Realia et naturalia

DISSERTATIONES
MATHEMATICAE
UNIVERSITATIS
TARTUENSIS
96

OLEG KOŠIK

Categorical equivalence in algebra

DISSERTATIONES MATHEMATICAE UNIVERSITATIS TARTUENSIS
96

DISSERTATIONES MATHEMATICAE UNIVERSITATIS TARTUENSIS
96

OLEG KOŠIK

Categorical equivalence in algebra

UNIVERSITY OF TARTU
PRESS

Faculty of Mathematics and Computer Science, University of Tartu, Tartu, Estonia

Dissertation has been accepted for the commencement of the degree of Doctor of Philosophy (PhD) in mathematics on May 11, 2015, by the Council of the Institute of Mathematics, Faculty of Mathematics and Computer Science, University of Tartu.

Supervisor:

Prof. Kalle Kaarli, Cand. Sc.
University of Tartu
Tartu, Estonia

Opponents:

Assist. Res. Erkko Lehtonen, D.Sc. (Tech.)
University of Lisbon
Lisbon, Portugal

Prof. Peeter Puusemp, Cand. Sc.
Tallinn University of Technology
Tallinn, Estonia

Commencement will take place on June 25, 2015, at 14.15 in Liivi 2-403.

Publication of this dissertation has been granted by the Estonian Doctoral School of Mathematics and Statistics.

ISSN 1024-4212
ISBN 978-9949-32-836-9 (print)
ISBN 978-9949-32-837-6 (pdf)

European Union
European Social Fund

Investing in your future

Tartu Ülikooli Kirjastus
http://www.tyk.ee

Contents

Acknowledgements

First of all, I would like to express my deepest gratitude to my supervisor Prof. Kalle Kaarli. I thank him for all the ideas, advice and support he has been providing throughout my university studies in mathematics, and willingness to spend time and energy with me.

I want to thank co-supervisor Peter Mayr for giving great ideas to work together with and providing some other assistance with this PhD thesis. Also I would like to thank my co-author Tamás Waldhauser, working and spending time with whom was a great pleasure.

My special thanks go to my colleagues Aleksei Lissitsin and Indrek Zolk for their support during my whole university studies. I am also grateful to my family and other friends.

Finally, I am grateful to my high school math teachers Olga Kassatkina and Mihhail Gusev, who inspired me a lot to deal with mathematics.

My PhD studies were supported by Estonian Doctoral School of Mathematics and Statistics, which provided the possibility to attend several conferences, and to work together with Peter Mayr both in Linz and Tartu. This research was also supported by institutional research funding IUT20-57 of the Estonian Ministry of Education and Research.

Chapter 1

Introduction

1.1 Historical overview

A variety of algebras can be considered as a category in a natural way: the objects are the algebras in the variety, and the morphisms are the homomorphisms between them. The first classical example of varieties of algebras which are equivalent as categories is Kiiti Morita's theorem from 1958 ([32]). It provides necessary and sufficient algebraic conditions on two rings with unity in order their varieties of left modules to be equivalent as categories.

In 1969, Tah-Kai Hu showed that every variety categorically equivalent to the variety generated by the two-element Boolean algebra is generated by some primal algebra ([18]), i.e. a finite algebra for which all finitary operations on its universe are term operations. The first systematic study of categorical equivalence in algebra was carried out by Brian Davey and Heinrich Werner in their paper [11], published in 1983. Their work also exhibited a large number of algebraic properties preserved under categorical equivalence of varieties. Actually, the leading idea of Davey and Werner was to develop the theory of natural dualities which would generalize the classical duality between the variety of Boolean algebras and the category of topological Boolean spaces.

A purely algebraic characterization of categorical equivalence was given by Ralph McKenzie in 1996 ([30]). This characterization is very general and it gave a push for further investigations in this topic.

The notion of *categorically equivalent algebras* was first introduced explicitly by Clifford Bergman and Joel Berman in 1996 in [5]: two algebras **A** and **B** are called categorically equivalent if the varieties they generate are equivalent as categories, and the equivalence functor maps **A** to **B**. Bergman and Berman used McKenzie's result (Theorem 2.7) to characterize categorical equivalence for the finite algebras that in some way generalize primal algebras (congruence-primal, subalgebra-primal, and automorphism-primal algebras). As an example they described the categorical equivalence of two finite fields: for primes p and q, the fields $\mathbf{F}_{p^m}$ and $\mathbf{F}_{q^n}$ are categorically equivalent if and only if $m = n$.

In [6], the same authors provided a computational algorithm based on McKenzie's theorem for deciding whether two finite algebras are categorically equivalent. The authors however pointed out, that in general case their algorithm is not practical, even for small algebras.

Using McKenzie's method, Klaus Denecke and Otfried Lüders developed a characterization of categorical equivalence of finite algebras via algebras of their invariant relations ([12]), the paper appeared in 2001. (See Section 2.4 for more details.) Already in 1998, C. Bergman simplified this characterization for the algebras with a majority term operation ([7]) by observing that it is sufficient to consider just binary relations in this case. (See Section 2.5 for more details.)

In 1997, László Zádori used McKenzie's theorem to describe categorical equivalence of finite algebras via minimal relational sets ([43]). Using this description, he proved that two categorically equivalent finite groups must be weakly isomorphic ([42]).

In 2013, Shohei Izawa ([20]) and Mike Behrisch ([4], p. 130) used the result of Denecke and Lüders to develop a characterization of categorical equivalence of finite algebras via non-refinable covers. Applying this, Behrisch together with Tamás Waldhauser announced that they have strengthened Zádori's result by showing that two categorically equivalent finite semigroups must be weakly isomorphic.

1.2 Summary of the thesis

The aim of this thesis is to investigate categorical equivalence of algebras within certain classes. Theorem 2.11 by L. Zádori, Theorem 2.11 by M. Behrisch and T. Waldhauser, and Theorem 5.1 by C. Bergman and J. Berman, which characterize categorical equivalence of finite groups, finite semigroups, and finite fields, respectively, serve as our starting point.

The thesis has been organized as follows.

Chapter 1 contains a short historical overview of the categorical equivalence in algebra, a summary of the thesis and some technical remarks on the notation used in the thesis.

Chapter 2 familiarizes the reader with the tools and concepts used to study the categorical equivalence. We start with defining the notions of categorical equivalence and term equivalence, and give first examples. Then we list several algebraic properties preserved under categorical equivalence and introduce some algebraic methods for determining the categorical equivalence. In the last section we present the results for finite groups and semigroups which provide motivation for the study of term equivalent semigroups in Chapter 4.

In Chapter 3, we show that the condition of categorical equivalence for lattices and normal bands (of any cardinality) is very strict: two lattices are categorically equivalent if and only if they are isomorphic or dually isomorphic, and two normal bands are categorically equivalent if and only if they are isomorphic or anti-isomorphic. As a consequence, any two categorically equivalent semilattices are isomorphic. The key idea for the proofs is the refinement property of direct factorizations, which is introduced in the beginning of the chapter.

In Chapter 4, we investigate the term equivalence of semigroups. We find a large number of semigroup properties that are preserved by term equivalence. For some classes of semigroups, like commutative semigroups or bands, the term equivalence is trivial: the semigroups must be identical or dual. However, there exist examples of non-trivial term equivalence. We discuss separately completely regular and completely 0-simple semigroups.

In Chapter 5, the categorical equivalence of finite unitary rings is considered. We first reduce the general problem to the case of rings of prime power characteristic. We observe that semisimplicity is a categorical property and completely solve the problem when two finite semisimple rings are categorically equivalent. We also show that the rings of coprime characteristics can be categorically equivalent only if they are semisimple. The case of rings of the same characteristic remains open. In the end of the chapter we also take a look at one specific case of infinite rings: polynomial rings over a finite field.

Adding constants to the set of basic operations of an algebra can give us some interesting non-trivial examples of categorical equivalence. In Chapter 6, we define two algebras to be p-categorically equivalent if the algebras obtained from them by adding new constant operations for each of their elements are categorically equivalent. We show that non-direct extensions of finite simple non-abelian groups by a finite abelian group are p-categorically equivalent. In particular, any two symmetric groups $\mathcal{S}_m$ and $\mathcal{S}_n$, where $m, n > 4$, are p-categorically equivalent.

We also characterize the p-categorical equivalence of finite strictly locally affine complete algebras and finite strictly locally order affine complete lattices. The latter gives us non-trivial examples of p-categorically equivalent lattices.

Chapter 3 is based on [26]. Chapter 4 is a joint work with Peter Mayr from Johannes Kepler University, Linz, Austria. Chapter 5 is a joint work with Kalle Kaarli and Tamás Waldhauser from University of Szeged, Hungary.

1.3 Notation

An *algebra* $\mathbf{A} = (A; F)$ is a non-empty set A (the *universe* of $\mathbf{A}$) together with a sequence $F = (f_i \mid i \in I)$ of finitary operations on A, called the *basic operations* of $\mathbf{A}$. The cardinality of an algebra is the cardinality of its universe. The *signature* of $\mathbf{A}$ is the function $\mathcal{I}$ that assigns to each $i \in I$ the arity of the basic operation f_i.

For technical reasons, we formally disallow nullary operations in this thesis. There is no loss of generality here, because one can always replace nullary operations by unary constant operations. We do not permit the empty algebra, but every algebra will have an empty subuniverse.

We write $\mathbf{B} \leqslant \mathbf{A}$ to indicate that $\mathbf{B}$ is a subalgebra of $\mathbf{A}$. By $\operatorname{Sub}\mathbf{A}$ we denote the lattice of all subuniverses of $\mathbf{A}$. The lattice of all congruences of $\mathbf{A}$ is denoted by $\operatorname{Con}\mathbf{A}$, the automorphism group by $\operatorname{Aut}\mathbf{A}$.

We use the prefix notation, thus the composition fg of two functions f and g is defined by $(fg)(x) = f(g(x))$.

We attempted to make this thesis as self-contained as possible. However, some elementary knowledge of universal algebra and category theory is useful. If required, the adequate background information about universal algebra can be found, for instance, in [8] or [31], and about category theory in [29] or [37].

Chapter 2

Categorical equivalence in general

In this chapter we build the basement for our subsequent research. We define the notions of categorical equivalence and term equivalence, look at some basic properties of categorical equivalence and review some important results we will need in the following chapters, in particular the criteria for determining the categorical equivalence.

2.1 Basic notions

A *variety* is a class of algebras of the same signature closed under the formation of subalgebras, products, and homomorphic images. A variety of algebras can be considered as a category in a natural way: the objects are the algebras in the variety, and the morphisms are the homomorphisms between them.

Two categories C and D are said to be *equivalent* if there are covariant functors $F: C \to D$ and $G: D \to C$ such that the composite functors $F \circ G$ and $G \circ F$ are naturally isomorphic to the identity functors on D and C, respectively.

The following is well-known from category theory.

Proposition 2.1. *A covariant functor $H: V \to W$ between varieties V and W is a categorical equivalence if and only if the following conditions hold:*

- *for all $\mathbf{A}, \mathbf{B} \in V$, the functor H defines a bijection between* $\mathrm{Hom}(\mathbf{A}, \mathbf{B})$ *and* $\mathrm{Hom}(H(\mathbf{A}), H(\mathbf{B}))$*;*
- *for every algebra $\mathbf{D} \in W$ there is an algebra $\mathbf{C} \in V$ such that $H(\mathbf{C})$ is isomorphic to $\mathbf{D}$.*

By Var(**A**) we denote the variety generated by an algebra **A**.

Definition 2.2. Two algebras **A** and **B** are called *categorically equivalent,* if there is a categorical equivalence between the varieties Var(**A**) and Var(**B**) that maps **A** to **B**. We denote this $\mathbf{A} \equiv_c \mathbf{B}$.

A *term operation* of an algebra **A** is any finitary operation on A that can be constructed by means of composition from basic operations and projection maps. A finite algebra **A** is called *primal* if every operation on A is a term operation of **A**. The first example for categorical equivalence of algebras arises from the fundamental result of T. K. Hu in [18]:

Theorem 2.3. *Every primal algebra is categorically equivalent to the two-element Boolean algebra.*

One proof of this theorem (different from the original one) will be presented in Section 2.4.

Definition 2.4. Two algebras are called *term equivalent* if their base sets and term operations coincide. We denote this $\mathbf{A} \equiv_t \mathbf{B}$. Two algebras **A** and **B** are called *weakly isomorphic,* if there exists an algebra **C** isomorphic to **A** and term equivalent to **B**.

For example, a group $(G; 1, ^{-1}, \cdot)$ and the algebra $(G; *)$, where the binary operation $*$ is defined by $x * y = x \cdot y^{-1}$, are term equivalent.

In Section 2.3, we will see that weak isomorphism implies categorical equivalence. On the other hand, weak isomorphism preserves cardinality, whereas categorical equivalence does not. The latter follows from Theorem 2.3, because primal algebras of any cardinality exist. In particular, categorical equivalence does not imply weak isomorphism.

2.2 Categorical properties

All algebraic notions and properties that can be expressed by means of categorical language are preserved under categorical equivalence. We list several algebraic concepts preserved under categorical equivalence. We will comment on some of them; the full proofs can be found in [11], Proposition 3.1 and Theorem 3.3, and in [30], Theorem 3.1.

Theorem 2.5. *Let V and W be categorically equivalent varieties with the equivalence functor $H : V \to W$. Then:*

(1) *H maps embeddings to embeddings;*

(2) *H maps surjective homomorphisms to surjective homomorphisms;*

(3) *for any $\mathbf{A} \in V$, the algebras $\mathbf{A}$ and $H(\mathbf{A})$ are categorically equivalent;*

(4) *H induces a categorical equivalence between any subvariety of V and a subvariety of W;*

(5) *if V satisfies a linear Mal'cev condition, then W satisfies the same condition.*

(A Mal'cev condition is *linear* if it does not involve composition of terms. In particular, congruence-permutability and congruence-distributivity can be expressed via such condition.)

The functor H preserves embeddings since embeddings are precisely monomorphisms in a variety as a category.

Surjective homomorphisms are preserved although in general they do not coincide with the categorical epimorphisms. The proof follows from the fact that $\phi \in \mathrm{Hom}(\mathbf{A}, \mathbf{B})$ is surjective iff, whenever $\phi = \delta\pi$, where $\pi \in \mathrm{Hom}(\mathbf{A}, \mathbf{C})$, and $\delta \in \mathrm{Hom}(\mathbf{C}, \mathbf{B})$ is injective, then δ is an isomorphism. In a variety, the algebraic notion of isomorphism coincides with the categorical one.

For (3), it is easy to see that the functor $H' = H|_{\mathrm{Var}(\mathbf{A})}$ is an equivalence functor between $\mathrm{Var}(\mathbf{A})$ and $\mathrm{Var}(H(\mathbf{A}))$. Indeed, H' satisfies the first condition of Proposition 2.1 since H satisfies it. The second condition is satisfied because categorical equivalence preserves products, also subalgebras by (1), and homomorphic images by (2). The same reasoning holds for (4).

For the proof of (5), see [11], Proposition 3.3.

Theorem 2.6. *Let $\mathbf{A}$ and $\mathbf{B}$ be categorically equivalent algebras. Then the following statements hold.*

(1) *For any positive integer n, the algebras $\mathbf{A}^n$ and $\mathbf{B}^n$ are categorically equivalent.*

(2) *The endomorphism monoids* $\mathrm{End}\,\mathbf{A}$ *and* $\mathrm{End}\,\mathbf{B}$ *are isomorphic.*

(3) *The automorphism groups* $\mathrm{Aut}\,\mathbf{A}$ *and* $\mathrm{Aut}\,\mathbf{B}$ *are isomorphic.*

(4) *The subuniverse lattices* $\mathrm{Sub}\,\mathbf{A}$ *and* $\mathrm{Sub}\,\mathbf{B}$ *are isomorphic. The corresponding subalgebras are categorically equivalent.*

(5) *The congruence lattices* Con**A** *and* Con**B** *are isomorphic. The corresponding quotient algebras are categorically equivalent.*

(6) *If* **A** *is finite, then* **B** *is finite; if* **A** *is infinite, then* **B** *is infinite of the same cardinality as* **A**.

(7) *If* **A** *is finitely generated, then* **B** *is finitely generated.*

We note that Theorem 2.5 (5) extends also to categorically equivalent algebras. For example, if **A** and **B** are categorically equivalent and **A** has a Mal'cev term operation (i.e. $m(x,y,y) = m(y,y,x) = x$ for all $x,y \in A$), then **B** has a Mal'cev term operation too.

(1) holds since categorical equivalence functors preserve categorical products (if they exist), and varieties are closed under direct powers. (2) is obvious, and (3) holds since categorical equivalence preserves isomorphisms. (4) follows from Theorem 2.5 (1) and 2.5 (3), and (5) follows from Theorem 2.5 (2) and 2.5 (3).

For the proofs of (6) and (7), see [11], Proposition 3.3.

Of course, not every algebraic concept is categorical. A significant example of an algebraic concept that is not categorical is the concept of an algebra being free in a class ([30], p. 222).

2.3 McKenzie's theorem

In [30], R. McKenzie introduced the first purely algebraic characterization of categorical equivalence.

Let **A** be an algebra, n a positive integer, and s a unary term operation of **A**. Here we assume that the set of natural numbers contains zero.

- For every natural number p and every sequence $g_1, g_2, \ldots, g_n$ of pn-ary term operations of **A**, $(g_1, \ldots, g_n)$ denotes the p-ary operation on A^n that maps $(\overline{a}_1, \ldots, \overline{a}_p)$ to $(g_1(\tilde{a}), g_2(\tilde{a}), \ldots, g_n(\tilde{a}))$, where $\overline{a}_i = (a_{1i}, \ldots, a_{ni})$ is an element of A^n, and

$$\tilde{a} = (a_{11}, a_{21}, \ldots, a_{n1}, a_{12}, \ldots, a_{np}) \in A^{pn}.$$

- The n-th *matrix power* of **A** is an algebra $\mathbf{A}^{[n]}$ with the universe A^n, such that for every natural number p and every sequence $g_1, \ldots, g_n$ of pn-ary term operations of **A**, $\mathbf{A}^{[n]}$ has a basic p-ary operation $(g_1,\ldots,g_n)$, and these are all basic operations of $\mathbf{A}^{[n]}$.

- The unary operation s is *idempotent* if for every $x \in A$, $s(s(x)) = s(x)$, and s is *invertible* if for some r there are an r-ary term operation w and unary term operations $t_1,\ldots,t_r$ of **A** such that, for every $a \in A$,

$$w(st_1(a), st_2(a), \ldots, st_r(a)) = a.$$

- Let s be an idempotent term operation of **A**. By $\mathbf{A}(s)$ we denote the algebra with the universe $s(A)$, such that for each natural number p and a p-ary term operation g of **A**, $\mathbf{A}(s)$ has a basic operation $g_s = s \circ g|_{s(A)}$, and these are all basic operations of $\mathbf{A}(s)$.

