condition (d)), we can prove that the same notion can be captured by a single equation, as the following proposition shows:

**Proposition 2.1.** *A structure* $\mathbf{D} = \langle D, +, ', 1\rangle$ *of type* $(2, 1, 0)$ *that satisfies equations (a), (b), (c), (e) and (f) in Definition 2.4 satisfies condition (d) if and only if it satisfies*

$$1 + x = 1. \tag{2.1}$$

*Proof.* We first derive $1 + x = 1$, assuming (d). $1 + (1 + x) = 1 + x$ by axiom (f), and $0 + (1 + x) = 1 + x$ by (b), hence $1 + x = 1$ for (d), as desired.
For the converse, suppose $1 + x = 1$ holds and assume, for $a, b \in D$, that $a + b = a' + b = b$. First observe that by Lemma 2.2-(ii), $(a' + b)' + a = a$, so $b' + a = a$. Similarly $(a + b)' + a' = a'$, hence $b' + a' = a'$. Now, substituting $z$ by $b'$, $y$ by $a$ and $x$ by $a'$ in (e), we obtain $(((b'+a)'+(b'+a'))'+(b'+a)')+b = b$. As $b' + a = a$ and $b' + a' = a'$, we get $b = ((a' + a')' + a') + b = (a'' + a') + b = (a + a') + b = 1 + b = 1$ as desired. ■

**Corollary 2.1.** *The class of orthogroupoids forms a variety axiomatized by equations (a), (b), (c), (e) and (f) in* Definition 2.4 *and* (2.1)*.*

Let $\mathbf{D}$ be an orthogroupoid. We now show that the relational system obtained from $\mathbf{D}$ is an orthogonal relational system, whose relation is also reflexive.

**Theorem 2.1.** *Let* $\mathbf{D} = \langle D, +, ', 1\rangle$ *be an orthogroupoid and* $R$ *the induced relation. Then the induced relational system* $\mathbf{A}(D) = \langle D, R, ', 1\rangle$ *is orthogonal and* $R$ *is reflexive.*

*Proof.* By Definition 2.4-(a), and Lemma 2.2-(iv) the mapping $x \mapsto x'$ is an involution on $\mathbf{A}(D)$. By Lemma 2.2-(iii), for all $x$, $(x, 1) \in R$ thus $\mathbf{A}(D) = \langle D, R, ', 1\rangle$ is a relational system with 1 and involution.
Since Lemma 2.3, $x + x = x$, i.e. $R$ is reflexive.
To prove that $\mathbf{A}(D)$ is orthogonal, we verify that conditions (a) and (b) in Definition 2.1 are satisfied.
By Definition 2.4-(c), $x + x' = 1$ for each $x \in D$. Obviously $1 \in U_R(x, x')$. Assume $z \in U_R(x, x')$. Then, by definition, $(x, z) \in R$ and $(x', z) \in R$ and hence $x + z = z$ and $x' + z = z$. Then, axiom (d) implies $z = 1$, proving that $U_R(x, x') = \{1\}$.
We now prove (b) of Definition 2.1. Assume $x \neq 0 \neq y$ and $x \perp y$. Then $(x, y') \in R$ and $(y, x') \in R$. The following three cases may arise:

(i) if $(x, y) \in R$ then $(y', x') \in R$ by (iv) of Lemma 2.2, hence $y + x' = y' + x' = x'$. Then, by axiom (d), $x' = 1$ and $x = 0$, a contradiction. So this case is impossible.
(ii) if $(x, y) \notin R$ but $(y, x) \in R$, then similarly $y' \in U_R(x, x') = \{1\}$, whence $y = 0$, which is again a contradiction.
(iii) the last possibility is that $(x, y) \notin R$ and $(y, x) \notin R$. By axiom (f), $x + y \in U_R(x, y)$. Assume $z \in U_R(x, y)$ with $z \neq x + y$. Replacing $x, y, z$ by $x', y', z'$ in axiom (e), respectively, we obtain

$$(((z' + y')' + (z' + x'))' + (z' + y'), z) \in R. \tag{2.2}$$

Since $x \perp y$, $(y, x') \in R$, and so

$$y + x' = x'. \tag{2.3}$$

Moreover, $z \in U_R(x, y)$ yields $(x, z) \in R$ and $(y, z) \in R$ thus also $(z', x') \in R$ and $(z', y') \in R$, which imply

$$z' + x' = x' \text{ and } z' + y' = y'. \tag{2.4}$$

Using equations (2.3) and (2.4), we obtain $x + y = x'' + y = (y + x')' + y = ((z' + y')' + (z' + x'))' + (z' + y')'$, thus, from equation 2.2, we conclude $(x + y, z) \in R$. This proves that $x + y$ is a supremal element for $x, y$ and hence $\mathbf{A}(D)$ is an orthogonal relational system. ■

A converse statement of Theorem 2.1 showing how to construct an orthogroupoid out of an orthogonal relational system requires two more lemmas.

**Lemma 2.4.** *Let $\mathbf{A} = \langle A, R\rangle$ be a relational system and let $R$ be reflexive. Then the following equations*

$$x + (x + y) = x + y = y + (x + y) \tag{2.5}$$

*hold in any induced groupoid.*

*Proof.* Three cases are possible:
(i) If $(x, y) \in R$ then $x + y = y$. Since $R$ is reflexive, also $(y, y) \in R$, thus $y \in U_R(x, y)$, i.e. $x + y \in U_R(x, y)$ whence $x + (x + y) = x + y = y + (x + y)$.
(ii) If $(x, y) \notin R$ but $(y, x) \in R$ then $x + y = x$. Using reflexivity of $R$, $(x, x) \in R$ and hence $x+y = x \in U_R(x, y)$, thus $x+(x+y) = x+y = y+(x+y)$.
(iii) If $(x, y) \notin R$ and $(y, x) \notin R$ then, by definition, $x+y$ is arbitrarily chosen in $U_R(x, y)$. Hence $x + (x + y) = x + y = y + (x + y)$. ■

**Lemma 2.5.** *Let* $\mathbf{A} = \langle A, R, ', 1\rangle$ *be an orthogonal relational system with* $R$ *a reflexive relation. If* $x, y$ *are two non-zero orthogonal elements in* $A$ *then* $(x, y) \notin R$ *and* $(y, x) \notin R$.

*Proof.* Assume $x \perp y$ and $x \neq 0 \neq y$. Then, by definition of orthogonality, $(x, y') \in R$ and $(y, x') \in R$. The following cases are possible:
(i) if $(x, y) \in R$ then $(y', x') \in R$ and hence $x' \in U_R(y, y')$. Therefore, $x' = 1$, i.e. $x = 0$, a contradiction;
(ii) if $(x, y) \notin R$ and $(y, x) \in R$ then $(x', y') \in R$ and hence $y' \in U_R(x, x')$, whence $y = 0$, again a contradiction.
The case in which $(x, y) \in R$ and $(y, x) \in R$ is ruled out by the previous two. Hence the only admissible case is $(x, y) \notin R$ and $(y, x) \notin R$. ■

**Lemma 2.6.** *Let* $\mathbf{A} = \langle A, R, ', 1\rangle$ *be an orthogonal relational system and* $\mathbf{D} = \langle D, +, ', 1\rangle$ *be an induced groupoid. Then* $\mathbf{D}$ *satisfies*

$$x + 0 = x. \tag{2.6}$$

*Proof.* By definition, for any $a \in D$, $(0, a) \in R$. Suppose that $(a, 0) \in R$ and $a \neq 0$. Then, $(1, a') \in R$. Since $(0, a') \in R$, we get that $\{a', 1\} \subseteq U_R(0, 1)$, which is a contradiction. Therefore $(a, 0) \notin R$, and thus, by Definition 2.2-(ii), $a + 0 = a$. ■

**Remark 2.1.** Let us notice that in general an orthogroupoid may falsify equation (2.6), as the orthogroupoid defined by the following table shows $(a + 0 = b)$.

| $+$ | $\mathbf{0}$ | $\mathbf{1}$ | $\mathbf{a}$ | $\mathbf{a'}$ | $\mathbf{b}$ | $\mathbf{b'}$ |
|---|---|---|---|---|---|---|
| $\mathbf{0}$ | 0 | 1 | $a$ | $a'$ | $b$ | $b'$ |
| $\mathbf{1}$ | 1 | 1 | 1 | 1 | 1 | 1 |
| $\mathbf{a}$ | $b$ | 1 | $a$ | 1 | $b$ | 1 |
| $\mathbf{a'}$ | $a'$ | 1 | 1 | $a'$ | 1 | $b'$ |
| $\mathbf{b}$ | $a$ | 1 | $a$ | 1 | $b$ | 1 |
| $\mathbf{b'}$ | $a'$ | 1 | 1 | $a'$ | 1 | $b'$ |

We can now prove a converse of Theorem 2.1 for orthogonal relational systems whose relation is both reflexive and transitive.

**Theorem 2.2.** *Let* $\mathbf{A} = \langle A, R, ', 1\rangle$ *be an orthogonal relational system with a reflexive and transitive relation* $R$. *Then any groupoid* $\mathbf{G}(A) = \langle A, +, ', 1\rangle$ *induced by* $\mathbf{A}$ *is an orthogroupoid.*

*Proof.* Consider an induced groupoid $\mathbf{G}(A) = \langle A, +, ', 1\rangle$ as defined in Definition 2.3. We check that $\mathbf{G}(A)$ is an orthogonal groupoid, i.e. it satisfies all the axioms presented in Definition 2.4.
Axioms (a) and (b) are obviously satisfied. By Lemma 2.4, $\mathbf{G}(A)$ satisfies (f). Now assume $x+z = z$ and $x'+z = z$ for some $x, z \in A$. Then $(x, z) \in R$ and $(x', z) \in R$, thus $z \in U_R(x, x') = \{1\}$, i.e. $z = 1$, proving the quasi-identity (d). It remains to show that (c) and (e) hold true. We first prove (e). Let $x, y, z \in A$ and set $b = (z + y)'$, $a = ((z + y)' + (z + x))'$. By Lemma 2.4 we have $b + a' = a'$, i.e. $(b, a') \in R$, whence $a \perp b$. Let us consider three different cases:
Case 1: $a = 0$, then $((z + y)' + (z + x))' + (z + y)') + z' = (z + y)' + z'$. Now, if $y = 0$ then $(z + y)' + z' = (z + 0)' + z' = z' + z'$, by equation (2.6), and (e) holds.
If $z = 0$ then $(z + y)' + z' = y' + 1 = 1 = z'$, proving (e).
If $x \neq 0 \neq y$ then, by reflexivity and Lemma 2.4, we have $(z, z + y) \in R$ thus also $((z + y)', z') \in R$ and hence $(z + y)' + z' = z'$, as desired.
Case 2: $b = 0$, then $((z+y)'+(z+x))'+(z+y)')+z' = (((0+(z+x))'+0)+z' = (z + x)' + z' = z'$, since Lemma 2.4, Lemma 2.6 and the definition of orthogonal system with involution.
Case 3: $a \neq 0 \neq b$ and $a \perp b$. Since Lemma 2.5, there is a supremal element $w$ for $a, b$ in $U_R(a, b)$ and $w = a+b$. Since $R$ is reflexive, also $(z, z+y) \in R$ by Lemma 2.4. However, $b' = z+y$ thus $(b, z') \in R$. Since $a' = (z+y)'+(z+x)$, also $(z+x, a') \in R$. By by Lemma 2.4 $(z, z+x) \in R$ and, since $R$ is transitive we can conclude $(z, a') \in R$ and also $(a, z') \in R$. Altogether we have shown that $z' \in U_R(a, b)$. Since $a + b$ is a supremal element for $a, b$, this yields $(a + b, z') \in R$. Consequently, $(a + b) + z' = z'$, proving (e).
Finally, we show axiom (c). If $x = 0$ then $x' = 1$ and hence $x+x' = 0+1 = 1$. Similarly for $x = 1$. If $x \neq 0$ and $x \neq 1$ then, since $R$ is reflexive, $x + x' \in U_R(x, x') = \{1\}$, hence $x + x' = 1$ ■

Let us remark that reflexivity and transitivity are necessary conditions to obtain, from Definition 2.3, an orthogroupoid out of an orthogonal relational system.

**Example 2.1.** Let $A = \{0, a, a', 1\}$ and

$$R = \{(a, a'), (a', a), (x, 1), (0, x) \ \ \forall x \in A\}.$$

It can be verified that $\mathbf{A} = \langle A, R, ', 1\rangle$ is an orthogonal relational system. Indeed: $U_R(0, 0') = U_R(1, 1') = \{1\}$; $U_R(a, a') = \{1\}$ and $U_R(a', a) = \{1\}$.

Since $(a, a') \in R$ we have $a \perp a$. $U_R(a, a) = U_R(a) = \{a', 1\}$, thus $a'$ is a supremal element in $U_R(a, a)$. $U_R(a', a') = U_R(a') = \{a, 1\}$, hence $a$ is a supremal element in $U_R(a', a')$. This shows $\mathbf{A} = \langle A, R, ', 1\rangle$ is an orthogonal relational system: notice that $R$ is not reflexive nor transitive.

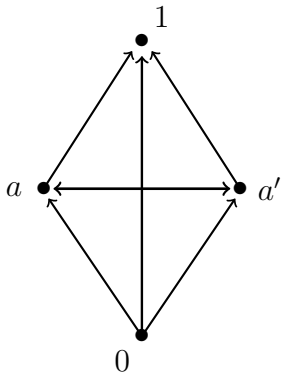



Figure 2.1: The graph of the orthogonal relational system $\mathbf{A}$.

An induced groupoid $\mathbf{G}(A) = \langle A, +, ', 1\rangle$ is defined as follows

| $+$ | $\mathbf{0}$ | $\mathbf{a}$ | $\mathbf{a}'$ | $\mathbf{1}$ |
|---|---|---|---|---|
| $\mathbf{0}$ | 0 | $a$ | $a'$ | 1 |
| $\mathbf{a}$ | $a$ | $a'$ | $a'$ | 1 |
| $\mathbf{a}'$ | $a'$ | $a$ | $a$ | 1 |
| $\mathbf{1}$ | 1 | 1 | 1 | 1 |

It can be seen that $\mathbf{G}(A)$ is not an orthogroupoid, since $a + a' = a' \neq 1$, against Definition 2.4-(c).

By Theorem 2.1, if $\mathbf{G}$ is an orthogroupoid and $R_G$ the induced relation then $R_G$ is reflexive. In order to prove a converse of this statement, in Theorem 2.2 we require, moreover, $R$ to be transitive. In this second example we show that transitivity is a necessary condition to obtain an orthogroupoid out of an orthogonal relational system.

**Example 2.2.** Let $B = \{0, a, b, a', b', c, c', 1\}$ and a binary relation

$$R = \{(a, b), (b, c), (b', a'), (c', b'), (a, c'), (c, a'), (0, x), (x, 1), (x, x) \ \ \forall x \in B\}.$$

It can be easily checked that $U_R(a, a') = U_R(b, b') = U_R(c, c') = \{1\}$. The orthogonal pairs are: $a \perp c, c' \perp b, b' \perp a$ and $U_R(a, c) = U_R(c', b) = U_R(b', a) =$

$\{1\}$. Therefore the structure $\mathbf{B} = \langle B, R, ', 1\rangle$ is an orthogonal relational system whose relation is reflexive but not transitive. By Definition 2.3 we have that $a+b = b$, $a+c' = c'$ and $c+b = c$ since $(c, b) \notin R$ but $(b, c) \in R$. Therefore in any groupoid induced by the system $\mathbf{B}$ axiom (e) in Definition 2.4 is falsified, indeed: $(((a+c')'+(a+b))'+(a+c')')+a' = ((c''+b)'+c'')+a' = (c'+c)+a' = 1+a' = 1$ since $(1, a') \notin R$ and $(a', 1) \in R$, but $a' \neq 1$.

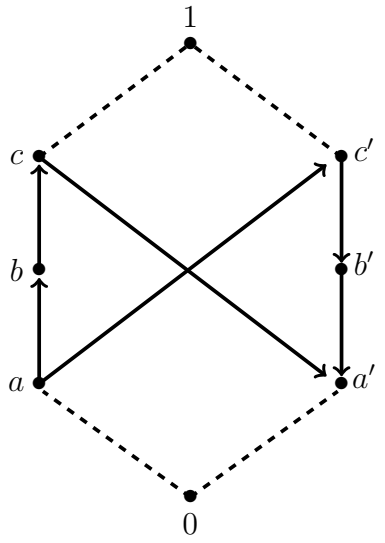



Figure 2.2: The graph representing the orthogonal relational system $\mathbf{B}$ (obvious arrows are omitted).

## 2.2 Central elements and decomposition

The aim of this section is to give a a characterization of the central elements of a variety of orthogroupoids. Contextually a direct decomposition theorem of this variety will follow. The section is based on the ideas developed in [68] and [56] on the general theory of *Church algebras*.

The notion of Church algebra is based on the simple observation that many well-known algebras, including Heyting algebras, rings with unit and combinatory algebras, possess a term $q$, satisfying the equations: $q(1, x, y) = x$ and $q(0, x, y) = y$. The term operation $q$ simulates the behaviour of the

if-then-else connective and, surprisingly enough, this yields strong algebraic properties.

An algebra $\mathbf{A}$ of type $\nu$ is a *Church algebra* if there are term definable elements $0^{\mathbf{A}}, 1^{\mathbf{A}} \in A$ and a term operation $q^{\mathbf{A}}$ s.t., for all $a, b \in A$, $q^{\mathbf{A}}\left(1^{\mathbf{A}}, a, b\right) = a$ and $q^{\mathbf{A}}\left(0^{\mathbf{A}}, a, b\right) = b$. A variety $\mathcal{V}$ of type $\nu$ is a Church variety if every member of $\mathcal{V}$ is a Church algebra with respect to the same term $q\left(x, y, z\right)$ and the same constants $0, 1$.

Taking up an idea from Vaggione [71], we say that an element $e$ of a Church algebra $\mathbf{A}$ is *central* if the congruence relations $\theta(e, 0), \theta(e, 1)$ form a pair of factor congruences on $\mathbf{A}$. A central element $e$ is nontrivial when $e \notin \{0, 1\}$. We denote the set of central elements of $\mathbf{A}$ (the centre) by $\mathrm{Ce}(A)$.

Church varieties are Pierce varieties, in the sense of [39]. Therefore, as a consequence of [39, Theorem 5], every Church algebra has factorable congruences, and then by [7, Corollary 1.4], the lattice of factor congruences is a boolean algebra. Setting

$$x \wedge y = q(x, y, 0), \quad x \vee y = q(x, 1, y) \quad x^* = q(x, 0, 1)$$

we can state the following general result for Church algebras:

**Theorem 2.3.** [68] *Let* $\mathbf{A}$ *be a Church algebra. Then*

$$\mathrm{Ce}(\mathbf{A}) = \langle \mathrm{Ce}(A), \wedge, \vee, ^*, 0, 1 \rangle$$

*is a Boolean algebra which is isomorphic to the Boolean algebra of factor congruences of* $\mathbf{A}$.

If $\mathbf{A}$ is a Church algebra of type $\nu$ and $e \in A$ is a central element, then we define $\mathbf{A}_e = (A_e, g_e)_{g \in \nu}$ to be the $\nu$-algebra defined as follows:

$$A_e = \{e \wedge b : b \in A\}; \quad g_e(e \wedge \overline{b}) = e \wedge g(e \wedge \overline{b}), \tag{2.7}$$

where $\overline{b}$ denotes the a n-tuple $b_1, ..., b_n$ and $e \wedge \overline{b}$ is an abbreviation for $e \wedge b_1, ..., e \wedge b_n$.

By [56, Theorem 4], we have that:

**Theorem 2.4.** *Let* $\mathbf{A}$ *be a Church algebra of type* $\nu$ *and* $e$ *be a central element. Then we have:*

1. *For every $n$-ary $g \in \nu$ and every sequence of elements $\overline{b} \in A^n$, $e \wedge g(\overline{b}) = e \wedge g(e \wedge \overline{b})$, so that the function $h : A \to A_e$, defined by $h(b) = e \wedge b$, is a homomorphism from $\mathbf{A}$ onto $\mathbf{A}_e$.*

2. *$\mathbf{A}_e$ is isomorphic to $\mathbf{A}/\theta(e, 1)$. It follows that $\mathbf{A} = \mathbf{A}_e \times \mathbf{A}_{e'}$ for every central element $e$, as in the Boolean case.*

We call *0-commutative* an orthogroupoid if it satisfies

$$x + 0 = 0 + x. \tag{2.8}$$

Since in Lemma 2.6, we proved that any orthogroupoid induced by an orthogonal relational system fulfills equation (2.8), then the class of 0-commutative orthogroupoid includes the kinds of induced groupoids we took in consideration.

In the context of 0-commutative orthogroupoids, a new operation $x \cdot y$ (multiplication) can be defined *à la De Morgan* by $(x' + y')'$. Few basic properties of multiplication are presented in the following:

**Lemma 2.7.** *Any 0-commutative orthogroupoid satisfies:*

1) $x \cdot 0 = 0 \cdot x = 0$;

2) $x \cdot 1 = 1 \cdot x = x$.

*Proof.* 1) $x \cdot 0 = (x' + 0')' = (x' + 1)' = (1 + x')' = 1' = 0$.
2) $x \cdot 1 = (x' + 1')' = (x' + 0)' = (0 + x')' = x'' = x$. ■

The following proposition shows that the variety of 0-commutative orthogroupoids is a Church variety.

**Proposition 2.2.** *0-commutative orthogroupoids form a Church variety, with witness term*

$$q(x, y, z) = (x + z) \cdot (x' + y).$$

*Proof.* Suppose $\mathbf{A}$ is a 0-commutative orthogroupoid and $a, b \in A$. Then, by Lemma 2.7-(2), $q(1, a, b) = (1 + b) \cdot (0 + a) = 1 \cdot a = a \cdot 1 = a$. Also, $q(0, a, b) = (0 + b) \cdot (1 + a) = b \cdot 1 = b$. ■

According with the results proved in [68], central elements of a Church variety can be described in a very general way.

**Proposition 2.3.** *If* $\mathbf{A}$ *is a Church algebra of type* $\nu$ *and* $e \in A$*, the following conditions are equivalent:*

(1) *e is central;*

(2) *for all* $a, b, \vec{a}, \vec{b} \in A$*:*

**a)** $q(e, a, a) = a$,

**b)** $q(e, q(e, a, b), c) = q(e, a, c) = q(e, a, q(e, b, c))$,

**c)** $q(e, f(\vec{a}), f(\vec{b})) = f(q(e, a_1, b_1), ..., q(e, a_n, b_n))$*, for every* $f \in \nu$,

**d)** $q(e, 1, 0) = e$.

In case $\mathbf{A}$ is a 0-commutative orthogroupoid, condition (a) reduces to

$$(e + a) \cdot (e' + a) = a. \tag{2.9}$$

Conditions (b) read

$$(e + c) \cdot (e' + ((e + b) \cdot (e' + a)) = (e + c) \cdot (e' + a), \tag{2.10}$$

$$(e + c) \cdot (e' + a) = ((e + ((e + c) \cdot (e' + b))) \cdot (e' + a). \tag{2.11}$$

Condition (c), whenever $f$ is equal to the constant 1, expresses a property valid for every element. Indeed $q(e, 1, 1) = (e + 1) \cdot (e' + 1) = 1 \cdot 1 = 1$. If $f$ coincides with the involution, (c) becomes

$$(e + b') \cdot (e' + a') = [(e + b) \cdot (e' + a)]'. \tag{2.12}$$

Finally if $f$ is equal to $+$, we get:

$$(e + (c + d)) \cdot (e' + (a + b)) = ((e + c) \cdot (e' + a)) + ((e + d) \cdot (e' + b)). \tag{2.13}$$

Condition (d) expresses a property that in fact holds for every element: $e \cdot 1 = e$.

**Proposition 2.4.** *Let* $\mathbf{A}$ *be an orthogonal 0-commutative groupoid and* $\mathrm{Ce}(A)$ *the set of central elements of* $\mathbf{A}$*, then* $\mathrm{Ce}(\mathbf{A}) = \langle \mathrm{Ce}(A), +, \cdot, ', 0, 1 \rangle$ *is a Boolean algebra.*

*Proof.* By Theorem 4.12 we only need to check that $\vee$, $\wedge$ and $^*$ correspond to $+$, $\cdot$, $'$, respectively. From Lemma 2.7 we obtain:

$$x \vee y = q(x, 1, y) = (x + y) \cdot (x' + 1) = (x + y) \cdot 1 = x + y$$

$$x^* = q(x, 0, 1) = (x + 1) \cdot (x' + 0) = 1 \cdot (0 + x') = 1 \cdot x' = x'$$

$$x \wedge y = (x^* \vee y^*)^* = (x' + y')' = x \cdot y$$

■

In the following part of the section, we aim at proving a general decomposition result for the variety of 0-commutative orthogroupoids, in terms of central elements. Given $\mathbf{A}$ a 0-commutative orthogroupoid and $e$ a central element of $\mathbf{A}$, we define the set

$$[0, e] = \{x \in A : (x, e) \in R, x + e = e + x\},$$

where $R$ is the relation induced by $\mathbf{A}$.

**Lemma 2.8.** *Let $\mathbf{A}$ be a 0-commutative orthogroupoid and $e$ a central element of $\mathbf{A}$. Then $\mathbf{A}_e = \langle A_e, +_e, {}'^e, e\rangle$ is the algebra $[\mathbf{0}, \mathbf{e}] = \langle [0, e], +, {}^e, e\rangle$, where for any $a \in [0, e]$ $a^e = e \cdot a'$.*

*Proof.* We first prove that $A_e = [0, e]$. Suppose $x \in A_e$, then, by definition of $A_e$, $x = e \wedge b$ for some $b \in A$, i.e. $x = e \wedge b = q(e, b, 0) = e \cdot (e' + b)$. Notice that in any orthogroupoid, $z' + (z' + (z' + y)') = z' + (z' + y)'$ (condition (f) in Definition 2.4), thus by Lemma 2.3 $(z' + (z' + y)')' + z = z$, i.e. $(z \cdot (z' + y)) + z = z$. Hence $x + e = (e \cdot (e' + b)) + e = e$. Furthermore notice that equation (4.12), with $a = 1$ and $c = 0$, reads: $e = (e + (e \cdot (e' + b))$. Hence we get that $e + x = e + (e \cdot (e' + b)) = e$, proving that $x \in [0, e]$, hence we have $A_e \subseteq [0, e]$.
For the converse inclusion suppose $x \in [0, e]$, hence $(x, e) \in R$ and $x + e = e + x = e$. By the property of central elements expressed by equation (4.10), $x = (e + x) \cdot (e' + x) = e \cdot (e' + x) = q(e, x, 0) = e \wedge x$. Thus $x \in A_e$, giving the desired inclusion.

We now prove that, for $x, y \in [0, e]$, $x +_e y = x + y$, where $+_e$ is the operation defined in (4.9). Let $x, y \in [0, e]$, then, by definition, $x + e = e + x = e$ and $y + e = e + y = e$. Then, $x +_e y = e \wedge (x + y) = q(e, x + y, 0) = q(e, x, 0) + q(e, y, 0)$ by condition (c) in Proposition 4.2. By definition of $q$, $q(e, x, 0) + q(e, y, 0) = (e \cdot (e' + x)) + (e \cdot (e' + y))$, but since $e + x = e$ and

$e+y = e$, $(e\cdot(e'+x))+(e\cdot(e'+y)) = ((e+x)\cdot(e'+x))+((e+y)\cdot(e'+y)) = x+y$, by equation (4.10). Thus $x + y \in A_e = [0, e]$ as desired.
As regards $^e$ notice that for any $x \in [0, e]$ we have $x^e = e\cdot x' = (e+0)\cdot(e'+x') = q(e, x', 0) = e \wedge x' = x'^e$. ■

**Theorem 2.5.** *Let* $\mathbf{A}$ *be a* 0*-commutative orthogroupoid and* $e$ *a central element of* $\mathbf{A}$*. Then* $\mathbf{A} \cong [\mathbf{0}, \mathbf{e}] \times [\mathbf{0}, \mathbf{e}']$.

*Proof.* Follows directly from Theorem 4.13, Proposition 2.2 and Lemma 2.8. ■

Proposition 4.2 states that the central elements of a Church variety are characterized by equations. This allows to prove the following

**Proposition 2.5.** *Let* $\mathbf{A}$ *be a* 0*-commutative orthogroupoid,* $e \in \mathrm{Ce}(\mathbf{A})$ *and* $c \in A_e$*. Then*

$$c \in \mathrm{Ce}(A) \Leftrightarrow c \in \mathrm{Ce}(A_e)$$

*Proof.* ($\Rightarrow$) It follows from the fact that 0-commutative orthogroupoids forms a Church variety, hence central elements are described by equations. By Theorem 4.13, $h : \mathbf{A} \to \mathbf{A}_e$ is an onto homomorphism such that for every $a \in A_e$, $h(a) = a$ and homomorphisms preserve equations.
($\Leftarrow$) Since central elements are characterized by equations, if $c_1$ is a central element of a 0-commutative orthogroupoid $\mathbf{A}_1$ and $c_2$ is a central element of a 0-commutative orthogroupoid $\mathbf{A}_2$, then $(c_1, c_2) \in \mathrm{Ce}(\mathbf{A}_1 \times \mathbf{A}_2)$, since equations are preserved by direct products. Suppose $c \in \mathrm{Ce}(A_e)$, the image of $c$ by the isomorphism of Theorem 4.13 is $(c, 0)$. Since 0 is always central, we have that $(c, 0)$ is a central element in $\mathbf{A}_e \times \mathbf{A}_{e'}$, implying that $c \in \mathrm{Ce}(\mathbf{A})$, as $\mathbf{A} \cong \mathbf{A}_e \times \mathbf{A}_{e'}$. ■

In Proposition 4.12 we have proved that $\mathrm{Ce}(\mathbf{A})$ is a Boolean algebra. We can consider the set of its atoms and denote them by $At(\mathbf{A})$.

**Lemma 2.9.** *If* $\mathbf{A}$ *is an orthogroupoid and* $e$ *is an atomic central element of* $\mathbf{A}$*, then* $At(\mathbf{A}_{e'}) = At(\mathbf{A}) \setminus \{e\}$.