Theorem 2.7 ([30], Corollary 6.1)**.** *For two algebras* **A** *and* **B**, $\mathbf{A} \equiv_c \mathbf{B}$ *if and only if there exist a positive integer m and a unary invertible idempotent term operation s of* $\mathbf{A}^{[m]}$ *such that* **B** *is term equivalent to an algebra isomorphic to* $\mathbf{A}^{[m]}(s)$.

Corollary 2.8. *Weakly isomorphic algebras are categorically equivalent.*

2.4 Invariant relations

In [12], K. Denecke and O. Lüders used Theorem 2.7 to give a characterization of categorical equivalence of finite algebras by invariant relations.

Let A be a finite set. For every positive integer n, let $\mathrm{Rel}_n(A)$ denote the set of all n-ary relations on A, and $\mathrm{Rel}(A) = \bigcup_{n\in\mathbb{N}} \mathrm{Rel}_n(A)$. Let $\theta \in \mathrm{Rel}_k(A)$ and $\lambda \in \mathrm{Rel}_l(A)$. On $\mathrm{Rel}(A)$ we define the following operations:

$$\begin{aligned}
\xi(\theta) &= \{(x_2,x_3,\ldots,x_k,x_1) \mid (x_1,x_2,\ldots,x_k) \in \theta\},\\
\tau(\theta) &= \{(x_2,x_1,x_3,\ldots,x_k) \mid (x_1,x_2,\ldots,x_k) \in \theta\},\\
\Delta(\theta) &= \{(x_1,x_2,\ldots,x_{k-1}) \mid (x_1,x_1,x_2,\ldots,x_{k-1}) \in \theta\},\\
\theta \circ \lambda &= \{(x_1,x_2,\ldots,x_{k+l-2}) \mid \exists x \in A\ (x_1,\ldots,x_{k-1},x) \in \theta,\\
&\quad \&\ (x,x_k,\ldots,x_{k+l-2}) \in \lambda\},\\
\delta^{\{1;2,3\}} &= \{(x,y,y) \mid x,y \in A\}.
\end{aligned}$$

(If $k = 1$, each of ξ, τ and Δ behaves like the identity map. If $k = l = 1$, then $\theta \circ \lambda = \theta \cap \lambda$.)

The algebra $(\mathrm{Rel}(A); \xi, \tau, \Delta, \circ, \delta^{\{1;2,3\}})$ is called the *full relation algebra* on A and by a *relation algebra* on A we mean any subalgebra of the full relation algebra.

Now let $\mathbf{A} = (A; F)$ be an algebra and $\theta \in \mathrm{Rel}_n(A)$. We say that θ is *F-invariant* if for all $f \in F$ and all n-tuples $x^1, x^2, \ldots, x^k \in \theta$, where k stands for the arity of f, we have $(f(x_1^1, \ldots, x_1^k), \ldots, f(x_n^1, \ldots, x_n^k)) \in \theta$. This actually means that θ is a subuniverse of $\mathbf{A}^n$.

It is not hard to verify that the set of all relations on A invariant under F is the universe of a relation algebra on A. We call this the relation algebra of $\mathbf{A}$ and denote it $\mathcal{R}(\mathbf{A})$. Then the following result holds:

Theorem 2.9 ([12])**.** *Let* $\mathbf{A}$ *and* $\mathbf{B}$ *be two finite algebras. Then* $\mathbf{A}$ *and* $\mathbf{B}$ *are categorically equivalent if and only if the relation algebras* $\mathcal{R}(\mathbf{A})$ *and* $\mathcal{R}(\mathbf{B})$ *are isomorphic.*

2.5 Majority algebras

The Denecke-Lüders Theorem has a simpler form in case of majority algebras. A ternary operation m on a set A is called a *majority operation* if for every $x, y \in A$,

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

A *majority algebra* is an algebra that has a majority term operation. For example, any lattice $(L; \vee, \wedge)$ is a majority algebra with the majority operation $m(x, y, z) = (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$.

For an algebra $\mathbf{A}$, let $\mathcal{S}(\mathbf{A})$ denote the algebraic structure $(\mathrm{Sub}(\mathbf{A}^2); \cap, \circ, \smile, \triangle, \nabla)$, where $\cap$ and $\circ$ are the binary operations of intersection and relational product, $\smile$ is the unary operation of taking the inverse relation, and $\triangle$ (diagonal) and $\nabla = A \times A$ are nullary operations.

In view of Theorem 2.5 (5) it is clear that if an algebra is categorically equivalent to a majority algebra, then it is a majority algebra itself. C. Bergmann proved the following result:

Theorem 2.10 ([7, Thm. 2.3])**.** *Let* $\mathbf{A}$ *be a finite majority algebra and* $\mathbf{B}$ *any algebra. Then* $\mathbf{A} \equiv_c \mathbf{B}$ *if and only if* $\mathbf{B}$ *is a finite majority algebra and the structures* $\mathcal{S}(\mathbf{A})$ *and* $\mathcal{S}(\mathbf{B})$ *are isomorphic.*

Now we use Theorem 2.10 to prove Theorem 2.3, which states that every primal algebra is categorically equivalent to the two-element Boolean algebra. By definition, every primal algebra has a majority term operation. Observe that for any primal algebra $\mathbf{A}$, $\triangle$ and ∇ are the only subalgebras of $\mathbf{A}^2$. Since the two-element Boolean algebra is itself primal (see e.g. [22], Section 3.1), the statement follows.

2.6 Finite groups and semigroups

In some cases categorical equivalence implies weak isomorphism.

L. Zádori used McKenzie's theorem to characterize categorical equivalence of finite algebras via minimal relational sets ([43]). Using this characterization, he proved the following theorem ([42]):

Theorem 2.11. *Finite groups are categorically equivalent if and only if they are weakly isomorphic.*

M. Behrisch developed a characterization of categorical equivalence of finite algebras via non-refinable covers (see the end of Section 3.4 in [4] for the outline of it). Applying this, M. Behrisch together with T. Waldhauser managed to extend the result of Zádori to finite semigroups (the result is being prepared to getting published):

Theorem 2.12. *Finite semigroups are categorically equivalent if and only if they are weakly isomorphic.*

This result motivates to take a closer look at term equivalence of semigroups. We will explore it in Chapter 4.

Chapter 3

Bands and lattices

In this chapter we show that the condition of categorical equivalence for lattices and normal bands (of any cardinality) is very strict: two lattices are categorically equivalent if and only if they are isomorphic or dually isomorphic, and two normal bands are categorically equivalent if and only if they are isomorphic or anti-isomorphic. As a consequence, any two categorically equivalent semilattices are isomorphic. The key idea here is the refinement property of direct factorizations.

3.1 Refinement property

An algebra $\mathbf{A}$ is called *directly irreducible* if $|A| > 1$, and $\mathbf{A} \simeq \mathbf{B} \times \mathbf{C}$ implies $|B| = 1$ or $|C| = 1$. An algebra $\mathbf{A}$ has the *unique factorization property* if

(1) $\mathbf{A}$ is isomorphic to a product of directly irreducible algebras;

(2) if

$$\mathbf{A} \simeq \prod_{i \in I} \mathbf{B}_i \simeq \prod_{j \in J} \mathbf{C}_j$$

for some index sets I and J and for directly irreducible algebras $\mathbf{B}_i$ and $\mathbf{C}_j$, then there is a bijection $\phi : I \to J$ such that $\mathbf{B}_i \simeq \mathbf{C}_{\phi(i)}$ for all $i \in I$.

An algebra $\mathbf{A}$ has the *refinement property* (for direct factorizations) if

$$A \simeq \prod_{i \in I} \mathbf{B}_i \simeq \prod_{j \in J} \mathbf{C}_j$$

implies the existence of algebras $\mathbf{D}_{ij}$ $(i \in I,\ j \in J)$ such that, for all $i \in I$ and $j \in J$,

$$\mathbf{B}_i \simeq \prod_{j\in J} \mathbf{D}_{ij} \quad \text{and} \quad \mathbf{C}_j \simeq \prod_{i\in I} \mathbf{D}_{ij}.$$

It is easy to see ([31], Section 5.6) that refinement property implies condition (2) of the unique factorization property (but does not imply condition (1)).

Let R be a (partial) order relation on a set A. The ordered set (A, R) is called *connected* if the conditions

$$B \cup C = A, \quad B \cap C = \emptyset, \quad R \subseteq B^2 \cup C^2$$

entail that $B = A$ or $C = A$.

Notions of direct irreducibility, the unique factorization property and the refinement property for ordered sets are defined in the same way as for algebras.

In [31], Section 5.6, the following facts that we will use later are proved:

Proposition 3.1. *Every connected ordered set has the refinement property.*

Proposition 3.2. *Every congruence distributive algebra has the refinement property.*

3.2 Normal bands

We say that two groupoids $(A, \cdot)$ and $(B, \cdot)$ are *anti-isomorphic*, if there is a bijection $\phi : A \to B$ such that $\phi(xy) = \phi(y)\phi(x)$ for any $x, y \in A$.

For a groupoid $\mathbf{A}$, we define $\mathbf{A}^*$ to be the groupoid with the same universe as $\mathbf{A}$, but with the multiplication $x * y := yx$. Clearly, $\mathbf{A}^*$ is, up to isomorphism, the only groupoid anti-isomorphic to $\mathbf{A}$.

We start with the following simple observations.

Lemma 3.3. *For any groupoids* $\mathbf{A}$ *and* $\mathbf{B}$, $(\mathbf{A} \times \mathbf{B})^* \simeq \mathbf{A}^* \times \mathbf{B}^*$.

Proof. Let $\phi_1 : \mathbf{A} \to \mathbf{A}^*$ and $\phi_2 : \mathbf{B} \to \mathbf{B}^*$ be anti-isomorphisms. Then the map $\phi : A \times B \to A^* \times B^*$ defined by $\phi((x, y)) = (\phi_1(x), \phi_2(y))$ is an anti-isomorphism. □

Proposition 3.4. *Anti-isomorphic groupoids are weakly isomorphic.*

Proof. Let $(A,\cdot)$ and $(B,\cdot)$ be two anti-isomorphic groupoids. Consider the groupoid $(B,*)$ with $x*y := yx$. Groupoids $(B,\cdot)$ and $(B,*)$ are anti-isomorphic, hence $(A,\cdot)$ and $(B,*)$ are isomorphic. On the other hand, $(B,\cdot)$ and $(B,*)$ are term-equivalent. Altogether we get that $(A,\cdot)$ and $(B,\cdot)$ are weakly isomorphic. □

Corollary 3.5. *Anti-isomorphic groupoids are categorically equivalent.*

A *band* is a semigroup consisting of idempotents. A *rectangular band* is a band satisfying the identity $xyx = x$. It can be easily seen ([25], Lemma 1) that every rectangular band is isomorphic to a direct product of a left zero band (satisfies the identity $xy = x$) and a right zero band (satisfies the identity $xy = y$). A band is called *normal* if it satisfies the identity $xyzx = xzyx$.

It is well-known (see for example [25], p. 262) that every band $\mathbf{S}$ is a semilattice $\mathbf{Y}$ of rectangular subbands $\mathbf{S}_e$, $e \in Y$. This means that $S = \bigcup\{S_e : e \in Y\}$ and $S_eS_f \subset S_{ef}$ for $e, f \in Y$. The semilattice $\mathbf{Y}$ is called the *structural semilattice* of $\mathbf{S}$. The rectangular bands $\mathbf{S}_e$, $e \in Y$, are called the *rectangular components* of $\mathbf{S}$. Both the structural semilattice and the rectangular components of a band are uniquely determined (up to isomorphism).

Lemma 3.6. *If a band* $\mathbf{S}$ *is isomorphic to the direct product of a semilattice* $\mathbf{Y}$ *and a rectangular band* $\mathbf{C}$*, then* $\mathbf{Y}$ *and* $\mathbf{C}$ *are uniquely determined, up to isomorphism.*

Proof. If $\mathbf{S} \simeq \mathbf{Y} \times \mathbf{C}$, where $\mathbf{Y}$ is a semilattice and $\mathbf{C}$ a rectangular band, then $\mathbf{Y}$ is the structural semilattice of $\mathbf{S}$ and the rectangular components are all isomorphic to $\mathbf{C}$. □

Lemma 3.7. *If* $\mathbf{Y}$ *is a semilattice and* $\mathbf{C}$ *a rectangular band, then* $(\mathbf{Y} \times \mathbf{C})^* \simeq \mathbf{Y} \times \mathbf{C}^*$.

Proof. Since semilattices are commutative, $\mathbf{Y}^* \simeq \mathbf{Y}$. Thus we have

$$(\mathbf{Y} \times \mathbf{C})^* \simeq \mathbf{Y}^* \times \mathbf{C}^* \simeq \mathbf{Y} \times \mathbf{C}^*.$$

□

Suppose $\mathbf{Y}$ is a chain semilattice, i.e., $\mathbf{Y}$ is linearly ordered, and $st = \min\{s,t\}$ for all $s, t \in Y$. Then $\mathbf{Y}^d$ denotes the dual chain semilattice, i.e., the semigroup $(Y,*)$, where $s*t = \max\{s,t\}$ for any $s, t \in Y$. If $\mathbf{C}$ is a rectangular band, then both $\mathbf{Y} \times \mathbf{C}$ and $\mathbf{Y}^d \times \mathbf{C}$ are normal bands. Every band isomorphic to $\mathbf{Y} \times \mathbf{C}$ is called a *chain normal band.* If $\mathbf{S}$ and $\mathbf{T}$ are bands isomorphic to $\mathbf{Y} \times \mathbf{C}$ and $\mathbf{Y}^d \times \mathbf{C}$, respectively, then $\mathbf{S}$ and $\mathbf{T}$ are called *dual chain normal bands.*

In 1985, B. M. Schein characterized normal bands with isomorphic endomorphism monoids.

Theorem 3.8 ([36, Thm. 3])**.** *Let* $\mathbf{S}$ *and* $\mathbf{T}$ *be normal bands with isomorphic endomorphism monoids. Then one of the following holds:*

(1) $\mathbf{S}$ *and* $\mathbf{T}$ *are isomorphic;*

(2) $\mathbf{S}$ *and* $\mathbf{T}$ *are anti-isomorphic;*

(3) $\mathbf{S}$ *and* $\mathbf{T}$ *are dual chain normal bands;*

(4) $\mathbf{S}$ *and* $\mathbf{T}$ *are chain normal bands and* $\mathbf{T}$ *is anti-isomorphic to the dual of* $\mathbf{S}$.

Now we are ready to prove the following result.

Theorem 3.9. *Normal bands are categorically equivalent if and only if they are isomorphic or anti-isomorphic.*

Proof. We need to show that categorically equivalent normal bands are isomorphic or anti-isomorphic. By Corollary 3.5, the converse is always true.

Take two categorically equivalent normal bands $\mathbf{S}$ and $\mathbf{T}$. By Theorem 2.6, their endomorphism monoids are isomorphic, thus one of the statements (1)-(4) of Theorem 3.8 is fulfilled. In case (1) or (2) we are done. So assume that (3) or (4) holds.

In case (3), $\mathbf{S} \simeq \mathbf{Y} \times \mathbf{C}$ and $\mathbf{T} \simeq \mathbf{Y}^d \times \mathbf{C}$ for some chain semilattice $\mathbf{Y}$ and some rectangular band $\mathbf{C}$. We may assume that $\mathbf{Y}$ has at least two elements, otherwise case (3) reduces to (1).

Consider the normal bands $\mathbf{S}^2 \simeq (\mathbf{Y} \times \mathbf{C})^2 \simeq \mathbf{Y}^2 \times \mathbf{C}^2$ and $\mathbf{T}^2 \simeq (\mathbf{Y}^d \times \mathbf{C})^2 \simeq (\mathbf{Y}^d)^2 \times \mathbf{C}^2$. They are also categorically equivalent and therefore have isomorphic endomorphism semigroups. Thus one of the cases (1)-(4) is fulfilled also for $\mathbf{S}^2$ and $\mathbf{T}^2$. We analyze each possibility.

Case 3.1. $\mathbf{S}^2 \simeq \mathbf{Y}^2 \times \mathbf{C}^2$ and $\mathbf{T}^2 \simeq (\mathbf{Y}^d)^2 \times \mathbf{C}^2$ are isomorphic.

By Lemma 3.6, we get that the semilattices $\mathbf{Y}^2$ and $(\mathbf{Y}^d)^2$ are isomorphic. Semilattices as ordered sets are connected, hence, by Proposition 3.1, they have the refinement property. Both $\mathbf{Y}^2$ and $(\mathbf{Y}^d)^2$ have factorization into directly irreducible ordered sets (chains $\mathbf{Y}$ and $\mathbf{Y}^d$ are directly irreducible), thus this factorization is unique. Therefore $\mathbf{Y}$ and $\mathbf{Y}^d$ are isomorphic as ordered sets and hence also as semilattices. Thus normal bands $\mathbf{S}$ and $\mathbf{T}$ are also isomorphic.

Case 3.2. $\mathbf{Y}^2 \times \mathbf{C}^2$ and $(\mathbf{Y}^d)^2 \times \mathbf{C}^2$ are anti-isomorphic.

Lemma 3.7 gives us that $\mathbf{Y}^2 \times \mathbf{C}^2 \simeq (\mathbf{Y}^d)^2 \times (\mathbf{C}^2)^*$, hence by Lemma 3.6, $\mathbf{Y}^2$ and $(\mathbf{Y}^d)^2$ are isomorphic. Like in Case 3.1, this implies that semilattices $\mathbf{Y}$ and $\mathbf{Y}^d$ are isomorphic and therefore $\mathbf{S} \simeq \mathbf{Y} \times \mathbf{C}$ and $\mathbf{T} \simeq \mathbf{Y}^d \times \mathbf{C}$ are also isomorphic.

Cases 3.3 and 3.4. $\mathbf{S}^2 \simeq \mathbf{Y}^2 \times \mathbf{C}^2$ is a chain normal band.

By Lemma 3.6, $\mathbf{Y}^2$ must be a chain semilattice. Since the square of at least two-element chain is not a chain, this is not possible. This completes the study of the case (3).

Finally, in case (4), $\mathbf{S} \simeq \mathbf{Y} \times \mathbf{C}$ and $\mathbf{T}$ is anti-isomorphic to $\mathbf{Y}^d \times \mathbf{C}$. By Lemma 3.7, $\mathbf{T} \simeq \mathbf{Y}^d \times \mathbf{C}^*$. Like in case (3), we consider the normal bands $\mathbf{S}^2 \simeq \mathbf{Y}^2 \times \mathbf{C}^2$ and $\mathbf{T}^2 \simeq (\mathbf{Y}^d)^2 \times (\mathbf{C}^*)^2$, which are also categorically equivalent and therefore have isomorphic endomorphism semigroups. One of the cases (1)-(4) of Theorem 3.8 is fulfilled for $\mathbf{S}^2$ and $\mathbf{T}^2$, and the analysis of them is exactly the same as for the cases (3.1)-(3.4).

The first two cases lead to $\mathbf{Y} \simeq \mathbf{Y}^d$, and thus $\mathbf{S} \simeq \mathbf{Y} \times \mathbf{C}$, $\mathbf{T} \simeq \mathbf{Y} \times \mathbf{C}^*$. From Lemma 3.7 we see that $\mathbf{S}$ and $\mathbf{T}$ are anti-isomorphic. The last two cases lead to contradiction.

The proof of the theorem is now complete. □

Corollary 3.10. *Categorically equivalent rectangular bands are isomorphic or anti-isomorphic.*

Corollary 3.11. *Categorically equivalent semilattices are isomorphic.*

Proof. Since the semilattice multiplication is commutative, anti-isomorphic semilattices are isomorphic. □

3.3 Lattices

Let $\mathbf{L} = (L; \vee, \wedge)$ be a lattice. The *dual lattice* of $\mathbf{L}$ is the lattice $\mathbf{L}^d = (L; \vee', \wedge')$, where $\vee'$ and $\wedge'$ are defined by $x \vee' y = x \wedge y$ and $x \wedge' y = x \vee y$ for all $x, y \in L$. We say that the lattices $\mathbf{L}$ and $\mathbf{L}'$ are *dually isomorphic*, if $\mathbf{L}' \simeq \mathbf{L}^d$. We denote this $\mathbf{L}' \simeq_d \mathbf{L}$.

From Corollary 6.4 in [30] it follows that two finitely generated projective lattices are categorically equivalent if and only if they are isomorphic or dually isomorphic. We are going to extend this result to arbitrary lattices. We will need the following easy lemma.

Lemma 3.12. *For any positive integer n and lattice* $\mathbf{L}$, $(\mathbf{L}^n)^d = (\mathbf{L}^d)^n$.

We say that $\operatorname{Sub}\mathbf{L}$ *determines* $\mathbf{L}$ if for an arbitrary lattice $\mathbf{K}$, $\operatorname{Sub}\mathbf{L} \simeq \operatorname{Sub}\mathbf{K}$ implies $\mathbf{L} \simeq \mathbf{K}$ or $\mathbf{L} \simeq_d \mathbf{K}$.

In [40] the following statement was proved:

Theorem 3.13. *If a lattice* $\mathbf{L}$ *is directly reducible, then* $\operatorname{Sub}\mathbf{L}$ *determines* $\mathbf{L}$.

Note that in this theorem $\mathbf{L}$ is determined not only in the class of directly reducible lattices, but in the class of all lattices.

Theorem 3.14. *Lattices are categorically equivalent if and only if they are isomorphic or dually isomorphic.*

Proof. Take two categorically equivalent lattices $\mathbf{L}$ and $\mathbf{K}$. By Theorem 2.6, they have isomorphic sublattice-lattices. If at least one of them, say $\mathbf{L}$, is directly reducible, then $\operatorname{Sub}\mathbf{L}$ determines $\mathbf{L}$, thus $\mathbf{L} \simeq \mathbf{K}$ or $\mathbf{L} \simeq_d \mathbf{K}$.

Now assume that none of $\mathbf{L}$ and $\mathbf{K}$ is directly reducible. The lattices $\mathbf{L}^2$ and $\mathbf{K}^2$ are also categorically equivalent by Theorem 2.6, and $\operatorname{Sub}\mathbf{L}^2 \simeq \operatorname{Sub}\mathbf{K}^2$. Since $\mathbf{L}^2$ is reducible, we obtain that $\mathbf{L}^2 \simeq \mathbf{K}^2$ or $\mathbf{L}^2 \simeq (\mathbf{K}^2)^d = (\mathbf{K}^d)^2$. Lattices have distributive congruence-lattices, thus by Proposition 3.2 they have the refinement property. Since, by assumption, $\mathbf{L}$ and $\mathbf{K}$ are directly irreducible, both $\mathbf{L}^2$ and $\mathbf{K}^2$ have factorization into directly irreducible lattices and therefore have unique factorization. Thus $\mathbf{L} \simeq \mathbf{K}$ or $\mathbf{L} \simeq \mathbf{K}^d$.

Conversely, assume that $\mathbf{L}$ and $\mathbf{K}$ are either isomorphic or dually isomorphic. The first case is trivial, in the second case $\mathbf{L}$ and $\mathbf{K}$ are weakly isomorphic, hence categorically equivalent. $\square$

Remark 3.15. Theorem 3.14 can be proved also by using Proposition 3.1, in which case Proposition 3.2 may be avoided.

Chapter 4

Term equivalent semigroups

From Chapter 2 we know that two finite semigroups are categorically equivalent iff they are weakly isomorphic. In view of that, it seems natural to investigate the term equivalence of semigroups. We find a large number of semigroup properties that are preserved by term equivalence. For some classes of semigroups, like commutative semigroups or bands, the term equivalence is trivial: the semigroups must be identical or dual. However, there exist examples of non-trivial term equivalence. We discuss separately completely regular and completely 0-simple semigroups.

4.1 General observations

A semigroup *term* in k variables is a finite word in the alphabet $\mathbf{x}_1, \ldots, \mathbf{x}_k$. On a fixed semigroup $(S;\cdot)$ such a term induces a k-ary term operation by evaluation. A *length* of a term is the length of the corresponding word.

Let $(S;\cdot)$ be a semigroup and $a \in S$. By $\langle a \rangle$ we denote the subsemigroup of $(S;\cdot)$ generated by a. The *index* $m(a)$ of a is the smallest positive integer m for which $a^m = a^r$ for some positive integer $r > m$. The *period* $n(a)$ of a is the smallest positive integer n for which $a^{m+n} = a^m$ for some positive integer m. If $\langle a \rangle$ is infinite, then both $m(a)$ and $n(a)$ are infinite. If $\langle a \rangle$ is finite, then $\langle a \rangle^* := \{a^{m(a)}, \ldots, a^{m(a)+n(a)-1}\}$ is a group. Note that a is contained in a group iff $m(a) = 1$.

Lemma 4.1. *Let $(S;\cdot)$ and $(S;+)$ be term equivalent semigroups. Then the following statements hold.*

(1) *The subsemigroups of $(S;\cdot)$ and $(S;+)$ are the same and term equivalent.*

(2) *The congruences of* $(S;\cdot)$ *and* $(S;+)$ *are the same and the corresponding quotient semigroups are term equivalent.*

(3) *The ideals of* $(S;\cdot)$ *and* $(S;+)$ *are the same.*

(4) *The idempotents of* $(S;\cdot)$ *and* $(S;+)$ *are the same.*

(5) *For every* $a \in S$*, the index and the period of* a *are the same with respect to* $\cdot$ *and* $+$*.*

Proof. The statements (1)-(4) follow straightforwardly from the fact that the basic operation of one semigroup is a term operation of the other one.

(5) Let $a \in S$. Note that $\{a^n | n \in \mathbb{N}\}$ is the intersection of all subsemigroups of $(S;\cdot)$ that contain a. Similarly, $\{na | n \in \mathbb{N}\}$ is the intersection of all subsemigroups of $(S;+)$ that contain a. From (1) it follows that $\{a^n | n \in \mathbb{N}\} = \{na | n \in \mathbb{N}\}$. So the subsemigroup generated by a is $\langle a\rangle$ with respect to both $\cdot$ and $+$.

Now assume that $\langle a\rangle$ is finite, and let m, n be the index and the period of a in $(S;\cdot)$. Then $\langle a\rangle^* = \{a^m, \ldots, a^{m+n-1}\}$ is the smallest ideal of $(\langle a\rangle, \cdot)$. By (3), $\langle a\rangle^*$ is an ideal in $(\langle a\rangle, +)$ as well. Hence the smallest multiplicative ideal of $\langle a\rangle$ contains the smallest additive ideal of $\langle a\rangle$. By exchanging $\cdot$ and $+$ we obtain the converse inclusion. Hence $\langle a\rangle^*$ also is the smallest ideal of $(\langle a\rangle, +)$. Since $n = |\langle a\rangle^*|$ and $m = |\langle a\rangle \setminus \langle a\rangle^*| + 1$, we obtain that m and n are also the index and the period for a with respect to $+$, respectively. □

Lemma 4.2. *Let* $(S;\cdot)$ *and* $(S;+)$ *be term equivalent semigroups. Assume that* $+$ *does not depend on both arguments. Then* $xy = x+y$ *for all* $x, y \in S$ *or* $xy = y+x$ *for all* $x, y \in S$*.*

Proof. Assume, without loss of generality, that $+$ does not depend on the second argument. Then there exists a function $f\colon S \to S$ such that $x+y = f(x)$ for all $x, y \in S$. Let $x, y, z \in S$. By associativity we obtain

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

That is, f is idempotent. Hence the only binary term operations of $(S;+)$ are $x, y, f(x)$, and $f(y)$. From the term equivalence of $(S;\cdot)$ and $(S;+)$ it follows that for all $x, y \in S$, $xy = f(x) = x+y$, or $xy = f(y) = y+x$, or $xy = x$ or $xy = y$. In the first two cases, the lemma is proved. In the last two cases, the only binary term operations of $(S;\cdot)$ are x and y, hence, from the term equivalence, also $x+y = x$ or $x+y = y$. □

Hence we may restrict ourselves to essentially binary operations when looking for non-trivial examples of term equivalent semigroups.

Two semigroups $(S;\cdot)$ and $(S;+)$ are called *dual*, if $xy = y + x$ for all $x, y \in S$. By the next lemma, two semigroups can be term equivalent without being identical or dual only if every element is contained in a group or has index 2. The order of every element is then bounded by some fixed integer. Thus such semigroups must be periodic.

Lemma 4.3. *Let* $(S;\cdot)$ *and* $(S;+)$ *be term equivalent semigroups. Assume that one of the following holds:*

(1) *for every integer* n *there exists* $a \in S$ *such that* $|\langle a\rangle| > n$*;*

(2) *there exists* $a \in S$ *with index at least 3.*

Then these semigroups are identical or dual.

Proof. By Lemma 4.2, we may assume that the operations of these two semigroups are essentially binary. Let **s** and **t** be semigroup terms such that their induced term operations s on $(S;+)$ and t on $(S;\cdot)$ satisfy

$$xy = s(x,y) \quad \text{and} \quad x + y = t(x,y) \quad \text{for all} \quad x, y \in S. \tag{4.1}$$

Let k and l denote the length of the terms **s** and **t**, respectively. Since the operations of our semigroups are essentially binary, we have $k \geqslant 2$ and $l \geqslant 2$. If $k = 2$, then we have for **s** four possibilities: $\mathbf{x}+\mathbf{x}$, $\mathbf{y}+\mathbf{y}$, $\mathbf{x}+\mathbf{y}$ and $\mathbf{y}+\mathbf{x}$. The first two of them contradict the assumption that the operation $\cdot$ is essentially binary. If, however, $\mathbf{s} = \mathbf{x}+\mathbf{y}$ or $\mathbf{s} = \mathbf{y}+\mathbf{x}$, then we are done. Thus, we may assume that $k > 2$, and similarly $l > 2$.

It follows from (4.1) that $2x = t(x,x) = x^l$ for every $x \in S$. Now, proceeding by induction on m, it is easily seen that for every positive integer m there exists an integer $r = r(m) > 2$ such that $mx = x^r$. Hence, $x^2 = s(x,x) = kx = x^{r(k)}$ for every $x \in S$. This shows that every $a \in S$ has index less than 3 and it generates the monogenic subsemigroup whose size is bounded by $r(k)$, a contradiction. □

A semigroup with zero $(S;\cdot)$ is called *nilpotent* if $S^n = \{0\}$ for some positive integer n.

Proposition 4.4. *If a semigroup* $(S;+)$ *is term equivalent to a nilpotent semigroup* $(S;\cdot)$*, then these semigroups are identical or dual to each other.*

Proof. Assume that S contains an element 0 such that $S^n = \{0\}$ for some positive integer n. Let $\mathbf{s}$ and $\mathbf{t}$ be semigroup terms as in the proof of Lemma 4.3. Let k and l be their lengths, respectively. If $k \leqslant 2$ or $l \leqslant 2$, then the result follows from Lemma 4.2, like in the proof of Lemma 4.3. Let now $k \geqslant 3$ and $l \geqslant 3$. Then

$$S^2 \subseteq \underbrace{S + \cdots + S}_{k} \subseteq S + S \subseteq S^l \subseteq S^3 \subseteq S^2\,,$$

implying $S^2 = S^3$. But then $S^2 = S^n = \{0\}$ and also $S + S = \{0\}$. Thus, $(S;+)$ and $(S;\cdot)$ are identical zero-semigroups. □

Theorem 4.5. *If a semigroup* $(S;\cdot)$ *is term equivalent to a commutative semigroup* $(S;+)$*, then these semigroups are identical.*

Proof. By Lemma 4.2, we may assume that $+$ and $\cdot$ depend on both arguments. Further, if there exists no finite bound on the size of monogenic subsemigroups of S or if there exists $a \in S$ of index $m(a) > 2$, then the result follows from Lemma 4.3. Thus assume that every $x \in S$ generates a finite subsemigroup with index $m(x) \leqslant 2$.

Since $(S;\cdot)$ and $(S;+)$ are term equivalent and $\cdot$ depends on both arguments, we have $k, l \in \mathbb{N}$ such that $xy = kx + ly$ for all $x, y \in S$. Note that if $k = l = 1$, then we are done. Otherwise we claim

$$\exists k, l \in \mathbb{N} \setminus \{1\}\ \forall x, y \in S\colon\ xy = kx + ly. \tag{4.2}$$

The term equivalence of $(S;\cdot)$ and $(S;+)$ implies that we have a term operation $t(x, y)$ on $(S;\cdot)$ such that $x + y = t(x, y)$ for all $x, y \in S$.

Consider the case $k > 1, l = 1$ (the case $k = 1, l > 1$ is similar). By applying $xy = kx + y$ repeatedly on $t(x, y)$, we have $a, b \in \mathbb{N}$ that are not both 1 such that $x + y = t(x, y) = ax + by$ for all $x, y \in S$. Note that a and b are not 0, because $+$ depends on both arguments. Since $+$ is commutative, we have

$$ax + by = x + y = y + x = ay + bx = bx + ay$$

for all $x, y \in S$. Now

$$xy = kx + y = akx + by = bkx + ay$$

yields (4.2).

Fix k, l as in (4.2). Let $x \in S$, and define $r(x) = m(x)n(x)$. By Lemma 4.1 (5), we have that $x^{r(x)}$ is the identity element of the group $(\langle x\rangle^*;\cdot)$, and likewise for the group $(\langle x\rangle^*;+)$. Note that $k \geqslant 2 \geqslant m(x)$, thus $kx \in \langle x\rangle^*$. We obtain

$$kx = kx + lx^{r(x)} = x \cdot x^{r(x)} = x^{r(x)+1}. \tag{4.3}$$

Similarly, for every $y \in S$ from $l \geqslant 2 \geqslant m(y)$ it follows $ly = y^{r(y)+1}$, implying $kx = lx$ for every $x \in S$. Now,

$$xy = kx + ky = ky + kx = yx,$$

that is, the semigroup $(S;\cdot)$ is commutative.

Now, the situation between $(S;+)$ and $(S;\cdot)$ is fully symmetric. By (4.2) applied to $(S;\cdot)$ we have $u \in \mathbb{N} \setminus \{1\}$ such that

$$x + y = x^u y^u \text{ for all } x, y \in S.$$

For $x, y \in S$ we obtain

$$\begin{aligned} xy = kx + ky = x^{r(x)+1} + y^{r(y)+1} &= (x^{r(x)+1})^u (y^{r(y)+1})^u = \\ &= \big((x^{r(x)})^u x^u\big)\big((y^{r(y)})^u y^u\big) = x^u y^u = x + y, \end{aligned}$$

which completes the proof. In the penultimate equality we used that $u \geqslant m(x)$ and $u \geqslant m(y)$. □

Corollary 4.6. *Let $(S;\cdot)$ and $(S;+)$ be term equivalent semigroups. Then for every $k \in \mathbb{N}$ and for every $x \in S$ we have $x^k = kx$.*

Proof. This follows from Theorem 4.5 since monogenic subsemigroups are commutative. □

In view of Theorem 4.5, we may assume, without loss of generality, that semigroups we are studying are non-commutative. For this reason, we use in the following the symbols $\cdot$ and $*$ for the semigroup operation, rather than $\cdot$ and $+$.

Lemma 4.7. *Let $(S;\cdot), (S;*)$ be term equivalent semigroups. Then there exist semigroup terms $\mathbf{s}(\mathbf{x},\mathbf{y})$ and $\mathbf{t}(\mathbf{x},\mathbf{y})$, such that their induced term operations s on $(S;*)$ and t on $(S;\cdot)$ satisfy*

$$xy = s(x, y),\ x * y = t(x, y) \textit{ for all } x, y \in S$$

and either

$$\mathbf{s} \textit{ and } \mathbf{t} \textit{ both start with } \mathbf{x} \textit{ and end with } \mathbf{y} \tag{4.4}$$

or

$$\mathbf{s} \textit{ and } \mathbf{t} \textit{ both start with } \mathbf{y} \textit{ and end with } \mathbf{x}. \tag{4.5}$$

Proof. For better clarity, we have replaced in this proof some insignificant parts of expressions by dots.

We assume that $(S;*)$ and $(S;\cdot)$ are neither identical nor dual to each other, otherwise the statement holds trivially. Then, by Lemma 4.2, the operations $*$ and $\cdot$ depend on both their arguments.