*Proof.* ($\supseteq$) Since $e$ is an atom of the Boolean algebra $\mathrm{Ce}(\mathbf{A})$, for any other atomic central element $c \in \mathbf{A}$, $c \cdot e = e \cdot c = 0$, therefore $e' + c' = 1$. By equation (4.10) we get $(e + c') \cdot (e' + c') = c'$, hence $(e + c') \cdot 1 = e + c' = c'$. Thus $eRc'$ (for R the relation induced by the orthogroupoid), then $cRe'$, by Lemma 2.2. Hence $c \in \mathbf{A}_{e'}$. By Proposition 4.4, $c \in \mathrm{Ce}(A_{e'})$. Moreover, if $d$

is a central element of $\mathbf{A}_{e'}$ such that $d < c$, then $d$ is a central element of $\mathbf{A}$ and since $c \in At(\mathbf{A})$ then necessarily $d = 0$.
($\subseteq$) Suppose $c \in At(\mathbf{A}_{e'})$, then in particular $c$ is a central element of $\mathbf{A}_{e'}$ and, by Proposition 4.4, $c \in \mathrm{Ce}(\mathbf{A})$. Let $d \in \mathrm{Ce}(\mathbf{A})$, with $c < d$, then we have $d \leq e'$ and therefore $d \in \mathrm{Ce}(\mathbf{A}_{e'})$ by Proposition 4.4. As, by assumption, $c \in At(\mathbf{A}_{e'})$ then $d = 0$, which shows that $c$ is an atomic central. We now claim that $c \neq e$. Indeed, suppose by contradiction that $c = e$, then since $c \leq e'$ we have $e \leq e'$, i.e. $e = e \cdot e' = 0$ which is a contradiction, as $e$ is atomic central by hypothesis. ■

The above lemma allows to prove the following

**Theorem 2.6.** *Let* $\mathbf{A}$ *be a* 0*-commutative orthogroupoid such that* $\mathrm{Ce}(\mathbf{A})$ *is an atomic Boolean algebra with countably many atoms, then*

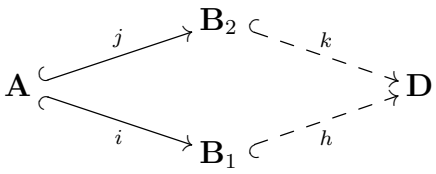
$$\mathbf{A} = \prod_{e \in At(\mathbf{A})} \mathbf{A}_e$$

*is a decomposition of* $\mathbf{A}$ *as a product of directly indecomposable algebras.*

*Proof.* The argument proceeds by induction on the number of elements of $At(\mathbf{A})$. If 1 is the only central atomic element, then $\mathbf{A}$ is directly indecomposable and clearly $\mathbf{A} = \mathbf{A}_1$. If there is an atomic central element $e \neq 1$, then $\mathbf{A} = \mathbf{A}_e \times \mathbf{A}_{e'}$ by Theorem 4.13. On the other hand $\mathrm{Ce}(\mathbf{A}_e) = \{0, e\}$, because if $\mathbf{A}_e$ had another element, say $d$, then $d$ would be a central element of $\mathbf{A}$ in virtue of Proposition 4.4 and $0 < d < e$ contradicting the fact that $e$ is an atom. Consequently $\mathbf{A}_e$ is directly indecomposable. By Lemma 4.8 $At(\mathbf{A}_{e'}) = At(\mathbf{A}) \setminus \{e\}$ and by induction hypothesis, $\mathbf{A}_{e'} = \prod_{c \in At(\mathbf{A}_{e'})} \mathbf{A}_c$, whence the result readily follows. ■

## 2.3 Amalgamation property

A *V-formation* (Figure 2.3) is a 5-tuple $(\mathbf{A}, \mathbf{B}_1, \mathbf{B}_2, i, j)$ such that $\mathbf{A}, \mathbf{B}_1, \mathbf{B}_2$ are similar algebras, and $i : \mathbf{A} \to \mathbf{B}_1, j : \mathbf{A} \to \mathbf{B}_2$ are embeddings. A class $\mathcal{K}$ of similar algebras is said to have the *amalgamation property* if for every V-formation with $\mathbf{A}, \mathbf{B}_1, \mathbf{B}_2 \in \mathcal{K}$ and $A \neq \emptyset$ there exists an algebra $\mathbf{D} \in \mathcal{K}$ and embeddings $h : \mathbf{B}_1 \to \mathbf{D}, k : \mathbf{B}_2 \to \mathbf{D}$ such that $k \circ j = h \circ i$. In such a case, we also say that $k$ and $h$ *amalgamate* the V-formation $(\mathbf{A}, \mathbf{B}_1, \mathbf{B}_2, i, j)$. $\mathcal{K}$ is said




(2.14)

Figure 2.3: A generic amalgamation schema

to have the *strong amalgamation property* if, in addition, such embeddings can be taken s.t. $k \circ j\,(\mathbf{A}) = h\,(\mathbf{B}_1) \cap k\,(\mathbf{B}_2)$.

Amalgamations were first considered for groups by Schreier [69] in the form of amalgamated free products. The general form of the $\mathsf{AP}$ was first formulated by Fraïsse [36], and the significance of this property to the study of algebraic systems was further demonstrated in Jónsson's pioneering work on the topic [47, 48, 49, 50]. The added interest in the $\mathsf{AP}$ for algebras of logic is due to its relationship with various syntactic interpolation properties. We refer the reader to [59] for relevant references and an extensive discussion of these relationships.

In this section, we show that the variety of orthogroupoids has the strong amalgamation property.

**Theorem 2.7.** *The variety of orthogroupoids has the strong amalgamation property.*

*Proof.* Let us suppose that we have a V-formation like the solid part of figure 2.3, and without loss of generality, let us assume that $B_1 \cap B_2 = A$. We are going to give an explicit construction of the amalgam of this V-formation. Let us consider $D = B_1 \cup B_2$. We define an operation $\oplus$ on $D$ as follows:

$$x \oplus y = \begin{cases} x +^{B_i} y, & \text{if } x, y \in B_i; \\ 1, & \text{otherwise.} \end{cases} \tag{2.15}$$

Notice that the assumption $B_1 \cap B_2 = A$ alone does not guarantee that the operation in (2.15) is well defined. Indeed, it may happen that, for some $x, y \in B_1 \cap B_2$, $x +^{B_1} y \neq x +^{B_2} y$. However, we can overcome this problem by assuming that the maps $h, k$ are such that, for any $a \in A$, $(h \circ i)(a) = (k \circ j)(a)$. This can be done without any loss of generality, since, for every V-formation $\langle A, B_1, B_2, i, j\rangle$, the elements can be renamed so to obtain a formation where $B_1 \cap B_2 = A$ and, for any $a \in A$, $(h \circ i)(a) = (k \circ j)(a)$.

From now on we will drop superscripts whenever no danger of confusion is impending. We can define a complementation $^*$ in $D$ as follows:

$$x^* = x^{\prime^{\mathbf{B}_i}} \tag{2.16}$$

Clearly the element 1 belongs to $D$. We show that $\mathbf{D} = \langle D, \oplus, ^*, 1\rangle$ is an orthogroupoid.
(a) $0 \oplus x = x$ holds since $0_{_D} = 0_{B_1} = 0_{B_2}$.
(b) $x \oplus 1 = 1$, since $1_{_D} = 1_{B_1} = 1_{B_2}$.
(c) notice that $x \in B_i$ with $i = 1, 2$ if and only if $x' \in B_i$, hence $x \oplus x^* = x + x' = 1$.
(d) due to Proposition 2.1 it is enough to show that $x + 1 = 1 + x = 1$. Since $1_D = 1_{B_1} = 1_{B_2}$, $1 \oplus x = 1 + x = 1$.
(e) we have to prove that

$$(((x \oplus y)^* \oplus (x \oplus z))^* \oplus (x \oplus y)^*) \oplus x^* = x^*. \tag{2.17}$$

We will proceed through a case-splitting argument.
**Case 1:** $x, y, z \in B_i$, where $i \in \{1, 2\}$. Then equation (2.17) holds since it holds in $B_i$.
**Case 2:** $x, y \in B_i$, $z \in B_j$, $z \notin B_i$, with $i, j \in \{1, 2\}$ and $i \neq j$. Then $x \oplus y = x + y$, while $x \oplus z = 1$. Then equation (2.17) reads: $(((x + y)' + 1)' + (x + y)') + x' = (0 + (x + y)') + x' = (x + y)' + x' = x'$, which holds by Lemma 2.2 (ii).
**Case 3:** $x \in B_i$, $y, z \in B_j$, $z \notin B_i$, with $i \neq j$. We then have $x \oplus y = 1 = x \oplus z$. Therefore $(1^* \oplus (x \oplus z))^* \oplus 1^*) \oplus x^* = ((0 \oplus 1)^* \oplus 0) \oplus x^* = (0 \oplus 0) \oplus x^* = 0 \oplus x^* = x^*$.
**Case 4:** $x, z \in B_i$, $y \in B_j$, $y \notin B_i$, with $i \neq j$. Then $x \oplus y = 1$ and $x \oplus z = x + z$. Equation (2.17) reads: $((0 + (x + z))' + 0) + x' = (x + z)' + x' = x'$, by Lemma 2.2 (ii).
It can be verified that no other case is possible.
(f) $x \oplus (x \oplus y) = x \oplus y$ reduces to $x + (x + y) = x + y$ if $x, y \in B_i$ and clearly holds. In case $x \in B_i$ and $y \in B_j$ and $x, y \notin B_i \cap B_j$, with $i \neq j$, then we get $x \oplus 1 = 1$ which always holds. Similarly for $y \oplus (x \oplus y) = x \oplus y$.
It is clear that $\mathbf{B}_i$ is a subalgebra of $\mathbf{D}$. Furthermore, by construction, the intersection of $\mathbf{B}_1$ and $\mathbf{B}_2$ as subalgebras of $\mathbf{D}$ is the algebra $\mathbf{A}$. Therefore, we have proven that $\mathbf{D}$ is a strong amalgam of $\mathbf{B}_1$ and $\mathbf{B}_2$. ■

As a byproduct of the previous theorem it follows that the orthogonal relational systems induced by the orthogroupoids in a V-formation are amalga-

mated, as relational structures, in the orthogonal relational system induced by their amalgam.

# Chapter 3

# Relational structures and residuation

The aim of this chapter is to further develop the central idea introduced in the previous chapter, namely that of associating an algebra to a certain kind of relational structure. The relational structure under consideration are *residuated*, in the sense that they are equipped with an additional residuated operation. In the same way as relational systems can be viewed as an attempt to a develop a generalization of the theory of partially ordered sets, the structures studied in this chapter aims to be a first step towards a generalization of the theory of (commutative) residuated lattices and of partially ordered commutative residuated monoids.

The chapter is structured as follows: in §3.1 the notion of residuated relational system is introduced and the basic properties are proved; in §3.2 we develop the concept of pre-ordered residuated system, which is nothing but a residuated relational systems whose relation is reflexive and transitive; finally §3.3 is devoted to the study of residuated directoids, an intermediate structure among residuated lattices and partially ordered commutative residuated monoid.

## 3.1 Residuated relational systems

**Definition 3.1.** A *residuated relational system* is a structure $\mathbf{A} = \langle A, \cdot, \to, 1, R\rangle$, where $\langle A, \cdot, \to, 1\rangle$ is an algebra of type $\langle 2, 2, 0\rangle$, while $R$ is a binary relation on $A$. The structure $\mathbf{A}$ satisfies the following properties:

1) $\langle A, \cdot, 1\rangle$ is a commutative monoid;

2) $(x, 1) \in R$, for each $x \in A$;

3) $(x \cdot y, z) \in R$ if and only if $(x, y \to z) \in R$.

We will refer to the operation $\cdot$ as multiplication, to $\to$ as its *residuum* and to condition (3) as *residuation*.
It is easy to notice that whenever the relation $R$ coincides with a partial ordering, then the structure $\mathbf{A}$ coincides with what in the literature is usually referred to as residuated integral pomonoid, see [7] for details. In particular, if $R$ is also a lattice ordering, then the relational system $\langle A, R\rangle$ is a lattice, turning the structure $\mathbf{A}$ into an integral, commutative residuated lattice.

Multiplication, as well as its residuum, can be defined as residuated maps on $A$. More precisely, letting $\mathbf{B} = \langle B, R_1\rangle$ and $\mathbf{C} = \langle C, R_2\rangle$ be two relational systems, we say that a map $f : B \to C$ is *residuated* if there exists a map $g : C \to B$, such that $(f(b), c) \in R_2$ if and only if $(b, g(c)) \in R_1$. The two maps, $f$ and $g$, form a *pair* of residuated maps. Setting $\mathbf{A} = \mathbf{B} = \mathbf{C}$ and defining for any $a \in A$, $f_a(x) = x \cdot a$ and $g_a(x) = a \to x$ we obtain that the two maps $f_a$ and $g_a$ form a residuated pair.

It is useful to recall here the general notions, already introduced in the previous chapter for relational systems, of upper cone, with respect to a pair of elements, and of supremal element.

**Definition 3.2.** For any elements $a, b \in A$, the *upper cone* of $a, b$ is the set

$$U_R(a, b) = \{c \in A : (a, c) \in R \text{ and } (b, c) \in R\}.$$

It is immediate to notice that in a residuated relational system, it may never be the case that $U_R(a, b) = \emptyset$ for any $a, b \in A$, as, by condition 2) in Definition 3.1, $1 \in U_R(a, b)$.

**Definition 3.3.** An element $w \in U_R(a, b)$ is a *supremal element* for $a, b$ if for each $z \in U_R(a, b)$, with $z \neq w$, then $(w, z) \in R$.

Obviously, whenever $R$ is a lattice order relation on $A$, then the supremal element for $a, b \in A$ always exists, is unique and coincides with $\sup(a, b)$. Similarly we can define the notion of supremal element for subsets of $A$: let $Z \subseteq A$, then we say that $\bigsqcup Z$ is a supremal element of $Z$ (with respect to the relation $R$) if $(\bigsqcup Z, z) \in R$, for each $z \in Z$.

The basic properties for residuated relational systems are subsumed in the following:

**Proposition 3.1.** *Let* $\mathbf{A} = \langle A, \cdot, \to, 1, R\rangle$ *be a residuated relational system, then*

a) *if* $x \to y = 1$ *then* $(x, y) \in R$.

b) $(x, 1 \to 1) \in R$, *for each* $x \in A$.

*Proof.* a) Suppose $x \to y = 1$. Since $(1, 1) \in R$ (by condition 2), then $(1, x \to y) \in R$, hence $(1 \cdot x, y) = (x, y) \in R$ by residuation.
b) by axioms (1) and (2) we have that $(x \cdot 1, 1) \in R$, hence, using residuation, $(x, 1 \to 1) \in R$.

■

The next proposition shows that, whenever the relation $R$ is anti-symmetric, then it can be defined in a residuated relational system $\mathbf{A}$ by an identity in the term reduct $\langle A, \cdot, \to, 1\rangle$, turning the residuated relational system $\mathbf{A}$ into an algebra of type $\langle 2, 2, 0\rangle$.

**Proposition 3.2.** *Let* $\mathbf{A} = \langle A, \cdot, \to, 1, R\rangle$ *be a residuated relational system, where* $R$ *is an anti-symmetric relation. Then* $(x, y) \in R$ *if and only if* $x \to y = 1$.

*Proof.* ($\Leftarrow$) holds in any residuated relational system, by Proposition 3.1.
($\Rightarrow$) Suppose that $(x, y) \in R$. Then $(1, x \to y) \in R$, by residuation. On the other hand, by condition 2 in Definition 3.1, $(x \to y, 1) \in R$, and since $R$ is anti-symmetric, it follows that $x \to y = 1$. ■

As already pointed out, residuated relational systems are introduced as a generalization of well known structures as integral and commutative residuated lattices and integral residuated pomonoids. In the following section we aim at studying a particular class of residuated relational systems, namely those whose binary relation $R$ is a pre-order.

## 3.2 Pre-ordered residuated systems

Recall that a pre-order relation on a set $A$ is a binary relation which is reflexive and transitive, which we will refer to as $\preceq$, and that $\langle A, \preceq\rangle$ is a *pre-ordered set*. We introduce the definition of *incomparable* elements on a pre-ordered set.

**Definition 3.4.** Let $\langle A, \preceq \rangle$ be a pre-ordered set and $a, b \in A$ two arbitrary elements. Then $a, b$ are *incomparable*, and we will write $a \parallel b$, with respect to the preorder, if $a \not\preceq b$ and $b \not\preceq a$.

It follows directly from the definition that the relation of incomparability is symmetric. We hereby introduce the formal definition of pre-ordered residuated system.

**Definition 3.5.** A *pre-ordered residuated system* is a residuated relational system $\mathbf{A} = \langle A, \cdot, \to, 1, \preceq \rangle$, where $\preceq$ is a pre-order on $A$, satisfying the further condition: for every $x, y, z \in A$, if $x \preceq y$ and $x \parallel z$, $y \parallel z$ then

$$\exists w \exists u (x, z \preceq w \ \ \textit{and} \ \ y, z \preceq u \ \ \textit{and} \ \ w \preceq u) \tag{3.1}$$

By convention we will indicate the upper cone of two arbitrary elements $x, y$ with $U_{\preceq}(x, y)$. By convention we also set $U_{\preceq}(x, x) = U_{\preceq}(x)$. It readily follows, by transitivity of $\preceq$, that whenever $x \preceq y$ then $U_{\preceq}(y) \subseteq U_{\preceq}(x)$.
The following proposition shows the basic properties of pre-ordered residuated systems.

**Proposition 3.3.** *Let* $\mathbf{A}$ *be a pre-ordered residuated system and* $Z \subseteq A$. *Then the followings hold:*

(a) $1 \preceq x \to 1$;

(b) $\cdot$ *preserves the pre-order in both positions;*

(c) $x \preceq y$ *implies* $y \to z \preceq x \to z$;

(d) $x \preceq y$ *implies* $z \to x \preceq z \to y$;

(e) *Suppose* $\bigsqcup Z$ *exists, then* $a \cdot \bigsqcup Z = \bigsqcup \{a \cdot z : z \in Z\}$;

(f) $1 \preceq (x \to x)$;

(g) $x \cdot y \preceq y$.

*Proof.* (a) $x = 1 \cdot x \preceq 1$, hence $1 \preceq x \to 1$, by residuation.
(b) Suppose $x \preceq y$. Since $\preceq$ is reflexive, $y \cdot z \preceq y \cdot z$, hence $y \preceq z \to (z \cdot y)$. Then, by transitivity, we get $x \preceq z \to (z \cdot y)$, therefore, by residuation, $x \cdot z \preceq y \cdot z$. Preservation of the pre-order in both positions follows trivially by commutativity of multiplication.
(c) Let $x \preceq y$, then $x \cdot (y \to z) \preceq y \cdot (y \to z) \preceq z$, where we have used

commutativity and residuation. By transitivity, $x \cdot (y \to z) \preceq z$, i.e. $y \to z \preceq x \to z$ by residuation (and commutativity).
(d) Let $x \preceq y$. By residuation and reflexivity of $\preceq$, $z \cdot (z \to x) \preceq x$, hence, by transitivity, $z \cdot (z \to x) \preceq y$, thus $z \to x \preceq z \to y$.
(e) Let $\bigsqcup Z = k$. We first show that $a \cdot k$ is an upper bound, with respect to the pre-order $\preceq$ for the set $\{a \cdot z : z \in Z\}$. $k \preceq z$, for each $z \in Z$, then by (b) $a \cdot k \preceq a \cdot z$. Now we show that $a \cdot k$ is *supremal* for the set $\{a \cdot z : z \in Z\}$. Suppose $a \cdot z \preceq m$, then by residuation $z \preceq a \to m$, hence, by transitivity, $k \preceq a \to m$. Thus $a \cdot k \preceq m$.
(f) follows from the fact that $1 \cdot x \preceq x$.
(g) $x \preceq 1 \preceq y \to y$. Hence, by transitivity and residutation, $x \cdot y \preceq y$. ■

Following the ideas developed in [27] and [30] and exploited also in the previous chapter, we can think of capturing some properties of a pre-ordered residuated relational systems by associating them to algebraic structures. We therefore introduce a binary operation as follows

**Definition 3.6.** Let $\mathbf{A} = \langle A, \cdot, \to, 1, \preceq \rangle$ be a pre-ordered residuated relational system. We define the following binary operation $\sqcup$ for any $x, y \in A$ as follows:

i) If $x \preceq y$ then $x \sqcup y = y$;

ii) If $x \not\preceq y$ and $y \preceq x$ then $x \sqcup y = y \sqcup x = x$;

iii) If $x \parallel y$ then $x \sqcup y = y \sqcup x \in U_{\preceq}(x, y)$.

Furthermore we add the following constraint

iv) If $x \preceq y$ and $\forall z$, $z \parallel y$ and $z \parallel x$, then $x \sqcup z$ and $y \sqcup z$ are arbitrarily chosen in $U_{\preceq}(x, z)$ and $U_{\preceq}(y, z)$ respectively, in such a way that $x \sqcup z \preceq y \sqcup z$.

Condition (3.1) and the fact that the upper cone of any two arbitrary elements is always non-empty assure that the operation $\sqcup$ is well defined.

The following elementary fact holds in any pre-ordered residuated system equipped with a binary operation defined as in Definition 3.6.

**Lemma 3.1.** *Let* $\mathbf{A}$ *a pre-ordered residuated system and* $\sqcup$ *a binary operation on* $A$*, defined as in* Definition 3.6*. Then for any* $x, y \in A$, $x \preceq x \sqcup y$ *(and* $y \preceq x \sqcup y$*)*

*Proof.* For any $x, y \in A$, the following cases may arise:

1. $x \preceq y$, then $x \sqcup y = y$ and clearly $x \preceq x \sqcup y$.
2. $x \not\preceq y$ and $y \preceq x$, then $x \sqcup y = x$, hence by reflexivity of $\preceq$, $x \preceq x \sqcup y$.
3. $x \parallel y$, then $x \preceq x \sqcup y$, since $x \sqcup y \in U_{\preceq}(x, y)$.

■

The above lemma expresses the intuitive fact that for any elements $x, y \in A$, $x \sqcup y \in U_{\preceq}(x, y)$.

Now we can give an algebraic counterpart to the concept of pre-ordered residuated system.

**Definition 3.7.** A *pre-ordered residuated quasi-directoid* is an algebra $\mathbf{A} = \langle A, \cdot, \to, \sqcup, 1\rangle$ of type $(2, 2, 2, 0)$ satisfying the following axioms:

a) $\langle A, \cdot, 1\rangle$ is a commutative monoid;

b) $x \sqcup 1 = 1$;

c) $x \sqcup x = x$;

d) $y \sqcup (x \sqcup y) = x \sqcup y$;

e) $x \sqcup ((x \sqcup y) \sqcup z) = (x \sqcup y) \sqcup z$;

f) $(x \cdot y) \sqcup z = z$ iff $x \sqcup (y \to z) = y \to z$.

g) If $x \sqcup y = y$ then $(x \sqcup z) \sqcup (y \sqcup z) = y \sqcup z$.

The terminology introduced in the definition above stresses the similarities with directoids [26]. Therefore the term reduct $\langle A, \sqcup\rangle$ shares similarities with a (join) directoid: indeed any join-directoid satisfies identities (c), (d) and (e). The difference (with respect to a directoid) concerns the failure of the identity $(x \sqcup y) \sqcup x = x \sqcup y$. We will refer to the operation $\sqcup$ as pseudo-join. Quasi identity (f) expresses a condition of residuation, namely the operation $\to$ can be interpreted as the residuum of multiplication.

It is our aim showing a correspondence between pre-ordered residuated systems and pre-ordered residuated quasi-directoids, so that it will appear clear that the latter represent the algebraic counterpart of the former.

**Theorem 3.1.** *Let* $\mathbf{A}$ *be a pre-ordered residuated system, and* $\sqcup$ *a binary operation on* $A$ *defined as in* Definition 3.6. *Then the algebra* $\langle A, \cdot, \to, \sqcup, 1\rangle$ *is a pre-ordered residuated quasi-directoid.*

*Proof.* We proceed checking that $\langle A, \cdot, \to, \sqcup, 1\rangle$ satisfies all the conditions in Definition 3.7.
a) trivially follows from the assumption that $\mathbf{A}$ is a pre-ordered residuated system.
b) $x \sqcup 1 = 1$ since $x \preceq 1$ for each $x \in A$.
c) $x \sqcup x = x$ since $\preceq$ is reflexive.
d) We proceed through a case-splitting argument.
Case 1: let $x \preceq y$. Then by Definition 3.6, $x \sqcup y = y$, hence $y \sqcup (x \sqcup y) = y \sqcup y = y = x \sqcup y$.
Case 2: let $x \not\preceq y$ and $y \preceq x$. Hence $x \sqcup y = y \sqcup x = x$. Then $y \sqcup (x \sqcup y) = y \sqcup x = x = x \sqcup y$.
Case 3: let $x \not\preceq y$ and $y \not\preceq x$. $x \sqcup y \in U_{\preceq}(x, y)$. Since $y \preceq x \sqcup y$, by Lemma 3.1, we get that $y \sqcup (x \sqcup y) = x \sqcup y$.
e) As for d), we consider all the possible cases that may arise.
Case 1: let $x \preceq y$. The right-hand side of equation (d) reads $x \sqcup ((x \sqcup y) \sqcup z) = x \sqcup (y \sqcup z) = y \sqcup z$, since $x \preceq y \preceq y \sqcup z$, by Lemma 3.1. Similarly, under this assumption, the right-hand side reads $(x \sqcup y) \sqcup z = y \sqcup z$.
Case 2: let $x \not\preceq y$ and $y \preceq x$. Then we have $x \sqcup ((x \sqcup y) \sqcup z) = x \sqcup (x \sqcup z) = x \sqcup z$, by Lemma 3.1. On the other hand, the right-hand side reads $(x \sqcup y) \sqcup z = x \sqcup z$.
Case 3: $x \not\preceq y$ and $y \not\preceq x$. Then, by definition, $x \sqcup y = y \sqcup x = w$, for a certain $w \in U_{\preceq}(x, y)$. Therefore, the left-hand side of equation (e) is $x \sqcup ((x \sqcup y) \sqcup z) = x \sqcup (w \sqcup z) = w \sqcup z$, as $x \preceq w \preceq w \sqcup z$. The right-hand side reads $((x \sqcup y) \sqcup z) = w \sqcup z$.
f) follows trivially from the fact that $\mathbf{A}$ is a pre-ordered residuated system.
g) Suppose $x \sqcup y = y$. By Lemma 3.1 $x \preceq x \sqcup y = y$. The following cases shall be considered, seperately.
Case 1: let $x \preceq z$, then $(x \sqcup z) \sqcup (y \sqcup z) = z \sqcup (y \sqcup z) = y \sqcup z$, as by Lemma 3.1 $z \preceq (y \sqcup z)$.
Case 2: let $x \not\preceq z$ and $z \preceq x$. Therefore $(x \sqcup z) \sqcup (y \sqcup z) = x \sqcup (y \sqcup z) = y \sqcup z$, because $x \preceq y \preceq y \sqcup z$.
Case 3: let $x \parallel z$. We claim that also $y \parallel z$. Indeed, assuming that $y \preceq z$ or $z \preceq y$ leads to contradiction with the assumption $x \parallel z$. Therefore, condition (iv) in Definition 3.6 implies that $x \sqcup z \preceq y \sqcup z$, giving the desired conclusion. ∎

It is worthwhile to underline that Theorem 3.1 does not ensure that any member of the class of pre-ordered residuated quasi-directoids is obtained out of a pre-ordered residuated system. It is also clear that in general, any relational system can be associated to more than one quasi-directoid, since for each pair of incomparable elements $x, y$, the element $x \sqcup y$ is not uniquely determined in the upper cone of the two elements.

Following the same idea developed in [27] and in the previous chapter, we can define a relation $\preceq_I$, *induced* by on a pre-ordered quasi-directoid $\mathbf{A}$, as follows:

$$x \preceq_I y \text{ if and only if } x \sqcup y = y. \tag{3.2}$$

Given a pre-ordered residuated quasi-directoid $\mathbf{A}$, we refer to the relational system $\langle A, \cdot, \to, 1, \preceq_I \rangle$, as to the induced relational system.

We can also prove a converse statement of Theorem 3.1, i.e. that the relational system induced by a pre-ordered residuated quasi-directoid is actually a pre-ordered residuated relational system.

**Theorem 3.2.** *Let $\mathbf{A} = \langle A, \cdot, \to, \sqcup, 1 \rangle$ a pre-ordered residuated quasi-directoid and $\preceq_I$ the induced relation on $A$. Then the relational system $\langle A, \cdot, \to, 1, \preceq_I \rangle$ is a pre-ordered residuated relational system.*

*Proof.* Suppose that $\mathbf{A}$ is a pre-ordered residuated quasi-directoid, i.e. it satisfies condition (a)-(f) in Definition 3.7.
We firstly prove that $\preceq_I$ is a pre-order on $A$. Since $x \sqcup x = x$, then $x \preceq_I x$ for each $x \in A$, i.e. $\preceq$ is reflexive. For transitivity, suppose that $a \preceq_I b \preceq_I c$, then $a \sqcup b = b$ and $b \sqcup c = c$. Therefore:

$$\begin{aligned} a \sqcup c &= a \sqcup (b \sqcup c) \\ &= a \sqcup ((a \sqcup b) \sqcup c) \\ &= (a \sqcup b) \sqcup c \\ &= b \sqcup c = c, \end{aligned}$$

hence $a \preceq_I c$. We still need to check that $\langle A, \cdot, \to, 1, \preceq_I \rangle$ satisfies conditions 1), 2), 3) of Definition 3.1 and condition (3.1) in Definition 3.5.
Condition 1) is trivially satisfied.
Conditions 2) and 3) are direct consequences of axiom b) and f), respectively.
Finally, axiom g) guarantees that condition (3.1) holds for $\preceq_I$. ■

The following fact shows that the pseudo-join $\sqcup$ is monotone on the right-hand side.

**Proposition 3.4.** *Let* $\mathbf{A}$ *a pre-ordered residuated quasi-directoid and* $\preceq$ *the pre-order relation induced on* $A$*. For any* $x, y \in A$*, if* $x \preceq y$ *then* $x \sqcup z \preceq y \sqcup z$*.*

*Proof.* Suppose $x \preceq y$, then, by Definition 3.7, $x \sqcup y = y$. Therefore - by condition (g) - $(x \sqcup y) \sqcup (x \sqcup z) = y \sqcup z$, i.e. $x \sqcup z \preceq y \sqcup z$. ■

We recall that any preorder relation on a set $A$ generates an equivalence as follows.

**Definition 3.8.** $(x, y) \in \theta$ *if and only of* $x \preceq y$ *and* $y \preceq x$*.*

The equivalence above turns out to be very useful to get a Pocrim out of pre-ordered residuated system. Moreover, notice that relation $\theta$ can be defined on pre-ordered residuated quasi-directoid using identities, indeed:

$$(x, y) \in \theta \quad \text{iff} \quad x \sqcup y = y \ \text{ and } \ y \sqcup x = x. \tag{3.3}$$

**Proposition 3.5.** *Let* $\mathbf{A}$ *be a pre-ordered residuated quasi-directoid and* $\preceq$ *the induced preorder. The relation* $\theta$ *is a congruence on* $\mathbf{A}$*.*

*Proof.* We already mentioned the fact that $\theta$ is an equivalence relation on $A$. Therefore we need to prove that it preserves operations in the type. Suppose $(x, y) \in \theta$. $(x \cdot z, y \cdot z) \in \theta$, as, by Proposition 3.3, multiplication preserves the preorder. As regards the residual, suppose $(x, y) \in \theta$, then, applying Proposition 3.3 (c)-(d), one gets $(x \to z, y \to z) \in \theta$ and $(z \to x, z \to y) \in \theta$. Finally Proposition 3.4 guarantees that $(x \sqcup z, y \sqcup z) \in \theta$ and $(z \sqcup x, z \sqcup y) \in \theta$ ■

The importance of relation $\theta$ is justified by the fact that the quotient $A/\theta$ turns naturally into a poset.