Let $\mathbf{s}_0(\mathbf{x},\mathbf{y})$, $\mathbf{t}_0(\mathbf{x},\mathbf{y})$ be semigroup terms such that their induced term operations s_0 on $(S;*)$ and t_0 on $(S;\cdot)$ satisfy

$$xy = s_0(x,y),\ x*y = t_0(x,y) \text{ for all } x,y \in S.$$

We first show that, without loss of generality, $\mathbf{s}_0$ and $\mathbf{t}_0$ start with the same letter. For that, suppose that $\mathbf{s}_0(\mathbf{x},\mathbf{y})$ starts with $\mathbf{x}$ and $\mathbf{t}_0(\mathbf{x},\mathbf{y})$ starts with $\mathbf{y}$. Then we have some $k \in \mathbb{N}$ such that for all $x,y \in S$,

$$xy = x^k * y * \dots, \tag{4.6}$$

$$x * y = y \cdot \dots. \tag{4.7}$$

Here we used that $\cdot$ depends on both arguments. Note that by Corollary 4.6, x^k is the same with respect to both $\cdot$ and $*$. We have

$$xy \overset{(4.6)}{=} x^k * \ y * \dots \overset{(4.7)}{=} (y \cdot \dots) * \dots \overset{(4.6)}{=} (y * \dots) * \dots = y * \dots$$

for all $x,y \in S$. It follows that there exists a term $\mathbf{s}_1(\mathbf{x},\mathbf{y})$ starting with $\mathbf{y}$ whose induced term operation s_1 on $(S;*)$ satisfies

$$xy = s_1(x,y) \text{ for all } x,y \in S.$$

Hence we may assume that $\mathbf{s}_0$ and $\mathbf{t}_0$ both start with $\mathbf{x}$ or both start with $\mathbf{y}$.

Now we consider several cases. We only need to study those cases where either $\mathbf{s}_0$ or $\mathbf{t}_0$ is not in the required form.

Case 1: $\mathbf{s}_0(\mathbf{x},\mathbf{y})$ and $\mathbf{t}_0(\mathbf{x},\mathbf{y})$ start and end with $\mathbf{x}$. Since $\cdot$ depends on both arguments, we have some positive integer k such that for all $x,y \in S$,

$$xy = x^k * y * \dots * x, \tag{4.8}$$

$$x * y = x \dots x. \tag{4.9}$$

It follows that

$$x * y \overset{(4.9)}{=} x \cdot (\dots \cdot x) \overset{(4.8)}{=} x^k * \dots * x = x * \dots * x \tag{4.10}$$

for all $x,y \in S$. Now

$$xy \overset{(4.8)}{=} x^k * y * (\dots * x) \overset{(4.10)}{=} x^k * (y * \dots * y) = x * \dots * y.$$

Similarly we get $x * y = x \dots y$ for all $x, y \in S$. Hence there exist **s** and **t** satisfying (4.4).

Case 2: $\mathbf{s}_0(\mathbf{x},\mathbf{y})$ and $\mathbf{t}_0(\mathbf{x},\mathbf{y})$ start both with **x** and end with distinct letters. Assume $xy = x * \dots * x$, $x * y = x \dots y$ for all $x, y \in S$. Exactly like in Case 1, we obtain $x * y = x * \dots * x$ and $xy = x * \dots * y$ for all $x, y \in S$. Hence there exist **s** and **t** satisfying (4.4).

Case 3: $\mathbf{s}_0(\mathbf{x},\mathbf{y})$ and $\mathbf{t}_0(\mathbf{x},\mathbf{y})$ start and end with **y**. This case is symmetric to Case 1. The same argument leads to $x * y = y * \dots * y$ and $xy = x * \dots * y$ for all $x, y \in S$. Hence there exist **s** and **t** satisfying (4.4).

Case 4: $\mathbf{s}_0(\mathbf{x},\mathbf{y})$ and $\mathbf{t}_0(\mathbf{x},\mathbf{y})$ start both with **y** and end with distinct letters. Assume $\mathbf{s}_0(\mathbf{x},\mathbf{y}) = \mathbf{y}\dots\mathbf{y}$, $\mathbf{t}_0(\mathbf{x},\mathbf{y}) = \mathbf{y}\dots\mathbf{x}$. Since $\cdot$ depends on both arguments, we have some positive integer k such that for all $x, y \in S$,

$$xy = y * \dots * x * y^k, \tag{4.11}$$

$$x * y = y \dots x. \tag{4.12}$$

It follows that

$$x * y \overset{(4.12)}{=} (y \cdot \dots) \cdot x \overset{(4.11)}{=} x * \dots * x^k = x * \dots * x \tag{4.13}$$

for all $x, y \in S$. Now

$$xy \overset{(4.11)}{=} y * \dots * x * y^k \overset{(4.13)}{=} y * \dots * (x * \dots * x) = y * \dots * x.$$

Hence there exist **s** and **t** satisfying (4.5). □

Now me derive some corollaries from Lemma 4.7.

Corollary 4.8. *If a semigroup $(S;*)$ is term equivalent to a band $(S;\cdot)$, then these semigroups are identical or dual to each other.*

Proof. By Lemma 4.1 (4), $(S;*)$ is a band.

Let $\mathbf{t}(\mathbf{x},\mathbf{y})$ be a semigroup term whose induced term operation t on $(S;\cdot)$ satisfies $x * y = t(x, y)$ for all $x, y \in S$. By Lemma 4.7, we may assume that **t** either starts with **x** and ends with **y**, or starts with **y** and ends with **x**. Since the band operation $\cdot$ is idempotent, the first possibility leads to $x * y = xy$, while the second one to $x * y = yx$. □

Green's relations $\mathcal{L}$, $\mathcal{R}$, $\mathcal{H}$, $\mathcal{D}$, $\mathcal{J}$ on a semigroup $(S;\cdot)$ are the equivalence relations on S defined by

$$\begin{aligned} a\mathcal{L}b &\Longleftrightarrow S^1a = S^1b, \\ a\mathcal{R}b &\Longleftrightarrow aS^1 = bS^1, \\ \mathcal{H} &= \mathcal{L} \wedge \mathcal{R}, \\ \mathcal{D} &= \mathcal{L} \vee \mathcal{R}, \\ a\mathcal{J}b &\Longleftrightarrow S^1aS^1 = S^1bS^1. \end{aligned}$$

Here $(S^1;\cdot)$ denotes $(S;\cdot)$, if it is a monoid, and $(S;\cdot)$ with adjoined identity element, otherwise.

Green's relations were introduced by J. A. Green in [16] and play an important role in the structure theory of semigroups. We use Lemma 4.7 to show that under term equivalence the relations $\mathcal{H}$, $\mathcal{J}$ and $\mathcal{D}$ are preserved, while the relations $\mathcal{L}$ and $\mathcal{R}$ are either preserved or flipped.

Theorem 4.9. *Let $(S;\cdot)$ and $(S;*)$ be term equivalent semigroups with Green's relations $(\mathcal{L},\mathcal{R},\mathcal{H},\mathcal{D},\mathcal{J})$ and $(\mathcal{L}',\mathcal{R}',\mathcal{H}',\mathcal{D}',\mathcal{J}')$, respectively. Then*

(1) *either ($\mathcal{L}=\mathcal{L}'$, $\mathcal{R}=\mathcal{R}'$) or ($\mathcal{L}=\mathcal{R}'$, $\mathcal{R}=\mathcal{L}'$);*

(2) $\mathcal{H}=\mathcal{H}'$, $\mathcal{D}=\mathcal{D}'$, $\mathcal{J}=\mathcal{J}'$.

Proof. (1) Lemma 4.7 implies that for every $x,y \in S$ either

$$xy = x * \ldots * y, \tag{4.14}$$
$$x * y = x \cdot \ldots \cdot y \tag{4.15}$$

or

$$xy = y * \ldots * x, \tag{4.16}$$
$$x * y = y \cdot \ldots \cdot x. \tag{4.17}$$

Let $a \in S$.

In the first case, (4.14) yields $aS \subseteq a * S$, and (4.15) yields $a * S \subseteq aS$. It follows that $aS = a * S$ for any $a \in S$. Hence, $\mathcal{R}=\mathcal{R}'$. Similarly one gets $\mathcal{L}=\mathcal{L}'$.

In the second case, (4.16) yields $aS \subseteq S * a$, and (4.17) yields $S * a \subseteq aS$. It follows that $aS = S * a$ for any $a \in S$. Hence, $\mathcal{R}=\mathcal{L}'$. Similarly one gets $\mathcal{L}=\mathcal{R}'$.

(2) Preservation of $\mathcal{H}$ and $\mathcal{D}$ follows from their definitions and (1).

Now, if $(S;\cdot)$ and $(S;*)$ are identical or dual, then $\mathcal{J}=\mathcal{J}'$ holds trivially. Otherwise, $(S;\cdot)$ and $(S;*)$ are periodic (Lemma 4.3). It is well known that for periodic semigroups, $\mathcal{D}$ and $\mathcal{J}$ coincide ([16], Theorem 3). Hence, $\mathcal{J}=\mathcal{J}'$. □

Next we exhibit a number of semigroup properties that are invariant under term equivalence. Clearly, all properties preserved by categorical equivalence are preserved also by term equivalence (e.g. being finitely generated).

A semigroup **S** is *completely regular* if every element of S lies in some subgroup of **S**. A semigroup $(S;\cdot)$ is *regular* if every element $a \in S$ is regular; an element $a \in S$ is *regular* if there exists an element $x \in S$ such that $axa = a$. A semigroup $(S;\cdot)$ is *inverse* if every element $x \in S$ has a unique *inverse element*, i.e. an element $y \in S$ such that $x = xyx$ and $y = yxy$.

Theorem 4.10. *Let* $(S;\cdot), (S;*)$ *be term equivalent semigroups. Then the following holds.*

(1) *If* $(S;\cdot)$ *has a zero* 0*, then* 0 *is also a zero with respect to* $*$.

(2) *If* $(S;\cdot)$ *has an identity* 1*, then* 1 *is also an identity with respect to* $*$*, and the semigroups* $(S;\cdot)$ *and* $(S;*)$ *are identical, dual, or both completely regular.*

(3) *If* $(S;\cdot)$ *is regular, then* $(S;*)$ *is regular.*

(4) *If* $(S;\cdot)$ *is inverse, then* $(S;*)$ *is inverse.*

(5) *If* $(S;\cdot)$ *is a group, then* $(S;*)$ *is a group.*

(6) *If* $(S;\cdot)$ *is completely regular, then* $(S;*)$ *is completely regular.*

Proof. (1) Since $\{0\}$ is an ideal in $(S;\cdot)$, it is also an ideal in $(S;*)$ by Lemma 4.1 (3).

(2) Let $x \in S$. Then $\langle x\rangle \cup \{1\}$ forms a commutative subsemigroup of $(S;\cdot)$. From Lemma 4.1 (1) and Theorem 4.5 it follows that $\cdot$ and $*$ coincide on $\langle x\rangle \cup \{1\}$. In particular $x * 1 = 1 * x = x$.

Next let $\mathbf{t}(\mathbf{x},\mathbf{y})$ be a semigroup term that induces a term operation t on $(S;\cdot)$ satisfying $x * y = t(x, y)$ for all $x, y \in S$. Let k and l be the multiplicities of $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{t}$. For $x \in S$, we obtain

$$x = x * 1 = t(x,1) = x^k,$$
$$x = 1 * x = t(1,x) = x^l.$$

If x has index greater than 1, this implies $k = l = 1$. Hence $t(x, y) = xy$ or $t(x, y) = yx$, that is, $(S;\cdot), (S;*)$ are identical or dual. Else every element in S generates a group, and $(S;\cdot), (S;*)$ are completely regular.

(3) Let $\mathbf{t}(\mathbf{x},\mathbf{y})$ be a word in $\mathbf{x},\mathbf{y}$. We claim that

$$\text{the word } \mathbf{t}(\mathbf{t}(\mathbf{x},\mathbf{y}),\mathbf{x}) \text{ begins and ends with } \mathbf{x}. \tag{4.18}$$

Observe that the first letter in $\mathbf{t}(\mathbf{t}(\mathbf{x},\mathbf{y}),\mathbf{x})$ is $\mathbf{x}$ no matter whether $\mathbf{t}(\mathbf{x},\mathbf{y})$ starts with $\mathbf{x}$ or $\mathbf{y}$. Indeed, if $\mathbf{t}(\mathbf{x},\mathbf{y}) = \mathbf{x}\circ\mathbf{u}(\mathbf{x},\mathbf{y})$, where $\mathbf{u}(\mathbf{x},\mathbf{y})$ is a word in $\mathbf{x},\mathbf{y}$ and $\circ$ stands for concatenation, then

$$\mathbf{t}(\mathbf{t}(\mathbf{x},\mathbf{y}),\mathbf{x}) = \mathbf{t}(\mathbf{x}\circ\mathbf{u}(\mathbf{x},\mathbf{y}),\mathbf{x}) = \mathbf{x}\circ\mathbf{u}(\mathbf{x},\mathbf{y})\circ\mathbf{u}(\mathbf{x}\circ\mathbf{u}(\mathbf{x},\mathbf{y}),\mathbf{x}).$$

If $\mathbf{t}(\mathbf{x},\mathbf{y}) = \mathbf{y}\circ\mathbf{u}(\mathbf{x},\mathbf{y})$, then

$$\mathbf{t}(\mathbf{t}(\mathbf{x},\mathbf{y}),\mathbf{x}) = \mathbf{x}\circ\mathbf{u}(\mathbf{t}(\mathbf{x},\mathbf{y}),\mathbf{x}).$$

Similarly the last letter in $\mathbf{t}(\mathbf{t}(\mathbf{x},\mathbf{y}),\mathbf{x})$ is $\mathbf{x}$ no matter whether $\mathbf{t}(\mathbf{x},\mathbf{y})$ ends with $\mathbf{x}$ or $\mathbf{y}$.

Now assume that $\mathbf{t}(\mathbf{x},\mathbf{y})$ induces a term operation t on $(S;*)$ such that $xy = t(x,y)$ for all $x,y \in S$. Let $a \in S$. Since $(S;\cdot)$ is regular, there is $b \in S$ such that

$$a = aba = t(t(a,b),a).$$

By (4.18), we have that $t(t(a,b),a) = a*c*a$ for some $c \in S$. Hence $a = a*c*a$, and $(S;*)$ is regular.

(4) Recall that a semigroup is inverse iff it is regular and its idempotents commute. The idempotents of $(S;\cdot)$ form a commutative subsemigroup of $(S;\cdot)$. By Lemma 4.1 and Theorem 4.5, the idempotents of $(S;*)$ also form a commutative subsemigroup, and, hence, $(S;*)$ is inverse.

(5) The statement immediately follows from the fact that a semigroup is a group iff it is inverse and has exactly one idempotent.

(6) This follows from (5) and Lemma 4.1. □

In [24] and [39], examples of term equivalent non-isomorphic finite groups were constructed. The finiteness implies that both identity and inverse can be expressed by multiplication. Hence these groups (with three basic operations) are also term equivalent as semigroups (with one basic operation).

If we have two groups that are term equivalent but not isomorphic, we can obtain semigroups that are not regular and still term equivalent in a nontrivial way.

Example 4.11. Term equivalent semigroups that are not regular, not isomorphic, and not dual to each other.

Let $(G;\cdot)$ and $(G;*)$ be term equivalent non-isomorphic finite groups with identity 1. Let a be distinct from the elements of G, and extend the operation $\circ \in \{\cdot;*\}$ to $S := G \cup \{a\}$ as follows:

$$x \circ a = a \circ x = x \quad \forall x \in G;$$
$$a \circ a = 1.$$

We first show that $(S;\cdot)$ and $(S;*)$ are term equivalent. By assumption we have binary term operations s on $(S;\cdot)$ and t on $(S;*)$ such that $xy = t(x,y)$, $x*y = s(x,y)$ for all $x,y \in G$. We claim that these identities hold for all elements of S. For $x \in G$, we have $t(x,a) = t(x,1) = x1 = xa$. Further, $t(a,a) = 1 = aa$. The remaining cases follow similarly. Hence, $(S;\cdot)$ and $(S;*)$ are term equivalent.

These semigroups are not regular, because a is not a regular element. Finally, since $(G;\cdot)$ and $(G;*)$ are neither isomorphic nor dual, the same holds obviously also for $(S;\cdot)$ and $(S;*)$.

4.2 Completely 0-simple and completely regular semigroups

Now we take a closer look at completely 0-simple and completely regular semigroups.

A semigroup is called *simple* if it has no proper ideals. A semigroup $(S;\cdot)$ with zero 0 is called *0-simple* if its only proper ideal is $\{0\}$ and $S^2 \neq \{0\}$. A semigroup $(S;\cdot)$ is called *completely simple* (*completely 0-simple*) if it is simple (0-simple) and contains a primitive idempotent, i.e. a non-zero idempotent that is not an identity for any other non-zero idempotent of $(S;\cdot)$.

Proposition 4.12. *Let $(S;\cdot),(S;*)$ be term equivalent semigroups. If $(S;\cdot)$ is completely 0-simple (completely simple), then $(S;*)$ is completely 0-simple (completely simple).*

Proof. If $(S;\cdot)$ is 0-simple (simple), then, by Lemma 4.1 (3) and Theorem 4.10 (1), $(S;*)$ is also 0-simple (simple).

Let e be a primitive idempotent in $(S;\cdot)$. We show that e is primitive in $(S;*)$, too. Suppose there is a non-zero idempotent $f \in S$, $f \neq e$, such that $e*f = f*e = f$. Then $\{e,f\}$ is a subsemigroup of $(S;*)$ with identity e. By Lemma 4.1 (1) and Theorem 4.10 (2), it must be also a subsemigroup of $(S;\cdot)$ with identity e, which is a contradiction. □

We say that a semigroup $(S;\cdot)$ is a *band of semigroups*, if for some band **Y**, $S = \bigcup_{\alpha\in Y} S_\alpha$, where S_α are subsemigroups of $(S;\cdot)$ such that $S_\alpha \cap S_\beta = \emptyset$ if $\alpha \neq \beta$ and $S_\alpha S_\beta \subseteq S_{\alpha\beta}$ for any $\alpha, \beta \in Y$.

Let **G** be a group. Then $\mathbf{G}^0$ denotes the group **G** with adjoined zero 0. Let Λ and I be non-empty sets and let P be a $\Lambda \times I$ matrix with entries $p_{\lambda,i}$ from G^0. Let $\mathcal{M}^0(G, I, \Lambda, P)$ be the set $(I \times G \times \Lambda) \cup \{0\}$ together with the multiplication

$$0 \cdot (i, s, \lambda) = (i, s, \lambda) \cdot 0 = 0 \cdot 0 = 0$$

for all triples (i, s, λ), and

$$(i, s, \lambda) \cdot (j, t, \mu) = \begin{cases} (i, sp_{\lambda,j}t, \mu), & \text{if } p_{\lambda,j} \neq 0, \\ 0, & \text{otherwise.} \end{cases}$$

This is a semigroup, called the *Rees Matrix semigroup with zero over a group*. If the entries of P are from G, then the *Rees Matrix semigroup over a group*, denoted $\mathcal{M}(G, I, \Lambda, P)$, is the set $I \times G \times \Lambda$ with the above multiplication restricted to it.

D. Rees proved in [35] that a semigroup is completely simple (completely 0-simple) iff it is isomorphic to a Rees matrix semigroup over a group (a regular Rees matrix semigroup with zero over a group).

It follows that every completely simple semigroup **S** is a rectangular band of isomorphic groups, which are precisely the $\mathcal{H}$-classes of **S** ([10]).

Proposition 4.13. *If completely simple semigroups $(S;*)$ and $(S;\cdot)$ are term equivalent, then their underlying groups are term equivalent and the rectangular bands either identical or dual.*

Proof. The first part of the statement follows from Theorem 4.10 (5). For the second part, observe that the equivalence relation $\mathcal{H}$ is a congruence relation in our case. Now, the claim follows from Lemma 4.1 (2) and Corollary 4.8. □

Proposition 4.14. *If a semigroup $(S;*)$ is term equivalent to a completely 0-simple semigroup $(S;\cdot)$, then these semigroups are identical, dual, or both completely regular.*

Proof. Let $(S;\cdot)$ be the completely 0-simple semigroup $\mathcal{M}^0(G, I, \Lambda, P)$.

Assume that $(S;\cdot)$ and $(S;*)$ are neither identical nor dual. Then, clearly, $|S| > 2$. We show that the product of any two non-zero elements of $(S;\cdot)$ is not zero, which means that $(S;\cdot)$ is isomorphic to a Rees matrix semigroup over a group, with zero adjoined, and thus is completely regular.

Suppose $p_{\lambda,i} = 0$ for some $i \in I$, $\lambda \in \Lambda$, i.e. $(\cdot,\cdot,\lambda)\cdot(i,\cdot,\cdot) = 0$.

Let $\mathbf{s}(\mathbf{x},\mathbf{y})$, $\mathbf{t}(\mathbf{x},\mathbf{y})$ be semigroup terms such that their induced term operations s on $(S;*)$ and t on $(S;\cdot)$ satisfy

$$xy = s(x,y) \text{ and } x*y = t(x,y) \text{ for all } x,y \in S.$$

Consider several cases.

Case 1. The term $\mathbf{t}(\mathbf{x},\mathbf{y})$ contains $\mathbf{xy}$ (as a subword), the term $\mathbf{s}(\mathbf{x},\mathbf{y})$ contains $\mathbf{yx}$. Then

$$(\cdot,\cdot,\lambda)*(i,\cdot,\cdot) = t((\cdot,\cdot,\lambda),(i,\cdot,\cdot)) = 0$$

and therefore for any $\mu \in \Lambda$, $j \in I$,

$$(i,\cdot,\mu)\cdot(j,\cdot,\lambda) = s((i,\cdot,\cdot),(\cdot,\cdot,\lambda)) = \ldots*(\cdot,\cdot,\lambda)*(i,\cdot,\cdot)*\ldots = 0$$

Then $S^2 = \{0\}$ contradicting the assumption that $(S;\cdot)$ is 0-simple.

Case 2. The term $\mathbf{t}(\mathbf{x},\mathbf{y})$ contains $\mathbf{yx}$, the term $\mathbf{s}(\mathbf{x},\mathbf{y})$ contains $\mathbf{xy}$. This case is similar to Case 1.

Case 3. $\mathbf{t}(\mathbf{x},\mathbf{y}) = \mathbf{x}\ldots\mathbf{xy}\ldots\mathbf{y}$, $\mathbf{s}(\mathbf{x},\mathbf{y}) = \mathbf{x}\ldots\mathbf{xy}\ldots\mathbf{y}$. Without loss of generality suppose that the multiplicity of $\mathbf{x}$ in $\mathbf{t}$ is at least 2. For any $y \in S$,

$$(i,\cdot,\lambda)*y = (i,\cdot,\lambda)\cdot(i,\cdot,\lambda)\cdot\ldots = 0,$$

whence

$$(i,\cdot,\lambda)\cdot y = s((i,\cdot,\lambda),y) = 0.$$

This yields $p_{\lambda,j} = 0$ for every $j \in I$. But then the set $\{(j,g,\lambda) | j \in I, g \in G\} \cup \{0\}$ is an ideal in $(S;\cdot)$. Hence, $(S;\cdot)$ is not 0-simple.

Case 4. $\mathbf{t}(\mathbf{x},\mathbf{y}) = \mathbf{y}\ldots\mathbf{yx}\ldots\mathbf{x}$, $\mathbf{s}(\mathbf{x},\mathbf{y}) = \mathbf{y}\ldots\mathbf{yx}\ldots\mathbf{x}$. This case is similar to Case 3. □

A *Brandt semigroup* is a completely 0-simple inverse semigroup.

Theorem 4.15. *A semigroup $(S;*)$ is term equivalent to a Brandt semigroup $(S;\cdot)$ if and only if they are identical, dual, or term equivalent groups with adjoined zero.*

Proof. The sufficiency is trivial. So, we prove the necessity.

Assume that $(S;*)$ and $(S;\cdot)$ are term equivalent, but neither identical nor dual to each other. From Proposition 4.14 it follows that both semigroups must be completely simple semigroups with adjoined zero. Since, on the one hand, idempotents in an inverse semigroup commute, and on the other hand, a completely simple semigroup is a rectangular band of groups, a completely simple semigroup is inverse if and only if it is a group. □

A. H. Clifford described in [9] the global structure of completely regular semigroups. Every completely regular semigroup **S** is a semilattice of completely simple semigroups, which are precisely the $\mathcal{D}$-classes of **S** ([10]). The underlying semilattice is called the *structural semilattice* of **S**.

Proposition 4.16. *Let* $(S;*), (S;\cdot)$ *be completely regular term equivalent semigroups. Then the structural semilattices of* $(S;*)$ *and* $(S;\cdot)$ *are identical and the corresponding completely simple subsemigroups are term equivalent.*

Proof. Since every completely regular semigroup **S** is a semilattice of the $\mathcal{D}$-classes of **S**, it is clear that the equivalence relation $\mathcal{D}$ is a congruence relation. Hence, by Lemma 4.1 (2), the structural semilattices of term equivalent completely regular semigroups are term equivalent. From Theorem 4.5 it follows that they are identical. By Theorem 4.9, the $\mathcal{D}$-classes of $(S;*)$ and $(S;\cdot)$ are the same, and since they are subsemigroups, they are term equivalent. □

It seems natural to ask the following question. Let $(S;*), (S;\cdot)$ be term equivalent semigroups such that $*$ and $\cdot$ are identical on all subgroups. Are $(S;*)$ and $(S;\cdot)$ identical or dual to each other?

In general, the answer to this question is negative.

Example 4.17. Let **G** be a finite non-commutative group. Let $S = G \times \mathbb{Z}_2$ be the universe of semigroups $(S;\cdot)$ and $(S;*)$, where for all $g, h \in G$ and $a, b \in \mathbb{Z}_2$,

$$(g,a)\cdot(h,b) := (gh,b), \qquad (g,a)*(h,b) := (gh,a).$$

The semigroups $(S;\cdot)$ and $(S;*)$ are term equivalent since for all $x, y \in S$,

$$x\cdot y = y^{|G|} * x * y, \qquad x * y = x\cdot y\cdot x^{|G|}.$$

To see that let $g, h \in G$ and $a, b \in \mathbb{Z}_2$. Then

$$(h,b)^{|G|} * (g,a) * (h,b) = (1,b) * (g,a) * (h,b) = (gh,b) = (g,a)\cdot(h,b)$$

and

$$(g,a)\cdot(h,b)\cdot(g,a)^{|G|} = (g,a)\cdot(h,b)\cdot(1,a) = (gh,a) = (g,a)*(h,b).$$

It is clear that $\cdot$ and $*$ are identical on the subgroups, but $(S;\cdot)$ and $(S;*)$ are neither identical nor dual to each other.

However, the semigroups in this example are still dually isomorphic via the bijection $\phi(g,a) = (g^{-1},a)$. It remains open, whether there exists an example of term equivalent semigroups such that the operations are identical on all subgroups, but the semigroups are neither isomorphic nor dually isomorphic.

As we found previously, the answer to the question, whether term equivalent semigroups identical on all subgroups must be identical or dual, is positive for bands. Also we can give an affirmative answer for Clifford semigroups.

Clifford semigroups are completely regular inverse semigroups. Their structure was completely described in [9]. Let **S** be a Clifford semigroup. Every semilattice component ($\mathcal{D}$-class) of **S** is a group. Let $S = \bigcup_{\alpha\in Y} S_\alpha$, where **Y** is a semilattice, $\mathbf{S}_\alpha$, $\alpha \in Y$ are groups such that $S_\alpha \cap S_\beta = \emptyset$ if $\alpha \neq \beta$ and $S_\alpha S_\beta \subseteq S_{\alpha\beta}$ for any $\alpha,\beta \in Y$. For each pair of elements $\alpha \geqslant \beta$ of Y, there is a homomorphism $\phi_{\alpha,\beta} : S_\alpha \to S_\beta$, called a *structural homomorphism*, such that
1) $\phi_{\alpha,\alpha}$ is the identity homomorphism on S_α;
2) if $\alpha \geqslant \beta \geqslant \gamma$ in G, then $\phi_{\alpha,\gamma} = \phi_{\beta,\gamma}\phi_{\alpha,\beta}$;
3) for any $\alpha,\beta \in Y$ and $a \in S_\alpha$, $b \in S_\beta$, $ab = \phi_{\alpha,\alpha\beta}(a)\phi_{\beta,\alpha\beta}(b)$.

Proposition 4.18. *Let $(S;*),(S;\cdot)$ be term equivalent Clifford semigroups. Assume the operations $*$ and $\cdot$ are identical on all subgroups. Then $(S;*)$ and $(S;\cdot)$ are identical.*

Proof. Let $t(x,y)$ be a term operation of $(S;\cdot)$ such that $x * y = t(x,y)$ for all $x,y \in S$. Let Y be the structural semilattice of S, and S_α, $\alpha \in Y$, be the maximal subgroups of S, as described above. Let 1_α denote the identity element of a group S_α.

We first show that the structural homomorphisms of $(S;*)$ and $(S;\cdot)$ are identical. Let $\alpha,\gamma \in Y$, $\alpha \geqslant \gamma$. Let $\phi_{\alpha,\gamma}$ and $\phi'_{\alpha,\gamma}$ be the structural homomorphisms corresponding to $*$ and $\cdot$, respectively. For any $a \in S_\alpha$, we have

$$\phi_{\alpha,\gamma}(a) = a * 1_\gamma = t(a,1_\gamma) = t(\phi'_{\alpha,\gamma}(a),1_\gamma) = \phi'_{\alpha,\gamma}(a) * 1_\gamma = \phi'_{\alpha,\gamma}(a).$$

Now let $\alpha,\beta \in Y$, $a \in S_\alpha$, $b \in S_\beta$. Since $*$ and $\cdot$ coincide on $S_{\alpha\beta}$, we get

$$a * b = \phi_{\alpha,\alpha\beta}(a) * \phi_{\beta,\alpha\beta}(b) = \phi_{\alpha,\alpha\beta}(a) \cdot \phi_{\beta,\alpha\beta}(b) = a \cdot b.$$

□

4.3 Concluding remarks

It was a long standing question whether two term equivalent groups must be isomorphic. See, for example, [42]. In 2004, K. A. Kearnes and Á. Szendrei

[24] answered this question negatively, by constructing two groups of the form $(\mathbb{Z}_7 \times \mathbb{Z}_{13}) \rtimes \mathbb{Z}_3$ that are term equivalent but not isomorphic. They pointed out that actually already in 1968, A. P. Street [39] constructed an example of two non-isomorphic term equivalent groups. The smallest order of the groups in that example was $2 \cdot 7 \cdot 43$. In that paper, the notion 'P-property' was used for term equivalence.

As we have seen, if a semigroup is term equivalent to a group, then it is a group itself (Theorem 4.10 (5)). At the same time, any two groups term equivalent as semigroups (with one basic operation) are also term equivalent as groups (with three basic operations). For this, it suffices to show how the operations identity and inverse of one group can be expressed as term operations of the other one. The identity element is the same in every two term equivalent monoids (Theorem 4.10 (2)). By Lemma 4.3, when two semigroups are term equivalent, they are identical, dual, or the order of every element is bounded by some finite constant. In the first two cases, the inverse element is preserved trivially. In the latter case, the exponent of both groups is finite, and thus the inverse element can be expressed by a term operation.

Many invariant properties of term equivalent groups are listed in [39].

As we pointed out after Theorem 4.10, term equivalent finite groups are also term equivalent as semigroups. However, term equivalent groups with infinite exponent might not be term equivalent as semigroups. It remains open whether such examples exist.

One may ask what happens if we drop the condition of associativity and consider just groupoids. As the following easy example shows, we cannot deduce much in this case.

Consider the groupoid $(\mathbb{Z}_n; -)$ and the abelian group $(\mathbb{Z}_n; +)$, with $n \geqslant 3$. They are term equivalent, because $x - y = x + (n-1)y$ and $x + y = x - ((y - y) - y)$. However, $(\mathbb{Z}_n; -)$ is not commutative, not associative and has no identity element.

Chapter 5

Rings

We reduce the problem of categorical equivalence for finite unitary rings to the case of rings of prime power characteristics. It is proved that categorically equivalent rings of coprime characteristics must be semisimple. The categorical equivalence problem for finite semisimple rings is completely solved.

5.1 Introduction

In the following we assume that all rings are with unity. This means, in particular, that the unity element 1 of a ring **R** is contained in every subring of **R**.

Recall that a finite algebra is called primal if all finitary operations on its universe are term operations. It is easy to see that all prime fields $\mathbb{Z}_p$ are primal (e.g. [13], Theorem 10.5.5). Thus, Theorem 2.3 yields $\mathbb{Z}_p \equiv_c \mathbb{Z}_q$ for any primes p and q. This result was generalized by C. Bergman and J. Berman:

Theorem 5.1. ([5], Example 5.10) *For any primes p and q and positive integers m and n, the finite fields $\mathbf{F}_{p^m}$ and $\mathbf{F}_{q^n}$ are categorically equivalent if and only if $m = n$.*

This fact is somewhat intriguing because as we have seen, in other well studied varieties (groups, semigroups, lattices) the finite categorically equivalent members have been proved to be weakly isomorphic, hence of the same size.

In the present chapter an attempt is made to study categorical equivalence of finite rings, in general. We first reduce the general problem to the case of rings of prime power characteristic. We observe that semisimplicity is a categorical property and completely solve the problem when two finite semisimple rings are categorically equivalent. We also show that the rings of coprime characteristics can be categorically equivalent only if they are semisimple. The case of rings of the same characteristic remains open. Our conjecture is that if this happens then the rings are isomorphic or anti-isomorphic.

In the end we also take a look at one specific case of infinite rings: polynomial rings over a finite field.

5.2 Reduction to p-rings

For a prime p, a *p-group* is a group, all of whose elements have orders a power of p. A finite group is a p-group iff its order is a power of p. A ring whose additive group is a p-group will be called a *p-ring* [1]. It is well known that every finite ring $\mathbf{R}$ can be represented as a direct product of non-zero p-rings, for different primes p. We shall call this decomposition of a ring $\mathbf{R}$ a *canonical* one. The factors of the canonical decomposition of $\mathbf{R}$ are called *p-components* of $\mathbf{R}$. We are going to show that every categorical equivalence between finite rings is actually induced by categorical equivalences between their p-components, possibly for different primes p.

The *characteristic* of a finite ring $\mathbf{R}$, denoted by char($\mathbf{R}$), is the exponent of the additive group of $\mathbf{R}$, that is, a smallest positive integer n such that $nR = 0$. Obviously, the characteristic of a p-ring is a power of p.

Since categorical equivalence functors preserve categorical products, we make the following technical observation that we need later:

Lemma 5.2. *Let V and W be categorically equivalent varieties with the equivalence functor $F : V \to W$, and let $\mathbf{A}_1, \mathbf{A}_2 \in V$. Then $H(\mathbf{A}_1 \times \mathbf{A}_2) \simeq H(\mathbf{A}_1) \times H(\mathbf{A}_2)$.*

We shall make use of the notion of independence introduced by Foster in [15] and developed further by Hu and Kelenson in [19]. The algebras $\mathbf{A}_1, \dots, \mathbf{A}_n$ of the same signature are called *independent* if there exists an n-ary term $t(x_1, \dots, x_n)$ such that in the algebra $\mathbf{A}_i$ the identity $t(x_1, \dots, x_n) \approx x_i$ holds, $i = 1, \dots, n$. Corollary 2.9 of [19] essentially states that algebras $\mathbf{A}_1, \dots, \mathbf{A}_n$ of a congruence permutable variety are independent if and only if, for any two of them, the intersection of the varieties they generate is trivial. Since the congruences of any ring permute, it follows that in the variety of rings the independence can be easily characterized, as mentioned in [19].

[1] The notion of p-ring has been used earlier for the rings defined by the identities $px \approx 0$ and $x^p \approx x$ where p is a prime number.

Proposition 5.3. *Finite rings* $\mathbf{R}_1, \ldots, \mathbf{R}_n$ *are independent in the category of rings with unity if and only if their characteristics are pairwise coprime.*

Corollary 2.9 of [19] also implies that in case of rings the independence is a categorical property in the following sense. If the variety V is generated by an independent system of rings $\mathbf{R}_1, \ldots, \mathbf{R}_n$ and $F : V \to W$ is an equivalence functor where W is some variety of rings then the system $F(\mathbf{R}_1), \ldots, F(\mathbf{R}_n)$ is independent, too.

Indeed, assume that for some $1 \leqslant i < j \leqslant n$, the intersection of $\mathrm{Var}(\mathbf{R}_i)$ and $\mathrm{Var}(\mathbf{R}_j)$ is trivial, i.e. is the variety consisting of the single one-element ring (up to isomorphism). In view of Theorem 2.5 (4) it must be mapped by F to the intersection of $\mathrm{Var}(F(\mathbf{R}_i))$ and $\mathrm{Var}(F(\mathbf{R}_j))$, which cannot be anything else than the variety of the single one-element ring (up to isomorphism).

Corollary 5.4. *The property to be a finite p-ring for some prime p is categorical.*

Proof. Assume that $\mathbf{R}$ is a finite p-ring and $\mathbf{S}$ is a ring categorically equivalent to $\mathbf{R}$. Then $\mathbf{S}$ is finite by Theorem 2.6 (6). Suppose that $\mathbf{S}$ is not a q-ring for some prime q. Then it is a direct product of two independent rings. By Lemma 5.2, since $\mathbf{R} \equiv_c \mathbf{S}$, the same must hold for $\mathbf{R}$, a contradiction. □

Two categories C and D are said to be *isomorphic* if there are covariant functors $F : C \to D$ and $G : D \to C$ such that the composite functors $F \circ G$ and $G \circ F$ are the identity functors on D and C, respectively.

For a category C, a *skeleton* of C is any full subcategory A such that each object of C is isomorphic to exactly one object in A. It is well known that two categories are equivalent if and only if their skeletons are isomorphic (as categories).