**Theorem 3.3.** [65, Theorem §5.2] *Let* $\langle A, \preceq \rangle$ *a pre-ordered set and* $\theta$ *the equivalance relation introduced in* Definition 3.8*.* $\theta$ *is an equivalence relation on* $A$ *and the binary relation* $\leq$ *defined on* $A/\theta$ *by:*

$$[a]_\theta \leq [b]_\theta$$

*for any* $[a]_\theta, [b]_\theta \in A/\theta$ *and* $a, b \in A$*, is a partial ordering on* $A/\theta$*.*

From Proposition 3.5 and Theorem 3.3 follows it is always possible to get a Pocrim as a quotient of a pre-ordered residuated quasi-directoid.

**Corollary 3.1.** *Let* $\mathbf{A}$ *a pre-ordered residuated quasi-directoid and* $\theta$ *the relation defined in Definition 3.8. Then* $\mathbf{A}/\theta$ *is a Pocrim.*

We now claim that the residuation condition can be expressed as an identity in the class of pre-ordered residuated quasi-directoid. To support our claim we preliminary prove the following fact.

**Proposition 3.6.** *Let* $\mathbf{A}$ *a pre-ordered residuated quasi-directoid and* $\preceq$ *the pre-order relation induced on* $A$*. Then the followings hold:*

(R1) $(x \to y) \cdot x \preceq y$;

(R2a) $(x \cdot y) \to z \preceq x \to (y \to z)$;

(R2b) $x \to (y \to z) \preceq (x \cdot y) \to z$;

(R3a) $x \to (x \sqcup y) \preceq 1$;

(R3b) $1 \preceq x \to (x \sqcup y)$.

*Proof.* (R1) $x \to y \preceq x \to y$ holds by reflexivity, hence the conclusion is obtained applying residuation.
(R2a) is derived as follows:

$$\begin{aligned}
&(x \cdot y \to z) \cdot (x \cdot y) \preceq z && \text{(R1)}\\
&((x \cdot y \to z) \cdot x) \cdot y \preceq z && \text{(Ass.)}\\
&(x \cdot y \to z) \cdot x \preceq y \to z && \text{(Res.)}\\
&x \cdot y \to z \preceq x \to (y \to z) && \text{(Res.)}
\end{aligned}$$

(R2b) is proved similarly:

$$\begin{aligned}
&x \to (y \to z) \preceq x \to (y \to z)\\
&(x \to (y \to z)) \cdot x \preceq y \to z && \text{(Res.)}\\
&((x \to (y \to z)) \cdot x) \cdot y \preceq z && \text{(Res.)}\\
&(x \to (y \to z)) \cdot (x \cdot y) \preceq z && \text{(Ass.)}\\
&x \to (y \to z) \preceq (x \cdot y) \to z && \text{(Res.)}
\end{aligned}$$

(R3a) is an instance of axiom b).
(R3b) $1 \cdot x = x \preceq x \sqcup y$ by Lemma 3.1, hence by residuation $1 \preceq x \to (x \sqcup y)$. ∎

It is not difficult to see that all the conditions in the proposition above can be expressed by equalities, by simply observing that $x \preceq y$ is equivalent to $x \sqcup y = y$, for each $x, y \in A$. We can now show that the residuation condition for pre-ordered residuated quasi-directoids can be expressed using identities only.

**Proposition 3.7.** *Let* $\mathbf{A}$ *be an algebra in the language of pre-ordered residuated quasi-directoids satisfying all the axioms in* Definition 3.7 *with the exception of condition* (f). *Then* $\mathbf{A}$ *satisfies axiom* (f) *if and only if it satisfies equations* (R1), (R2a), (R2b), (R3a), (R3b).

*Proof.* Observing that Proposition 3.6 has been proved with no use of condition (f), the proof of the right to left direction works as the proof of Proposition 3.6.
For the converse, we have to derive the residuation condition (f) using equations (R1), (R2a), (R2b), (R3a), (R3b). Suppose $a \cdot b \preceq c$, then $(a \cdot b) \sqcup c = c$. By (R3b), $1 \preceq a \cdot b \to (a \cdot b \sqcup c) = a \cdot b \to c \preceq a \to (b \to c)$, by (R2a). Thus $a = 1 \cdot a \preceq (a \to (b \to c)) \cdot a \preceq b \to c$, by (R1), hence $a \preceq b \to c$.
Suppose now that $a \preceq b \to c$, i.e. $a \sqcup (b \to c) = b \to c$. By (R3b) $1 \preceq a \to (a \sqcup (b \to c)) = a \to (b \to c) \preceq a \cdot b \to c$ by equation (R2b). Hence $a \cdot b = 1 \cdot (a \cdot b) \preceq (a \cdot b \to c) \cdot (a \cdot b) \preceq c$ by equation (R1), thus $a \cdot b \preceq c$. ■

It is an open problem to establish whether the class of pre-ordered residuated directoids forms a variety of a proper quasi-variety.

## 3.3 Residuated directoids

We introduce a class of algebras that we will call *residuated involutive directoids*, for short, hereafter, referred to as *residuated directoids*, which is meant to be a generalization of residuated lattices in the non-associative case.

**Definition 3.9.** A residuated directoid is an algebra $\mathbf{A} = \langle A, \cdot, \to, 0, 1, \sqcap \rangle$ of type $\langle 2, 2, 2, 0, 0 \rangle$, satisfying the following properties:

1. $\langle A, \cdot, 1 \rangle$ is a commutative monoid.
2. $\langle A, \sqcap, ', 0, 1 \rangle$ is a bounded involutive commutative directoid, where the involution is defined as $x' := x \to 0$.
3. $x \cdot y \leq z$ if and only if $x \leq y \to z$.

The relation $\leq$ is the partial order induced by the directoid, i.e. $x \leq y$ if and only if $x \sqcap y = x$. Recall that, in an involutive directoid [20], it is possible to define a dual operation á la De Morgan $x \sqcup y = (x' \sqcap y')'$. Since we assume the directoid to be bounded, this means that $x \sqcup 1 = 1$ and $x \sqcap 0 = 0$, i.e. the constant 0 is the least element in the induced order, while 1 is the top element.

(4) expressed the residuation condition.

The following proposition recaps most of the arithmetical properties of residuated directoids. Clearly, some properties holds also for pre-ordered residuated systems and have been proven in Proposition 3.3.

**Proposition 3.8.** *Let* $\mathbf{A}$ *be a residuated directoid,* $Z \subseteq A$ *then:*

(a) $x \to 1 = 1$.

(b) $x \leq y$ *iff* $x \to y = 1$.

(c) $x \to x = 1$.

(d) $x \cdot y \leq y$.

(e) $\cdot$ *is order preserving in both components;*

(f) $x \leq y$ *implies* $y \to z \leq x \to z$;

(g) $x \leq y$ *implies* $z \to x \leq z \to y$;

(h) $1 \to x = x$;

(i) $x \to y = \max\{z : z \cdot x \leq y\}$.

(l) $(x \to y) \cdot x \leq y$.

(m) $(x \to y) \to ((z \to x) \to (z \to y)) = 1$.

*Proof.* Since (a), (d), (e), (f) and (g) hold whenever the relation is a preorder (Proposition 3.3), in particular they hold for the partial order $\leq$.
(b) Suppose $x \leq y$, then by residuation we get that $1 \leq x \to y$, hence $x \to y = 1$. For the converse, suppose $x \to y = 1$; then $1 \leq 1 = x \to y$, by residuation we get $x \leq y$.
(c) Straightforward by (b), since $\leq$ is reflexive.
(h) $a \cdot 1 \leq a$, hence $a \leq 1 \to a$. Furthermore $1 \to a \leq 1 \to a$, thus, by

residuation, $1 \to a \leq a$.
(i) $x \to y \in \{z \cdot x \leq y\}$ is obvious by reflexivity of $\leq$. Now suppose $k \in \{z \cdot x \leq y\}$, then by residuation $k \leq x \to y$. (l) follows by residuation from $x \to y \leq x \to y$.
(m) Since $(x \to y) \cdot ((z \to x) \cdot z) \leq (x \to y) \cdot x \leq y$, the result is obtained using associativity of multiplication, residuation twice and (b).

■

(b) states that the partial ordering induced on $A$ is equivalently defined as $x \to y = 1$. This is in accordance with the content of Proposition 3.2 for residuated relational systems.
Condition (d) looks similar, although weaker, to a property holding in residuated lattices, where $x \cdot y \leq y$ implies $x \cdot y \leq x \wedge y$. This is not the case for residuated directoids, where the pseudo-meet $\sqcap$ differs from a lattice meet, as it is not, in general, the greatest lower bound.
Although the residuation condition is introduced in the form of a quasi identity, we can prove that it can be equivalently replaced by three identities (see Proposition 3.9). Therefore the class of residuated directoids forms an equational class.

**Proposition 3.9.** *The class of residuated directoids forms a finitely based variety. The identities axiomatizing the variety are:*

(L) *equations axiomatising the variety of bounded involutive directoids;*

(M) *equations axiomatising the variety of commutative monoids;*

(R1) $(x \cdot y) \to z = x \to (y \to z)$*;*

(R2) $(x \to y) \cdot x \leq y$*;*

(R3) $(x \sqcap y) \to y = 1$.

*Proof.* Suppose to have a residuated directoid: we show that it satisfies (R1), (R2) and (R3).
(R2) is clearly obtained by residuation from $x \to y \leq x \to y$.
(R3) is obtained by Proposition 3.8-(b), observing that $x \sqcap y \leq y$.
As regards (R1): $x \to (y \to z) \leq x \to (y \to z)$, using residuation twice (and associativity of $\cdot$) we get $(x \to (y \to z)) \cdot (x \cdot y) \leq z$, hence $x \to (y \to z) \leq xy \to z$ (again by residuation). Similarly for the other inequality.
Conversely, we show that residuation can be derived using (L), (M), (R1),

(R2) and (R3). Suppose $a \cdot b \leq c$, hence $(a \cdot b) \sqcap c = a \cdot b$. By (R3) and (R1), $((a \cdot b) \sqcap c) \to c = 1 = a \to (b \to c)$. Therefore $a = 1 \cdot a = (a \to (b \to c)) \cdot a \leq b \to c$ by (R2), hence $a \leq b \to c$.
For the converse, let $a \leq b \to c$. By definition of the order and (R3) we have $(a \sqcap (b \to c)) \to (b \to c) = 1$, hence $a \to (b \to c) = 1$ and by (R1), $(a \cdot b) \to c = 1$. Using (R2), $a \cdot b = 1 \cdot (a \cdot b) = ((a \cdot b) \to c) \cdot a \cdot b \leq c$, hence $a \cdot b \leq c$ as desired. ■

We are going to show that, as for commutative residauted lattices, congruences in residuated directoids correspond to certain subalgebras, which we will refer to as *filters*.

**Definition 3.10.** Let $\mathbf{A}$ be a residuated directoid. A subset $F \subseteq A$ is a filter if and only if, for any $x, y \in A$, the following conditions are satisfied:

(i) If $x \in F$ and $x \leq y$ then $y \in F$,

(ii) If $x, y \in F$ then $x \cdot y \in F$,

(iii) If $x, y \in F$ then $x \sqcap y \in F$,

(iv) If $x \to y \in F$ and $y \to x \in F$ then $(x \sqcap z) \to (y \sqcap z) \in F$.

It follows from condition (i), in the definition above, that whenever $x \in F$ then $x \sqcup y \in F$, since $x \leq x \sqcup y$ for any $x, y$.

It is not difficult to prove that filters are closed under arbitrary intersections (Proposition 3.10). Therefore, given a residuated directoid $\mathbf{A}$, the set of filters forms a complete lattice, which will be denoted by $\mathfrak{Fil}(\mathbf{A})$.

**Proposition 3.10.** *Let $\mathbf{A}$ be a residuated directoid. Then the set of filters of $\mathbf{A}$ is closed under arbitrary intersection.*

*Proof.* Let $\{F_i\}_{i \in \mathcal{I}}$ an indexed family of filters of $\mathbf{A}$. We claim that $\bigcap_{i \in \mathcal{I}} F_i$ is a filter, i.e. we need to prove that it satisfies conditions (i)-(iv) in Definition 3.10. We just show one such condition, as the proof runs analogously for the others. Suppose $a \in \bigcap_{i \in \mathcal{I}} F_i$ and $a \leq b$. Then $a \in F_i$, for all $i \in \mathcal{I}$. Since $F_i$ is a filter for all $i \in \mathcal{I}$, then $b \in F_i$ for all $i \in \mathcal{I}$. Therefore $b \in \bigcap_{i \in \mathcal{I}} F_i$. ■

Conditions (i) and (ii) in Definition 3.10 admit an equivalent characterization using the residual operation, instead of multiplication (Propositions 3.11 and 3.12).

**Definition 3.11.** Let **A** be a residuated directoid. A subset $I \subseteq A$ is an implicative filter if and only if for any $x, y \in A$:

(a) $1 \in I$.

(b) if $x \in I$ and $x \to y \in I$ then $y \in I$.

**Proposition 3.11.** *Every filter F is also an implicative filter.*

*Proof.* We have to show that (a) and (b) are satisfied by F.
(a) Since $F$ is not empty, this means there exists an element $a \in F$, but $a \leq 1$, hence $1 \in F$ by (i).
(b) Let $a \in F$ and $a \to b \in F$. Then, by (ii), $a \cdot (a \to b) \in F$. Since $a \cdot (a \to b) \leq b$, then $b \in F$ by (i). ■

**Proposition 3.12.** *Every implicative filter I is upward closed and closed under multiplication.*

*Proof.* Let $I$ be an implicative filter of a residuated directoid **A**. Suppose $a \in I$ and $a \leq b$. Then by Proposition 3.8 (ii), $a \to b = 1 \in I$, because $I$ is an implicative filter. Therefore $b \in I$, proving that $I$ is upward closed.
Let $a, b \in I$. Since $a \cdot b \leq b$, by Proposition 3.8, we have that $1 = b \to b \leq b \to (a \cdot b)$, hence $b \to (a \cdot b) = 1$. Therefore $a \cdot b \in I$, because $b \in I$ by assumption. This proves the closure of $I$ under multiplication. ■

We aim at showing that the notion of filter introduced above actually corresponds to a *congruence filter*, i.e. we establish a correspondence - more properly a lattice isomorphism - between congruences and filters. In order to have that, let us begin by showing how to get a congruence out of a filter.

**Definition 3.12.** Let **A** be a residuated directoid and $F \subseteq A$ a filter. We define the following binary relation: $\Theta_F = \{(x, y) \in A^2 | x \to y, y \to x \in F\}$.

The binary relation $\Theta_F$ admits an equivalent formulation that will turn out to be useful in what follows.

**Lemma 3.2.** $\Theta_F = \{(x, y) \in A^2 | x \cdot h \leq y, y \cdot h \leq x,$ *for some* $h \in F\}$

*Proof.* Suppose $a \cdot h \leq b$ and $b \cdot h \leq a$ for some $h \in F$. Then, by residuation, $h \leq a \to b$ and $h \leq b \to a$, hence $a \to b \in F$ and $b \to a \in F$ by (i) in Definition 3.10. Conversely, suppose $a \to b \in F$ and $b \to a \in F$, then $(a \to b) \sqcap (b \to a) \in F$, by (iii) in Definition 3.10. Finally, by setting $h = (a \to b) \sqcap (b \to a)$ one gets the desired inclusion. ■

We now show that the relation $\Theta_F$ is actually a congruence on any residuated directoid.

**Theorem 3.4.** *Let* $\mathbf{A}$ *be a residuated directoid and* $F \subseteq A$ *a filter. Then* $\Theta_F$ *is a congruence on* $\mathbf{A}$*.*

*Proof.* We start showing that $\Theta_F$ is an equivalence relation. Reflexivity and symmetry are straightforward. For transitivity, suppose that $(a, b) \in \Theta_F$ and $(b, c) \in \Theta_F$, then, by Lemma 3.2, there exist two elements $h, k \in F$ such that $a \cdot h \leq b$, $b \cdot h \leq a$ and $b \cdot k \leq c$, $c \cdot k \leq b$. Then, since multiplication is monotone (and associative) we get that $(a \cdot h) \cdot k \leq b \cdot k \leq c$, i.e. $a \cdot (h \cdot k) \leq c$. Analogously one gets also that $c \cdot (k \cdot h) \leq a$. Noticing that $h \cdot k = k \cdot h \in F$, because, by Proposition 3.12, filters are closed under multiplication, then $(a, c) \in \Theta_F$.
We next show that $\Theta_F$ is compatible with the operations. Suppose $(a, b) \in \Theta_F$ and $(c, d) \in \Theta_F$. Hence there exists $m, n \in F$ s.t.

$$a \cdot m \leq b \text{ and } b \cdot m \leq a;$$

$$c \cdot n \leq d \text{ and } d \cdot n \leq c.$$

Since $m, n \in F$, also $m \sqcap n \in F$. Let $p = m \sqcap n$. Since $p \leq m$, then $a \cdot p \leq a \cdot m \leq b$, $b \cdot p \leq a$, $c \cdot p \leq d$ and $d \cdot p \leq c$. Since multiplication is monotone we have that $(a \cdot c) \cdot p^2 \leq b \cdot d$ and $(b \cdot d) \cdot p^2 \leq a \cdot c$; obviously $p^2 \in F$, then $(a \cdot c, b \cdot d) \in \Theta_F$.
Let us now focus on the residual. From $b \cdot p \leq a$ we have that $(b \cdot p) \cdot (a \to c) \leq a \cdot (a \to c) \leq c$ (by monotonicity of multiplication and Proposition (3.9), hence $(b \cdot p^2) \cdot (a \to c) \leq p \cdot c \leq d$, where in the last passage we have used the hypothesis. Thus, by residuation $p^2 \cdot (a \to c) \leq b \to d$. Analogously one can prove $p^2 \cdot (b \to d) \leq a \to c$, i.e. $(a \to c, b \to d) \in \Theta_F$.
Finally, since $a \to b \in F$ and $b \to a \in F$, then, by condition (iv) in Definition 3.10, $(a \sqcap c) \to (b \sqcap c) \in F$ and also $(c \sqcap b) \to (d \sqcap b) \in F$ (since $c \to d, d \to c \in F$). Upon setting $x = b \sqcap c = c \sqcap b$, $y = b \sqcap d = d \sqcap b$ and $z = a \sqcap c$, by Proposition 3.8-(m) and the fact that any filter is an implicative filter (Proposition 3.11) we get that $(a \sqcap c) \to (b \sqcap d) \in F$. Analogously one proves that $(b \sqcap d) \to (a \sqcap c) \in F$. ■

We have proved that every filter determines a congruence. We still have to prove the converse, more precisely we claim that the congruence class of the constant 1 gives rise to a filter.

**Theorem 3.5.** *Let* $\mathbf{A}$ *be a residuated directoid and* $\theta$ *a congruence on* $\mathbf{A}$. *Then the subset* $F_\theta \subseteq A$, *defined as* $a \in F_\theta$ *if and only if* $(a, 1) \in \theta$, *is a filter of* $\mathbf{A}$.

*Proof.* We check that every property listed in Definition 3.10 is satisfied by $F_\theta$.
(i) Let $a \in F_\theta$ and $a \leq b$. Then, by definition, $(a, 1) \in \theta$ and since $\theta$ is a congruence (it preserves also the defined operation $\sqcup$), $(a \sqcup b, 1 \sqcup b) \in \theta$. $1 \sqcup b = 1$ and, by assumption, $a \sqcup b = b$, thus $(b, 1) \in \theta$, i.e. $b \in F_\theta$.
(ii) Let $a, b \in F_\theta$, then $(a, 1) \in \theta$ and $(b, 1) \in \theta$. Since $\theta$ is a congruence, $(a \cdot b, 1 \cdot 1) \in \theta$, i.e. $a \cdot b \in F_\theta$.
(iii) Let $a, b \in F_\theta$, then $(a, 1) \in \theta$ and $(b, 1) \in \theta$. Since $1 \sqcap 1 = 1$ and $\theta$ is a congruence, we have that $(a \sqcap b, 1) \in \theta$.
(iv) Suppose $(a \to b, 1) \in \theta$, $(b \to a, 1) \in \theta$. Then $[a]_\theta = [b]_\theta$ and it is easily verified that $(a \sqcap c \to b \sqcap c, 1) \in \theta$. ■

Let $\mathbf{A}$ be a residuated directoid. In the next theorem we prove the isomorphism between $\mathbf{Con}(\mathbf{A})$ and the (complete) lattice of filters on $\mathbf{A}$.

**Theorem 3.6.** *Let* $\mathbf{A}$ *be a residuated directoid. Then* $\mathbf{Con}(\mathbf{A})$ *is isomorphic to* $\mathfrak{Fil}(\mathbf{A})$. *The isomorphism is given by* $\theta \longmapsto F_\theta$ *and* $F \longmapsto \theta_F$.

*Proof.* It is easy to check that the given maps are both isotone. It is sufficient then to prove that they are mutually inverse, i.e. $\theta_{F_\theta} = \theta$ and $F_{\theta_F} = F$.
Let $(a, b) \in \theta_{F_\theta}$, then by Lemma 3.2 there exists an element $h \in F_\theta$ s.t. $a \cdot h \leq b$ and $b \cdot h \leq a$. Theorem 3.5 assures that $F_\theta$ is a filter and so, by definition, $(h, 1) \in \theta$. Since $\theta \in \mathbf{Con}(\mathbf{A})$, also $(a \cdot h, a) \in \theta$ and consequently $((a \cdot h) \sqcup b, a \sqcup b) \in \theta$. Analogously, $((b \cdot h) \sqcup a, a \sqcup b) \in \theta$. Therefore $((b \cdot h) \sqcup a, (a \cdot h) \sqcup b) \in \theta$, i.e. $(a, b) \in \theta$, proving $\theta_{F_\theta} \subseteq \theta$.
Conversely, let $(a, b) \in \theta$, then $(a \to b, 1 \to b) \in \theta$ and $(b \to a, 1 \to a) \in \theta$, i.e. $(a \to b, 1) \in \theta$ and $(b \to a, 1) \in \theta$. By setting $h = (a \to b) \sqcap (b \to a)$ we have that $a \cdot h \leq a \cdot (a \to b) \leq b$ and $b \cdot h \leq b \cdot (b \to a) \leq a$, with $h \in F_\theta$. Therefore $(a, b) \in \theta_{F_\theta}$, showing $\theta \subseteq \theta_{F_\theta}$.
To prove that $F_{\theta_F} = F$, first recall that

$$F_{\theta_F} = \{x \in A : (x, 1) \in F\}$$

Let $a \in F$. By Proposition 3.8, $a \to 1 = 1$ and $1 \to a = a$, therefore $a \to 1 \in F$ and $1 \to a \in F$ and this implies $(a, 1) \in \theta_F$. Hence $a \in F_{\theta_F}$ showing that $F \subseteq F_{\theta_F}$.

Conversely, suppose $a \in F_{\theta_F}$, i.e. $(a, 1) \in \theta_F$. Thus, by Lemma 3.2 there exists an element $h \in F$ s.t. $a \cdot h \leq 1$ and $1 \cdot h \leq a$. Therefore $h \leq a$, which implies $a \in F$, giving $F_{\theta_F} \subseteq F$. ■

# Chapter 4

# Quantum structures as near semirings

Over the last decade, the relations between prominent algebraic structures and (semi)ring theory have stirred increasing attention (see, e.g., [39, 3]). It was shown by Belluce, Di Nola, Ferraioli [4] and Gerla [39] that MV-algebras can be represented by certain semirings, called MV-semirings. We will show in this chapter that this approach can be raised to a considerably more general level. Indeed, we will see that a number of other algebraic structures of prominent importance to non classical logics are representable as semiring-like structures. Our attention will be mainly focused on basic algebras and orthomodular lattices. Basic algebras can not be represented as semirings since they do not satisfy both distributivity laws, but only right-distributivity, and multiplication need not to be associative. These observations suggest that a substantial weakening of the concept of semiring would be required to embrace such algebras. An appropriate generalization can be found in [28, 29] where H. Länger and I. Chajda discuss the concept of *near semiring*. Taking up ideas from [4] and [35], in order to provide a semiring-like representation of basic algebras, we specialize the concept of near semiring and introduce the notion of Łukasiewicz near semiring and orthomodular near semiring.

The chapter is structured as follows: in § 4.1 we introduce the notions of near semiring, near semiring with involution and Łukasiewicz near semiring and discuss some basic properties of these three classes. In § 4.2 we prove that basic algebras can be represented by Łukasiewicz near semirings. In § 4.3 we discuss several universal algebraic properties of Łukasiewicz near

semirings: congruence regularity, congruence permutability and congruence distributivity. In § 4.4 we introduce the concept of orthomodular near semiring, and we show that orthomodular lattices can be represented by means of these algebraic structures. Finally, in § 4.5, we claim that the variety of involutive integral near semirings is a Church variety [68]. This yields an explicit description of central elements and, consequently, a series of direct decomposition theorems.

## 4.1 Near semirings

**Definition 4.1.** A near semiring is an algebra $\mathbf{R} = \langle R, +, \cdot, 0, 1\rangle$ of type $\langle 2, 2, 0, 0\rangle$ such that

(i) $\langle R, +, 0\rangle$ is a commutative monoid;

(ii) $\langle R, \cdot, 1\rangle$ is a groupoid satisfying $x \cdot 1 = x = 1 \cdot x$ (a unital groupoid);

(iii) $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$;

(iv) $x \cdot 0 = 0 \cdot x = 0$.

We will refer to the operations $+$ and $\cdot$ as sum and multiplication, respectively, and we call the identity in (iii) *right distributivity*. Near semirings generalize semirings into a non-associative and weakly-distributive context. Indeed a semiring is a near semiring such that $\langle R, \cdot, 1\rangle$ is a monoid (i.e. $\cdot$ is also associative) that satisfies *left distributivity*, i.e. $x\cdot(y+z) = (x\cdot y)+(x\cdot z)$, for all $x, y, z \in R$. Throughout the chapter, a near semiring $\mathbf{R}$ is called *associative* if it satisfies $(x\cdot y)\cdot z = x\cdot(y\cdot z)$, *commutative* if it satisfies $x\cdot y = y\cdot x$; *idempotent* if it satisfies $x + x = x$ and *integral* if $x + 1 = 1$ holds.

**Remark 4.1.** Let $\mathbf{R}$ be an idempotent near semiring. Then $\langle R, +\rangle$ is a semilattice. In particular, $\langle R, +\rangle$ can be considered as a join-semilattice, where the induced order is defined as $x \leq y$ iff $x + y = y$ and the constant 0 is the least element. Moreover, whenever $\mathbf{R}$ is *integral*, the constant 1 is the greatest element with respect to the induced order $\leq$.

**Remark 4.2.** Let $\mathbf{R}$ be an idempotent commutative semiring, whose multiplication is also idempotent ($x \cdot x = x$). More precisely, we are here considering the commutative version of structures which are usually referred to as *idempotent semirings*, see [73] for details. Then clearly $\langle R, \cdot\rangle$ is also a

semilattice, in particular a meet-semilattice. Notice that in general $\langle R, +, \cdot \rangle$ need not to be a lattice. Indeed, the absorption laws may fail[1], for example the identity $x \cdot (x+y) = x$ does not always hold. Moreover, the order induced by the multiplication, which is $x \leqslant y$ iff $x \cdot y = x$ may differ from $\leq$. These facts are shown in the following example.

**Example 4.1.** Consider a near semiring $\mathbf{R}$, where $R = \{0, 1, a\}$ and whose sum and multiplication are defined by the following tables:

| $+$ | 0 | $a$ | 1 |
|---|---|---|---|
| 0 | 0 | $a$ | 1 |
| $a$ | $a$ | $a$ | $a$ |
| 1 | 1 | $a$ | 1 |

| $\cdot$ | 0 | a | 1 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| $a$ | 0 | $a$ | $a$ |
| 1 | 0 | $a$ | 1 |

It is easy to check that $\mathbf{R}$ is both additively and multiplicatively idempotent, commutative and associative, thus $\langle R, \cdot \rangle$ is a meet-semilattice. Moreover, $\mathbf{R}$ is not integral: as $a + 1 = a \neq 1$; and the absorption laws do not hold: $1 \cdot (a+1) = 1 \cdot a = a \neq 1$. For this reason, the orders induced by $+$ and $\cdot$ are different (see Figure 4.1).

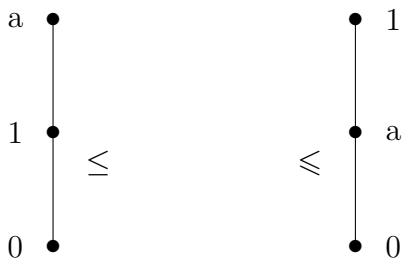



Figure 4.1: The Hasse diagrams of the two partial orderings induced by sum, $\leq$ (left hand side), and multiplication, $\leqslant$ (right hand side).

[1]Let us remark that, since near semirings satisfy right distributivity only, we may have different forms of absorption.

The following lemma states that in any near semiring, multiplication is monotone on the right hand side, due to right distributivity.

**Lemma 4.1.** *Let* $\mathbf{R}$ *be a near semiring. Then,* $x \leq y$ *implies* $x \cdot z \leq y \cdot z$.

*Proof.* Suppose $x \leq y$, i.e. $x+y = y$. Therefore $y \cdot z = (x+y) \cdot z = (x \cdot z)+(y \cdot z)$, which implies that $x \cdot z \leq y \cdot z$. ■

As near semirings are in general not distributive (left distributive indeed does not hold), multiplication is not monotone in the left component. However we will encounter special cases where distributivity holds for some elements, namely for *central elements*.

**Definition 4.2.** Let $\langle R, +, \cdot, 0, 1\rangle$ be an *idempotent* near semiring, with $\leq$ the induced order. A map $\alpha : R \to R$ is called an *involution* on R if it satisfies the following conditions for each $x, y \in R$:

(a) $\alpha(\alpha(x)) = x$;

(b) if $x \leq y$ then $\alpha(y) \leq \alpha(x)$.

The algebra $\mathbf{R} = \langle R, +, \cdot, 0, 1, \alpha\rangle$ will be called an *involutive near semiring*.

Sometimes, if no confusion is possible, we will write $\alpha\alpha x$ in place of $\alpha(\alpha(x))$. Some basic arithmetical properties of involutive near semirings are presented in the following lemma.

**Lemma 4.2.** *Let* $\mathbf{R}$ *be an involutive near semiring . Then*

(i) $\alpha(x + y) + \alpha(x) = \alpha(x)$.