Theorem 5.5. *Finite rings* $\mathbf{R}$ *and* $\mathbf{S}$ *are categorically equivalent if and only if there is a one-to-one correspondence between their p-components such that the corresponding p-components are categorically equivalent.*

Proof. Assume first that $\mathbf{R}$ and $\mathbf{S}$ are categorically equivalent finite rings and let F be a functor that establishes this equivalence. Now, if $\mathbf{R} = \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ where $\mathbf{R}_i$, $i = 1, \ldots, n$, are the p-components of $\mathbf{R}$, then Lemma 5.2 implies that $\mathbf{S}$ is isomorphic to the direct product of $F(\mathbf{R}_1), \ldots, F(\mathbf{R}_n)$. By Theorem 2.5 (3), $\mathbf{R}_i \equiv_c F(\mathbf{R}_i)$, $i = 1, \ldots, n$. Thus, we have to show that $F(\mathbf{R}_1), \ldots, F(\mathbf{R}_n)$ are the p-components of $\mathbf{S}$. By Corollary 5.4, there exist primes q_i such that the characteristic of $F(\mathbf{R}_i)$ is a power of q_i, $i = 1, \ldots, n$. It remains to show that $q_i \neq q_j$ if $i \neq j$. But this easily follows from Proposition 5.3.

Let now $\mathbf{R}$ and $\mathbf{S}$ be finite rings with canonical decompositions $\mathbf{R} = \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ and $\mathbf{S} = \mathbf{S}_1 \times \cdots \times \mathbf{S}_n$. Assume that a functor F_i establishes categorical equivalence between $\mathbf{R}_i$ and $\mathbf{S}_i$, $i = 1, \ldots, n$. Then F_i induces an isomorphism between skeletons of the categories $\mathrm{Var}(\mathbf{R}_i)$ and $\mathrm{Var}(\mathbf{S}_i)$, $i = 1, \ldots, n$. Since $\mathbf{R}_1, \ldots, \mathbf{R}_n$ are independent, from Theorem 2.7 of [19] it follows that every ring $\mathbf{T} \in \mathrm{Var}(\mathbf{R})$ admits a decomposition $\mathbf{T} = \mathbf{T}_1 \times \cdots \times \mathbf{T}_n$, where the direct factors $\mathbf{T}_i \in \mathrm{Var}(\mathbf{R}_i)$ are unique, up to isomorphism. The similar statement holds also for every member of $\mathrm{Var}(\mathbf{S})$. This allows us to conclude that the formula $F(\mathbf{T}) = F_1(\mathbf{T}_1) \times \cdots \times F_n(\mathbf{T}_n)$ determines an isomorphism between skeletons of the categories $\mathrm{Var}(\mathbf{R})$ and $\mathrm{Var}(\mathbf{S})$. Since obviously $F(\mathbf{R}) = \mathbf{S}$, we get $\mathbf{R} \equiv_c \mathbf{S}$. □

In view of Theorem 5.5, our main problem splits in two:

1. Describe when a finite p-ring and a finite q-ring with $p \neq q$ can be categorically equivalent.
2. Describe when two finite p-rings can be categorically equivalent.

In this chapter we solve the first problem. The second problem remains open. We are not aware of any pair of finite categorically equivalent p-rings that would be neither isomorphic nor anti-isomorphic. Our conjecture is that there is no such pair.

5.3 Rings $\mathbb{Z}_n$

Obviously the rings $\mathbb{Z}_n$ are, up to isomorphism, the only rings with no proper subrings. Therefore, if $\mathbb{Z}_n$ is categorically equivalent to a ring $\mathbf{R}$, the latter must be isomorphic to some ring $\mathbb{Z}_m$. In this section we are going to establish when exactly two rings $\mathbb{Z}_m$ and $\mathbb{Z}_n$ are categorically equivalent. We first sharpen Theorem 5.1 by showing that a finite field $\mathbf{F}_{p^k}$ can be categorically equivalent only to $\mathbf{F}_{q^k}$. We use the following well-known fact:

Lemma 5.6. *For any finite field* $\mathbf{F}_{p^k}$, $\mathrm{Aut}\,\mathbf{F}_{p^k} \simeq (\mathbb{Z}_k, +)$.

Proof. The only automorphisms of the finite field $\mathbf{F}_{p^k}$ are the Frobenius automorphisms $x \to x^{p^i}$, $i = 0, 1, \ldots, k-1$. □

Let n be a positive integer. The full matrix ring over a finite field $\mathbf{F}$ is denoted by $\mathrm{Mat}_n(\mathbf{F})$.

Theorem 5.7. *If the finite field $\mathbf{F}_{p^k}$ is categorically equivalent to some ring $\mathbf{R}$ then there exists a prime q such that $\mathbf{R} \simeq \mathbf{F}_{q^k}$.*

Proof. Since by Theorem 2.6 finiteness and simplicity are preserved by categorical equivalence, $\mathbf{R}$ must be a finite simple ring. Thus, $\mathbf{R}$ is isomorphic to some ring $\mathrm{Mat}_n(\mathbf{F})$ where $\mathbf{F}$ is a finite field and n is a positive integer. Assume that $n \geqslant 2$ and consider the automorphism groups of $\mathbf{F}_{p^k}$ and $\mathbf{R}$. The first of them is by Lemma 5.6 cyclic, while the other, as well-known, is non-abelian. Thus, $n = 1$, that is, $\mathbf{R} \simeq \mathbf{F}$. Now our claim follows from Theorem 5.1. □

Corollary 5.8. *A ring categorically equivalent to the ring $\mathbb{Z}_p$ with a prime p is isomorphic to some ring $\mathbb{Z}_q$ with a prime q.*

In order to prove the main result of the present section, we need the following lemma.

Lemma 5.9. *For any primes p and q and positive integers k and l, the rings $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_{q^l}$ are categorically equivalent if and only if: 1) $k = l = 1$ or 2) $p = q$ and $k = l$.*

Proof. The sufficiency is obvious since, as we mentioned in the introduction, $\mathbb{Z}_p \equiv_c \mathbb{Z}_q$ for all primes p and q. For necessity, assume that $\mathbb{Z}_{p^k} \equiv_c \mathbb{Z}_{q^l}$. The ring $\mathbb{Z}_{p^k}$ has $k+1$ ideals and the ring $\mathbb{Z}_{q^l}$ has $l+1$. Since categorically equivalent algebras have isomorphic congruence lattices (Theorem 2.6 (5)), we immediately have $k = l$. Assume $k \geqslant 2$. The ideal lattices of $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_{q^k}$ are again isomorphic, with corresponding quotient rings categorically equivalent. Hence $\mathbb{Z}_{p^k}/(p^2) \simeq \mathbb{Z}_{p^2}$ and $\mathbb{Z}_{q^k}/(q^2) \simeq \mathbb{Z}_{q^2}$ must be categorically equivalent.

If $\mathbb{Z}_{p^2} \equiv_c \mathbb{Z}_{q^2}$ then $\mathbb{Z}^3_{p^2} \equiv_c \mathbb{Z}^3_{q^2}$. Hence, the subring lattices of $\mathbb{Z}^3_{p^2}$ and $\mathbb{Z}^3_{q^2}$ must be isomorphic. We are going to show that the subring lattice of $\mathbb{Z}^3_{p^2}$ has exactly $p+1$ atoms. Then, of course, the subring lattice of $\mathbb{Z}^3_{q^2}$ has exactly $q+1$ atoms which allows us to conclude $p = q$.

The smallest subring of $\mathbb{Z}^3_{p^2}$ is one consisting of all diagonal elements (a, a, a). Thus, any atom $\mathbf{X}$ of the subring lattice of $\mathbb{Z}^3_{p^2}$ is a subring of $\mathbb{Z}^3_{p^2}$ generated by a single non-diagonal triple $(a_1, a_2, a_3) \in \mathbb{Z}^3_{p^2}$. Since $(a_3, a_3, a_3) \in X$, we may assume, without loss of generality, that $a_3 = 0$. Assume that $pa_1 \neq 0$. Easy straightforward calculations show that then the set

$$Y = \{(i + jpa_1, i + jpa_2, i) \mid i = 0, \dots, p^2 - 1, j = 0, \dots, p - 1\}$$

is a subuniverse of the ring $\mathbb{Z}_{p^2}^3$ and is contained in X. Also, Y contains the non-diagonal element $(pa_1, pa_2, 0)$, but $(a_1, a_2, 0) \notin Y$. This contradicts the assumption that $\mathbf{X}$ is an atom of the subring lattice of $\mathbb{Z}_{p^2}^3$. Thus, $pa_1 = 0$ and similarly $pa_2 = 0$. Now, one can easily check that the set

$$Z = \{i + ja_1, i + ja_2, i) \mid i = 0, \dots, p^2 - 1, j = 0, \dots, p - 1\}$$

is a subuniverse of the ring $\mathbb{Z}_{p^2}^3$. In view of the choice of $\mathbf{X}$, we have $X = Z$.

We have seen that every non-zero pair $(a_1, a_2) \in \mathbb{Z}_{p^2}$ with $pa_1 = pa_2 = 0$ determines an atom of the subring lattice of $\mathbb{Z}_{p^2}^3$. The number of such pairs is $p^2 - 1$ and it is easy to see that two pairs of this form determine the same subring if and only if one of them can be obtained from the other multiplying by $i \in \{1, \dots, p-1\}$. Thus, the number of atoms is $(p^2 - 1)/(p - 1) = p + 1$. □

Now we are ready to formulate and prove the general result. For any positive integer n, we denote $q(n) = n/r$ where r is the squarefree part of n, that is, the product of all prime divisors p of n such that p^2 does not divide n.

Theorem 5.10. *The rings $\mathbb{Z}_{n_1}$ and $\mathbb{Z}_{n_2}$ are categorically equivalent if and only if n_1 and n_2 have the same number of (different) prime divisors, and $q(n_1) = q(n_2)$.*

Proof. This is a straightforward consequence of Theorem 5.5 and Lemma 5.9. □

Every finite ring $\mathbf{R}$ has a unique minimal subring. This is the subring generated by $1 \in R$ and obviously it is isomorphic to $\mathbb{Z}_n$ where $n = \mathrm{char}(\mathbf{R})$. Clearly, if two finite rings are categorically equivalent then so are their minimal subrings. Hence we have the following corollary from Theorem 5.10.

Corollary 5.11. *Let $\mathbf{R}$ and $\mathbf{S}$ be a finite p-ring and a finite q-ring, respectively. If $\mathbf{R} \equiv_c \mathbf{S}$ then either $\mathrm{char}(\mathbf{R}) = \mathrm{char}(\mathbf{S})$ or $\mathrm{char}(\mathbf{R}) = p$ and $\mathrm{char}(\mathbf{S}) = q$.*

5.4 Rings of order p^2

Since all rings of prime order are categorically equivalent to each other (they all are isomorphic to the rings $\mathbb{Z}_p$), it is natural to consider, as the next step, the rings of order p^2, for a prime p. Theorem 5.15, the main result of this section shows that a ring categorically equivalent to a ring of order p^2 is of order q^2 for some prime q. Moreover, we show exactly how this can happen. This result has several applications; see the proofs of Theorems 5.16 and 5.20.

It is easy to see (e.g. [3] or [14]) that for a prime p, there are up to isomorphism exactly four different rings of order p^2:

1. $\mathbf{F}_{p^2}$;
2. $\mathbb{Z}_p \times \mathbb{Z}_p$;
3. $\mathbb{Z}_{p^2}$;
4. $\mathbb{Z}_p[x]/(x^2) \simeq \{a + b\varepsilon \mid a, b \in \mathbb{Z}_p\}, \varepsilon^2 = 0$.

We already know that $\mathbf{F}_{p^2} \equiv_c \mathbf{F}_{q^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p \equiv_c \mathbb{Z}_q \times \mathbb{Z}_q$ for any primes p and q. As we shall see soon, these are the only non-trivial occurrences of categorical equivalence involving a ring of order p^2. To prove this, we need some simple lemmas.

A ring is called *semisimple* if it is isomorphic to a finite direct product of simple rings.

Lemma 5.12. *If a finite semisimple ring* $\mathbf{R}$ *is categorically equivalent to a ring* $\mathbf{S}$*, then* $\mathbf{S}$ *is finite semisimple, too.*

Proof. Let F be the equivalence functor from $\mathrm{Var}(\mathbf{R})$ to $\mathrm{Var}(\mathbf{S})$ such that $F(\mathbf{R}) = \mathbf{S}$. Since $\mathbf{R}$ is finite and semisimple, we have $\mathbf{R} \simeq \mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ where $\mathbf{R}_1, \ldots, \mathbf{R}_n$ are simple rings. Since, by Lemma 5.2 and Theorem 2.6 (5), direct products and simplicity are preserved by equivalence functors, we see that $\mathbf{S}$ is isomorphic to the direct product of simple rings $F(\mathbf{R}_1), \ldots, F(\mathbf{R}_n)$. Hence, $\mathbf{S}$ is semisimple. □

For a ring $\mathbf{R}$, the *Jacobson radical* is the intersection of all maximal left ideals of $\mathbf{R}$ (equivalently, it is the intersection of all maximal right ideals of $\mathbf{R}$). For shortness, in the following we will call the Jacobson radical just the *radical*. The following well-known facts can be found, for example, in [1], Chapter 8. The radical is a (two-sided) ideal, and in case of a finite ring, it is in fact the intersection of all maximal (two-sided) ideals. A finite ring $\mathbf{R}$ is semisimple if and only if its radical is zero, and the radical is the smallest ideal J such that $\mathbf{R}/J$ is semisimple. This yields the following corollary:

Corollary 5.13. *Assume that finite rings* $\mathbf{R}$ *and* $\mathbf{S}$ *are categorically equivalent and this equivalence induces the lattice isomorphism* $\Phi : \mathrm{Con}(\mathbf{R}) \to \mathrm{Con}(\mathbf{S})$*. Then* Φ *maps the radical of* $\mathbf{R}$ *to the radical of* $\mathbf{S}$*.*

An ideal I of a ring is called *nilpotent* if some power of it is zero. Assume that I is non-zero and n is the smallest integer such that $I^n = 0$. Then I^{n-1} is non-zero, but $(I^{n-1})^2 = 0$. The radical of a finite ring is nilpotent ([1]). Thus we get:

Lemma 5.14. *The radical of a finite ring* $\mathbf{S}$*, if non-zero, contains a non-zero ideal* K *of* $\mathbf{S}$ *such that* $K^2 = 0$.

Theorem 5.15. *Let* $\mathbf{R}$ *and* $\mathbf{S}$ *be categorically equivalent non-isomorphic rings and* $|R| = p^2$ *where* p *is a prime. Then either* $\mathbf{R}$ *is of Type (1) and* $\mathbf{S} \simeq \mathbf{F}_{q^2}$ *for some prime* $q \neq p$*, or* $\mathbf{R}$ *is of Type (2) and* $\mathbf{S} \simeq \mathbb{Z}_q \times \mathbb{Z}_q$ *for some prime* $q \neq p$.

Proof. We consider separately four cases depending in which type the ring $\mathbf{R}$ falls. Let F be a functor that establishes categorical equivalence between $\mathbf{R}$ and $\mathbf{S}$, $F(\mathbf{R}) = \mathbf{S}$.

If $\mathbf{R} = \mathbf{F}_{p^2}$ then by Theorem 5.7 we have $\mathbf{S} \simeq \mathbf{F}_{q^2}$ for some prime q. Since $\mathbf{R} \not\simeq \mathbf{S}$, the primes p and q are different.

Let $\mathbf{R} = \mathbb{Z}_p \times \mathbb{Z}_p$. Since F preserves products, $\mathbf{S} = F(\mathbb{Z}_p) \times F(\mathbb{Z}_p)$ but then by Corollary 5.8 there is a prime q such that $F(\mathbb{Z}_p) \simeq \mathbb{Z}_q$. Clearly, $p \neq q$ because otherwise $\mathbf{R}$ and $\mathbf{S}$ would be isomorphic.

Let now $\mathbf{R} = \mathbb{Z}_{p^2}$. Since the rings $\mathbb{Z}_n$ are, up to isomorphism, exactly the rings with no proper subrings, there exists an integer n such that $\mathbf{S} \simeq \mathbb{Z}_n$. But then Theorem 5.10 yields $n = p^2$.

It remains to consider the case when $\mathbf{R}$ is of Type (4). Thus, assume that $R = \{a + b\varepsilon \mid a, b \in \mathbb{Z}_p\}$ where $\varepsilon^2 = 0$. We know that $\mathbf{S}$ must be finite (Theorem 2.6 (6)), and by Corollary 5.11, it must have prime characteristic, say q. Thus, $\mathbf{S}$ can be considered as a vector space over $\mathbb{Z}_q$. Obviously the only proper non-zero ideal of $\mathbf{R}$ is $I = \{a\varepsilon \mid a \in \mathbb{Z}_p\}$, which is the radical of $\mathbf{R}$. Now, if J is the ideal of $\mathbf{S}$ corresponding under F to I, then $\mathbf{R}/I \equiv_c \mathbf{S}/J$ which by Corollary 5.8 implies that $\mathbf{S}/J$ is isomorphic to $\mathbb{Z}_q$. Corollary 5.13 gives that J is the radical of $\mathbf{S}$ and $J \neq 0$ because by Lemma 5.12 semisimplicity is a categorical property.

We next show that $|J| = q$. By Lemma 5.14, J contains a non-zero ideal K of $\mathbf{S}$ with $K^2 = 0$. Since J is the only proper non-zero ideal of $\mathbf{S}$, we have $K = J$. We pick an arbitrary non-zero element $t \in J$ and consider the $\mathbb{Z}_q$-subspace L of $\mathbf{S}$ generated by t. Clearly, $|L| = q$. Since $S/J \simeq \mathbb{Z}_q$, every element $s \in S$ has the form $s = a \cdot 1 + u$ where $a \in \mathbb{Z}_q$ and $u \in J$. It follows that $st = (a \cdot 1 + u)t = at + ut = at \in L$ and similarly $ts = at \in L$. Thus, L is an ideal of $\mathbf{S}$. As above, J must be the only proper non-zero ideal of $\mathbf{S}$, so we conclude $L = J$ and $|S| = q^2$. Since $t^2 = 0$, the ring $\mathbf{S}$ is of Type (4), indeed.

It remains to notice that the rings of Type (4) corresponding to different primes cannot be categorically equivalent because their automorphism groups are of different size. Indeed, it is easy to see that the automorphisms of $\mathbf{R}$ are precisely the mappings of the form $a + b\varepsilon \mapsto a + b\lambda\varepsilon$ where λ is a non-zero element of $\mathbb{Z}_p$. Thus, $|\mathrm{Aut}\,\mathbf{R}| = p - 1$. □

Now we derive an important consequence of Theorem 5.15 and Corollary 5.11. It shows, in essence, that a finite non-semisimple p-ring can be categorically equivalent only to a ring of the same characteristic.

Theorem 5.16. *Let* $\mathbf{R}$ *be a finite non-semisimple* p*-ring for some prime* p*. If* $\mathbf{R}$ *is categorically equivalent to a ring* $\mathbf{S}$ *then* $\mathrm{char}(\mathbf{R}) = \mathrm{char}(\mathbf{S})$.

Proof. Assume that $\mathrm{char}(\mathbf{R}) \neq \mathrm{char}(\mathbf{S})$. Then by Corollary 5.11 $\mathrm{char}(\mathbf{R}) = p$ and $\mathrm{char}(\mathbf{S}) = q$ where q is a prime different from p. Since $\mathbf{R}$ is not semisimple, its radical is non-zero, and by Lemma 5.14 there exists a non-zero element $e \in R$ such that $e^2 = 0$.

Now consider the subring $\mathbf{R}_1$ of $\mathbf{R}$ consisting of all elements of the form $a + be$ where $a, b \in \mathbb{Z}_p$. It is categorically equivalent to a subring $\mathbf{S}_1$ of $\mathbf{S}$. However, it is easily seen that $\mathbf{R}_1$ is a Type (4) ring of order p^2. Thus, by Theorem 5.15, we have $\mathbf{R}_1 \simeq \mathbf{S}_1$, implying $p = q$. This contradiction proves the theorem. □

Corollary 5.17. *Finite categorically equivalent rings of coprime characteristics are semisimple.*

Proof. Let $\mathbf{R}$ and $\mathbf{S}$ be finite rings of coprime characteristics, $\mathbf{R} \equiv_c \mathbf{S}$, and let $\mathbf{R}_1, \ldots, \mathbf{R}_n$ be the factors of the canonical decomposition for $\mathbf{R}$. Then, by Theorem 5.5 there is the same number of factors in the canonical decomposition for $\mathbf{S}$; let them be $\mathbf{S}_1, \ldots, \mathbf{S}_n$. Without loss of generality, we have $\mathbf{R}_i \equiv_c \mathbf{S}_i$, $i = 1, \ldots, n$. Since obviously $\mathrm{char}(\mathbf{R}_i)$ and $\mathrm{char}(\mathbf{S}_i)$ are coprime, Theorem 5.16 implies that $\mathbf{R}_i$ and $\mathbf{S}_i$ are semisimple for $i = 1, \ldots, n$. Hence also $\mathbf{R}$ and $\mathbf{S}$ as direct products of semisimple rings are semisimple. □

5.5 Semisimple rings

In this section we consider categorical equivalence of semisimple rings. Since finite semisimple rings are direct products of finitely many simple rings, as a first step, we consider the case of finite simple rings, which, as well known, are full matrix rings over finite fields (in particular, they are p-rings for some prime p). Our approach is based on the fact that categorically equivalent algebras must have isomorphic automorphism groups. In order to prove the main result, we need two lemmas.

Let $\mathbf{K}$ be a finite field, n a positive integer. By $\operatorname{Inn}\operatorname{Mat}_n(\mathbf{K})$ we denote the set of all inner automorphisms of $\operatorname{Mat}_n(\mathbf{K})$, i.e. $\alpha \in \operatorname{Inn}\operatorname{Mat}_n(\mathbf{K})$ if there exists $Q \in \mathrm{GL}_n(\mathbf{K})$ such that for every $X \in \operatorname{Mat}_n(\mathbf{K})$, $\alpha(X) = Q^{-1}XQ$.

A group is called *solvable* if its composition series has only commutative factors.

Lemma 5.18. *Let $\mathbf{K}$ be a finite field and $n \geqslant 2$ an integer. The group $\operatorname{Aut}\operatorname{Mat}_n(\mathbf{K})$ is solvable if and only if $n = 2$ and $\mathbf{K}$ is isomorphic either to $\mathbb{Z}_2$ or $\mathbb{Z}_3$. In all other cases $\operatorname{Aut}\operatorname{Mat}_n(\mathbf{K})$ has a single non-abelian composition factor which is isomorphic to the projective special linear group $\mathrm{PSL}(n,\mathbf{K})$.*

Proof. We first prove that

$$\operatorname{Aut}\operatorname{Mat}_n(\mathbf{K}) \simeq \operatorname{Inn}\operatorname{Mat}_n(\mathbf{K}) \rtimes \operatorname{Aut}\mathbf{K} \tag{5.1}$$

where $\rtimes$ denotes semidirect product of groups. This can be derived using [34], Chapter I, Theorem 3.1, but we present here the direct proof.

For every $\sigma \in \operatorname{Aut}\mathbf{K}$, define $\overline{\sigma} \in \operatorname{Aut}\operatorname{Mat}_n(\mathbf{K})$ as follows: for every $A \in \operatorname{Mat}_n(\mathbf{K})$, $(\overline{\sigma}(A))_{ij} = \sigma(A_{ij})$.

Take any $\varphi \in \operatorname{Aut}\operatorname{Mat}_n(\mathbf{K})$. Denote by I the identity matrix of $\operatorname{Mat}_n(\mathbf{K})$. Let $Z = \{cI \mid c \in K\}$ be the set of scalar matrices. Observe that $(Z,+,\cdot) \simeq \mathbf{K}$ and Z is the center of $\operatorname{Mat}_n(\mathbf{K})$. We define σ as the automorphism of $\mathbf{K}$ that corresponds to $\varphi|_Z \in \operatorname{Aut} Z$. Thus, $\sigma(c)I = \varphi(cI)$ for every $c \in K$.

Now define $\alpha : \operatorname{Mat}_n(\mathbf{K}) \to \operatorname{Mat}_n(\mathbf{K})$ by $\alpha = \varphi\overline{\sigma}^{-1}$. The map α is an automorphism of $\operatorname{Mat}_n(\mathbf{K})$ whose restriction to Z is the identity map. For every $X \in \operatorname{Mat}_n(\mathbf{K})$ and $c \in K$, it satisfies

$$\alpha(cX) = \alpha(cIX) = \alpha(cI)\cdot\alpha(X) = (cI)\cdot\alpha(X) = c\cdot\alpha(X).$$

Hence, α is also an automorphism of $\operatorname{Mat}_n(\mathbf{K})$ considered as an algebra over the field $\mathbf{K}$. Since $\operatorname{Mat}_n(\mathbf{K})$ is a central simple algebra over $\mathbf{K}$, we get by the Skolem-Noether theorem that α is an inner automorphism of $\operatorname{Mat}_n(\mathbf{K})$.

So we got that $\varphi = \alpha\overline{\sigma}$, where $\alpha \in \operatorname{Inn}\operatorname{Mat}_n(\mathbf{K})$ and $\sigma \in \operatorname{Aut}\mathbf{K}$. Observe also that $\operatorname{Inn}\operatorname{Mat}_n(\mathbf{K})$ is a normal subgroup of $\operatorname{Aut}\operatorname{Mat}_n(\mathbf{K})$ and that $\{\overline{\sigma} \mid \sigma \in \operatorname{Aut}\mathbf{K}\}$ is a subgroup of $\operatorname{Aut}\operatorname{Mat}_n(\mathbf{K})$ (isomorphic to $\operatorname{Aut}\mathbf{K}$).

It remains to prove that the intersection of $\operatorname{Inn}\operatorname{Mat}_n(\mathbf{K})$ and $\{\overline{\sigma} \mid \sigma \in \operatorname{Aut}\mathbf{K}\}$ is trivial. For this, suppose that for some $\alpha_0 \in \operatorname{Inn}\operatorname{Mat}_n(\mathbf{K})$ and $\sigma_0 \in \operatorname{Aut}\mathbf{K}$,

$\alpha_0(X) = \overline{\sigma}_0(X)$ for all $X \in \mathrm{Mat}_n(\mathbf{K})$. We show that α_0 and $\overline{\sigma}_0$ are identity maps on $\mathrm{Mat}_n(\mathbf{K})$. For any $c \in \mathbf{K}$, we have $\alpha_0(cI) = cI$, but $\overline{\sigma}_0(cI) = cI$ for all $c \in \mathbf{K}$ only if $\sigma_0 = 1_{\mathbf{K}}$. This completes the proof of (5.1).

Therefore, since the automorphism group of a finite field is cyclic (Lemma 5.6), the solvability of $\mathrm{Aut}\,\mathrm{Mat}_n(\mathbf{K})$ is equivalent to that of $\mathrm{Inn}\,\mathrm{Mat}_n(\mathbf{K})$. Further, since $\mathrm{Inn}\,\mathrm{Mat}_n(\mathbf{K})$ is isomorphic to the quotient group of $\mathrm{GL}(n,\mathbf{K})$ over its center, the solvability of $\mathrm{Inn}\,\mathrm{Mat}_n(\mathbf{K})$ is equivalent to that of $\mathrm{GL}(n,\mathbf{K})$. Now, since $\mathrm{GL}(n,\mathbf{K})/\mathrm{SL}(n,\mathbf{K}) \simeq \mathbf{K}^*$, and $\mathrm{PSL}(n,\mathbf{K})$ is isomorphic to the quotient group of $\mathrm{SL}(n,\mathbf{K})$ over its center, we see that the solvability of $\mathrm{GL}(n,\mathbf{K})$ is equivalent to that of $\mathrm{PSL}(n,\mathbf{K})$. Finally, our claim follows from a classical fact of group theory: the group $\mathrm{PSL}(n,\mathbf{K})$ with $n \geqslant 2$ is solvable if and only if $n = 2$ and $|\mathbf{K}|$ is 2 or 3 (then we have $\mathrm{PSL}(2,\mathbf{F}_2) \simeq S_3$ and $\mathrm{PSL}(2,\mathbf{F}_3) \simeq A_4$), and in all other cases it is simple non-abelian (see, for example, [41], Section 1.2). □

Lemma 5.19. *Every atom in the lattice of subrings of* $\mathrm{Mat}_2(\mathbb{Z}_p)$ *has cardinality* p^2*.*

Proof. Since $\mathbb{Z}_p$ is a prime field, every subring of $\mathrm{Mat}_2(\mathbb{Z}_p)$ is a vector space over $\mathbb{Z}_p$. The proper non-trivial subrings of this ring have dimension 2 or 3, hence it is sufficient to prove that no subring of dimension 3 is an atom. If $\mathbf{S} \leqslant \mathrm{Mat}_2(\mathbb{Z}_p)$ is a 3-dimensional subring, then it can be defined by a single homogeneous linear equation, i.e., there exist coefficients $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_p$ (not all zero) such that

$$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \; a, b, c, d \in \mathbb{Z}_p, \ \alpha a + \beta b + \gamma c + \delta d = 0 \right\}.$$

Since the identity matrix belongs to S, we must have $\alpha + \delta = 0$. If $\gamma \neq 0$, then S contains the p^2-element subring

$$\left\{ \begin{pmatrix} a & b \\ \lambda b & a \end{pmatrix} \middle| \; a, b \in \mathbb{Z}_p \right\}$$

with $\lambda = -\beta\gamma^{-1}$, therefore $\mathbf{S}$ is not an atom. If $\beta \neq 0$, then a similar argument works, so in the remaining cases we can assume that $\beta = \gamma = 0$ and $\delta = -\alpha \neq 0$. Then we have

$$S = \left\{ \begin{pmatrix} a & b \\ c & a \end{pmatrix} \middle| \; a, b, c \in \mathbb{Z}_p \right\};$$

however, this set is not closed under multiplication. □

We know that if a finite simple ring $\mathbf{R}$ is categorically equivalent to a ring $\mathbf{S}$ then $\mathbf{S}$ is finite simple, too. We also know that if $\mathbf{R}$ is a finite field then so is $\mathbf{S}$.

Moreover, we know that then there exist primes p and q and a positive integer k such that one of the two rings is isomorphic to $\mathbf{F}_{p^k}$ and the other to $\mathbf{F}_{q^k}$. The following theorem shows that in all other cases categorically equivalent finite simple rings are isomorphic.

Theorem 5.20. *Let* $\mathbf{K}_1$ *and* $\mathbf{K}_2$ *be finite fields and* $n_1, n_2 \geqslant 2$ *positive integers.* $\mathrm{Mat}_{n_1}(\mathbf{K}_1) \equiv_c \mathrm{Mat}_{n_2}(\mathbf{K}_2)$ *if and only if* $n_1 = n_2$ *and* $\mathbf{K}_1 \simeq \mathbf{K}_2$.

Proof. The sufficiency is obvious. For necessity, assume that $\mathrm{Mat}_{n_1}(\mathbf{K}_1) \equiv_c \mathrm{Mat}_{n_2}(\mathbf{K}_2)$. Then $\mathrm{Aut}\,\mathrm{Mat}_{n_1}(\mathbf{K}_1) \simeq \mathrm{Aut}\,\mathrm{Mat}_{n_2}(\mathbf{K}_2)$.

Let first $\mathrm{Aut}\,\mathrm{Mat}_{n_1}(\mathbf{K}_1)$ be non-solvable. Then, by Lemma 5.18, $\mathrm{PSL}(n_1, \mathbf{K}_1) \simeq \mathrm{PSL}(n_2, \mathbf{K}_2)$. The only non-trivial possibilities for that are the exceptional isomorphisms $\mathrm{PSL}(2, \mathbf{F}_7) \simeq \mathrm{PSL}(3, \mathbf{F}_2)$ and $\mathrm{PSL}(2, \mathbf{F}_4) \simeq \mathrm{PSL}(2, \mathbf{F}_5)$ (see [41], Section 1.2) which leaves the possibility that $\mathrm{Mat}_2(\mathbf{F}_7) \equiv_c \mathrm{Mat}_3(\mathbf{F}_2)$ and/or $\mathrm{Mat}_2(\mathbf{F}_4) \equiv_c \mathrm{Mat}_2(\mathbf{F}_5)$. The first of them can be excluded by comparison of the automorphism groups. Elementary calculations (see, for example, [41], Section 3.3.1) give $|\mathrm{GL}_2(\mathbf{F}_7)| = 48{\cdot}42$. Since the center of this group is of size 6 and $|\mathrm{Aut}(\mathbf{F}_7)| = 1$ by Lemma 5.6, the formula (5.1) gives $|\mathrm{Aut}\,\mathrm{Mat}_2(\mathbf{F}_7)| = (48 \cdot 42)/6 = 336$. On the other hand, $|\mathrm{GL}_3(\mathbf{F}_2)| = 7 \cdot 6 \cdot 4 = 168$, the center of this group is trivial and $|\mathrm{Aut}(\mathbf{F}_2)| = 1$, so the formula (5.1) gives $|\mathrm{Aut}\,\mathrm{Mat}_3(\mathbf{F}_2)| = 168$. Hence, $\mathrm{Aut}\,\mathrm{Mat}_2(\mathbf{F}_7) \not\simeq \mathrm{Aut}\,\mathrm{Mat}_3(\mathbf{F}_2)$ and, consequently, $\mathrm{Mat}_2(\mathbf{F}_7) \not\equiv_c \mathrm{Mat}_3(\mathbf{F}_2)$.

Now consider the rings $\mathrm{Mat}_2(\mathbf{F}_4)$ and $\mathrm{Mat}_2(\mathbf{F}_5)$. We shall show that there is an atom $\mathbf{A}$ in the subring lattice of $\mathrm{Mat}_2(\mathbf{F}_4)$ which is not categorically equivalent to any atom of the subring lattice of $\mathrm{Mat}_2(\mathbf{F}_5)$, thus $\mathrm{Mat}_2(\mathbf{F}_4)$ and $\mathrm{Mat}_2(\mathbf{F}_5)$ cannot be categorically equivalent. The ring $\mathbf{A}$ consists of all matrices in $\mathrm{Mat}_2(\mathbf{F}_4)$ having the form $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ with $a, b \in \{0, 1\}$. Clearly, the size of $\mathbf{A}$ is 2^2, it is a ring of Type (4) in Section 5.4, and its only proper subring is the smallest subring of $\mathrm{Mat}_2(\mathbf{F}_4)$. On the other hand, by Lemma 5.19, every atom in the lattice of subrings of $\mathrm{Mat}_2(\mathbf{F}_5)$ has cardinality 5^2. Hence, by Theorem 5.15, none of the latter is categorically equivalent to $\mathbf{A}$.

It remains to consider the case when the group $\mathrm{Aut}\,\mathrm{Mat}_{n_1}(\mathbf{K}_1)$ is solvable. In view of Lemma 5.18, this leaves the possibility that $\mathrm{Mat}_2(\mathbb{Z}_2) \equiv_c \mathrm{Mat}_2(\mathbb{Z}_3)$. However, this is not the case because the automorphism groups of these two rings have different sizes: 6 and 24, respectively. □

Now we are ready to describe categorical equivalences between finite semisimple rings. This result shows that our conjecture that all categorical equivalences between finite rings are consequences of Theorem 5.1 holds for semisimple rings.

Theorem 5.21. *Let* $\mathbf{R}$ *and* $\mathbf{S}$ *be semisimple rings with* p*-components* $\mathbf{R}_1,\dots,\mathbf{R}_n$ *and* $\mathbf{S}_1,\dots,\mathbf{S}_n$*, respectively. Then* $\mathbf{R}$ *and* $\mathbf{S}$ *are categorically equivalent if and only if there is a permutation* $\pi \in S_n$*, such that for every* $i \in \{1,\dots,n\}$*, one of the following two conditions holds:*

a. $\mathbf{R}_i$ *and* $\mathbf{S}_{\pi(i)}$ *are isomorphic, or*

b. $\mathbf{R}_i \simeq \mathbf{F}_{p^{k_1}} \times \cdots \times \mathbf{F}_{p^{k_t}}$ *and* $\mathbf{S}_{\pi(i)} \simeq \mathbf{F}_{q^{k_1}} \times \cdots \times \mathbf{F}_{q^{k_t}}$ *for some primes* p *and* q *and positive integers* $k_1,\dots,k_t$*.*

Proof. First, to prove the "only if" part, let us suppose that $\mathbf{R}$ and $\mathbf{S}$ are categorically equivalent. By Theorem 5.5, there is a permutation $\pi \in S_n$, such that $\mathbf{R}_i \equiv_c \mathbf{S}_{\pi(i)}$ for every i. Assume that $\mathbf{R}_i$ is a p-ring and $\mathbf{S}_i$ is a q-ring; then $\mathbf{R}_i$ is of the form $\mathbf{R}_i \simeq \mathrm{Mat}_{n_1}(\mathbf{F}_{p^{k_1}})\times\cdots\times\mathrm{Mat}_{n_t}(\mathbf{F}_{p^{k_t}})$. If F is a categorical equivalence that maps $\mathbf{R}_i$ to $\mathbf{S}_i$, then we have $\mathbf{S}_i \simeq F(\mathrm{Mat}_{n_1}(\mathbf{F}_{p^{k_1}})) \times \cdots \times F(\mathrm{Mat}_{n_t}(\mathbf{F}_{p^{k_t}}))$. Clearly, these direct factors are simple rings, hence they are also matrix rings over finite fields: $F(\mathrm{Mat}_{n_j}(\mathbf{F}_{p^{k_j}})) \simeq \mathrm{Mat}_{m_j}(\mathbf{F}_{q^{l_j}})$ for $j = 1,\dots,t$. By Theorems 5.7 and 5.20, we have $n_j = m_j$ and $k_j = l_j$ for every j. If $n_j \geq 2$ for some j, then, again by Theorem 5.20, we have also $p = q$, and then $\mathbf{R}_i \simeq \mathbf{S}_{\pi(i)}$ follows, i.e., (a) holds. If $n_1 = \cdots = n_t = 1$, then p and q may be different, and in this case condition (b) is satisfied.