(ii) $\mathbf{R}$ *is* integral *if and only if* $\alpha(0) = 1$ *(and consequently* $\alpha(1) = 0$*).*

*Proof.* (i) Since $+$ is idempotent, we have that $\alpha(x) = \alpha(x)+\alpha(x)$. Moreover, since $x + y = (x + x) + y = x + (x + y)$, $x \leq x + y$ and $\alpha$ is an involution on $R$, $\alpha(x + y) \leq \alpha(x)$. Therefore $\alpha(x + y) + \alpha(x) \leq \alpha(x) + \alpha(x) = \alpha(x)$. The converse $\alpha(x) \leq \alpha(x) + \alpha(x + y)$ holds because $\langle R, +\rangle$ is a join-semilattice as we noticed in Remark 4.1.
(ii) Suppose that $\mathbf{R}$ is integral, i.e. $x \leq 1$ for each $x \in R$, then $\alpha(1) \leq \alpha(x)$. Since $\alpha$ is an involution we have that $\alpha(1) + x = x$ for each $x \in R$, which means that $\alpha(1)$ is a neutral element with respect to the sum and since

$\langle R, +, 0\rangle$ is a (commutative) monoid, the neutral is unique[2], thus $\alpha(1) = 0$ and $\alpha(0) = 1$. For the converse, suppose $\alpha(0) = 1$. Then, by (i), we have that $\alpha(x + y) \leq \alpha(x)$, which, for $x = 0$, implies $\alpha(y) \leq \alpha(0) = 1$, which means that for each $x \in R$ we have $x \leq 1$, i.e. $\mathbf{R}$ is integral. ■

**Remark 4.3.** Notice that, in general, $x \leq \alpha(0)$, however $\alpha(0) = 1$ does not hold in any involutive near semiring (see e.g. Example 4.2), as this would imply that every involutive near semiring is also integral.

**Example 4.2.**

| $'$ | 0 | 1 | 2 |
|---|---|---|---|
| | 2 | 1 | 0 |

| $+$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 1 | 2 |
| 2 | 2 | 2 | 2 |

| $\cdot$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 2 |

**Theorem 4.1.** *Let* $\mathbf{R}$ *be an involutive near semiring and define two new operations as* $x +_\alpha y = \alpha(\alpha(x) + \alpha(y))$ *and* $x \cdot_\alpha y = \alpha(\alpha(x) \cdot \alpha(y))$. *Then:*

(a) $x + y = \alpha(\alpha(x) +_\alpha \alpha(y))$, $x \cdot y = \alpha(\alpha(x) \cdot_\alpha \alpha(y))$;

(b) $\mathbf{R}_\alpha = \langle R, +_\alpha, \cdot_\alpha, \alpha, \alpha(0), \alpha(1)\rangle$ *is an involutive near semiring.*

*Proof.* (a) By definition of $+_\alpha$ we have that $\alpha(\alpha(x) +_\alpha \alpha(y)) = \alpha\alpha(\alpha\alpha(x) + \alpha\alpha(y)) = x + y$. The proof runs analogously for $\cdot_\alpha$.
(b) We start by showing that $\langle R, +_\alpha, \alpha(0)\rangle$ is a commutative monoid. Commutativity of $+_\alpha$ trivially follows by definition. Furthermore:

$$\begin{aligned}
(x +_\alpha y) +_\alpha z &= \alpha(\alpha(x +_\alpha y) + \alpha(z)) && \text{(Def. } +_\alpha\text{)}\\
&= \alpha(\alpha\alpha(\alpha(x) + \alpha(y)) + \alpha(z)) && \text{(Def. } +_\alpha\text{)}\\
&= \alpha((\alpha(x) + \alpha(y)) + \alpha(z)) && \text{(Inv.)}\\
&= \alpha(\alpha(x) + (\alpha(y) + \alpha(z))) && \text{(Ass. } +\text{)}\\
&= \alpha(\alpha(x) + \alpha(y +_\alpha z)) && \text{(Def. } +_\alpha\text{)}\\
&= x +_\alpha (y +_\alpha z) && \text{(Def } +_\alpha\text{)},
\end{aligned}$$

[2]This is in fact valid for semigroups.

proving associativity of $+_\alpha$. Finally,

$$\begin{aligned} x +_\alpha \alpha(0) &= \alpha(\alpha(x) + \alpha(\alpha(0))) && \text{(Def. } +_\alpha) \\ &= \alpha(\alpha(x) + 0) && \text{(Inv.)} \\ &= \alpha(\alpha(x)) = x && \text{(Monoid)} \end{aligned}$$

The fact that $\alpha(0)$ is also a left neutral follows from commutativity. The proof of the fact that $\langle R, \cdot_\alpha, \alpha(1)\rangle$ is a groupoid with $\alpha(1)$ as neutral element is analogous.
Furthermore, $x \cdot_\alpha \alpha(0) = \alpha(\alpha(x) \cdot \alpha(\alpha(0)) = \alpha(\alpha(x) \cdot 0) = \alpha(0)$ and similarly to show that $\alpha(0) \cdot_\alpha x = \alpha(0)$.
It only remains to show that right distributivity holds.

$$\begin{aligned} (x +_\alpha y) \cdot_\alpha z &= \alpha(\alpha(x +_\alpha y) \cdot \alpha(z)) && \text{(Def. } \cdot_\alpha) \\ &= \alpha(\alpha\alpha(\alpha(x) + \alpha(y)) \cdot \alpha(z)) && \text{(Def. } +_\alpha) \\ &= \alpha((\alpha(x) + \alpha(y)) \cdot \alpha(z)) && \text{(Inv.)} \\ &= \alpha((\alpha(x) \cdot \alpha(z)) + (\alpha(y) \cdot \alpha(z))) && \text{(Distr.)} \\ &= (x \cdot_\alpha z) +_\alpha (y \cdot_\alpha z) && \text{(Def.)} \end{aligned}$$

Therefore $\langle R, +_\alpha, \cdot_\alpha, \alpha(0), \alpha(1)\rangle$ is a near semiring. ■

In general, for a given near semiring $\mathbf{R}$, we will refer to $\mathbf{R}_\alpha$ as the *dual* near semiring.

Semirings were previously associated to fuzzy structure. In particular it was shown by Belluce, Di Nola, Ferraioli [4] and Gerla [39] that MV-algebras are term-equivalent to certain semirings. Following the same idea, we aim at showing that some algebraic structures deriving from quantum logics are term equivalent to certain near semirings. For this reason we introduce the notion of Łukasiewicz near semiring.

**Definition 4.3.** Let $\mathbf{R}$ be an involutive near semiring. $\mathbf{R}$ is called a *Łukasiewicz near semiring* if it satisfies the following additional identity

(Ł) $\alpha(x \cdot \alpha(y)) \cdot \alpha(y) = \alpha(y \cdot \alpha(x)) \cdot \alpha(x)$.

A *semiring* satisfying (Ł) will be called a *Łukasiewicz semiring*.

Identity (Ł), in Definition 4.3, clearly reflects Łukasiewicz identity in the standard axiomatization of MV-algebras. As already mentioned, in general the constant 1 need not necessarily be the top element with respect to the

order $\leq$. However, as shown in the next lemma, this is always the case for Łukasiewicz near semiring. This fact will be frequently used throughout the chapter.

**Lemma 4.3.** *Let* $\mathbf{R}$ *be Łukasiewicz near semiring. Then*

(a) $x \cdot \alpha(x) = \alpha(x) \cdot x = 0$;

(b) $\mathbf{R}$ *is integral;*

(c) $x \cdot \alpha(x + y) = 0$;

(d) $(x + y) \cdot \alpha(x) = y \cdot \alpha(x)$;

(e) $x + y = \alpha(\alpha(x \cdot \alpha(y)) \cdot \alpha(y))$.

*Proof.* (a) Let us observe that, upon setting $x = 0$ and $y = 1$ in (Ł), we get $\alpha(0) \cdot \alpha(1) = \alpha(0 \cdot \alpha(1)) \cdot \alpha(1) = \alpha(1 \cdot \alpha(0)) \cdot \alpha(0) = \alpha(\alpha(0)) \cdot \alpha(0) = 0$. Since 0 is the unit with respect to the sum, we have that $0 + \alpha(x) = \alpha(x)$, i.e. $0 \leq \alpha(x)$. Therefore $x \leq \alpha(0)$ and then $x + \alpha(0) = \alpha(0)$. Using these two facts, we obtain

$$\begin{aligned} 0 &= (x + \alpha(0)) \cdot \alpha(1) \\ &= (x \cdot \alpha(1)) + (\alpha(0) \cdot \alpha(1)) && \text{(Distr.)} \\ &= (x \cdot \alpha(1)) + 0 \\ &= x \cdot \alpha(1) \end{aligned}$$

We finally get

$$\begin{aligned} x \cdot \alpha(x) &= \alpha(\alpha(x)) \cdot \alpha(x) \\ &= \alpha(1 \cdot \alpha(x)) \cdot \alpha(x) \\ &= \alpha(x \cdot \alpha(1)) \cdot \alpha(1) && \text{(Ł)} \\ &= \alpha(0) \cdot \alpha(1) \\ &= 0. \end{aligned}$$

Since $\alpha$ is an involution, it follows that also $\alpha(x) \cdot x = 0$.
(b) $\alpha(1) = 1 \cdot \alpha(1) = 0$, by (a). Then by Lemma 4.2 (ii) we have that $\mathbf{R}$ is integral.
(c) Since $x \leq x+y$. Then, by Lemma 4.1, $x \cdot \alpha(x+y) \leq (x+y) \cdot \alpha(x+y) = 0$.
(d) It is enough using right distributivity and (a), indeed $(x + y) \cdot \alpha(x) =$

$(x \cdot \alpha(x)) + (y \cdot \alpha(x)) = 0 + (y \cdot \alpha(x)) = y \cdot \alpha(x)$.
(e)

$$\begin{aligned}
&\alpha(x \cdot \alpha(y)) \cdot \alpha(y) = \alpha(y \cdot \alpha(x)) \cdot \alpha(x) && (\text{Ł})\\
&= \alpha((x + y) \cdot \alpha(x)) \cdot \alpha(x) && (\text{Item (d)})\\
&= \alpha(x \cdot \alpha(x + y)) \cdot \alpha(x + y) && (\text{Ł})\\
&= \alpha(0) \cdot \alpha(x + y) && (\text{Item (c)})\\
&= 1 \cdot \alpha(x + y) && (\text{Item (b)})\\
&= \alpha(x + y).
\end{aligned}$$

Therefore $x + y = \alpha(\alpha(x \cdot \alpha(y)) \cdot \alpha(y))$ ■

Item (d) in Lemma 4.3 states that in a Łukasiewicz near semiring sum can be expressed by means of multiplication. In other words, the variety of Łukasiewicz near semiring can be equivalently axiomatized with multiplication as the only binary operation in the type. It is not difficult to check that commutativity of the sum is assured by (Ł) via Lemma 4.3 (d). The following lemma shows that, in the specific case of Łukasiewicz near semirings, the order induced by the sum is equivalently expressed by multiplication.

**Lemma 4.4.** *Let* $\mathbf{R}$ *be a Łukasiewicz near semiring. Then* $x \leq y$ *if and only if* $x \cdot \alpha(y) = 0$.

*Proof.* Let $a \leq b$, for some $a, b \in R$. Then $a + b = b$ and, by Lemma 4.3-(c), we get that $0 = a \cdot \alpha(a + b) = a \cdot \alpha(b)$.
Conversely, suppose that $a \cdot \alpha(b) = 0$ for some $a, b \in R$.

$$\begin{aligned}
&a + b = \alpha(\alpha(a \cdot \alpha(b)) \cdot \alpha(b))) && (\text{Lemma 4.3(e)})\\
&= \alpha(\alpha(0) \cdot \alpha(b)) && (\text{Assumption})\\
&= b.
\end{aligned}$$

Therefore $a \leq b$. ■

The next Theorem shows the link between Łukasiewicz near semirings and Łukasiewicz semirings.

**Theorem 4.2.** *Let* $\mathbf{R}$ *be a Łukasiewicz near semiring whose multiplication is associative. Then multiplication is also commutative, and therefore* $\mathbf{R}$ *is a commutative Łukasiewicz semiring.*

*Proof.* Suppose $\langle R, \cdot \rangle$ is a semigroup. Then

$$\begin{aligned}
&\alpha(x \cdot y) \cdot (y \cdot x) = (\alpha(x \cdot y) \cdot y) \cdot x && \text{(Assumption)}\\
&= (\alpha(\alpha(y) \cdot \alpha(x)) \cdot \alpha(x)) \cdot x && \text{(Ł)}\\
&= (\alpha(\alpha(y) \cdot \alpha(x)) \cdot (\alpha(x) \cdot x) && \text{(Assumption)}\\
&= (\alpha(\alpha(y) \cdot \alpha(x)) \cdot 0 && \text{(Lemma 4.3)}\\
0.&
\end{aligned}$$

Therefore $\alpha(x \cdot y) \cdot (y \cdot x) = 0$. Analogously, $\alpha(y \cdot x) \cdot (x \cdot y) = 0$. Applying Lemma 4.4 to both the equations, we obtain that $\alpha(x \cdot y) \leq \alpha(y \cdot x)$ and $\alpha(y \cdot x) \leq \alpha(x \cdot y)$. Therefore $\alpha(x \cdot y) = \alpha(y \cdot x)$, i.e. $x \cdot y = y \cdot x$. Therefore, multiplication commutes. Hence, to prove that $\mathbf{R}$ is a Łukasiewicz semiring, it suffices to observe that left distributivity follows straight away from right distributivity. ■

As immediate consequences of the previous result, we have:

**Corollary 4.1.** *Every Łukasiewicz semiring is commutative.*

**Corollary 4.2.** *A Łukasiewicz near semiring is a Łukasiewicz semiring if and only if multiplication is associative.*

Since by Lemma 4.3 any Łukasiewicz near semiring is integral, we can introduce a notion of *interval* on a Łukasiewicz near semiring $\mathbf{R}$: $[a, 1] = \{x \in R : a \leq x\}$. The next results shows how to equip any interval with an antitone involution.

**Theorem 4.3.** *Let* $\mathbf{R}$ *be a Łukasiewicz near semiring,* $\leq$ *the induced order, and* $a \in R$*. The map* $h_a : [a, 1] \to [a, 1]$*, defined by* $x \mapsto x^a = \alpha(x \cdot \alpha(a))$ *is an antitone involution on the interval* $[a, 1]$*.*

*Proof.* We first show that $h_a$ is well defined. Indeed, since $\mathbf{R}$ is integral (Lemma 4.3) we have that $x \leq 1$, thus $x \cdot \alpha(a) \leq 1 \cdot \alpha(a)$ by monotonicity, then $a = \alpha(\alpha(a)) = \alpha(1 \cdot \alpha(a)) \leq \alpha(x \cdot \alpha(a)) = x^a$, i.e. $x^a \in [a, 1]$. Moreover, $h_a$ is antitone. Suppose $x, y \in [a, 1]$ with $x \leq y$. Since multiplication is monotone (Lemma 4.1) we get that $x \cdot \alpha(a) \leq y \cdot \alpha(a)$. Therefore $y^a = \alpha(y \cdot \alpha(a)) \leq \alpha(x \cdot \alpha(a)) = x^a$, i.e. $h_a$ is antitone.
Since for any $x \in [a, 1]$, $a \leq x$, i.e. $a + x = x$, then by Lemma 4.3-(c)

$$a \cdot \alpha(x) = a \cdot \alpha(a + x) = 0 \qquad (*)$$

From this fact we obtain that:

$$\begin{aligned} x^{aa} &= \alpha(x^a \cdot \alpha(a)) = \alpha(\alpha(x \cdot \alpha(a)) \cdot \alpha(a)) && \text{(Definition)} \\ &= \alpha(\alpha(a \cdot \alpha(x)) \cdot \alpha(x)) && (Ł) \\ &= \alpha(\alpha(0) \cdot \alpha(x)) && (*) \\ &= \alpha(1 \cdot \alpha(x)) && \text{(Integrality)} \\ &= \alpha(\alpha(x)) = x. \end{aligned}$$

This shows that $h_a$ is an antitone involution on the interval $[a, 1]$. ■

Let us observe that, in [18, 23], the involution constructed in the theorem above is termed *sectional involution*.

## 4.2 Basic algebras as near semirings

Basic algebras were introduced in the last decade by Chajda, Halaš and Kühr, as a common generalization of both MV-algebras and orthomodular lattices. They can be regarded as a non-associative and non-commutative generalization of MV algebras. These algebras are in bijective correspondence with bounded lattices having an antitone involution on every principal filter (*sectional antitone involutions*). An introductory as well as comprehensive survey on basic algebras can be found in [18].

In this section we discuss the links between Łukasiewicz near semirings and basic algebras. Let us recall that a basic algebra is an algebra $\mathbf{A} = \langle A, \oplus, \neg, 0 \rangle$ satisfying the following identities:

(BA1) $x \oplus 0 = x$;

(BA2) $\neg(\neg x) = x$;

(BA3) $\neg(\neg x \oplus y) \oplus y = \neg(y \oplus \neg x) \oplus x$;

(BA4) $\neg(\neg(\neg(x \oplus y) \oplus y) \oplus z) \oplus (x \oplus z) = 1$,

where $0' = 1$ and (BA3) is the *Łukasiewicz identity*.

It is not difficult to show that every MV algebra is a basic algebra. More precisely the class of MV algebras is a subvariety of the variety of basic

algebras and it is axiomatized by the identity expressing associativity of $\oplus$,[3] see [18]. Every basic algebra is in fact a bounded lattice, where the lattice order is defined as $x \leq y$ iff $x' \oplus y = 1$, the join operation is defined as $x \vee y = (x' \oplus y)' \oplus y$, while the meet is defined á la de Morgan: $x \wedge y = (x' \vee y')'$. It can be verified that 0 and 1 are the bottom and the top elements, respectively, of the lattice.

Conversely, let us remark that, in any bounded lattice with sectional antitone involutions $\langle L, \vee, \wedge, ({}^a)_{a \in L}, 0, 1\rangle$ (see for details [21], [18]), it is possible to define two operations

$$x' = x^0, \quad x \oplus y := (x^0 \vee y)^y, \tag{4.1}$$

such that $\langle L, \oplus, ', 0, 1\rangle$ is a basic algebra. It can be proven that this correspondence is one to one. We will use this fact to establish a correspondence between Łukasiewicz near semirings and basic algebras.

**Theorem 4.4.** *If* $\mathbf{R}$ *is a Łukasiewicz near semiring, then the structure* $\mathbf{B}(\mathbf{R}) = \langle R, \oplus, \alpha, 0\rangle$*, where* $x \oplus y$ *is defined by* $\alpha((\alpha(x) + y) \cdot \alpha(y))$ *is a basic algebra.*

*Proof.* The reduct $\langle R, +, 1\rangle$ is a (join) semilattice whose top element is 1 (Remark 4.1 and Lemma 4.3-(b)). From Theorem 4.1, we have that $\langle R, +_\alpha\rangle$ is the dual meet semilattice. Therefore $\langle R, +, +_\alpha, 0, 1\rangle$ is a bounded lattice. Furthermore, by Theorem 4.3 the map $x \mapsto x^a = \alpha(x \cdot \alpha(a))$ is an antitone involution on the interval $[a, 1]$ for all $a \in R$. So $\langle R, +, +_\alpha, ({}^a)_{a \in R}, 0, 1\rangle$ is a bounded involution lattice with sectional antitone involutions. And therefore it can be made into a basic algebra upon setting the operations as in equations (4.1). It follows that $x^0 = x' = \alpha(x)$ and $x \oplus y = \alpha((\alpha(x) + y) \cdot \alpha(y))$. ■

The next result shows a converse of the previous theorem: any basic algebra induces a Łukasiewicz near semiring.

**Theorem 4.5.** *If* $\mathbf{B} = \langle B, \oplus, ', 0\rangle$ *is a basic algebra, then the structure* $\mathbf{R}(\mathbf{B}) = \langle B, +, \cdot, \alpha, 0, 1\rangle$*, where* $x+y$*,* $x \cdot y$ *and* $\alpha(x)$ *are defined by* $(x' \oplus y)' \oplus y$*,* $(x' \oplus y')'$*,* $x'$*, and* $1 = 0'$*, respectively, is a Łukasiewicz near semiring.*

*Proof.* As we mentioned, in any basic algebras $(x' \oplus y)' \oplus y$ defines a join-semilattice, whose least and greatest elements are, respectively, 0 and 1. This

[3]Indeed, it is shown in [18] that if $\oplus$ is associative then it is also commutative.

assures that $\langle R, +, 0\rangle$ is a commutative monoid. Furthermore, it was shown in [18] that $(x+y)\cdot z = (x\cdot z)+(y\cdot z)$. Let us now prove that 1 is a neutral element for the multiplication. We note that

$$\begin{aligned} x\cdot 1 &= (x'\oplus 1')' && \text{(Def. }\cdot\text{)}\\ &= (x'\oplus 0)' && \text{(Int.)}\\ &= x'' && \text{(BA1)}\\ &= x && \text{(BA2)} \end{aligned}$$

Upon observing that, in basic algebras, $x\oplus 0 = x$ (BA1) implies $0\oplus x = x$, then one analogously proves that $1\cdot x = x$. To prove that 0 is an annhilator of multiplication, we show that

$$\begin{aligned} x\cdot 0 &= (x'\oplus 0')' && \text{(Def. }\cdot\text{)}\\ &= (x'\oplus 1)' && \text{(Int.)}\\ &= 1' && \text{(BA)}\\ &= 0. \end{aligned}$$

The proof that $0\cdot x = 0$ is analogous. Therefore $\mathbf{R}(\mathbf{B})$ is a near semiring. Since $\alpha(x) = x'$, it is clear that it is also an antitone involution. We are left with checking that $\mathbf{R}(\mathbf{B})$ satisfies the conditions of a Łukasiewicz near semiring, Definition 4.3.
As regards condition (Ł),

$$\begin{aligned} \alpha(x\cdot\alpha(y))\cdot\alpha(y) &= ((x\oplus y)'\oplus y)' && \text{(Def.)}\\ &= ((y\oplus x)'\oplus x)' && \text{(BA3)}\\ &= \alpha(y\cdot\alpha(x))\cdot\alpha(x) \end{aligned}$$

This concludes the proof that $\mathbf{R}(\mathbf{B})$ is a Łukasiewicz near semiring. ■

The results above state a correspondence between near Łukasiewicz semirings and basic algebras. In order to analyze the maps used to establish such correspondence, we will refer to the variety of basic algebras and of Łukasiewicz near semiring as $\mathcal{B}$ and $\mathcal{R}$, respectively. In Theorem 4.5 we considered a map $f : \mathcal{B} \to \mathcal{R}$ associating to each basic algebra a Łukasiewicz near semiring $\mathbf{R}(\mathbf{B})$. On the other hand, in Theorem 4.4, we applied a map $g : \mathcal{R} \to \mathcal{B}$, associating to any Łukasiewicz near semiring $\mathbf{R}$ a basic algebra $\mathbf{B}(\mathbf{R})$.

The next theorem shows that $\mathbf{B}(\mathbf{R}(\mathbf{B}))$ actually coincides with $\mathbf{B}$ and, viceversa, that $\mathbf{R}$ coincides with $\mathbf{R}(\mathbf{B}(\mathbf{R}))$.

**Theorem 4.6.** *The maps $f$ and $g$ are mutally inverse.*

*Proof.* We start by checking that $\mathbf{B}(\mathbf{R}(\mathbf{B})) = \mathbf{B}$. We first note that $f(x') = \alpha(x)$ and $g(\alpha(x)) = x'$. Therefore $f(g(\alpha(x))) = \alpha(x)$ and $g(f(x')) = x'$. We have to prove that $x \oplus y = x \mathbin{\widehat{\oplus}} y$, where by $x \mathbin{\widehat{\oplus}} y$ we indicate the sum in $\mathbf{B}(\mathbf{R}(\mathbf{B}))$. We use the fact that $\mathbf{R}(\mathbf{B})$ is a Łukasiewicz near semiring (Theorem 4.5), whose sum and multiplication are indicated by $\widehat{+}$ and $\widehat{\cdot}$, respectively.

$$\begin{aligned}
x \mathbin{\widehat{\oplus}} y &= \alpha((\alpha(x) \mathbin{\widehat{+}} y) \mathbin{\widehat{\cdot}} \alpha(y)) && \text{(Def.)}\\
&= \alpha((\alpha(x) \mathbin{\widehat{\cdot}} \alpha(y)) \mathbin{\widehat{+}} (y \mathbin{\widehat{\cdot}} \alpha(y))) && \text{(Distr.)}\\
&= \alpha((\alpha(x) \mathbin{\widehat{\cdot}} \alpha(y)) \mathbin{\widehat{+}} 0) && \text{(Lemma 4.3)}\\
&= \alpha((\alpha(x) \mathbin{\widehat{\cdot}} \alpha(y)) = x \oplus y.
\end{aligned}$$

This is enough to have that $\mathbf{B}(\mathbf{R}(\mathbf{B})) = \mathbf{B}$. To see that $\mathbf{R}(\mathbf{B}(\mathbf{R})) = \mathbf{R}$ we need to check that $x \mathbin{\widehat{+}} y = x + y$ and $x \mathbin{\widehat{\cdot}} y = x \cdot y$. We begin with the latter equality: $x \mathbin{\widehat{\cdot}} y = (x' \mathbin{\widehat{\oplus}} y')' = x \cdot y$. Concerning the former, we have that $x \mathbin{\widehat{+}} y = (x' \mathbin{\widehat{\oplus}} y)' \mathbin{\widehat{\oplus}} y = \alpha((\alpha(x \cdot \alpha(y))) \cdot \alpha(y)) = x + y$ by Lemma 4.3-(e). ■

As a corollary of the term-equivalence between basic algebras and Łukasiewicz near semirings, we get the one-to-one correspondence between MV-algebras and the variety of commutative Łukasiewicz near semiring. The following results readily follow from Theorems 4.4 and 4.5 and the fact that a basic algebra is an MV-algebra if and only if $\oplus$ is associative.

**Corollary 4.3.** *Let $\mathbf{M} = \langle M, \oplus, ', 0\rangle$ an MV-algebra. Then the structure $\mathbf{R}(\mathbf{M}) = \langle B, +, \cdot, \alpha, 0, 1\rangle$, where $x+y$, $x \cdot y$ and $\alpha(x)$ are defined by $(x' \oplus y)' \oplus y$, $(x' \oplus y')'$, $x'$, and $1 = 0'$ respectively, is a Łukasiewicz semiring.*

**Corollary 4.4.** *Let $\mathbf{R} = \langle R, +, \cdot, \alpha, 0, 1\rangle$ be a Łukasiewicz semiring and let $x \oplus y = \alpha((\alpha(x) + y) \cdot \alpha(y))$. Then $\mathbf{M}(\mathbf{R}) = \langle R, \oplus, \alpha, 0\rangle$ is an MV-algebra.*

Corollaries above are tightly related to a very similar result in [4], where it is shown that to every MV-algebra corresponds an *MV-semiring*: a commutative semiring with involution that satisfies the identity (c) in Lemma 4.3 (in our terminology) and

$$x + y = \alpha(\alpha(x) \cdot \alpha(\alpha(x) \cdot y)). \tag{4.2}$$

## 4.3 Congruence Properties of Łukasiewicz near semirings

In this section we prove several conditions concerning the congruence properties of Łukasiewicz near semirings. Recall that an algebra $\mathbf{A}$ is *congruence regular* if any congruence $\theta \in Con(\mathbf{A})$ is determined by any of its cosets; namely if $\theta, \phi \in Con(\mathbf{A})$ and $a \in A$ then

$$[a]_\theta = [a]_\phi \quad \text{implies} \quad \theta = \phi$$

A variety $\mathcal{V}$ is *congruence regular* if every member of $\mathcal{V}$ is congruence regular. A theorem due to Csákány shows (see [19] for details) that a variety $\mathcal{V}$ is congruence regular if and only if there exists a set of ternary terms $t_i(x, y, z)$ with $i \geq 1$ such that

$$t_i(x, y, z) = z \text{ for any } i \text{ if and only if } x = y$$

An algebra $\mathbf{A}$ is said to be *congruence permutable* if for any two congruences $\theta, \phi \in Con(\mathbf{A})$ it holds that $\theta \circ \phi = \phi \circ \theta$.
An algebra $\mathbf{A}$ is *congruence distributive* if the complete lattice of its congruences is distributive.
A variety $\mathcal{V}$ is congruence permutable (congruence distributive, resp.) if every member of $\mathcal{V}$ is congruence permutable (congruence distributive, resp.).
Finally, an algebra $\mathbf{A}$ is *arithmetical* if it is both congruence permutable and congruence distributive. A variety $\mathcal{V}$ is arithmetical if each algebra $\mathbf{A} \in \mathcal{V}$ is arithmetical.

Recall from chapter 1 that congruence permutability is equivalent to the existence of a certain (uniformly defined) term operation. Precisely, a variety $\mathcal{V}$ is congruence permutable if and only if there exists a ternary term operation $p(x, y, z)$ such that the identities

$$p(x, x, y) = y \text{ and } p(x, y, y) = x$$

hold in $\mathcal{V}$. The term $p$ is usually referred to as a Mal'cev term for $\mathcal{V}$.
Similarly, congruence distributivity is witnessed by the existence of the so-called Jónsson terms. In particular, a variety $\mathcal{V}$ is congruence distributive if there exists a ternary term operation $M(x, y, z)$, for which the identities

$$M(x, x, y) = M(x, y, x) = M(y, x, x) = x$$

hold in $\mathcal{V}$. $M$ is usually referred to as a majority term for $\mathcal{V}$.

**Theorem 4.7.** *The variety of Łukasiewicz near semirings is congruence regular, with witness terms:*

$$\begin{aligned} t_1(x,y,z) = &\quad ((x \cdot \alpha(y)) + (y \cdot \alpha(x)) + z \\ t_2(x,y,z) = &\quad \alpha((x \cdot \alpha(y)) + (y \cdot \alpha(x))) \cdot z \end{aligned}$$

*Proof.* All we need to check is that $t_1(x,y,z) = t_2(x,y,z) = z$ if and only if $x = y$. Suppose that $x = y$; then $t_1(x,x,z) = ((x \cdot \alpha(x)) + (x \cdot \alpha(x)) + z = (0 + 0) + z = 0 + z = z$. On the other hand $t_2(x,x,z) = \alpha((x \cdot \alpha(x)) + (x \cdot \alpha(x))) \cdot z = \alpha(0 + 0) \cdot z = 1 \cdot z = z$. For the converse, suppose $t_1(x,y,z) = t_2(x,y,z) = z$, which, setting $a = (x \cdot \alpha(y)) + (y \cdot \alpha(x))$, reads

$$a + z = z \tag{4.3}$$

$$\alpha(a) \cdot z = z \tag{4.4}$$

Equation (4.3) above implies that $a \leq z$, hence $\alpha(z) \leq \alpha(a)$. We now claim that $a = 0$. Indeed

$$\begin{aligned} a &= \alpha(\alpha(a)) \\ &= \alpha(\alpha(a) + \alpha(z)) && \text{(Eq. (4.3))} \\ &= \alpha(\alpha(a) \cdot z) \cdot z && \text{(Lemma 4.3)} \\ &= \alpha(z) \cdot z && \text{(Eq. (4.4))} \\ &= 0 \end{aligned}$$

Therefore $a = (x \cdot \alpha(y)) + (y \cdot \alpha(x)) = 0$. Since $\langle R, + \rangle$ is a join-semilattice with 0 as least element, $(x \cdot \alpha(y)) + (y \cdot \alpha(x)) = 0$ implies that $x \cdot \alpha(y) = 0$ and $y \cdot \alpha(x) = 0$. Using Lemma 4.4, we get $x \leq y$ and $y \leq x$, proving that $x = y$ as desired. ■

**Theorem 4.8.** *The variety of Łukasiewicz near semirings is arithmetical, with witness Mal'cev term*

$$p(x,y,z) = \alpha((\alpha(x \cdot \alpha(y)) \cdot \alpha(z)) + (\alpha(z \cdot \alpha(y)) \cdot \alpha(x))).$$

*Proof.* We first show that the term $p(x,y,z)$ is a Mal'cev term for the variety of Łukasiewicz near semiring: $p(x,y,y) = x$ and $p(x,x,y) = y$.

$$\begin{aligned} p(x,y,y) &= \alpha((\alpha(x \cdot \alpha(y)) \cdot \alpha(y)) + (\alpha(y \cdot \alpha(y)) \cdot \alpha(x))) \\ &= \alpha((\alpha(x + y) + \alpha(x)) && \text{(Lemma 4.3)} \\ &= \alpha(\alpha(x)) = x && \text{(Lemma 4.2)} \end{aligned}$$

Similarly,

$$\begin{aligned} p(x,x,y) &= \alpha((\alpha(x\cdot\alpha(x))\cdot\alpha(y))+(\alpha(y\cdot\alpha(x))\cdot\alpha(x))) \\ &= \alpha((\alpha(y)+\alpha(x+y)) && \text{(Lemma 4.3)} \\ &= \alpha(\alpha(y))=y && \text{(Lemma 4.2)} \end{aligned}$$

Therefore the variety of Łukasiewicz near semirings is congruence permutable. Moreover, the following ternary term

$$M(x,y,z)=\alpha(\alpha(x)+\alpha(y))+\alpha(\alpha(y)+\alpha(z))+\alpha(\alpha(z)+\alpha(x))$$

is a majority term for the variety of Łukasiewicz near semiring. A simple calculation shows that $M(x,x,y)=M(x,y,x)=M(y,x,x)=x$. This proves that the variety considered is also congruence distributive, hence by definition it is arithmetical as claimed. ■

## 4.4 Orthomodular lattices as near semirings

Orthomodular lattices were introduced in 1936 by Birkhoff and von Neumann, as an algebraic account of the logic of quantum mechanics. A detailed discussion can be found in [5]. The aim of this section is to show that orthomodular lattices are term equivalent to a subvariety of Łukasiewicz near semirings.

Let us briefly recall that an *orthomodular lattice* (*OML*, for short) is an algebra $\mathbf{L}=\langle L,\vee,\wedge,',0,1\rangle$ of type $\langle 2,2,1,0,0\rangle$ such that $\langle L,\vee,\wedge,0,1\rangle$ is a bounded lattice, $'$ is an orthocomplementation, i.e. $x\wedge x'=0$, $x\vee x'=1$. Furthermore $'$ is an involutive, antitone map ($x\leq y$ implies $y'\leq x'$) that satisfies the so called *orthomodular law*:

$$x\leq y \;\;\Rightarrow\;\; y=x\vee(y\wedge x'). \tag{4.5}$$

The orthomodular law can be equivalently expressed by the identity

$$(x\vee y)\wedge(x\vee(x\vee y)')=x, \tag{4.6}$$

which, in turn, is equivalent to the dual form:

$$(x\wedge y)\vee(y\wedge(x\wedge y)')=y. \tag{4.7}$$

In the following lemma we recap some basic facts relative to OMLs which will be useful in what follows. Let $a, b$ two elements of an OML $\mathbf{L}$, we say that $a$ and $b$ *commute* (in symbols $aCb$) iff $a = (a \wedge b) \vee (a \wedge b')$. For the proof of the following lemma see [5] or [52].

**Lemma 4.5.** *Let* $\mathbf{L}$ *be an orthomodular lattice and* $a, b, c \in L$*. Then*

(i) *If* $aCb$ *then* $bCa$

(ii) *If* $a \leq b$ *then* $aCb$

(iii) *If* $aCb$ *then* $aCb'$

(iv) *If two elements among* $a, b, c$ *commutes with the third, then* $(a \vee b) \wedge c = (a \wedge c) \vee (a \wedge c)$ *and* $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$

In the previous section, we introduced Łukasiewicz near semirings as a structure term-equivalent to basic algebras. Here, to provide a similar term equivalence with respect to OMLs, we will consider orthomodular near semirings.

**Definition 4.4.** An *orthomodular near semiring* $\mathbf{R}$ is a Łukasiewicz near semiring that fulfills the following identity:

$$x = x \cdot (x + y) \tag{4.8}$$

The next lemma shows some basic properties of orthomodular near semirings.

**Lemma 4.6.** *Let* $\mathbf{R}$ *be an orthomodular near semiring. Then:*

*(a)* $x \cdot x = x$*;*

*(b)* $x = x \cdot \alpha((\alpha(y \cdot \alpha(x)) \cdot \alpha(x))$*;*

*(c)* $x + \alpha(x) = 1$*;*

*(d) If* $x \leq y$ *then* $x \cdot y = y$*.*

*Proof.* (a) Straightforward, by setting $y = 0$ (or also $x = y$) in equation (4.8).
(b) follows directly using equation (4.8) and Lemma 4.3-(e).
(c) By Lemma 4.3-(e), we have $x + \alpha(x) = \alpha(\alpha(x \cdot x) \cdot x) = \alpha(\alpha(x) \cdot x) = 1$, where we have used (a).
(d) Let $a \leq b$, then $a + b = b$. Therefore $a = a \cdot (a + b) = a \cdot b$. ■

We first show that an orthomodular near semiring can always be obtained out of an OML.

**Theorem 4.9.** *Let* $\mathbf{L} = \langle L, \vee, \wedge, ', 0, 1\rangle$ *an orthomodular lattice and define multiplication via the so-called Sasaki projection:* $x \cdot y := (x \vee y') \wedge y$. *Then* $\mathbf{R}(\mathbf{L}) = \langle L, +, \cdot, ', 0, 1\rangle$ *is an orthomodular near semiring, where* $x+y = x \vee y$.

*Proof.* It is evident that $\langle L, \vee, 0\rangle$ is a commutative, idempotent monoid. Furthermore, $x \cdot 1 = (x \vee 1') \wedge 1 = (x \vee 0) \wedge 1 = x$, and $1 \cdot x = (1 \vee x') \wedge x = 1 \wedge x = x$. Therefore $\langle R, \cdot, 1\rangle$ is a groupoid with 1 as neutral element. To prove right distributivity we make use of Lemma 4.5. Upon observing that $z' \leq x \vee z'$, $z' \leq y \vee z'$, we have that $z'$ commutes (in the sense of Lemma 4.5) with both $x \vee z'$ and $y \vee y'$, therefore $z$ does. For this reason we get:

$$\begin{aligned}
&(x \vee y) \cdot z = ((x \vee y) \vee z') \wedge z && \text{(Definition)}\\
&= ((x \vee z') \vee (y \vee z')) \wedge z && \text{(Lattice prop.)}\\
&= ((x \vee z') \wedge z) \vee ((y \vee z') \wedge z) && \text{(Lemma 4.5-(iv))}\\
&= (x \cdot z) \vee (y \cdot z).
\end{aligned}$$

It is not difficult to check that 0 annihilates multiplication. Indeed, $x \cdot 0 = (x \vee 0') \wedge 0 = 0$ and $0 \cdot x = (0 \vee x') \wedge x = x' \wedge x = 0$. We now show that $\mathbf{R}(\mathbf{L})$ is Łukasiewicz near semiring (see Definition 4.3). First let us observe that:

$$\begin{aligned}
&(x \cdot y')' \cdot y' = (((x \vee y) \wedge y')' \vee y) \wedge y' && \text{(Definition)}\\
&= (((x \vee y)' \vee y) \vee y) \wedge y' && \text{(De Morgan)}\\
&= ((x \vee y)' \vee y) \wedge y' && \text{(Ass., Idem.)}
\end{aligned}$$

Reasoning similarly one gets $(y \cdot x')' \cdot x' = ((x \vee y)' \vee x) \wedge x'$.
Simply observing that $x \leq x \vee y$ and applying the orthomodular law, we have $x \vee y = x \vee ((x \vee y) \wedge x')$. Therefore,

$$\begin{aligned}
&(x \vee y)' = (x \vee ((x \vee y) \wedge x'))'\\
&= x' \wedge ((x \vee y) \wedge x')' && \text{(De Morgan)}\\
&= x' \wedge ((x \vee y)' \vee x) && \text{(De Morgan)}\\
&= ((x \vee y)' \vee x) \wedge x' && \text{(Comm.)}\\
&= (y \cdot x')' \cdot x'
\end{aligned}$$

Analogously, using the fact that $y \leq x \vee y$ one gets, by the orthomodular law, that $(x \vee y)' = ((x \vee y)' \vee y) \wedge y' = (x \cdot y')' \cdot y'$. Therefore $(x \cdot y')' \cdot y' = (y \cdot x')' \cdot x'$

as claimed. We finally check that also equation (4.8) holds. This is a simple consequence of the orthomodular law: $x \cdot (x+y) = (x \vee (x \vee y)') \wedge (x \vee y) = x$ by equation (4.6). Therefore, $\mathbf{R}(\mathbf{L}) = \langle L, \vee, \cdot, ', 0, 1 \rangle$ is an orthomodular near semiring.[4] ■

We can also prove the converse, stating a correspondence between orthomodular lattices and orthomodular near semirings.

**Theorem 4.10.** *Let* $\mathbf{R}$ *be an orthomodular near semiring. Setting* $x \vee y = x + y$, $x' = \alpha(x)$, *and then defining* $x \wedge y = (x' \vee y')'$, *then* $\mathbf{L}(\mathbf{R}) = \langle R, \vee, \wedge, ', 0, 1 \rangle$ *is an orthomodular lattice.*

*Proof.* Since $\mathbf{R}$ is integral we know that $\langle R, + \rangle$ is a join-semilattice with 1 as top element, and consequently $\langle R, \vee \rangle$ is. On the other hand, since $\alpha$ is an antitone involution then $\langle R, \wedge \rangle$ is a meet-semilattice with 0 as least element. As meet and join are defined dually, $\langle R, \vee, \wedge, 0, 1 \rangle$ is a bounded lattice. Furthermore, $x \vee x' = 1$ is guaranteed by Lemma 4.6 and thus it follows that $x \wedge x' = 0$.
We are left with the task of showing that the orthomodular law holds too. So, suppose $a \leq b$, then

$$\begin{aligned}
a \vee (b \wedge a') &= a + \alpha(\alpha(b) + a) \\
&= a + \alpha(a + \alpha(b)) && \text{(Comm.)} \\
&= a + (\alpha(a \cdot b) \cdot b) && \text{(Lemma 4.3)} \\
&= (a \cdot b) + (\alpha(a) \cdot b) && \text{(Lemma 4.6-(d))} \\
&= (a + \alpha(a)) \cdot b && \text{(Distr.)} \\
&= 1 \cdot b = b.
\end{aligned}$$

This allows to conclude that $\mathbf{L}(\mathbf{R})$ is an orthomodular lattice. ■

The theorems above have shown how to get an orthomodular lattice out of an orthomodular semirings and viceversa. In other words, there are maps $f$, $g$, from the variety of orthomodular lattices to the variety of orthomodular semiring and from the variety of orthomodular near semirings to the variety of orthomodular lattices, respectively, assigning to any OML an orthomodular semiring, and vice versa. We now show that:

[4] Notice that $\langle L, \vee, \cdot \rangle$, in general, is not a lattice.

**Theorem 4.11.** *The maps $f$ and $g$ are mutually inverse:* $\mathbf{L} = \mathbf{L}(\mathbf{R}(\mathbf{L}))$ *and* $\mathbf{R} = \mathbf{R}(\mathbf{L}(\mathbf{R}))$.

*Proof.* Let $\mathbf{L}\langle L, \vee, \wedge, ', 0, 1\rangle$ be an orthomodular lattice. It follows from Theorem 4.9 that $\mathbf{R}(\mathbf{L})$ is an orthomodular near semiring, and from Theorem 4.10 that the structure $\mathbf{L}(\mathbf{R}(\mathbf{L})) = \langle L, \bar{\vee}, \bar{\wedge}, ', 0, 1\rangle$ is an orthomodular lattice. It is straightforward to check that the involutions on $\mathbf{L}(\mathbf{R}(\mathbf{L}))$ and $\mathbf{L}$ coincide, as well as $x \bar{\vee} y = x \vee y$. Therefore we also have that $x \bar{\wedge} y = (x' \bar{\vee} y')' = (x' \vee y')' = x \wedge y$. So $\mathbf{L} = \mathbf{L}(\mathbf{R}(\mathbf{L}))$.
On the other hand, by Theorems 4.9 and 4.10 we obtain that the structure $\mathbf{R}(\mathbf{L}(\mathbf{R})) = \langle R, \widehat{+}, \widehat{\cdot}, \widehat{\alpha}, 0, 1\rangle$ is an orthomodular near semiring. Again it is straightforward to check that $\widehat{\alpha}(x) = \alpha(x)$ and $x \mathbin{\widehat{+}} y = x + y$. It is less evident that $x \mathbin{\widehat{\cdot}} y = x \cdot y$. Indeed:

$$\begin{aligned} x \mathbin{\widehat{\cdot}} y &= (x \vee y') \wedge y \\ &= ((x \vee y')' \vee y')' \\ &= \alpha(\alpha(x + \alpha(y)) + \alpha(y)), \end{aligned}$$

where $\vee$, $\wedge$ and $'$ are join, meet and complementation, respectively, of the orthomodular lattice $\mathbf{L}(\mathbf{R})$. We are finally left with showing that $\alpha(\alpha(x + \alpha(y)) + \alpha(y)) = x \cdot y$.
Our first move is to prove that $\alpha(\alpha(x + \alpha(y)) + \alpha(y)) = y \cdot (x + \alpha(y))$.

$$\begin{aligned} &\alpha(\alpha(x + \alpha(y)) + \alpha(y)) = \alpha(\alpha(y) + \alpha(x + \alpha(y))) && \\ &= \alpha(\alpha(y) \cdot (x + \alpha(y))) \cdot (x + \alpha(y)) && \text{(Lemma 4.3)} \\ &= \alpha(\alpha(y)) \cdot (x + \alpha(y)) && \text{(4.8)} \\ &= y \cdot (x + \alpha(y)). && \end{aligned}$$

Moreover,

$$\begin{aligned} &\alpha((x \cdot y) \cdot y = \alpha((x \cdot y) + \alpha(y)) && \text{(Lemma 4.3)} \\ &= \alpha(\alpha(y) + (x \cdot y)) && \text{(Comm.)} \\ &= \alpha(\alpha(y) \cdot \alpha(x \cdot y)) \cdot \alpha(x \cdot y) && \text{(Lemma 4.3)} \\ &= \alpha(\alpha(y)) \cdot \alpha(x \cdot y) && \text{(by Lemma 4.6, since } \alpha(y) \leq \alpha(x \cdot y)) \\ &= y \cdot \alpha(x \cdot y). && \end{aligned}$$

Using the derivation above, which we will refer to as $(\star)$, we finally prove our claim:

$$\begin{aligned}
y \cdot (x + \alpha(y)) &= y \cdot \alpha(\alpha(x \cdot y) \cdot y) && \text{(Lemma 4.3)} \\
&= \alpha((\alpha(x \cdot y) \cdot y) \cdot y) \cdot y && (\star) \\
&= \alpha(\alpha(x \cdot y) \cdot y) \cdot y && \text{(by Lemma 4.6, since } \alpha(x \cdot y) \cdot y \leq y) \\
&= (x + \alpha(y)) \cdot y && \text{(Lemma 4.3)} \\
&= (x \cdot y) + (\alpha(y) \cdot y) && \text{(Right Distr.)} \\
&= x \cdot y. && \text{(Lemma 4.3)}
\end{aligned}$$

■

## 4.5 Central elements and decomposition

The aim of this section is to give a a characterization of the central elements and consequently some decomposition theorems for the variety of integral involutive near semirings. Such results apply to both the variety of Łukasiewicz near semirings and orthomodular near semirings as the they are both integral. The section is based on the ideas developed in [68] and [56] on the general theory of *Church algebras*.

Recall from chapter 2 that a Church algebra is an algebra possessing a ternary term operation $q$, satisfying the equations: $q(1, x, y) = x$ and $q(0, x, y) = y$. The term operation $q$ simulates the behavior of the if-then-else connective and, surprisingly enough, this yields rather strong algebraic properties.

An algebra $\mathbf{A}$ of type $\nu$ is a *Church algebra* if there are term definable elements $0^{\mathbf{A}}, 1^{\mathbf{A}} \in A$ and a ternary term operation $q^{\mathbf{A}}$ s.t., for all $a, b \in A$, $q^{\mathbf{A}}\left(1^{\mathbf{A}}, a, b\right) = a$ and $q^{\mathbf{A}}\left(0^{\mathbf{A}}, a, b\right) = b$. A variety $\mathcal{V}$ of type $\nu$ is a Church variety if every member of $\mathcal{V}$ is a Church algebra with respect to the same term $q\,(x, y, z)$ and the same constants $0, 1$.

Taking up an idea from D. Vaggione [71], we say that an element $e$ of a Church algebra $\mathbf{A}$ is *central* if the pair $(\theta(e, 0), \theta(e, 1))$ is a pair of factor congruences on $\mathbf{A}$. A central element $e$ is nontrivial when $e \notin \{0, 1\}$. We denote the set of central elements of $\mathbf{A}$ (the centre) by $\mathrm{Ce}(A)$.

Setting

$$x \wedge y = q(x, y, 0), \quad x \vee y = q(x, 1, y) \quad x^* = q(x, 0, 1)$$

we can state the following general result for Church algebras:

**Theorem 4.12.** [68] *Let* $\mathbf{A}$ *be a Church algebra. Then*

$$\mathrm{Ce}(\mathbf{A}) = \langle \mathrm{Ce}(A), \wedge, \vee, ^*, 0, 1\rangle$$

*is a Boolean algebra which is isomorphic to the Boolean algebra of factor congruences of* $\mathbf{A}$.

If $\mathbf{A}$ is a Church algebra of type $\nu$ and $e \in A$ is a central element, then we define $\mathbf{A}_e = (A_e, g_e)_{g\in\nu}$ to be the $\nu$-algebra defined as follows:

$$A_e = \{e \wedge b : b \in A\}; \quad g_e(e \wedge \overline{b}) = e \wedge g(e \wedge \overline{b}), \tag{4.9}$$

where $\overline{b}$ denotes the a n-tuple $b_1, ..., b_n$ and $e \wedge \overline{b}$ is an abbreviation for $e \wedge b_1, ..., e \wedge b_n$.

By [56, Theorem 4], we have that:

**Theorem 4.13.** *Let* $\mathbf{A}$ *be a Church algebra of type* $\nu$ *and* $e$ *be a central element. Then we have:*

1. *For every n-ary* $g \in \nu$ *and every sequence of elements* $\overline{b} \in A^n$, $e \wedge g(\overline{b}) = e \wedge g(e \wedge \overline{b})$, *so that the function* $h : A \to A_e$, *defined by* $h(b) = e \wedge b$, *is a homomorphism from* $\mathbf{A}$ *onto* $\mathbf{A}_e$.

2. $\mathbf{A}_e$ *is isomorphic to* $\mathbf{A}/\theta(e, 1)$. *It follows that* $\mathbf{A} = \mathbf{A}_e \times \mathbf{A}_{e'}$ *for every central element* $e$, *as in the Boolean case.*

**Proposition 4.1.** *The class of intergral involutive near semirings is a Church variety, as witnessed by the term:*

$$q(x, y, z) = (x \cdot y) + (\alpha(x) \cdot z).$$

*Proof.* Suppose $\mathbf{R}$ is an integral involutive near semiring and $a, b \in R$. Then $q(1, a, b) = (1 \cdot a) + (\alpha(1) \cdot b) = a + (0 \cdot b) = a + 0 = a.$ and $q(0, a, b) = (0 \cdot a) + (\alpha(0) \cdot b) = 0 + (1 \cdot b) = 0 + b = b.$ ■

Since both the varieties of Łukasiewicz and orthomodular near semirings are subvarieties of integral involutive near semiring, it follows that both of them are Church varieties. In this section we apply the theory of Church algebras to the more general class of integral involutive near semirings. According with the results in [68, Proposition 3.6], in a Church variety central elements are amenable to a very general description.

**Proposition 4.2.** *If* $\mathbf{A}$ *is a Church algebra of type* $\nu$ *and* $e \in A$*, the following conditions are equivalent:*

(1) *e is central;*

(2) *for all* $a, b, \vec{a}, \vec{b} \in A$*:*

**a)** $q(e, a, a) = a$,

**b)** $q(e, q(e, a, b), c) = q(e, a, c) = q(e, a, q(e, b, c))$,

**c)** $q(e, f(\vec{a}), f(\vec{b})) = f(q(e, a_1, b_1), ..., q(e, a_n, b_n))$, *for every* $f \in \nu$,

**d)** $q(e, 1, 0) = e$.

In case $\mathbf{A}$ is an integral involutive near semiring, condition (a) reduces to

$$(e \cdot a) + (\alpha(e) \cdot a) = a. \tag{4.10}$$

Conditions (b) read

$$(e \cdot ((e \cdot a) + (\alpha(e) \cdot b))) + (\alpha(e) \cdot c)) = (e \cdot a) + (\alpha(e) \cdot c), \tag{4.11}$$

$$(e \cdot a) + (\alpha(e) \cdot c) = (e \cdot a) + (\alpha(e) \cdot ((e \cdot b) + (\alpha(e) \cdot c))). \tag{4.12}$$

Condition (c), whenever $f$ is the constant 0, expresses a property that holds for every element: $(e \cdot 0) + (\alpha(e) \cdot 0) = 0$. On the other hand, if $f$ coincides with the nullary operation 1, we obtain (for a central element $e$)

$$q(e, 1, 1) = (e \cdot 1) + (\alpha(e) \cdot 1) = e + \alpha(e) = 1. \tag{4.13}$$

If $f$ coincides with the involution, (c) reads

$$(e \cdot \alpha(a)) + (\alpha(e) \cdot \alpha(b)) = \alpha((e \cdot a) + (\alpha(e) \cdot b)). \tag{4.14}$$

Whenever $f$ is $+$, we obtain:

$$(e \cdot (a + c)) + (\alpha(e) \cdot (b + d)) = ((e \cdot a) + (\alpha(e) \cdot b)) + ((e \cdot c) + (\alpha(e) \cdot d)), \tag{4.15}$$

this, by the associativity of the sum, is equal to

$$((e \cdot a) + (e \cdot c)) + ((\alpha(e) \cdot b) + (\alpha(e) \cdot d)), \tag{4.16}$$

which is a sort of distributivity for central elements. Whenever $f$ is the multiplication, this condition simplifies to

$$(e \cdot (a \cdot c)) + (\alpha(e) \cdot (b \cdot d)) = ((e \cdot a) + (\alpha(e) \cdot b)) \cdot ((e \cdot c) + (\alpha(e) \cdot d)). \quad (4.17)$$

Condition (d) expresses a general property that holds true for every element: $(e \cdot 1) + (\alpha(e) \cdot 0) = e + 0 = e$. Proposition 4.2 states that, in Church algebras, central elements can be described by means of identities. This, in fact, will be very useful in proving the results in this section. However, we aim to show that the axiomatization of central elements can be streamlined to a *minimal set* (see Appendix 4.6) of two identities. The following lemma introduces some results which are very useful to prove the minimality of such an axiomatization.

**Lemma 4.7.** *Let* $\mathbf{R}$ *be an integral involutive near semiring, and* $e \in R$ *an element that satisfies the following identities:*

1. $(e \cdot \alpha(x)) + (\alpha(e) \cdot \alpha(y)) = \alpha((e \cdot x) + (\alpha(e) \cdot y))$;
2. $(e \cdot (x \cdot z)) + (\alpha(e) \cdot (y \cdot u)) = ((e \cdot x) + (\alpha(e) \cdot y)) \cdot ((e \cdot z) + (\alpha(e) \cdot u))$.

*Then* $e$ *satisfies the following:*

(i) $(e \cdot x) + \alpha(e) = x + \alpha(e)$;

(ii) $e \cdot (e \cdot x) = e \cdot x = (e \cdot x) \cdot e$;

(iii) $e \cdot \alpha(e) = 0$;

(iv) $e \cdot x = x \cdot e$;

(v) $e \cdot (x + y) = (e \cdot x) + (e \cdot y)$;

(vi) *if* $x \leq y$ *then* $e \cdot x \leq e \cdot y$;

(vii) $e \cdot (\alpha(e) \cdot x) = 0$.

*Proof.* (i) Since $e \leq 1$, then $e \cdot x \leq 1 \cdot x = x$. Therefore $(e \cdot x) + \alpha(e) \leq x + \alpha(e)$. For the converse, first notice that, as $e \cdot \alpha(x) \leq \alpha(x)$, then $x \leq \alpha(e \cdot \alpha(x)) = (e \cdot x) + \alpha(e)$, where the last equality is obtained by setting $y = 1$ in identity (1) (and the fact that $\alpha$ is an involution).
(ii) The first equality readily follows from (2) upon setting $y = u = 0$ and

$x = 1$, while the second by setting $y = u = 0$ and $z = 1$.
(iii) can be derived by setting $x = u = 1$ and $y = z = 0$ in identity (2).
(iv)

$$\begin{aligned}
e \cdot x &= (e \cdot x) \cdot e && \text{(ii)}\\
&= ((e \cdot x) \cdot e) + (\alpha(e) \cdot e) && \text{(iii)}\\
&= ((e \cdot x) + \alpha(e)) \cdot e && \text{(Distr)}\\
&= (x + \alpha(e)) \cdot e && \text{(i)}\\
&= (x \cdot e) + (\alpha(e) \cdot e) && \text{(Distr)}\\
&= (x \cdot e) + 0 && \text{(iii)}\\
&= x \cdot e.
\end{aligned}$$

(v)

$$\begin{aligned}
e \cdot (x + y) &= (x + y) \cdot e && \text{(iv)}\\
&= (x \cdot e) + (y \cdot e) && \text{(Distr)}\\
&= (e \cdot x) + (e \cdot y) && \text{(iv)}
\end{aligned}$$

(vi) Let $x \leq y$, i.e. $x + y = y$. Then $e \cdot y = e \cdot (x + y) = (e \cdot x) + (e \cdot y)$, i.e. $e \cdot x \leq e \cdot y$.
(vii) In case $y = u = 0$, in condition (3), we obtain: $e \cdot (x \cdot z) = (e \cdot x) \cdot (x \cdot y)$. If, moreover, $x = \alpha(e)$, we obtain that $e \cdot (\alpha(e) \cdot z) = (e \cdot \alpha(e)) \cdot (e \cdot z) = 0$, by (iii). ■

We now put Lemma 4.7 to good use and prove that, in an involutive near semiring, central elements are neatly characterized by two simple equations.

**Theorem 4.14.** *Let* $\mathbf{R}$ *be an involutive near semiring. Then an element* $e \in R$ *is central if and only if it satisfies the following equations for any* $x, y, z, u \in R$*:*

1. $(e \cdot \alpha(x)) + (\alpha(e) \cdot \alpha(y)) = \alpha((e \cdot x) + (\alpha(e) \cdot y))$*;*
2. $(e \cdot (x \cdot z)) + (\alpha(e) \cdot (y \cdot u)) = ((e \cdot x) + (\alpha(e) \cdot y)) \cdot ((e \cdot z) + (\alpha(e) \cdot u))$.

*Proof.* ($\Rightarrow$) If $e$ is a central element then (1), (2) hold by Proposition 4.2.
($\Leftarrow$) Using again Proposition 4.2, and identities (1) and (2), we have to derive equations (4.10), (4.11), (4.12), (4.13) and (4.15). We start by deriving

(4.13): upon setting $x = y = 0$, identity (1) reads: $e+\alpha(e) = \alpha(0) = 1$.Using (4.13), we obtain (4.10) as follows

$$\begin{aligned} &(e \cdot x) + (\alpha(e) \cdot x) = (e + \alpha(e)) \cdot x && \text{(Distr.)} \\ &= 1 \cdot x && (4.13) \\ &= x. \end{aligned}$$

Equation (4.15) immediately follows from the associativity of the sum and the fact that $e \cdot (x + y) = (e \cdot x) + (e \cdot y)$ from Lemma 4.7. In order to prove (4.11) and (4.12) we use some auxiliary facts stated in Lemma 4.7.

$$\begin{aligned} &(e \cdot ((e \cdot a) + (\alpha(e) \cdot b))) + (\alpha(e) \cdot c) = \\ &= (e \cdot (e \cdot a)) + (e \cdot (\alpha(e) \cdot b)) + (\alpha(e) \cdot c) && \text{(Lemma 4.7.(v))} \\ &= (e \cdot a) + (e \cdot (\alpha(e) \cdot b)) + (\alpha(e) \cdot c) && \text{(Lemma 4.7.(ii))} \\ &= (e \cdot a) + 0 + (\alpha(e) \cdot c) && \text{(Lemma 4.7.(vii))} \\ &= (e \cdot a) + (\alpha(e) \cdot c) \end{aligned}$$

With a slight modification of the reasoning above one can derive condition (4.12). ■

The next proposition yields a more informative version of the general result stated in Theorem 4.12.

**Proposition 4.3.** *Let* $\mathbf{R}$ *be an integral involutive near semiring and* $\mathrm{Ce}(R)$ *the set of central elements of* $\mathbf{R}$. *Then* $\mathrm{Ce}(\mathbf{R}) = \langle \mathrm{Ce}(R), +, \cdot, \alpha, 0, 1 \rangle$ *is a Boolean algebra.*

*Proof.* By Theorem 4.12, $\mathrm{Ce}(\mathbf{R}) = \langle \mathrm{Ce}(R), \wedge, \vee, ^*, 0, 1 \rangle$ is a Boolean algebra, where $\wedge, \vee, ^*$ are defined as follows

$$x \wedge y = q(x, y, 0), \quad x \vee y = q(x, 1, y) \quad x^* = q(x, 0, 1)$$

Using this result, we just check that, for central elements, $\wedge, \vee, ^*$ coincide with $\cdot, +, \alpha$, respectively. We can easily obtain that $x \wedge y = q(x, y, 0) = (x \cdot y) + (\alpha(x) \cdot 0) = x \cdot y$, and $x^* = q(x, 0, 1) = (x \cdot 0) + (\alpha(x) \cdot 1) = \alpha(x)$. It only remains to show that $x + y = \alpha(\alpha(x) \cdot \alpha(y))$. Notice first that, by equation (4.14), with $a = 0$, $b = y'$ and $e = x$ (this is legitimated by the fact that we are only concerned with central elements), we have

$$x + (\alpha(x) \cdot y) = \alpha(\alpha(x) \cdot \alpha(y)) \qquad (\dagger)$$

Since, for central elements, multiplication coincides with the Boolean meet, we have that $\alpha(x) \cdot \alpha(y) \leq \alpha(x)$ and $\alpha(x) \cdot \alpha(y) \leq \alpha(y)$. As $\alpha$ is antitone, $x \leq \alpha(\alpha(x) \cdot \alpha(y))$ and $y \leq \alpha(\alpha(x) \cdot \alpha(y))$, which implies that $x + y \leq \alpha(\alpha(x) \cdot \alpha(y)) + \alpha(\alpha(x) \cdot \alpha(y)) = \alpha(\alpha(x) \cdot \alpha(y))$. For the converse, $\alpha(x) \cdot y \leq y$, so $x + (\alpha(x) \cdot y) \leq x + y$, i.e. $\alpha(\alpha(x) \cdot \alpha(y)) \leq x + y$, by (†). This proves that $x + y = x \vee y$. ■

From the previous proposition we have that if $\mathbf{R}$ is an integral involutive near semiring and $e$ is a central element, then $\alpha(e)$ is also central. Our next step will be proving a decomposition theorem for involutive intergral near semiring. Let $e$ be a central element of an integral involutive near semiring $\mathbf{R}$, and set

$$[0, e] = \{x : x \leq e\}$$

A complementation can be naturally defined on $[0, e]$ by: $x^e = e \cdot \alpha(x)$. Then, upon considering the algebra $[\mathbf{0}, \mathbf{e}] = \langle [0, e], +, \cdot, ^e, 0, e \rangle$, we can prove the following:

**Theorem 4.15.** *Let* $\mathbf{R}$ *an integral involutive near semiring and* $e$ *a central element of* $\mathbf{R}$. *Then* $\mathbf{R} \cong [\mathbf{0}, \mathbf{e}] \times [\mathbf{0}, \mathbf{e}']$

*Proof.* As $\mathbf{R}$ is a Church algebra, it satisfies Theorem 4.13, hence all we have to prove reduce to the following:

(1) $R_e = [0, e]$

(2) for $x, y \leq e$, $x + y = e \wedge (x + y)$, $x \cdot y = e \wedge (x \cdot y)$ and $x^e = e \wedge \alpha(x)$.

(1) Suppose $x \in R_e$, i.e. $x = e \wedge b$ for some $b \in R$. By definition of $\wedge$, $e \wedge b = q(e, b, 0) = (e \cdot b) + (\alpha(e) \cdot 0) = e \cdot b$. Now, as $b \leq 1$, by Lemma 4.7 we have that $e \cdot b \leq e \cdot 1 = e$, i.e. $x \in [0, e]$, proving $R_e \subseteq [0, e]$. For the converse, suppose $x \in [0, e]$, i.e. $x \leq e$. We want to find an element $b \in R$ such that $x = e \wedge b$. First notice that, under the assumption that $e$ is central, it follows by Theorem 4.14 and Lemma 4.7 that $\alpha(e) \cdot x = 0$, which we use to prove

that

$$\begin{aligned} 0 &= \alpha(e) \cdot e \\ &= \alpha(e) \cdot (e + x) && \text{(Assumption)} \\ &= (\alpha(e) \cdot e) + (\alpha(e) \cdot x) && \text{(Lemma 4.7)} \\ &= 0 + \alpha(e) \cdot x && \text{(Lemma 4.7)} \\ &= \alpha(e) \cdot x. \end{aligned}$$

We use the fact above to show that $e \cdot x = x$. Since, by equation (4.13), $1 = e + \alpha(e)$, we have that $x = (e+\alpha(e)) \cdot x = (e \cdot x) + (\alpha(e) \cdot x) = (e \cdot x) + 0 = e \cdot x$. Remembering that $e \wedge b = q(e, b, 0) = (e \cdot b) + (\alpha(e) \cdot 0) = e \cdot b$ and setting $b = x + \alpha(e)$ we get

$$\begin{aligned} e \wedge b &= e \cdot b \\ &= e \cdot (x + \alpha(e)) && \text{(subs)} \\ &= (e \cdot x) + (e \cdot \alpha(e)) && \text{(Lemma 4.7)} \\ &= (e \cdot x) + 0 && \text{(Prop 4.3)} \\ &= e \cdot x = x. \end{aligned}$$

Therefore, $x$ can be expressed as the meet of $e$ with an element of $R$, showing that $[0, e] \subseteq R_e$.
(2) In this part of the proof we make use of the following facts

$$x \wedge y = q(x, y, 0) = x \cdot y \text{ and if } x \leq e, \text{then } e \cdot x = x$$

Let $x, y \leq e$. Then $e \wedge (x + y) = e \cdot (x + y) = x + y$. Similarly, $e \wedge (x \cdot y) = e \cdot (x \cdot y) = x \cdot y$. Finally $x^e = e \wedge \alpha(e) = e \cdot \alpha(e)$ ■

Taking advantage from the fact that, in a Church algebra, central elements are equationally characterizable (Proposition 4.2 and Theorem 4.14), we can prove the following:

**Proposition 4.4.** *Let* $\mathbf{R}$ *be a involutive integral near semiring,* $e \in \mathrm{Ce}(\mathbf{R})$ *and* $c \in R_e$. *Then*

$$c \in \mathrm{Ce}(R) \Leftrightarrow c \in \mathrm{Ce}(R_e)$$

*Proof.* ($\Rightarrow$) By Theorem 4.14, central elements are described by equations. Furthermore, by Theorem 4.13, $h : \mathbf{R} \to \mathbf{R}_e$ is an onto homomorphism such that for every $x \in R_e$, $h(x) = x$. The fact that equations are preserved by

homomorphisms yields the desired conclusion.
($\Leftarrow$) Let us observe that, since central elements are characterized by equations and equations are preserved by direct products, if $c_1$ and $c_2$ are central elements of two integral involutive near semirings $\mathbf{R}_1$ and $\mathbf{R}_2$, then $(c_1, c_2) \in \mathrm{Ce}(\mathbf{R}_1 \times \mathbf{R}_2)$. Suppose $c \in \mathrm{Ce}(R_e)$, the image of $c$ under the isomorphism of Theorem 4.13 is $(c, 0)$. On the other hand, 0 is always central element, therefore we have that $(c, 0)$ is a central element in $\mathbf{R}_e \times \mathbf{R}_{e'}$, implying that $c \in \mathrm{Ce}(\mathbf{R})$, as $\mathbf{R} \cong \mathbf{R}_e \times \mathbf{R}_{e'}$. ■

We have seen, in Proposition 4.3, that $\mathrm{Ce}(\mathbf{R}) = \langle Ce(R), +, \cdot, \alpha, 0, 1\rangle$ is a Boolean algebra. Therefore it makes sense to consider the set of its atoms, which we denote by $At(\mathbf{R})$.

**Lemma 4.8.** *If $\mathbf{R}$ is an involutive integral near semiring and $e \in At(\mathbf{R})$, an atomic central element of $\mathbf{R}$, then $At(\mathbf{R}_{\alpha(e)}) = At(\mathbf{R}) \setminus \{e\}$.*

*Proof.* ($\supseteq$) Suppose that $e$ is an atom of the Boolean algebra $\mathrm{Ce}(\mathbf{R})$. Then, for any other atomic central element $c \in \mathbf{R}$, $c \wedge e = c \cdot e = e \cdot c = 0$, therefore $\alpha(e) + \alpha(c) = 1$. Furthermore, $c = 1 \cdot c = (e + \alpha(e)) \cdot c = (e \cdot c) + (\alpha(e) \cdot c) = 0 + (\alpha(e) \cdot c) = \alpha(e) \cdot c$, which shows that $c \leq \alpha(e)$. Thus, by Proposition 4.4, $c \in \mathbf{R}_{\alpha(e)}$. We have to show that $c$ is also an atom. So, suppose $d$ is a central element of $\mathbf{R}_{\alpha(e)}$ such that $d < c$, then, by Proposition 4.4, $d$ is a central element of $\mathbf{R}$ and as, by assumption, $c \in At(\mathbf{R})$, then necessarily $d = 0$, showing that $c$ is also an atom in $\mathbf{R}_{\alpha(e)}$.
($\subseteq$) Suppose $c \in At(\mathbf{R}_{\alpha(e)})$, then in particular $c$ is a central element of $\mathbf{R}_{\alpha(e)}$ and, by Proposition 4.4, $c \in \mathrm{Ce}(\mathbf{R})$. Let $d \in \mathrm{Ce}(\mathbf{R})$, with $c < d$, then we have $d \leq \alpha(e)$ and therefore $d \in \mathrm{Ce}(\mathbf{R}_{\alpha(e)})$ by Proposition 4.4. As, by assumption, $c \in At(\mathbf{R}_{\alpha(e)})$ then $d = 0$, which shows that $c$ is an atomic central. We finally claim that $c \neq e$. Indeed, suppose by contradiction that $c = e$, then since $c \leq \alpha(e)$ we have $e \leq \alpha(e)$, i.e. $e = e \cdot \alpha(e) = 0$ which is a contradiction, as $e$ is atomic central by hypothesis. ■

The above lemma is used to prove the following

**Theorem 4.16.** *Let $\mathbf{R}$ be an involutive integral near semiring such that $\mathrm{Ce}(\mathbf{R})$ is an atomic Boolean algebra with countably many atoms, then*

$$\mathbf{R} = \prod_{e \in At(\mathbf{R})} \mathbf{R}_e$$

*is a decomposition of $\mathbf{R}$ as a product of directly indecomposable algebras.*

*Proof.* The claim is proved by induction on the number of elements of $At(\mathbf{R})$. If 1 is the only central atomic element, then $\mathbf{R}$ is directly indecomposable and clearly $\mathbf{R} = \mathbf{R}_1$. If there is an atomic central element $e \neq 1$, then $\mathbf{R} = \mathbf{R}_e \times \mathbf{R}_{\alpha(e)}$ by Theorem 4.13. On the other hand $\mathrm{Ce}(\mathbf{R}_e) = \{0, e\}$, because if $\mathbf{R}_e$ had another element, say $d$, then $d$ would be a central element of $\mathbf{R}$ in virtue of Proposition 4.4 and $0 < d < e$ contradicting the fact that $e$ is an atom. Consequently $\mathbf{R}_e$ is directly indecomposable. By Lemma 4.8, $At(\mathbf{R}_{\alpha(e)}) = At(\mathbf{R}) \setminus \{e\}$ and by induction hypothesis, $\mathbf{R}_{\alpha(e)} = \prod_{c \in At(\mathbf{R}_{\alpha(e)})} \mathbf{R}_c$, whence our result follows. ■

## 4.6 Appendix on central elements

We claimed in section §4.5 that the axiomatization of central element for the variety of integral involutive near semirings can be reduced to a minimal set of two identities. More precisely, Theorem 4.14 states that an element $e$ of an involutive near semiring is central if and only if it satisfies the following identities:

1. $(e \cdot \alpha(x)) + (\alpha(e) \cdot \alpha(y)) = \alpha((e \cdot x) + (\alpha(e) \cdot y))$;

2. $(e \cdot (x \cdot z)) + (\alpha(e) \cdot (y \cdot u)) = ((e \cdot x) + (\alpha(e) \cdot y)) \cdot ((e \cdot z) + (\alpha(e) \cdot u))$.

Here we provide a justification of the *minimality* of such axiomatization. Indeed, we are now going to show that identities (1) and (2) are independent.

**Example 4.3.** *The integral involutive near semiring* $\mathbf{A}$*, where sum, multiplication and the antitone involution* $\alpha$ *are defined as in the following tables, satisfies* (1) *but not* (2)*.*

| $\alpha$ | |
|---|---|
| 0 | 1 |
| 1 | 0 |
| $e$ | $a$ |
| $a$ | $e$ |
| $b$ | $c$ |
| $c$ | $b$ |

| $+$ | 0 | 1 | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | $e$ | $a$ | $a$ | $c$ |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $e$ | $e$ | 1 | $e$ | 1 | 1 | $e$ |
| $a$ | $a$ | 1 | 1 | $a$ | $a$ | $a$ |
| $b$ | $a$ | 1 | 1 | a | a | a |
| $c$ | $c$ | 1 | $e$ | $a$ | $a$ | $c$ |

| $\cdot$ | 0 | 1 | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | $e$ | $a$ | $b$ | $c$ |
| $e$ | 0 | $e$ | $e$ | 0 | $c$ | $c$ |
| $a$ | 0 | $a$ | 0 | $a$ | $a$ | 0 |
| $b$ | 0 | $b$ | 0 | $a$ | $a$ | 0 |
| $c$ | 0 | $c$ | 0 | 0 | 0 | 0 |

It is routine to check that **A** is an integral involutive near semiring, satisfying also identity (1). A counterexample to identity (2) is given by setting: $x = b$, $z = 1$ and $y = u = 0$.

**Example 4.4.** The integral involutive near semiring **B**, where sum, multiplication and the antitone involution $\alpha$ are defined as in the following tables, satisfies (2) but not (1).

| $\alpha$ | |
|---|---|
| 0 | 1 |
| $a$ | $a$ |
| 1 | 0 |

| $+$ | 0 | 1 | $a$ |
|---|---|---|---|
| 0 | 0 | 1 | $a$ |
| 1 | 1 | 1 | 1 |
| $a$ | $a$ | 1 | $a$ |

| $\cdot$ | 0 | 1 | $a$ |
|---|---|---|---|
| 0 | 0 | 0 | $a$ |
| 1 | 0 | 1 | $a$ |
| $a$ | 0 | $a$ | $a$ |

It is routine to check that **B** is an integral involutive near semiring satisfying equation (2). A counterexample to identity (1) is given simply setting $e = 0$ and $x = y = z = a$. As a consequence of the examples above we can conclude:

**Corollary 4.5.** *Equations* (1) *and* (2) *in* Theorem 4.14 *are independent.*

# Chapter 5

# Appendix: extensions of the Rubik's Cube

The present chapter may sound a bit off topic at a first glance and for this reason has been inserted as an appendix. It is focused on the application of algebra, in particular of group theory, to puzzles. Erno Rubik, in 1974, invented the most famous and appreciated puzzle of all times that still goes under his name as Rubik's Cube. A few years later, in 1981, Peter Sebesteny, following Rubik's idea, invented his own cube, called the Rubik's Revenge, meant to be a more difficult puzzle with respect its predecessor. In a sort of race to make the puzzle more and more difficult to solve, a few years later it was invented the Professor's Cube, which share some features both with the Rubik's and the Rubik's Revenge.

The Rubik's Cube attracted the attention of many mathematicians (see, e.g. [2], [51], [53]) who successfully gave a group theoretical analysis and solution to the puzzle.

Any *Cubemaster* knows that dismantling the cube and reassembling it randomly may cause in most of the cases that the puzzle is not solvable anymore. A question arises naturally to the mathematician: under which conditions is a cube solvable? The answer came a few years after the Cube was born. Indeed, Bandelow [2] has provided necessary and sufficient conditions for the solvability of the cube in a Theorem which he has christened "the first law of cubology" (see Theorem 5.1 below). This suggests how important the question appears to mathematicians. As far as we know, the same question has not been answered for the extensions of the Rubik's Cube, namely the Rubik's Revenge and the Professor's Cube. Our aim here is to

provide an answer to this question for those extensions.

The chapter is structured as follows: in §5.1 we introduce the group theoretical approach to the Rubik's Cube and present the main results known in literature. In §5.2 we go through the analysis of Rubik's Revenge, state "the first law of cubology" for it, and prove some corollaries. For example we provide necessary and sufficient conditions for a randomly assembled Rubik's Revenge to be solvable. §5.3 is devoted to the proof of "the first law of cubology" for the Rubik's Revenge. Our proof is based on the algebraic tools on the Rubik's Revenge developed in [55]. To the author's best knowledge reference [55] is the only place where a group theoretical approach to the Revenge is given (the reader is referred e.g. to [1] and to several places in the web for the description of the instructions needed to solve the Rubik's Revenge).
In §5.4 we describe the structure of the Professor's Cube and state the "the first law of cubology" for it. In §5.5 we address a study of the group of the Professor's Cube and prove some results concerning subgroups, which allow a purely algebraic proof of the main Theorem in §5.4.

## 5.1 A group theoretical approach to the Rubik's Cube

The Rubik's cube is composed by 26 small cubes, which we will refer to as "cubies" (as in [32]). After a quick look, one can notice that 8 are *corner* cubies, i.e. cubies with 3 visible coloured faces, 12 are *edge* cubies, with just 2 visible faces and the remaining 6 have one visible face: the *center* cubies.

The cube, obviously, has 6 faces, each of which can be moved either clockwise or anticlockwise. Moving a face implies the movement of any of the cubies lying in the moved slice, with the exception of the center piece, occupying the same (spatial) position: in other words, *centers* are fixed.

Solving the cube means having every face of a unique colour: centers, being fixed, establish which colour the face shall have. For example, if one sees a face with the center coloured in white, then it means that, when the cube is solved, the whole face will be of white colour. Of course, the same applies to all the other faces.

Any *Cubemaster* knows that if the cube is disassembled and then reassem-

bled randomly, it may happen that it is not solvable anymore, as pieces shall be assembled following a precise pattern. On the other hand, mathematicians know that such problems can be studied using group theory [51], [55], [53], [70], [37].
It is easily verified that the moves of the cube form a group, generated by the basic moves, generally referred to as $R, L, F, B, U, D$ (as in [2] and [53]). Corner and edge cubies can be moved as well as twisted, so they can change position (in space) as well as orientation. A natural way to express a pattern is introducing permutations to describe for position changes and orientation for twisting. In this way, a random pattern corresponds to a configuration, that can be captured by a 4-tuple $(\sigma, \tau, x, y)$, as done in [2]. Permutations involving corner cubies are necessarily disjoint from the ones involving edges, as this is imposed by the construction of the cube itself: $\sigma$ refers to a permutation of corners, while $\tau$ is a permutation on edges. Thus, in principle, $\sigma \in \mathbf{S}_8$, while $\tau \in \mathbf{S}_{12}$. When the cube is solved, clearly $\sigma = id_{S_8}$ and $\tau = id_{S_{12}}$.
Orientations can be characterized using vectors. As corners are eight and they have three visible faces, they may assume three possible different orientations, so the vector describing corners' orientation is $x \in (\mathbb{Z}_3)^8$; while edge cubies are twelve, but they have only two possible orientation, the vector is $y \in (\mathbb{Z}_2)^{12}$.
Let us make clear how to calculate a random configuration of the Rubik's Cube. We assume the convention that we look at the Cube in order to have the white face on top and the red in front. Then we associate a number to the spatial position of each corner as well as of each edge. We assign a number from 1 to 8 to the position occupied by each corner[1]. We number 1 the up-front-left corner and then associate numbers 2, 3, 4 just counting the others standing in the upper face clockwise. For corners standing in the down face, the down-front-left corner is assigned number 5 and the others take 6, 7 and 8 counting clockwise.

[1]The idea is suggested by Bandelow [2] who uses the suggestive terminology of "second skin" for the spatial positions occupied by cubies.

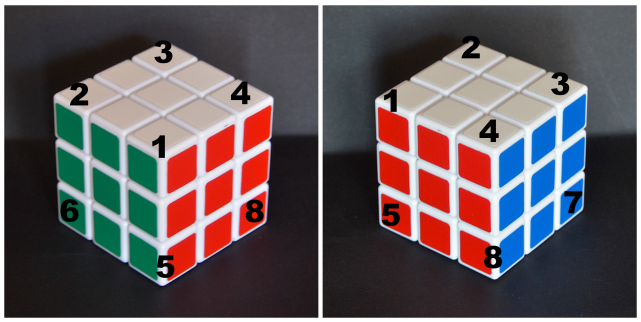



Figure 5.1: Enumeration of the spatial positions occupied by corners

The same can be done with respect to edges: we assign numbers from 1 to 4 for the spatial positions of edges in the up face, starting from the front-up and counting then clockwise on the upper face. We number 5 the front-left position in the middle layer and then counting clockwise we give numbers 6, 7 and 8 to the others in the same layer. Finally we assign numbers from 9 to 12 to edge spatial positions in the down face, with 9 assigned to the front-down and the other counting clockwise.

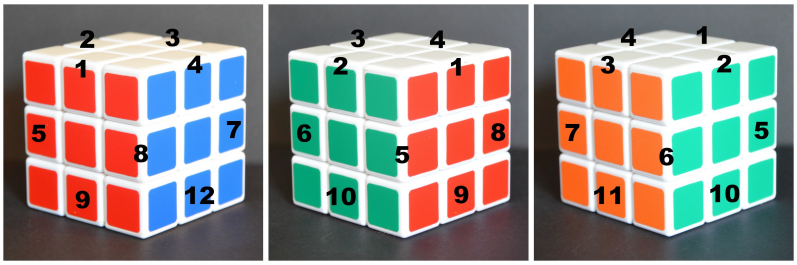



Figure 5.2: Enumeration of the spatial posistions for edges.

Now let us see how to assign the component $x_i \in \mathbb{Z}_3$ for each $i \in \{1, ..., 8\}$. First of all, we decide that for corners having a white sticker, the latter is assigned with number 0 and the other stickers take number 1 and 2 moving clockwise on the cubie's faces, starting from the white one (the idea is taken from [32]). Similarly, for corners having a yellow sticker, it takes number 0 and the others 1 and 2 counting clockwise.

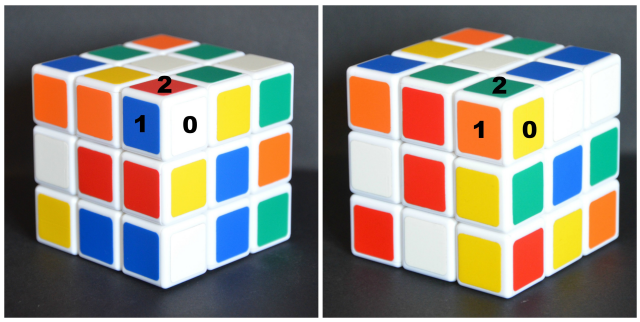



Figure 5.3: Example of assignation of numbers to stickers for corner cubies.

The convention for calculating components of vector $x$ for a random configuration is the following: we associate to the corner living in the i-th spatial position the orientation number $x_i \in \mathbb{Z}_3$, defined as the number of the corner's sticker lying on the white or yellow face of the cube. Referring for example to the random configurations illustrated in both sides of Fig. 5.3, we would get $x_4 = 2$, as the corner standing in position four has the sticker taking number 2 ($x = 2$) in the upper face of the cube.

We proceed similarly for edges, i.e. we establish that for edges having a white or a yellow sticker, those ones take number 0 and the other stickers take 1 (examples in the left-hand side of Fig. 5.4). For the remaining 4 edges, we decide that red and orange stickers take 0, while green and blue ones take 1 (examples in the right-hand side of Fig. 5.4).

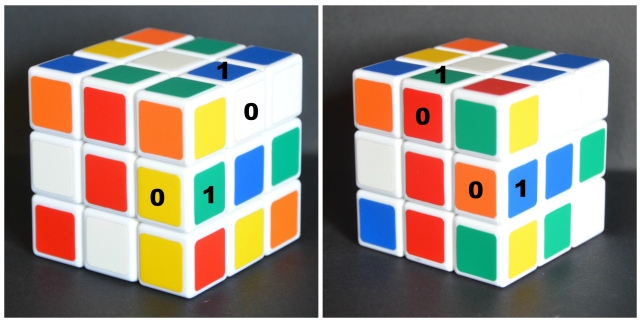



Figure 5.4: Assignation of numbers to stickers for edge cubies.

Determining $y$ is done fixing four sides to look at the cube: up (white), down (yellow), front (red) and back (orange). This is enough since the white face is always opposed to the yellow, while the red is opposed to the orange.

We associate to the edge living in the i-th spatial position the orientation number $y_i \in \mathbb{Z}_2$, defined as the number of the edge sticker lying respectively on the white, yellow face (for the edges standing in the up and down face), red or orange face (for those standing in the middle layer) of the cube. For the random configuration illustrated in the left-hand side of Fig. 5.4, we have $y_4 = 1$, as the edge occupying position 4 has its blue sticker (taking number 1) lying in the upper face of the Cube; similarly $y_8 = 0$ since the edge in position 8 has its yellow sticker (taking number 0) living in the front face of the Cube. Following the same principle for different stickers' colours and for the random configuration illustrated in the right-hand side of Fig. 5.4, we have $y_1 = 1$ and $y_8 = 0$. It shall be clear for the convention we have introduced that, whenever the Cube is solved, one has $x_i = 0$ for all $i \in \{1, ..., 8\}$ and $y_i = 0$ for all $i \in \{1, ..., 12\}$.

We say that a configuration $c$ is *valid* if one can reach the configuration $c_s = (id_{S_8}, id_{S_{12}}, 0, 0)$, i.e. the configuration where the cube is solved, by a finite number of moves.

The "first law of cubology" [2] (Theorem 1, page 42) provides necessary and sufficient conditions for a configuration to be valid.

**Theorem 5.1. (First law of cubology)** *A configuration $c = (\sigma, \tau, x, y)$ of the Rubik's Cube is valid if and only if*

*i)* $sgn(\sigma) = sgn(\tau)$;

*ii)* $\sum_i x_i \equiv 0 (\text{mod } 3)$;

*iii)* $\sum_i y_i \equiv 0 (\text{mod } 2)$.

From this theorem we get that the probability for a randomly assembled Rubik's cube to be solvable is $\frac{1}{12}$ and hence one gets:

**Corollary 5.1.** ([2] Theorem 2, page 44) *The total number of possible patterns*[2] *is* $\frac{8! \cdot 3^8 \cdot 12! \cdot 2^{12}}{12}$.

Some relevant mathematical properties of the Rubik's Cube follow from the above theorem, see [2] and [51] for details.

[2]By possible patterns, here it is meant the ones in the valid configuration.

## 5.2 Configurations of the Rubik's Revenge

The Rubik's Revenge has been created a few years after the original Rubik's cube: every face is composed by four slices instead of three. The Rubik's Revenge is composed by 56 cubies: 8 are corner cubies exactly as in the original Cube, 24 are edge cubies and the remaining 24 are center cubies. At first glance, the big difference with the Rubik's Cube is that center pieces are not fixed anymore (clearly, also the number of edges is duplicated). As center cubies can be moved, they do not determine which colour a face shall assume in the resolution of the Revenge. However, it is enough to choose a random corner to determine the colour that every face shall assume. Throughout this appendix we mean the Revenge oriented so to have the white face on top and the red one in front. Hence the white-red-green corner, for example, shall occupy the up-front-left position in the solved Cube. In order to have that, after a quick look to the Revenge, we search the white-red-green corner and establish that position one is exactly located where such corner is living in, hence we rotate the whole cube so to have such a corner standing in the up-front-left position.

As for the original Cube, the set of moves naturally inherits the structure of a group, which we denote by $\mathbf{M}_4$. This group is generated by the twelve clockwise rotations of slices denoted by $R, L, F, B, U, D, C_R, C_F, C_U, C_L, C_B$, $C_D$, where $R, L, F, B, U, D$ are twists of the external slices, respectively, right, left, front, back, up and down face, while $C_F, C_R, C_U, C_L, C_B, C_D$ are the twists of the central-front, central-right, central-up, central-left, central-back and central down slice respectively (some of which is illustrated in Fig. 5.5). Any of those elements has order 4.

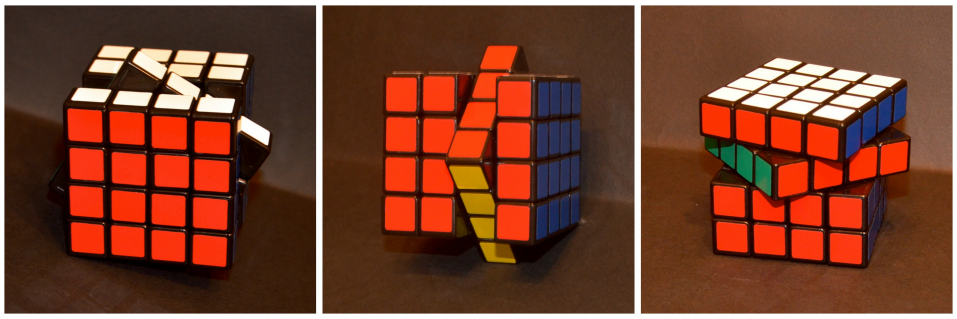


Figure 5.5: The moves $C_F, C_R$ (left-hand side and central pictures) and the move $C_U^{-1}$ (right-hand side).

The number of stickers one can find on the Revenge is equal to 96, so it appears natural to define a homomorphism

$$\varphi : \mathbf{M}_4 \longrightarrow \mathbf{S}_{96},$$

which sends a move $m \in \mathbf{M}_4$ to the permutation $\varphi(m) \in \mathbf{S}_{96}$ induced on the Revenge by the move $m$. The image $\varphi(\mathbf{M}_4) \subset \mathbf{S}_{96}$ corresponds to those permutations in $\mathbf{S}_{96}$ *induced* by moves of the Revenge.

**Remark 5.1.** The inclusion $\varphi(\mathbf{M}_4) \subset \mathbf{S}_{96}$ is (obviously) strict. For example, it may never happen that an element of $\mathbf{M}_4$ sends a corner to the position occupied by a center or an edge.

We can then define the group of the Rubik's Revenge $\mathbf{G}_4 := \varphi(\mathbf{M}_4)$. By the well known "isomorphism theorem", $\mathbf{G}_4 = \mathbf{M}_4/\ker(\varphi)$, i.e. it is the group of the moves obtained by identifying all the combination of moves leading to the identical permutation.

Let us consider the subset of $\mathbf{S}_{96}$ corresponding to permutations and/or orientation changes of corners, edges and center cubies: the set all of these permutations will be called the *space of the configurations of the Revenge* and will be denoted by $\mathcal{S}_{Conf}$.

**Remark 5.2.** It is known that a single edge cubie can not be flipped[3]; however we may theoretically think to flip a single edge (and hence changing its orientation) by swapping its stickers. Therefore, unlike the Rubik's Cube, the cardinality of $\mathcal{S}_{Conf}$ is larger than the number of patterns we can get by dismantling and reassembling the cube.

Clearly $\mathbf{G}_4 \subset \mathcal{S}_{Conf} \subset \mathbf{S}_{96}$ and $|\mathcal{S}_{Conf}| < 96!$. More precisely

$$|\mathcal{S}_{Conf}| = (24!)^2 \cdot 2^{24} \cdot 3^8 \cdot 8!. \tag{5.1}$$

The group $\mathbf{G}_4$ acts on the left on $\mathcal{S}_{Conf}$:

$$\mathbf{G}_4 \times \mathcal{S}_{Conf} \longrightarrow \mathcal{S}_{Conf}$$

$$(g, s) \longmapsto g \cdot s$$

[3]This is mathematically proved in [55] (Theorem 2), and is also a physical constrain (see http://www.instructables.com/id/How-to-put-a-4x4-Rubiks-Cube-Together/, for a detailed description on the construction of the Rubik's Revenge).

where $\cdot$ represents the composition in $\mathbf{S}_{96}$. This gives rise to a left action of $\mathbf{M}_4$ on the space of configurations, by $m \cdot s = g \cdot s$, where $g = \varphi(m)$, and vice-versa. For this reason, from now on, we will not make any distinction between the two actions on $\mathcal{S}_{Conf}$. Notice that the action of $\mathbf{G}_4$ on $\mathcal{S}_{Conf}$ is *free* (in contrast with that of $\mathbf{M}_4$), i.e. if $g \cdot s = s$ then $g = id$. Hence this action yields a bijection between the group $\mathbf{G}_4$ and the orbit $\mathbf{G}_4 \cdot s = \{g \cdot s \mid g \in \mathbf{G}_4\}$ of an arbitrary $s \in \mathcal{S}_{Conf}$, obtained by sending $g \in \mathbf{G}_4$ into $g \cdot s \in \mathcal{S}_{Conf}$.

**Remark 5.3.** It is easily seen that the space of configuration $\mathcal{S}_{Conf}$ is a subgroup of $\mathbf{S}_{96}$ containing $\mathbf{G}_4$ as a subgroup. Then the left action $g \cdot s$, $g \in \mathbf{G}_4$ and $s \in \mathcal{S}_{Conf}$, can be also seen as the multiplication in $\mathcal{S}_{Conf}$ and the orbit $\mathbf{G}_4 \cdot s$ of $s \in \mathcal{S}_{Conf}$ is nothing but the right coset of $\mathbf{G}_4$ in $\mathcal{S}_{Conf}$ with respect to $s$.

Characterizing mathematically the notion of configuration, for the Rubik's Revenge, requires a bit more work than for the Rubik's cube: centers (and edges) of the same colour are in principle undistinguishable, so we have to label them. Indeed corners are univocally identified by the colour of their faces, but ambiguity may arise concerning edges and centers.

All we need to do for describing positions of each edge (or center) by permutations, is to label all of them. A number between 1 and 24 is the label for center cubies. Once all centers have been marked, the position of each of them in a random pattern can be described by a permutation $\rho \in \mathbf{S}_{24}$.

Regarding corners, things work like in the Rubik's cube, so a permutation $\sigma \in \mathbf{S}_8$ describes their positions.

The twenty-four edge cubies can be divided in twelve pairs, namely those ones with the same colour. The two members of a pair are labelled with different letters: $a$ and $b$, respectively. This is enough to provide a description of edges' positions by using a permutation $\tau \in \mathbf{S}_{24}$. We refer to an edge labelled with $a$ (respectively $b$) as an edge of *type* $a$ (respectively *type* $b$). Obviously the type of a cubie ($a$ or $b$) is not dependent on the position the edge is lying in (it is a sort of ontological feature in our description).

Describing orientations of corners can be achieved by a vector $x \in (\mathbb{Z}_3)^8$ in the same way described in the previous section.

**Remark 5.4.** Due to the convention introduced above that the white-red-green corner is always set in the up-front-left position, i.e. in position 1, it will always happen that $x_1 = 0$.

In order to introduce such a vector for edges' orientation, we have to describe the spatial positions for edges. We proceed as done for the Rubik's Cube (see Fig. 5.2), by using only twelve numbers (instead of 24) and the label $a$ and $b$.

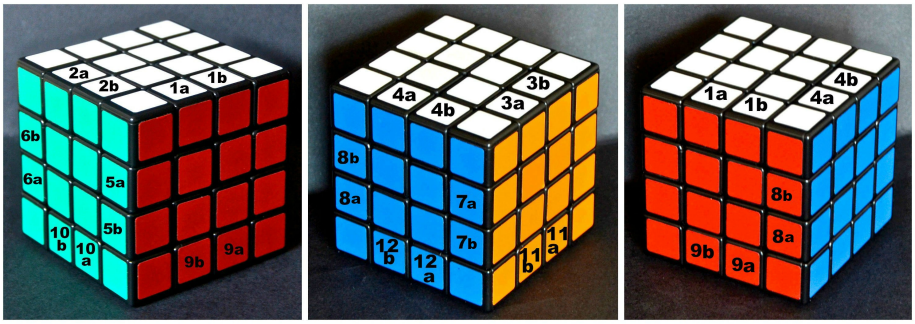



Figure 5.6: Schema of the assignation of numbers to the spatial position of edge cubies, by using labels $a$,$b$ (and twelve numbers).

Concerning edges orientation, we can do the same as for the Rubik's Cube, shifting to two 12-tuple $y_a = (y_{1_a}, y_{2_a}, ..., y_{12_a})$, with $y_{i_a} \in \mathbb{Z}_2$ and $y_b = (y_{1_b}, y_{2_b}, ..., y_{12_b})$, with $y_{i_b} \in \mathbb{Z}_2$ (edges are twenty-four, divided in pairs a and b).

As numbers have been associated to both cubies and spatial positions, so do types $a$ and $b$, that is we also have $a$-spatial positions and $b$-spatial positions, other than edges of type $a$ and $b$.

It follows from our discussion that the space of configurations $\mathcal{S}_{Conf}$ is in bijection with the set of 5-tuples $(\sigma, \tau, \rho, x, y)$, where $\sigma \in S_8$, $\tau \in S_{24}$ , $\rho \in S_{24}$, while $x \in (\mathbb{Z}_3)^8$ and $y \in (\mathbb{Z}_2)^{24}$. From now on we identify $\mathcal{S}_{Conf}$ with such 5-tuples. The 5-tuple $c_i = (id_{S_8}, id_{S_{24}}, id_{S_{24}}, 0, 0)$ will be called the *initial configuration*.

At the beginning of the section we claimed that the group of the moves $\mathbf{M}_4$ is generated by twelve elements. In fact, having introduced the formal notion of configuration, we may notice that nine generators are enough, as three moves involving central slices can be constructed as compositions of other basic moves. Notice, for example that $C_L := L^{-1}C_R R$ (center-left) and the same applies to other central moves that we will refer to as $C_B$ (center-back) and $C_D$ (center-down).

**Definition 5.1.** A configuration of the Rubik's Revenge is *valid* when it is in the orbit of the initial configuration under the action of $\mathbf{G}_4$.

We now present some basic facts concerning orbits, which are useful to prove the main result of this section.

**Lemma 5.1.** *If two configurations* $(\sigma, \tau, \rho, x, y)$ *and* $(\sigma', \tau', \rho', x', y')$ *are in the same orbit then* $sgn(\sigma)sgn(\rho) = sgn(\sigma')sgn(\rho')$.

*Proof.* If $(\sigma, \tau, \rho, x, y)$ and $(\sigma', \tau', \rho', x', y')$ are in the same orbit, then $(\sigma', \tau', \rho', x', y') = g \cdot (\sigma, \tau, \rho, x, y)$, for some $g \in \mathbf{G}_4$. Hence it is enough to show that basic moves $R, L, F, B, U, D, C_R, C_F, C_U$ preserve condition $sgn(\sigma)sgn(\rho) = sgn(\sigma')sgn(\rho')$.
The action of $g$ on corners is disjoint from the action of centers. It is easy to notice that any move among $\{R, L, F, B, U, D\}$ consists of a 4-cycle on both corners and centers, hence $sgn(\sigma') = -sgn(\sigma)$ and $sgn(\rho') = -sgn(\rho)$, hence $sgn(\sigma)sgn(\rho) = sgn(\sigma')sgn(\rho')$. On the other hand, moves $C_R, C_F, C_U$ are identities on corners and consist of two 4-cycles on centers, implying that $sgn(\sigma) = sgn(\sigma')$ and $sgn(\rho) = sgn(\rho')$, hence $sgn(\sigma)sgn(\rho) = sgn(\sigma')sgn(\rho')$ also in this case. ■

The following lemma states a property holding for both the Rubik's cube and the Revenge; for this reason, the proof is intentionally omitted (see [2] for details).

**Lemma 5.2.** *If* $(\sigma, \tau, \rho, x, y)$ *and* $(\sigma', \tau', \rho', x', y')$ *are configurations in the same orbit then* $\sum x'_i \equiv \sum x_i \pmod 3$.

Before stating the main result of this section, we make some considerations concerning edge cubies, which will be used also for the edges of the Professor's Cube. We are aware of the fact that in a random configuration, an edge of type $a$ (resp. $b$) can occupy either an a-position or a b-position, as sketched for example in Fig. 5.7. Hence, using the information encoded in $\tau \in \mathbf{S}_{24}$ we may associate to any edge a number $i_{t,s}$, with $t, s \in \{a, b\}$, where $i_t$ indicates the spatial position and $s$ refers to the type of the edge. There are always orientation numbers associated to any edge $i_{t,s}$ which, by convention, are indicated by $y_{i_{t,s}} := y_{i_t}$.

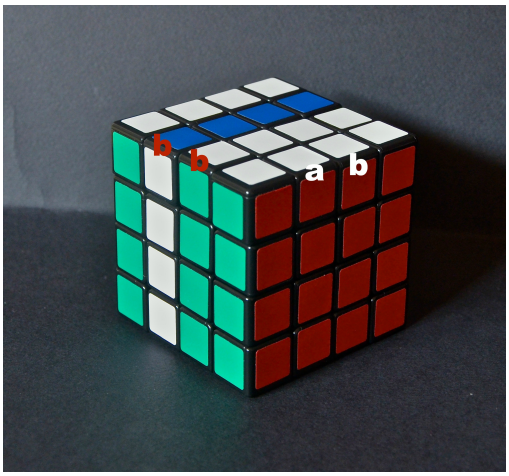



Figure 5.7: Letters a,b represents label associated to edges. In the above configuration we notice an edge of type $a$ in position $1_a$ and an edge of type $b$ in position $1_b$, hence the associated numbers will read $1_{a,a}$, $1_{b,b}$. In position 2 we find two edges of type $b$, hence $2_{b,b}$ and $2_{a,b}$. Notice that the two edges in position 2 have two different orientations, namely $y_{2_{a,b}} = 1$, $y_{2_{b,b}} = 0$.

We can now give the conditions for a configuration to be valid: this is actually the "first law of cubology" for the Rubik's Revenge:

**Theorem 5.2.** *A configuration $(\sigma, \tau, \rho, x, y)$ is valid if and only if*

1. $sgn(\sigma) = sgn(\rho)$
2. $\sum_i x_i \equiv 0 \pmod 3$
3. $y_{i_{t,s}} = 1 - \delta_{t,s}$, $\forall i = 1, ..., 12$,

*where $\delta_{a,a} = \delta_{b,b} = 1$ and $\delta_{a,b} = \delta_{b,a} = 0$.*

Condition 3 expresses the substantial difference between the Rubik's cube and the Rubik's Revenge. It can be intuitively formulated by saying that whenever an edge of type $a$ (type $b$, respectively) occupies an $a$- position ($b$-position) is "well oriented".

Next section is dedicated to the proof of this theorem. Our proof will not be constructive, i.e. we do not show the moves actually needed to solve the cube, as we will use some group-theoretical results. Here we present some corollaries.

**Corollary 5.2.** *The order of* $\mathbf{G}_4$ *is* $\frac{(24!)^2 \cdot 8! \cdot 3^7}{2}$ .

*Proof.* Since the action of $\mathbf{G}_4$ is free, then $|\mathbf{G}_4| = |\mathbf{G}_4 \cdot s|$ for all $s \in \mathcal{S}_{Conf.}$. It follows that $|\mathbf{G}_4| = \frac{|\mathcal{S}_{Conf.}|}{N}$, where $N$ is the number of orbits. Theorem 5.2 yields $N = 2 \cdot 3 \cdot 2^{24}$ and the results follows by (5.4). ■

Corollary 5.5 agrees with result presented in the last section of [55].

In order to study the solvability of the Revenge we give the following:

**Definition 5.2.** A *randomly assembled* Rubik's Revenge is a pattern of the Revenge obtained by any permutation and/or orientation change of corners, edges[4] and center cubies of the solved Revenge.

**Corollary 5.3.** *The probability that a randomly assembled Rubik's Revenge is solvable is* $\frac{1}{2^{12} \cdot 3}$ .

*Proof.* In a randomly assembled Rubik's Revenge center and edge cubies are not labelled, thus centers can always be moved so to have condition 1 in Theorem 5.2 satisfied. The 24 equations in condition 3 are reduced to 12: this can be obtained by assigning a label $a$ or $b$ to each edge in a pair, depending on its orientation, in such a way that $y_{i_{t,s}} = 1 - \delta_{t,s}$. ■

We have already mentioned (see footnote 3) the fact that the Revenge sold on the market is different from the Revenge we consider in this paper. In fact, the most relevant feature of the Revenge sold on the market is that any member of a pair of edges of the same colours is different from its companion. This has the physical effect that it is impossible to assemble the cube putting an edge of type $a$ (respectively type $b$) in a '$b$-position' (resplectively $a$-position), without changing the orientation of both edges in a pair. This yields that condition 3 in Theorem 5.2 can be always achieved, due to the internal mechanism of the Revenge. Thus (surprisingly enough) we get:

**Corollary 5.4.** *The probability that a randomly assembled Rubik's Revenge sold on the market is solvable is* $\frac{1}{3}$.

[4]Here we allow also edge flips (see Remark 5.6).

## 5.3 Proof of Theorem 5.2

We first introduce some already known results [55] on the structure of $\mathbf{G}_4$ which are of fundamental importance for proving Theorem 5.2.

In order to prove Theorem 5.2 we describe some significant subgroups of $\mathbf{G}_4$, denoted by $\mathbf{C}$, $\mathbf{Z}$ and $\mathbf{E}$ respectively. $\mathbf{C}$ is the subgroup of $\mathbf{G}_4$ which permutes corner cubies (no matter the action on orientation), and act as the identity on other pieces. $\mathbf{Z}$ is the subgroup permuting centers only, leaving corners and edges fixed; $\mathbf{E}$ permutes edges only.[5] Although the proofs of these results can be found in [55], they are also included here for sake of completeness. Notice that our proofs are essentially the same, but in terms of the action of $\mathbf{G}_4$ on $\mathcal{S}_{Conf.}$.

**Theorem 5.3.** $\mathbf{C} \cong \mathbf{A}_8$*, the alternating group of even permutation.*

We report to [37] for the proof of the above theorem.
In the next theorem we make use of the commutator, formally for $m, n \in \mathbf{G}$, $[m, n] = m \cdot n \cdot m^{-1} \cdot n^{-1}$.
Center cubies are 24, hence necessarily $\mathbf{Z} \leqslant S_{24}$.

**Theorem 5.4.** $\mathbf{Z} \cong \mathbf{A}_{24}$*, the alternating group of even permutation.*

*Proof.* We first show that $\mathbf{A}_{24} \leqslant \mathbf{Z}$. The move

$$z = [[C_F, C_D], U^{-1}] \tag{5.2}$$

is a 3-cycle on center and an identity on edges and corners. In fact, it is easy to check that the action of $z$ on the initial configuration gives: $z \cdot (id_{S_8}, id_{S_{24}}, id_{S_{24}}, 0,$
$0) = (id_{S_8}, id_{S_{24}}, \rho_1, 0, 0)$, where $\rho_1$ is 3-cycle.

Observe that any three target centers can be moved to the positions permuted by $z$ by a certain $g \in \mathbf{G}_4$. Such a $g$ admits an inverse $g^{-1} \in \mathbf{G}_4$, hence by $g \cdot z \cdot g^{-1}$ we may cycle any center cubies. As $\mathbf{A}_{24}$ is generated by any 3-cycle on a set of twenty-four elements, we have the desired inclusion.

For $\mathbf{Z} \leqslant \mathbf{A}_{24}$, we show that any odd permutation involving centers permutes necessarily also corners or edges, hence it cannot be in $\mathbf{Z}$. Indeed,

[5] Since each may assume three different orientations, it is known [37], [55] that the subgroup of corners corresponds to the wreath product $\mathbf{H} = \mathbf{S}_8 \bigotimes_{Wr} \mathbb{Z}_3$. However, we aim at describing the quotient subgroup $\mathbf{C} = \mathbf{H}/\mathbf{T}$, where $\mathbf{T}$ is the (normal) subgroup consisting of all al possible twists.

suppose that there exist $\alpha \in \mathbf{Z}$ s.t. $sgn(\alpha) = -1$. Such an $\alpha$ shall be obtained as a sequence of basic moves. Without loss of generality we can assume that $\alpha$ is a sequence of $L, R, U, D, F, B$, since the moves $C_R, C_F, C_U$ consist of an even permutation on centers. On the other hand, $L, R, U, D, F, B$ induces a 4-cycle on centers. However, all those moves must have permuted corners too, thus there exist a $\beta = (\beta_1, \beta_2) \in \mathbf{S}_8 \times \mathbf{E}$, s.t. $sgn(\beta) = -1$. Hence $\beta_1 \neq id_{S_8}$, implying that $\alpha \notin \mathbf{Z}$, the desired contradiction. ■

Now we consider the subgroup $\mathbf{E}$ of moves involving edges only. Edges are 24 each of which can assume two different orientation, however *no single edge can be flipped* [55, Theorem 2]. The direct consequence of this fact is that $\mathbf{E} \leqslant S_{24}$. Actually we can prove more:

**Theorem 5.5.** $\mathbf{E} \cong \mathbf{S}_{24}$

*Proof.* We first show that $\mathbf{A}_{24} \leqslant \mathbf{E}$. Indeed the move

$$e = [C_L^{-1}, [L, U^{-1}]] \tag{5.3}$$

is of a 3-cycle on edges. As done for centers, one can bring any target edge in the positions switched by $e$ using an element of $g \in \mathbf{G}_4$ and then solving the mess created by $g^{-1}$. In this way, one obtains any 3-cycles in $\mathbf{E}$, proving the inclusion.
We are left with proving that there is at least an odd permutation in $\mathbf{E}$, which implies necessarily that $\mathbf{E} \cong \mathbf{S}_{24}$.
Consider the move $C_R$: it gives rise to an even permutation on centers (two 4-cycles) and an odd one on edges (one 4-cycle). As by Theorem 5.4 $\mathbf{Z} \cong \mathbf{A}_{24}$, it exists an element $z_0 \in \mathbf{Z}$ such that $z_0 \cdot \varphi(C_R)$ acts as a 4-cycles of edges only. Hence $z_0 \cdot \varphi(C_R) \in \mathbf{E}$ and $sgn(z_0 \cdot \varphi(C_R)) = -1$. ■

We have now all the essential ingredients to prove the "first law of cubology" for the Rubik's Revenge.

**Proof of Theorem 5.2**

($\Rightarrow$) Assuming $(\sigma, \tau, \rho, x, y)$ is valid means that it is in the orbit of the initial configuration $(id_{S_8}, id_{S_{24}}, id_{S_{24}}, 0, 0)$.

1. By Lemma 5.1 we have that $sgn(\sigma)sgn(\rho) = sgn(id_{S_8})sgn(id_{S_{24}}) = 1$, hence $sgn(\sigma) = sgn(\rho)$, for their product must be equal to 1.

2. $\sum_i x_i \equiv 0 (\text{mod } 3)$ follows trivially from Lemma 5.2 and the fact that $(\sigma, \tau, \rho, x, y)$ is valid.

3. In the initial configuration $(id_{S_8}, id_{S_{24}}, id_{S_{24}}, 0, 0)$ it holds $y_{i_t} = 0$ for all $i \in \{1, ..., 12\}$ and $\delta_{a,a} = \delta_{b,b} = 1$, hence $y_{i_{t,s}} = 1 - \delta_{t,s} = 0$.

As $(\sigma, \tau, \rho, x, y)$ is in the orbit of the initial configuration, it is obtained by a sequence of basic moves, thus we need to check that those moves preserve condition $y_{i_{t,s}} = 1 - \delta_{t,s}$.

We consider moves splitted in two sets: $M_1 = \{R, U, D, L\}$ and $M_2 = \{F, B, C_R, C_F, C_U\}$; hence we have two possibilities: we may assume a move, say $m$, either $m \in M_1$ or $m \in M_2$.
Assume $m \in M_1$. Recall that for the convention we have introduced about the assignation of orientation numbers to edges, $m$ does not change edge cubies' orientation, so we get $y_{i_{t,s}} = 0$ for all $i \in \{1, ..., 12\}$. Furthermore $m$ acts on a configuration moving edges occupying an a-position in edges in a-position and the same holds for b-positions and hence $\delta_{t,s} = 1$.

Let now $m \in M_2$. $m$ changes orientations of some edges (the ones that it is actually permuting): more precisely it gives rise to a cycle of four edges or to two cycles of four edges each. Let $i_{t,s}$ be one of those edges, then $y_{i_{t,s}} = 1$ and $\delta_{t,s} = 0$ since a-positions and b-positions are swapped by $m$.

($\Leftarrow$) We have to show that once conditions 1, 2 and 3 are satisfied we are always able to solve the cube. In the random configuration $(\sigma, \tau, \rho, x, y)$ we can check (just by watching the Revenge) whether $\rho$ is even or odd. If $sgn(\rho) = -1$, it is enough to apply one among $\{R, L, U, D, F, B\}$ to get $sgn(\rho) = +1$. If $sgn(\rho) = +1$, then $\rho \in \mathbf{A}_{24}$, hence, by Theorem 5.4, $\rho \in \mathbf{Z}$, so there exists $z_1 \in \mathbf{Z}$ s.t. $z_1 \cdot (\sigma, \tau, \rho, x, y) = (\sigma, \tau, id_{S_{24}}, x, y)$.
By condition 1. $sgn(\sigma) = sgn(\rho)$, hence in the configuration $(\sigma, \tau, id_{S_{24}}, x, y)$, $sgn(\sigma) = +1$. Then $\sigma \in \mathbf{A}_8$, and by Theorem 5.7, there exists $c \in \mathbf{C}$ such that $c \cdot (\sigma, \tau, id_{S_{24}}, x, y) = (id_{S_8}, \tau, id_{S_{24}}, x, y)$.

Now, we proceed setting edges in their correct positions; $\tau$ is a permutation of 24 elements, however Theorem 5.5 $\mathbf{E} \cong \mathbf{S}_{24}$, hence there is an $e_1 \in \mathbf{E}$ such that
$e_1 \cdot (id_{S_8}, \tau, id_{S_{24}}, x, y) = (id_{S_8}, id_{S_{24}}, id_{S_{24}}, x, y)$. Condition (3) implies that, as all edge cubies are correctly positioned, then they are also correctly oriented, thus $y = 0$, so $(id_{S_8}, id_{S_{24}}, id_{S_{24}}, x, y) = (id_{S_8}, id_{S_{24}}, id_{S_{24}}, x, 0)$.

Now the labelled Revenge has been reduced to Rubik's Cube, as any pair of edge can be seen as an unique big edge. So we have actually reduced the

Rubik's Revenge to a Rubik's Cube whose corners can be correctly oriented, whenever condition 2 is satisfied (see [2] for details).

We have proved that the initial configuration $(id_{S_8}, id_{S_{24}}, id_{S_{24}}, 0, 0)$ is in the orbit of $(\sigma, \tau, \rho, x, y)$, hence the latter is valid, concluding the proof of the theorem.

## 5.4 Configurations of the Professor's Cube

The Professor's cube is a further extension of the Rubik's Revenge. Any of its faces, is composed by five slices instead of three (as for the Rubik's Cube) and of four as for the Rubik's Revenge. For this reason, the Professor's Cube is composed by 98 cubies: 8 corner cubies (three stickers each), exactly as in the original Cube, 36 edge cubies (two stickers each) and the remaining 54 center cubies (one sticker only). At first glance, the Professor's Cube shares a remarkable feature with the Rubik's Cube: in every face, one among the 9 central cubies, namely the most central one, is fixed. This represent a big difference with respect to the Rubik's Revenge where any center cubie instead can be moved. Furthermore the number of edges is exactly the sum of the 24 edges (coupled in twelve pairs) of the Rubik's Revenge and the 12 edges of the Rubik's Cube: we will refer to the formers as *coupled edges*, while to the latters as *single edges*. Concerning the eight moving centers in each face, we refer to some of them as *center corners*, namely the ones standing on the diagonals of the fixed center piece, and to the remaining ones as *center edges*, which actually stands on the side of the fixed center piece. It follows that in the cube, both center corners and center edges are 24.

The colour that every face shall assume solving the cube is determined by the colour of the most central cubie (the fixed one) in each face. As a matter of convention, throughout the whole chapter we mean the Professor's Cube oriented so to have the white face on top and the red one in front (the same convention adopted in the previous pages for the other cubes).

Exactly as for the smaller cubes treated in the previous sections, the set of moves naturally inherits the structure of a group, which we denote by $\mathbf{M}_5$. In this case, the group is generated by the twelve clockwise rotations of slices denoted by $R, L, F, B, U, D, C_R, C_F, C_U, C_L, C_B, C_D$, where $R, L, F, B, U, D$ denote twists of the external slices (respectively, right, left, front, back, up and down face), while $C_F, C_R, C_U, C_L, C_B, C_D$ are twists of the central-front, central-right, central-up, central-left, central-back and central-down slice re-

spectively. It is not difficult to check that any of those elements has order 4. As we have done in the previous section for the Rubik's Revenge, we introduce the group of the Professor's cube as a quotient of $\mathbf{M}_5/\ker(\varphi)$, where $\varphi$ is the group homomorphism

$$\varphi : \mathbf{M}_5 \longrightarrow \mathbf{S}_{150},$$

sending a move $m \in \mathbf{M}_5$ to a permutation $\varphi(m) \in \mathbf{S}_{150}$, which corresponds to the permutation in the symmetric group $\mathbf{S}_{150}$ *induced* by the move $m$ of the Revenge. Number 150 is required for it is the number of stickers composing the Professor's Cube.

**Remark 5.5.** The inclusion $\varphi(\mathbf{M}_5) \subset \mathbf{S}_{150}$ is (obviously) strict.

In other words, the group $\mathbf{G}_5$ consists of the moves we get identifying all the combination of moves leading to the identical permutation.

The subset of $\mathbf{S}_{150}$ corresponding to permutations and/or orientation changes of corners, edges and center cubies will be called the *space of the configuration of the Professor's Cube* and will be denoted by $\mathcal{S}_{Conf}$.[6]

**Remark 5.6.** We already pointed out that in the Rubik's Revenge a single edge cubie can not be flipped ([55, Theorem 2]). In the Professor's Cube the analogous of the statement holds for coupled edges only and not for every edge in general. However we may theoretically think to flip a single edge (and hence changing its orientation only) by swapping its stickers. Therefore, unlike the Rubik's Cube, the cardinality of $\mathcal{S}_{Conf}$ is larger than the number of patterns one may get by dismantling and reassembling the cube.

Clearly $\mathbf{G}_5 \subset \mathcal{S}_{Conf} \subset \mathbf{S}_{150}$ and $|\mathcal{S}_{Conf}| < 150!$. More precisely

$$|\mathcal{S}_{Conf}| = (24!)^3 \cdot 2^{36} \cdot 12! \cdot 3^8 \cdot 8!. \tag{5.4}$$

The group $\mathbf{G}_5$ acts on the left on $\mathcal{S}_{Conf}$:

$$\mathbf{G}_5 \times \mathcal{S}_{Conf} \longrightarrow \mathcal{S}_{Conf}$$

$$(g, s) \longmapsto g \cdot s,$$

[6]With a little notational abuse we indicate the space of configurations of the Professor's Cube with the same letter as for the Rubik's Revenge. We hope it will not be confusing, as, from now on, we will refer to the space of configurations of the Professor's Cube only.

where $\cdot$ stands for the composition in $\mathbf{S}_{150}$. This gives rise to a left action of $\mathbf{M}_5$ on the space of configurations, by $m \cdot s = g \cdot s$, where $g = \varphi(m)$, and vice-versa. For this reason, from now on, we will not make any distinction between the two actions on $\mathcal{S}_{Conf}$. Notice that the action of $\mathbf{G}_5$ on $\mathcal{S}_{Conf}$ is *free* (in contrast with that of $\mathbf{M}_5$), i.e. if $g \cdot s = s$ then $g = id$. Hence this action yields a bijection between the group $\mathbf{G}_5$ and the orbit $\mathbf{G}_5 \cdot s = \{g \cdot s \mid g \in \mathbf{G}_5\}$ of an arbitrary $s \in \mathcal{S}_{Conf}$, obtained by sending $g \in \mathbf{G}_5$ into $g \cdot s \in \mathcal{S}_{Conf}$.

**Remark 5.7.** It is easily seen that the space of configuration $\mathcal{S}_{Conf}$ is a subgroup of $\mathbf{S}_{150}$ containing $\mathbf{G}_5$ as a subgroup. Then the left action $g \cdot s$, $g \in \mathbf{G}_5$ and $s \in \mathcal{S}_{Conf}$, can be also seen as the multiplication in $\mathcal{S}_{Conf}$ and the orbit $\mathbf{G}_5 \cdot s$ of $s \in \mathcal{S}_{Conf}$ is nothing but the right coset of $\mathbf{G}_5$ in $\mathcal{S}_{Conf}$ with respect to $s$.

Some pieces in the Professor's Cube, namely corners, single edges and (fixed) centers, are univocally identified by the colours of their stickers. On the other hand, ambiguity may arise concerning coupled edges, center corners and center edges. For this reason, in order to characterize mathematically the notion of configuration, it is necessary to label all center edges, center corners and coupled edges. A number between 1 and 24 works as a label for center corners as well as center edges.[7] Once all center cubies have been marked, the position of each of them in a random pattern can be described by a permutation, more precisely $\rho \in \mathbf{S}_{24}$ for center corners and $\lambda \in \mathbf{S}_{24}$ for center edges.

Regarding corners, everything works like in the Rubik's Cube, so a permutation $\sigma \in \mathbf{S}_8$ describes their positions and a vector $x \in (\mathbb{Z}_3)^8$ the orientation.

We may think of the single edges as the edges of the Rubik's Cube, hence their position is described by a permutation $\tau \in \mathbf{S}_{12}$ and the orientation by a vector $z \in (\mathbb{Z}_2)^{12}$. On the other hand, the twenty-four coupled edges can be divided in twelve pairs, namely those ones with the same colour. The two members of a pair are labelled with different letters: $a$ and $b$, respectively, in the exact same way done in the previous section for the edges of the Rubik's Revenge. This is enough to provide a description of edges' positions by using a permutation $\tau_1 \in \mathbf{S}_{24}$. We refer to an edge labelled with $a$ (respectively $b$) as an edge of *type a* (respectively *type b*). Obviously the type is not dependent on the position the edge is lying in. The distinction between

[7]Notice that a center edge can never assume the position of a center corner and viceversa.

types $(a, b)$ referring to (edge) cubies and types referring to (edge) spatial positions is the same discussed in the previous section for the case of Rubik's Revenge.

For describing orientations of coupled edges, we proceed as done in the previous section for the Rubik's Revenge, using only twelve numbers (instead of 24) and the label $a$ and $b$.
Instead of using a vector with twenty-four component, we use two 12-tuple $y_a = (y_{1_a}, y_{2_a}, ..., y_{12_a})$, with $y_{i_a} \in \mathbb{Z}_2$ and $y_b = (y_{1_b}, y_{2_b}, ..., y_{12_b})$, with $y_{i_b} \in \mathbb{Z}_2$ (edges are twenty-four, divided in pairs a and b).

It follows that the space of configurations $\mathcal{S}_{Conf}$ is in bijection with the set of 8-tuples $(\sigma, \tau, \tau_1, \rho, \lambda, x, y, z)$, where $\sigma \in S_8$, $\tau \in S_{12}$ , $\tau_1 \in S_{24}$, $\rho \in S_{24}$, $\lambda \in S_{24}$ while $x \in (\mathbb{Z}_3)^8$, $y \in (\mathbb{Z}_2)^{24}$ and $z \in (\mathbb{Z}_2)^{12}$. From now on we identify $\mathcal{S}_{Conf}$ with such 8-tuples. The 8-tuple $(id_{S_8}, id_{S_{12}}, id_{S_{24}}, id_{S_{24}}, id_{S_{24}}, 0, 0, 0)$ will be called the *initial configuration*.

**Definition 5.3.** A configuration $c$ of the Rubik's Revenge is *valid* when it is in the orbit of the initial configuration $c$ under the action of $\mathbf{G}_5$.

Before stating the main result of this section, we make some considerations concerning coupled edge cubies. As happens for the Rubik's Revenge, an edge of type $a$ (resp. $b$) in a random configuration, can occupy either an a-position or a b-position. It follows that, by using the information encoded in $\tau_1 \in \mathbf{S}_{24}$, we may associate to any edge a number $i_{t,s}$, with $t, s \in \{a, b\}$, where $i_t$ indicates the spatial position, while $s$ refers to the type of the edge. There always are orientation numbers associated to any edge $i_{t,s}$ which will be $y_{i_{t,s}} := y_{i_t}$.

We can now give the conditions for a configuration to be valid: this is actually the "first law of cubology" for the Professor's Cube.

**Theorem 5.6.** *A configuration $(\sigma, \tau, \tau_1, \rho, \lambda, x, y, z)$ of the Professor's Cube is valid if and only if*

1. $sgn(\sigma) = sgn(\tau) = sgn(\rho)$
2. $sgn(\lambda) = sgn(\sigma) \cdot sgn(\tau_1)$
3. $\sum_i x_i \equiv 0 \mod 3$
4. $\sum_i z_i \equiv 0 \mod 2$

5. $y_{i_{t,s}} = 1 - \delta_{t,s}$, $i = 1, ..., 12$,

*where* $\delta_{a,a} = \delta_{b,b} = 1$ *and* $\delta_{a,b} = \delta_{b,a} = 0$.

Next section is devoted to the proof of this theorem. Our proof will not be constructive, in the sense that we do not show how to solve the cube, but we will use some purely group-theoretical results.

As a corollary of Theorem 5.6 we get the order of $\mathbf{G}$

**Corollary 5.5.** *The order of* $\mathbf{G}$ *is* $(24!)^3 \cdot 2^5 \cdot 12! \cdot 8! \cdot 3^7$.

*Proof.* It is easy to check that the action of $\mathbf{G}$ on $\mathcal{S}_{Conf.}$ is free. Therefore $|\mathbf{G}| = |\mathbf{G} \cdot s|$ for all $s \in \mathcal{S}_{Conf.}$. It follows that $|\mathbf{G}| = \frac{|\mathcal{S}_{Conf.}|}{N}$, where $N$ is the number of orbits. Theorem 5.6 yields $N = 2^3 \cdot 2^3 \cdot 2 \cdot 3 \cdot 2^{24}$ and the results follows by (5.4). ■

In order to study the solvability of the Professor's Cube we give the following:

**Definition 5.4.** A *randomly assembled* Professor's Cube is a pattern of the cube obtained by any permutation and/or orientation change of corners, single edges, coupled edges [8], central edges and central corners of the solved Cube.

**Corollary 5.6.** *The probability that a randomly assembled Professor's cube is solvable is* $\frac{1}{2^{12} \cdot 12}$ .

*Proof.* In a randomly assembled Professor's Cube central pieces (both edges and corners) and coupled edge cubies are not labelled, thus central pieces can always be moved in order to have condition 2 in Theorem 5.6 satisfied, while condition 1 reduces simply to $sgn(\sigma) = sgn(\tau)$. The 24 equations in condition 5 are reduced to 12: this is can be obtained by assigning a label $a$ or $b$ to each edge in a pair, depending on its orientation, in such a way that $y_{i_{t,s}} = 1 - \delta_{t,s}$. ■

In the previous section, we focused on the Rubik's Revenge and observed that the Revenge sold on the market is actually different from the Revenge we took under consideration. The same holds for the Professor's Cube: the mathematical description actually leads us to deal with an object which is slightly different from the real one. In fact, as the most relevant feature

[8] Here we also allow edge flips (see Remark 5.6).

of the Revenge sold on the market is that any member of a pair of edges of the same colours is different from its companion, the same statement holds in the Professor's Cube for coupled edges. This fact has the physical effect that it is impossible to assemble the cube putting an edge of type $a$ (respectively type $b$) in a '$b$-position' (resplectively $a$-position), without changing the orientation of both edges in a pair. This yields that condition 5 in Theorem 5.6 can be always achieved, due to the internal mechanism of the Professor's Cube. Thus, surprisingly enough, we recover the Professor's Cube sold on the market out of our theoretical analysis and we get:

**Corollary 5.7.** *The probability that a randomly assembled Professor's Cube sold on the market is solvable is* $\frac{1}{12}$ .

## 5.5 On the subgroups of the Group of the Professor's Cube

In this section we study of the structure of $\mathbf{G}_5$. In particular we aim at showing that some subgroups of $\mathbf{G}_5$, namely those ones that permute corners, single edges, coupled edges, central corners and central edges are all alternating groups. This allows an elegant, although non constructive, proof of Theorem 5.6.

The significant subgroups of $\mathbf{G}_5$ we want to study will be denoted by $\mathbf{C}$, which permutes corner cubies (no matter the action on orientation), and act as the identity on other pieces; $\mathbf{E}$, permuting single edges only (and acting as identity on every other piece); $\mathbf{E_c}$, acting on coupled edges only; $\mathbf{Z_c}$ permuting central corners only and finally $\mathbf{Z_e}$ acting only on central edges.[9]

It is easy to notice that corners and single edges in the Professor's Cube act exactly as corners and edges of thte Rubik's Cube. Indeed the corresponding subgroups permuting them only ($\mathbf{C}$ and $\mathbf{E}$ respectively) are exactly those of the Rubik's Cube. Since each corner may assume three different orientations, it is known [37], [55] that the subgroup of corners corresponds to the wreath product $\mathbf{H} = \mathbf{S}_8 \bigotimes_{Wr} \mathbb{Z}_3$. However, we aim at describing the quotient subgroup $\mathbf{C} = \mathbf{H}/\mathbf{T}$, where $\mathbf{T}$ is the (normal) subgroup consisting

[9]With a notational abuse we denote the subgroups of $\mathbf{G}_5$ with the same letters used for the subgroups of $\mathbf{G}_4$. We believe that there is no danger of confusion for the reader at this stage.

of all possible twists.

**Theorem 5.7.** $\mathbf{C} \cong \mathbf{A}_8$, *the alternating group of even permutation.*

**Theorem 5.8.** $\mathbf{E} \cong \mathbf{A}_{12}$, *the alternating group of even permutation.*

The content of the above theorems is a well known fact concerning the Rubik's Cube, hence we remand to [37] for a proof.

Actually the presence of coupled edges and of different kinds of center pieces make the Professor's Cube essentially different both from the Rubik's and the Revenge cubes.

Central corner cubies are 24, hence necessarily $Z_{_c} \subseteq S_{24}$.

**Theorem 5.9.** $\mathbf{Z_c} \cong \mathbf{A}_{24}$, *the alternating group of even permutation.*

*Proof.* We first show that $\mathbf{A}_{24} \leqslant \mathbf{Z_c}$. The move

$$z = [[C_F, C_D], U^{-1}] \tag{5.5}$$

is a 3-cycle on central corners and acts as an identity on all the other pieces (the fact is easily verified by performing the move on the cube).

Observe that any three arbitrary target central corner can be moved to the positions permuted by $z$ by a certain $g \in \mathbf{G}_5$. Such a $g$ admits an inverse $g^{-1} \in \mathbf{G}_5$, hence by $g \cdot z \cdot g^{-1}$ we may cycle any center cubies. As $\mathbf{A}_{24}$ is generated by any 3-cycle on a set of twenty-four elements, we have the desired inclusion. For $\mathbf{Z_c} \leqslant \mathbf{A}_{24}$, we show that any odd permutation involving central corners permutes necessarily also some other piece, hence it cannot be in $\mathbf{Z_c}$. Indeed, suppose that there exist $\alpha \in \mathbf{Z_c}$ s.t. $sgn(\alpha) = -1$. Such an $\alpha$ shall be obtained as a sequence of basic moves. Without loss of generality we can assume that $\alpha$ is a sequence of $L, R, U, D, F, B$, since the moves $C_R, C_F, C_U, C_L, C_B, C_D$ consist of an even permutation on central corners. On the other hand, any of the moves among $L, R, U, D, F, B$ induces a 4-cycle on central corners. However, all those moves must have permuted some other piece, thus there exist a $\beta = (\beta_1, \beta_2, \beta_3, \beta_4) \in \mathbf{C} \times \mathbf{E} \times \mathbf{E_c} \times \mathbf{Z_e}$, s.t. $sgn(\beta) = -1$. But since $\beta_3$ consists of 2 cycles of 4 elements (on coupled edges) then $Sg(\beta_3) = +1$. This implies that one among $\beta_1$, $\beta_2$ and $\beta_4$ is different from the identity, therefore $\alpha \notin \mathbf{Z_c}$, which gives rise to a contradiction. ■

We now aim at characterising the subgroup $\mathbf{Z}_e$ permuting central edges only.

**Theorem 5.10.** $\mathbf{Z_e} \cong \mathbf{A}_{24}$, *the alternating group of even permutation.*

*Proof.* We proceed following the same idea of the proof of Theorem 5.9. Indeed it is easy to check that the move

$$w = [[RC_R(LC_L)^{-1}, C_D], U] \tag{5.6}$$

is a 3-cycle on central corners and acts as an identity on all the other pieces.

Notice again that any three arbitrary target central edge can be places in the positions permuted by $w$ by a certain $g \in \mathbf{G}_5$. Such a $g$ admits an inverse $g^{-1} \in \mathbf{G}_5$, hence by $g \cdot w \cdot g^{-1}$ we may cycle any center cubies. As $\mathbf{A}_{24}$ is generated by any 3-cycle on a set of twenty-four elements, we have shown that $\mathbf{A}_{24} \leqslant \mathbf{Z}_{\mathbf{c}}$.

For $\mathbf{Z}_{\mathbf{e}} \leqslant \mathbf{A}_{24}$, we show that any odd permutation involving central corners permutes necessarily also some other piece, hence it cannot be in $\mathbf{Z}_{\mathbf{c}}$. Indeed, suppose that there exist $\alpha \in \mathbf{Z}_{\mathbf{c}}$ s.t. $sgn(\alpha) = -1$. Such an $\alpha$ shall be obtained as a sequence of basic moves. We can distinguish basic moves as belonging to two disjoint subsets, $M_1 = \{R, L, U, D, F, B\}$ and $M_2 = \{C_i\}$, where $i \in \{R, L, U, D, F, B\}$.

Moves in $M_2$ do not permute single edges nor corners, hence if $\alpha$ is a composition of them, then there exists necessarily a move $\beta = (\beta_1, \beta_2) \in \mathbf{E}_{\mathbf{c}} \times \mathbf{Z}_{\mathbf{c}}$ s.t. $Sg(\beta) = -1$. But since $\beta_2$ consists of two cycles of 4 elements each on central edges, then $\beta_2$ is different from the identity, implying that $\alpha \notin \mathbf{Z}_{\mathbf{e}}$.

On the other hand, if $\alpha$ is generated by moves in $M_1$ then there exist a $\beta = (\beta_1, \beta_2, \beta_3, \beta_4) \in \mathbf{C} \times \mathbf{E} \times \mathbf{E}_{\mathbf{c}} \times \mathbf{Z}_{\mathbf{c}}$, s.t. $sgn(\beta) = -1$. But since $\beta_3$ consists of 2 cycles of 4 elements (on coupled edges) then $Sg(\beta_3) = +1$. This implies that one among $\beta_1$, $\beta_2$ and $\beta_4$ is different from the identity, therefore $\alpha \notin \mathbf{Z}_{\mathbf{c}}$, which gives contradiction. ■

Now we are left with considering the subgroup $\mathbf{E}_{\mathbf{c}}$ of moves involving coupled edges only. Those edges are 24, each of which can assume two different orientations, however *no single edge in a couple can be flipped*. This is an observation deriving from the fact that the very same proof of this fact for the edges in the Rubik's Revenge [55] applies to coupled edges in the Professor's Cube.

Surprisingly enough, the subgroup of permutation of coupled edges is different from the subgroup moving edges only in the Rubik's Revenge and such a difference basically derives from the structure of central pieces.

**Theorem 5.11.** $\mathbf{E}_{\mathbf{c}} \cong \mathbf{A}_{24}$

*Proof.* We first show that $\mathbf{A}_{24} \leqslant \mathbf{E}$. Indeed the move

$$e = [C_L^{-1}, [L, U^{-1}]] \tag{5.7}$$

is of a 3-cycle on coupled edges. As previously done for centers, one can bring any target edge in the positions switched by $e$ using an element of $g \in \mathbf{G}_5$ and then solving the mess created by $g^{-1} \in \mathbf{G}_5$. In this way, one obtains any 3-cycles in $\mathbf{E}$, proving the desired inclusion.
For the other inclusion it is enough to apply an argument by contradiction as done in the proofs of Theorems 5.9 and 5.10 showing that it is impossible to have an odd permutation in $\mathbf{E_c}$. ■

The group theoretical results proved above allows us to give a proof of the main theorem stated in the previous section.

### Proof of Theorem 5.3

($\Rightarrow$) The left to the right direction is proven by checking that conditions 1,2,3,4,5 are preserved by the basic moves. As any move is generated by them and the initial configuration trivially satisfies all the conditions from 1 to 5, this implies that any valid configuration does.

1. We divide the basic moves into two subsets, $M_1 = \{R, L, U, D, F, B\}$ and $M_2 = \{C_R, C_L, C_U, C_D, C_F, C_B\}$. Moves in $M_1$ consist of cycles of 4 elements each on corners, single edges and central corners, hence necessarily preserve condition $sgn(\sigma) = sgn(\tau) = sgn(\rho)$. On the other hand, moves in $M_2$ act as identity on both corners and single edges and as two cycles of 4 elements each on central corners, therefore $sgn(\sigma) = sgn(\tau) = sgn(\rho)$.

2. Referring to the same partition of basic rules introduced above, it happens that any move in $M_1$ acts as cycle of 4 elements on center as well as on corners and as two cycles of 4 elements each on coupled edges, therefore $sgn(\lambda) = sgn(\sigma) \cdot sgn(\tau_1)$. It remains to check the moves in $M_2$, but those are identities on corners and cycles of 4 elements each both on central edges and on coupled edges, hence the condition is preserved.

3. $\sum_i x_i \equiv 0 (\text{mod } 3)$ follows from the fact that moves changing orientations of corners can be only generated by $R, L, U, D, F, B$. Then corners of

the Professor's Cube work exactly as those ones of the Rubik's Cube, where such a condition holds.

4. $\sum_i z_i \equiv 0 (\text{mod } 3)$ is satisfied for the same reason of 3, i.e. singles edges orientation can be changes only by $R, L, U, D, F, B$ and these moves always preserve the condition.

5. First of all notice that in the initial configuration, it holds $y_{i_t} = 0$ for all $i \in \{1, ..., 12\}$ and $\delta_{a,a} = \delta_{b,b} = 1$, therefore $y_{i_{t,s}} = 1 - \delta_{t,s} = 0$.

As a valid configuration is in the orbit of the initial one, it is obtained by a sequence of basic moves, thus we need to check that those moves preserve condition $y_{i_{t,s}} = 1 - \delta_{t,s}$.

We consider moves splitted again in two sets (this time differently from above): $M_j = \{R, U, D, L\}$ and $M_k = \{F, B, C_R, C_F, C_U, C_L, C_B, C_D\}$; hence we have two possibilities: we may assume a basic move, say $m$, either $m \in M_j$ or $m \in M_k$.
Assume $m \in M_j$. Recall that for the convention we have introduced about the assignation of orientation numbers to edges, $m$ does not change edge cubies' orientation, so we get $y_{i_{t,s}} = 0$ for all $i \in \{1, ..., 12\}$. Furthermore $m$ acts on a configuration moving edges occupying an a-position in edges in a-position and the same holds for b-positions and hence $\delta_{t,s} = 1$.

Let now $m \in M_k$. $m$ changes orientations of some edges (the ones that it is actually permuting): more precisely it gives rise to a cycle of four edges or to two cycles of four edges each. Let $i_{t,s}$ be one of those edges, then $y_{i_{t,s}} = 1$ and $\delta_{t,s} = 0$ since a-positions and b-positions are swapped by $m$.

($\Leftarrow$) We have to show that once conditions 1, 2, 3, 4 and 5 are satisfied then it is possible to bring the cube back to the initial configuration. Assume that the Professor's Cube is in a random configuration $(\sigma, \tau, \tau_1, \rho, \lambda, x, y, z)$ satisfying conditions 1-5. We can check (simply by watching the cube) whether $\sigma \in \mathcal{S}_8$ is even or odd. If $sgn(\sigma) = -1$, it is enough to apply one among $\{R, L, U, D, F, B\}$ to get $sgn(\sigma) = +1$. Therefore in any case we can reduce to a configuration s.t. $sgn(\sigma) = +1$. It follows that $\sigma \in \mathbf{A}_8$, and, by Theorem 5.7, $\sigma \in \mathbf{C}$, hence there exists $c_1 \in \mathbf{C}$ s.t. $c_1 \cdot (\sigma, \tau, \tau_1, \rho, \lambda, x, y, z) = (id_{\mathcal{S}_8}, \tau, \tau_1, \rho\lambda, x, y, z)$.
By condition 1 we now have that $sgn(\sigma) = sgn(\tau) = sgn(\rho) = sgn(id) = +1$. Then $\tau \in \mathbf{A}_{12}$ and $\rho \in \mathbf{A}_{24}$. By Theorems 5.8 and 5.9, there exist two moves, $e \in \mathbf{E}$ and $z \in \mathbf{Z}_{\mathbf{c}}$ respectively, such that $(e \circ z) \cdot (id_{\mathcal{S}_8}, \tau, \tau_1, \rho, \lambda, x, y, z) =$

$(id_{\mathcal{S}_8}, id_{\mathcal{S}_{12}}, \tau_1, id_{\mathcal{S}_{24}}, \lambda, x, y, z)$.

The cube has now corners, single edges and center corners in the correct positions. Since $sgn(\sigma) = +1$, condition 2 reduces to $sgn(\lambda) = sgn(\tau_1)$, therefore in the current configuration it may happen that either they are both positive or negative. In the latter case, they could turn to a positive sign just by applying for example $C_R$. $C_R$ actually changes also the positions of central corners that were correctly located in the previous steps, however $\rho$ can be brought back to identity, in virtue of Theorem 5.9 and the fact that $C_R$ induces an even permutation on central corners. Therefore in either case we can restrict to the case $sgn(\lambda) = sgn(\tau_1) = +1$, and by Theorems 5.10 and 5.11 one is always able to find two moves $f \in \mathbf{E_c}$ and $t \in \mathbf{Z_e}$ such that $(f \circ t) \cdot (id_{\mathcal{S}_8}, id_{\mathcal{S}_{12}}, \tau_1, id_{\mathcal{S}_{24}}, \lambda, x, y, z) = (id_{\mathcal{S}_8}, id_{\mathcal{S}_{12}}, id_{\mathcal{S}_{24}}, id_{\mathcal{S}_{24}}, id_{\mathcal{S}_{24}}, x, y, z)$.

Using the algebraic results from the previous section we actually could locate all the pieces in their correct positions. Condition 5 implies necessarily that they are also located with the correct orientation.

It remains only to fix corners and single edges's orientations. But as they work as in the Rubik's cube, it is a well known fact that they can be always correctly oriented whenever conditions 3 and 4 are fulfilled, see [2]

We have proved that the initial configuration is in the orbit of a random one satisfying conditions 1-5.

# Bibliography


[1] J. Adams. *How to solve Rubik's Revenge*. The Dial Press, New York, 1982.

[2] C. Bandelow. *Inside Rubik's Cube and Beyond*. Birkhäuser, 1982.

[3] L.P. Belluce and A. Di Nola. Commutative rings whose ideals form an mv-algebra. *Mathematical Logic Quarterly*, 55(5):468–486, 2009.

[4] L.P. Belluce, A. Di Nola, and A.R. Ferraioli. MV-semirings and their sheaf representations. *Order*, 30(1):165–179, 2013.

[5] L. Beran. *Orthomodular Lattices: Algebraic Approach*. Mathematics and its Applications. Springer Netherlands, 2011.

[6] G. Birkhoff and J. von Neumann. The logic of Quantum Mechanics. *Annals of Mathematics*, 37(4):823–843, 1936.

[7] W. J. Blok and J. G. Raftery. Varieties of Commutative Residuated Integral Pomonoids and Their Residuation Subreducts. *Journal of Algebra*, 190(2):280 – 328, 1997.

[8] K. Blount and C. Tsinakis. The structure of residuated lattices. *International Journal of Algebra and Computation*, 13(4):437–461, 2003.

[9] S. Bonzio, I. Chajda, and A. Ledda. Orthogonal relational systems. *Soft Computing*, to appear.

[10] S. Bonzio, I. Chajda, and A. Ledda. Representing Quantum structures as near semirings. *Manuscript*, under review.

[11] S. Bonzio, A. Loi, and L. Peruzzi. The first law of cubology for the Rubik's Revenge. *Mathematica Slovaca*, to appear.

[12] M. Botur. An example of a commutative basic algebra which is not an MV-algebra. *Mathematica Slovaca*, 60:171–178, 2010.

[13] M. Botur and R. Halaš. Finite commutative basic algebras are MV-effect algebras. *Journal of Multiple Valued Logic and Soft Computing*, 14:69–80, 2008.

[14] S. Burris and H.P. Sankappanavar. *A course in universal algebra*. Graduate texts in mathematics. Springer-Verlag, 1981.

[15] I. Chajda. Congruences in transitive relational systems. *Miskolc Mathematical Notes*, 5:19–23, 2004.

[16] I. Chajda. Basic algebras and their applications. an overview. In *Contributions to general algebra*, number 20, pages 1–10, 2012.

[17] I. Chajda. An axiomatization of orthogonal posets. *Soft Computing*, 18:1–4, 2014.

[18] I. Chajda. Basic algebras, logics, trends and applications. *Asian-European Journal of Mathematics*, 08(03):1550040–1550086, 2015.

[19] I. Chajda, G. Eigenthaler, and H. Länger. *Congruence classes in universal algebra*. Research and exposition in mathematics. Heldermann, 2003.

[20] I. Chajda, J. Gil-Fèrez, M. Kolařík, R. Giuntini, A. Ledda, and F. Paoli. On some properties of directoids. *Soft Computing*, 19:955–964, 2015.

[21] I. Chajda, R. Halaš, and J. Kühr. *Semilattice structures*. Research and exposition in mathematics. Heldermann, 2007.

[22] I. Chajda, R. Halaš, and J. Kühr. The Join of the Varieties of MV-algebras and the Variety of Orthomodular Lattices. *International Journal of Theoretical Physics*, to appear.

[23] I. Chajda and M. Kolařík. Interval basic algebras. *Novi Sad Journal of Mathematics*, 39(2), 2009.

[24] I. Chajda and M. Kolařík. Independence of axiom system of basic algebras. *Soft Computing*, 13:41–43, 2009.

[25] I. Chajda and H. Länger. Quotients and homomorphisms of relational systems. *Acta Universitatis Palackianae Olomucensis, Mathematica*, 49:37–47, 2010.

[26] I. Chajda and H. Länger. *Directoids: An Algebraic Approach to Ordered Sets*. Research and exposition in mathematics. Heldermann Verlag, 2011.

[27] I. Chajda and H. Länger. Groupoids associated to relational systems. *Mathematica Bohemica*, 138:15–23, 2013.

[28] I. Chajda and H. Länger. Commutative basic algebras and coupled near semirings. *Soft Computing*, 19(5):1129–1134, 2015.

[29] I. Chajda and H. Länger. A representation of basic algebras by coupled right near semirings. *Acta Scientiarum Mathematicarum*, 81(34):361–374, 2015.

[30] I. Chajda and H. Länger. Groupoids corresponding to relational systems. *Miskolc Mathematical Notes*, forthcoming.

[31] C.C. Chang. Algebraic analysis of many-valued logics. *Transanctions of the American Mathematical Society*, 88:457–490, 1958.

[32] J. Chen. Group theory and the Rubik's cube. Notes.

[33] R. L. Cignoli, I. M. d'Ottaviano, and D. Mundici. *Algebraic Foundations of Many-Valued Reasoning*. Trends in Logic. Springer, 1999.

[34] M.L. Dalla Chiara, R. Giuntini, and R. Greechie. *Reasoning in Quantum Theory: Sharp and Unsharp Quantum Logics*. Trends in Logic. Springer Netherlands, 2004.

[35] A. Di Nola and B. Gerla. Algebras of Lukasiewicz's logic and their semiring reducts. *Contemporary Mathematics*, 377:131–144, 2005.

[36] R. Fraïsse. Sur l'extension aux relations de quelques propriétés des ordres. *Annales scientifiques de l'École normale supérieure*, 71:363–388, 1954.

[37] A.H. Frey and D. Singmaster. *Handbook of Cubik Math*. Enslow Publishers, 1982.

[38] N. Galatos, P. Jipsen, T. Kowalski, and H. Ono. *Residuated Lattices: An Algebraic Glimpse at Substructural Logics*. Studies in Logic and the Foundations of Mathematics. Elsevier, 2007.

[39] B. Gerla. Many valued logics and semirings. *Neural Networks World*, (5):467–480, 2003.

[40] P.A. Grillet. *Abstract Algebra*. Graduate Texts in Mathematics. Springer, 2007.

[41] J. B. Hart, L. Rafter, and C. Tsinakis. The structure of commutative residuated lattices. *International Journal of Algebra and Computation*, 12(4):509–524, 2002.

[42] I.N. Herstein. *Abstract algebra*. Macmillan Publisher, 1990.

[43] D. Higgs. Dually residuated commutative monoids with identity element as least element do not form an equational class. *Mathematica Japonica*, 29:69–75, 1984.

[44] K. Iséki. On BCK-algebras with condition (S). *Mathematica Japonica*, 24:625–626, 1980.

[45] J. Ježek and R. Quackenbush. Directoids: algebraic models of up-directed sets. *Algebra Universalis*, 27(1):49–69, 1990.

[46] B. Jónsson. Algebras whose congruence lattices are distributive. *Mathematica Scandinavica*, 21:110–121.

[47] B. Jónsson. Universal relational structures. *Mathematica Scandinavica*, 4:193–208, 1956.

[48] B. Jónsson. Homogeneous universal relational structures. *Mathematica Scandinavica*, 8:137–142, 1960.

[49] B. Jónsson. Sublattices of a free lattice. *Canadian Journal of Mathematics*, 13:146–157, 1961.

[50] B. Jónsson. Algebraic extensions of relational systems. *Mathematica Scandinavica*, 11:179–205, 1962.

[51] D. Joyner. *Adventures in Group Theory*. The Johns Hopkins University Press, 2008.

[52] G. Kalmbach. *Orthomodular lattices*. L.M.S. monographs. Academic Press, 1983.

[53] C. Kosniowski. *Conquer that Cube*. Cambridge University Press, 1981.

[54] W. Krull. Axiomatische Begruendung der allgemeinen Ideal Theorie. *Sitzung der Physikalisch-Medicinische Societaet zu Erlangen*, 56:47 – 63, 1924.

[55] M. E. Larsen. Rubik's revenge: The group theoretical solution. *The American Mathematical Monthly*, 92(6):381–390, 1985.

[56] A. Ledda, F. Paoli, and A. Salibra. On semi-Boolean-like algebras. *Acta Universitatis Palackianae Olomucensis, Mathematica*, 52:101–120, 2013.

[57] J. Łoś. Quelques remarques theorémes et problémes sur les classes definissables d'algébres. In T. Skolem et al., editor, *Mathematical Interpretation of Formal Systems, Studies in Logic and the Foundations of Mathematics*, pages 98–113. North-Holland, Amsterdam, 1955.

[58] A. I. Mal'cev. On the general theory of algebraic systems. *Matematiceski Sbornik*, 35:3–20, 1954.

[59] G. Metcalfe, F. Montagna, and C. Tsinakis. Amalgamation and interpolation in ordered algebras. *Journal of Algebra*, 402:21–82, 2014.

[60] G. Metcalfe, F. Paoli, and C. Tsinakis. Ordered algebras and logic. In H. Hosni and F. Montagna, editors, *Probability, Uncertainty, Rationality*, pages 1–85. Edizioni della Normale di Pisa, 2010.

[61] A. De Morgan. On the syllogism, no. iv, and on the logic of relations. *Transactions Cambridge Philosophical Society*, 10:331–358, 1860.

[62] C. S. Peirce. Description of a notation for the logic of relatives, resulting from an amplification of the conceptions of boole's calculus of logic. In *Collected Papers of Charles Sanders Peirce. III. Exact Logic*. Harvard University Press, 1933.

[63] R. Pöschel. Graph algebras and graph varieties. *Algebra Universalis*, 27(4):559–577, 1990.

[64] V. Pratt. Origins of the calculus of binary relations. In *Proceedings of MFCS'93*, pages 142–155. Springer-Verlag, 1992.

[65] H. Rasiowa and R. Sikorski. *The Mathematics of Metamathematics*. Monografie Matematyczne. Państwowe Wydawn. Naukowe, 1963.

[66] J. Riguet. Relations binaires, fermetures, correspondances de galois. *Bulletin de Société Mathématique de France*, 76:114–155.

[67] J.J. Rotman. *Advanced Modern Algebra*. Prentice Hall, 2002.

[68] A. Salibra, A. Ledda, F. Paoli, and T. Kowalski. Boolean-like algebras. *Algebra Universalis*, 69(2):113–138, 2013.

[69] O. Schreier. Die untergruppen der freien gruppen. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5:161–183, 1927.

[70] D. Signmaster. *Notes on the Rubik's Magic Cube*. Enslow Publishers, 1977.

[71] D. Vaggione. Varieties in which the pierce stalks are directly indecomposable. *Journal of Algebra*, 184:424–434, 1996.

[72] M. Ward and R. P. Dilworth. Residuated lattices. *Transactions of the American Mathematical Society*, 45:335 – 354, 1939.

[73] Z. Xianzhong, K. P. Shum, and Y. Q. Guo. $\mathcal{L}$-subvarieties of the variety of idempotent semirings. *Algebra Universalis*, 46:75–96, 2001.