Now, for the "if" part, assume that there is a permutation π as stated in the theorem. According to Theorem 5.5, it suffices to verify that $\mathbf{R}_i \equiv_c \mathbf{S}_{\pi(i)}$ for every i. This is clear if (a) holds, so let us suppose (b), and let us set $k = k_1\cdot\ldots\cdot k_n$. By Theorem 5.1, there is a categorical equivalence functor F between $\mathrm{Var}(\mathbf{F}_{p^k})$ and $\mathrm{Var}(\mathbf{F}_{q^k})$, such that $F(\mathbf{F}_{p^k}) = \mathbf{F}_{q^k}$. Observe that $\mathbf{F}_{p^{k_i}}$ is (isomorphic to) a subfield of $\mathbf{F}_{p^k}$, and Theorem 5.1 shows that $\mathbf{F}_{q^{k_i}}$ is the only subfield of $\mathbf{F}_{q^k}$ that is categorically equivalent to $\mathbf{F}_{p^{k_i}}$. Thus, we must have $F(\mathbf{F}_{p^{k_i}}) \simeq \mathbf{F}_{q^{k_i}}$ for $i = 1,\dots,t$, and this implies

$$F(\mathbf{R}_i) \simeq F(\mathbf{F}_{p^{k_1}} \times \cdots \times \mathbf{F}_{p^{k_t}}) \simeq \mathbf{F}_{q^{k_1}} \times \cdots \times \mathbf{F}_{q^{k_t}} \simeq \mathbf{S}_{\pi(i)}.$$

□

5.6 Polynomial rings

So far we have discussed only finite rings. Now we take also a look at one specific infinite case. The motivation is that since by Theorem 5.1, there is non-trivial categorical equivalence for finite fields, one may ask if this equivalence extends to the polynomial rings over them. It appears though that this is not the case.

Proposition 5.22. *Let* $\mathbf{K}_1$ *and* $\mathbf{K}_2$ *be finite fields. The rings* $\mathbf{K}_1[x]$ *and* $\mathbf{K}_2[x]$ *are categorically equivalent iff* $\mathbf{K}_1 = \mathbf{K}_2$.

Proof. Denote by $\mathrm{Id}(\mathbf{R})$ the lattice of two-sided ideals of the ring $\mathbf{R}$. It is well known that this lattice is isomorphic to $\mathrm{Con}(\mathbf{R})$. Suppose $\mathbf{K}_1[x] \equiv_c \mathbf{K}_2[x]$. From Theorem 2.6 (5) it follows that there exists a lattice isomorphism $\Phi : \mathrm{Id}(\mathbf{K}_1[x]) \to \mathrm{Id}(\mathbf{K}_2[x])$ such that $\mathbf{K}_1[x]/I \equiv_c \mathbf{K}_2[x]/\Phi(I)$ for every $I \in \mathrm{Id}(\mathbf{K}_1[x])$. We observe that any proper ideal I of $\mathbf{K}_1[x]$ has zero intersection with the subring of constant polynomials in $\mathbf{K}_1[x]$. Therefore the quotient ring $\mathbf{K}_1[x]/I$ necessarily contains a subring isomorphic to $\mathbf{K}_1$. In particular, the quotient ring $\mathbf{K}_1[x]/I$ is isomorphic to $\mathbf{K}_1$ if and only if the ideal I is generated by a polynomial of degree 1. (Recall that $\mathbf{K}_1[x]$ is a principal ideal ring; thus every ideal of $\mathbf{K}_1[x]$ is a principal ideal.) It follows that the ideals I of $\mathbf{K}_1[x]$ generated by polynomials of degree 1 are characterized among all proper ideals of $\mathbf{K}_1[x]$ by the property: $\mathbf{K}_1[x]/I$ has the smallest number of subrings. This implies that the lattice isomorphism Φ must map all ideals of $\mathbf{K}_1[x]$ generated by polynomials of degree 1 to the ideals of $\mathbf{K}_2[x]$ generated by polynomials of degree 1. It remains to notice that $\mathbf{K}[x]$ has exactly $|K|$ ideals generated by a polynomial of degree 1. $\square$

Chapter 6

P-categorical equivalence

Adding constants to the set of basic operations of an algebra can give us some interesting non-trivial examples of categorical equivalence. We define two algebras to be p-categorically equivalent if the algebras obtained from them by adding new constant operations for each of their elements are categorically equivalent. It appears that non-direct extensions of finite simple non-abelian groups by a finite abelian group are p-categorically equivalent. In particular, any two symmetric groups $\mathcal{S}_m$ *and* $\mathcal{S}_n$*, where* $m, n > 4$*, are p-categorically equivalent.*

We characterize the p-categorical equivalence of finite strictly locally affine complete algebras and finite strictly locally order affine complete lattices. The latter gives us non-trivial examples of p-categorically equivalent lattices.

6.1 Definition and relation to the categorical equivalence

We denote by $\mathbf{A}^+$ the algebra obtained from an algebra $\mathbf{A}$ by adding to its basic operations all constant operations, one for each element of A. Thus the term operations of $\mathbf{A}^+$ are precisely all polynomial operations of $\mathbf{A}$.

Definition 6.1. We call algebras $\mathbf{A}$ and $\mathbf{B}$ *p-categorically equivalent* if $\mathbf{A}^+$ and $\mathbf{B}^+$ are categorically equivalent. We denote this $\mathbf{A} \equiv_p \mathbf{B}$.

A finite algebra $\mathbf{A}$ is called *functionally complete* if every operation on A is a polynomial operation of $\mathbf{A}$. From Theorem 2.3 we get immediately the following corollary.

Proposition 6.2. *Every two functionally complete algebras are p-categorically equivalent.*

In [7], C. Bergman proved the following result.

Theorem 6.3. *Categorically equivalent algebras are p-categorically equivalent.*

The proof of Bergman was purely categorical. In his paper, Bergman mentioned that this result can be also proved using Theorem 2.7 of R. McKenzie. Here we carry out this proof.

Proof. We use the following three observations.

Observation 1. Let m be a positive integer. Then algebras $(\mathbf{A}^{[m]})^+$ and $(\mathbf{A}^+)^{[m]}$ are term equivalent.

We need to show that every basic operation f of $(\mathbf{A}^{[m]})^+$ is a term operation of $(\mathbf{A}^+)^{[m]}$, and vice versa.

If f is a basic operation of $\mathbf{A}^{[m]}$, then, obviously, it is also a basic operation of $(\mathbf{A}^+)^{[m]}$. Otherwise f is a constant $\overline{a} = (a_1, \dots, a_m) \in A^m$. But every a_i as a constant is a basic operation of $\mathbf{A}^+$, therefore $\overline{a}$ is also a basic operation of $(\mathbf{A}^+)^{[m]}$.

Conversely, assume that $g = (g_1, \dots, g_m)$ is a p-ary basic operation of $(\mathbf{A}^+)^{[m]}$, where every $g_i(x_1, \dots, x_{mp})$ is an mp-ary term operation of $\mathbf{A}^+$, i.e. a superposition of projections, basic operations and constants of $\mathbf{A}$. Replace all constants $a_1, \dots, a_k$ appearing in all g_i-s by variables $y_{11}, \dots, y_{1k}$ to obtain term operations $g'_i(x_1, \dots, x_{mp}, y_{11}, \dots, y_{1k})$ satisfying the condition

$$g'_i(x_1, \dots, x_{mp}, a_1, \dots, a_k) = g_i(x_1, \dots, x_{mp}).$$

For a tuple $\overline{x} = (x_1, \dots, x_m)$, let Pr_i denote the i-th projection map, i.e. $\mathrm{Pr}_i(\overline{x}) = x_i$. Now in every g'_i substitute $y_{1j} = \mathrm{Pr}_1(y_{1j}, \dots, y_{mj})$ for $1 \leqslant j \leqslant k$ to obtain $m(p+k)$-ary term operations $h_i(x_{11}, \dots, x_{mp}, y_{11}, \dots, y_{mk})$ of $\mathbf{A}$. Then $h = (h_1, \dots, h_m)$ is a $(p+k)$-ary basic operation of $\mathbf{A}^{[m]}$.

Now for $1 \leqslant j \leqslant k$ take $(y_{1j}, \dots, y_{mj}) = (a_j, \dots, a_j)$. Notice that $(a_j, \dots, a_j) \in (\mathbf{A}^{[m]})^+$. Then

$$\begin{aligned}&\hat{g}((x_{11}, \dots, x_{m1}), \dots, (x_{1p}, \dots, x_{mp})) := \\ &\quad h((x_{11}, \dots, x_{m1}), \dots, (x_{1p}, \dots, x_{mp}), (a_1, \dots, a_1), \dots, (a_k, \dots, a_k))\end{aligned}$$

is a p-ary term operation of $(\mathbf{A}^{[m]})^+$. Furthermore,

$$\begin{aligned} &h_i(x_{11},\dots,x_{mp},a_1,\dots,a_1,\dots,a_k,\dots,a_k) = \\ &\quad = g_i'(x_1,\dots,x_{mp},Pr_1(a_1,\dots,a_1),\dots,Pr_1(a_k,\dots,a_k)) \\ &\quad = g_i'(x_1,\dots,x_{mp},a_1,\dots,a_k) = g_i(x_1,\dots,x_{mp}), \end{aligned}$$

thus $\hat{g} = g$.

Observation 2. Let s be an invertible idempotent unary term of an algebra $\mathbf{A}$*. Then the algebras* $\mathbf{A}(s)^+$ *and* $\mathbf{A}^+(s)$ *are term equivalent.*

Again, we need to show that every basic operation f of $\mathbf{A}(s)^+$ is a term operation of $\mathbf{A}^+(s)$, and vice versa.

If f is a basic operation of $\mathbf{A}(s)$, then, clearly, it is also a basic operation of $\mathbf{A}^+(s)$. Otherwise it is a constant of algebra $\mathbf{A}(s)^+$, say a. Then there exists $b \in A$ such that $s(b) = a$. But b is a basic operation of $\mathbf{A}^+$, thus $b_s = s(b)$ is a basic operation of $\mathbf{A}^+(s)$.

Conversely, assume that g_s is a basic operation of $\mathbf{A}^+(s)$, where $g(x_1,\dots,x_n)$ is some term operation of $\mathbf{A}^+$. Replace all constants $a_1,\dots,a_k$ appearing in g by variables $y_1,\dots,y_k$ to obtain a term operation $h(x_1,\dots,x_n,y_1,\dots,y_k)$ of $\mathbf{A}$, to which corresponds the basic operation h_s of $\mathbf{A}(s)$ (as well as that of $\mathbf{A}(s)^+$).

Since s is invertible, for some r there are an r-ary term operation w and unary term operations $t_1,\dots,t_r$ on $\mathbf{A}$ such that for every a_j, $1 \leqslant j \leqslant k$,

$$w(st_1(a_j),st_2(a_j),\dots,st_r(a_j)) = a_j.$$

Note that $b_{ij} := st_i(a_j) \in s(A)$, where $1 \leqslant i \leqslant r$, thus b_{ij} are constants of $\mathbf{A}(s)^+$.

Now set $\hat{g}(x_1,\dots,x_n) := h_s(x_1,\dots,x_n,w(b_{11},\dots,b_{r1}),\dots,w(b_{1k},\dots,b_{rk}))$. Then $\hat{g}$ is a term operation of $\mathbf{A}(s)^+$ and

$$\begin{aligned} &\hat{g}(x_1,\dots,x_n) = h_s(x_1,\dots,x_n,w(b_{11},\dots,b_{r1}),\dots,w(b_{1k},\dots,b_{rk})) = \\ &\quad = s(h(x_1,\dots,x_n,a_1,\dots,a_k)) = s(g(x_1,\dots,x_n)) = g_s(x_1,\dots,x_n), \end{aligned}$$

yielding $g_s = \hat{g}$.

Observation 3. If $\mathbf{A} \equiv_t \mathbf{B}$*, then* $\mathbf{A}^+ \equiv_t \mathbf{B}^+$.

If $\mathbf{A}$ and $\mathbf{B}$ are term equivalent, then they are also polynomially equivalent, which means that $\mathbf{A}^+$ and $\mathbf{B}^+$ are term equivalent

Proof of the theorem. Assume that algebras $\mathbf{A}$ and $\mathbf{B}$ are categorically equivalent. Then there exist a positive integer m and a unary invertible idempotent term s such that $\mathbf{B}$ is term equivalent to an algebra isomorphic to $\mathbf{A}^{[m]}(s)$. Without loss of generality we may assume that $\mathbf{B}$ is term equivalent to $\mathbf{A}^{[m]}(s)$.

By Observations 3, 2 and 1 we get

$$\mathbf{B}^+ \equiv_t (\mathbf{A}^{[m]}(s))^+ \equiv_t (\mathbf{A}^{[m]})^+(s) \equiv_t (\mathbf{A}^+)^{[m]}(s).$$

If s is a unary invertible idempotent term of $\mathbf{A}^{[m]}$, then it is also the same for $(\mathbf{A}^+)^{[m]}$. Thus, by McKenzie's theorem $\mathbf{A}^+$ and $\mathbf{B}^+$ are categorically equivalent. $\square$

From Proposition 6.2 we see that the converse of Theorem 6.3 is not true. For example, every two finite unitary simple rings are p-categorically equivalent because they are functionally complete ([33], Theorem 7). But from our Chapter 5 we know that such rings need not be categorically equivalent.

6.2 Abelian groups

For finite abelian groups, the condition for p-categorical equivalence happens to be the same as for the usual categorical equivalence.

Proposition 6.4. *P-categorically equivalent finite abelian groups are isomorphic.*

Proof. Assume that for finite abelian groups $\mathbf{A}$ and $\mathbf{B}$, $\mathbf{A}^+ \equiv_c \mathbf{B}^+$. Then also $(\mathbf{A}^+)^2 \equiv_c (\mathbf{B}^+)^2$. Congruence lattices of categorically equivalent algebras are isomorphic by Theorem 2.6. Since congruences as equivalence relations are reflexive, constants don't affect congruences and thus

$$\operatorname{Con}\mathbf{A}^2 = \operatorname{Con}(\mathbf{A}^+)^2 \simeq \operatorname{Con}(\mathbf{B}^+)^2 = \operatorname{Con}\mathbf{B}^2.$$

For abelian groups, subgroups are in one-to-one correspondence with the congruences, thus the subgroup lattice is isomorphic to the congruence lattice. We obtain $\operatorname{Sub}\mathbf{A}^2 \simeq \operatorname{Sub}\mathbf{B}^2$, which implies $\mathbf{A} \simeq \mathbf{B}$, since for a finite abelian group, the subgroup lattice of the direct square determines the group up to isomorphism ([27]). $\square$

6.3 Simple non-abelian groups and their extensions

Finite simple non-abelian groups are functionally complete ([28]), so Proposition 6.2 yields

Proposition 6.5. *Every two finite simple non-abelian groups are p-categorically equivalent.*

Functional completeness implies that for any tuple $(g_1,\dots,g_k)$ of the elements of a finite simple non-abelian group $\mathbf{H}$ and a tuple $(h_1,\dots,h_k)$ of pairwise distinct elements of $\mathbf{H}$, there is a unary term operation t of $\mathbf{H}^+$ such that $t(h_i) = g_i$ for all $1 \leqslant i \leqslant k$.

The alternating group $\mathcal{A}_n$ is simple non-abelian for $n \geqslant 5$, hence any groups $\mathcal{A}_m$ and $\mathcal{A}_n$ with $m, n \geqslant 5$ are p-categorically equivalent. Note that if $m \neq n$, then $\mathcal{A}_m$ and $\mathcal{A}_n$ are not categorically equivalent, since categorically equivalent finite groups must be weakly isomorphic (Theorem 2.11), hence have the same size.

We consider the extensions of finite simple non-abelian groups by finite abelian groups, which are centerless. We call a group $\mathbf{G}$ an *extension* of a group $\mathbf{H}$ by a group $\mathbf{A}$, if $\mathbf{H}$ is a normal subgroup of $\mathbf{G}$ and $\mathbf{G}/\mathbf{H} \simeq \mathbf{A}$. (Note that in literature, many authors reverse the roles and say that $\mathbf{G}$ is an extension of $\mathbf{A}$.) A group is called *centerless*, if it has one-element center.

We call a subalgebra $\mathbf{S}$ of an algebra $\mathbf{A}^k$ *non-diagonal*, if for every pair of indices $1 \leqslant i < j \leqslant k$ there is an element $x = (x_1,\dots,x_n) \in S$ such that $x_i \neq x_j$.

Lemma 6.6. *Let* $\mathbf{H}$ *be a finite simple non-abelian group,* $\mathbf{G}$ *its centerless extension by a finite abelian group, and k a positive integer. Let* $\mathbf{S}$ *be a non-diagonal subalgebra of* $(\mathbf{G}^+)^k$. *Then* $H^k \subseteq S$.

Proof. Observe that the subalgebras of $(\mathbf{G}^+)^k$ have precisely the same universe as the subgroups of $\mathbf{G}^k$ containing all diagonal elements $(a,\dots,a)$, $a \in G$.

If $k = 1$, the only subalgebra of $(\mathbf{G}^+)^k$ is $\mathbf{G}^+$ itself.

Take $k = 2$ and consider a non-diagonal subalgebra $\mathbf{S}$ of the algebra $(\mathbf{G}^+)^2$. It has an element (a, b) such that $a \neq b$. We claim that there is an element $(x_1, x_2) \in S$ such that $x_1, x_2 \in H$, and $x_1 \neq x_2$. Assume that this is not true.

The element $(a,b)(b^{-1},b^{-1}) = (ab^{-1}, bb^{-1}) = (ab^{-1}, 1)$ belongs to S, and $x_0 := ab^{-1} \neq 1$ since $a \neq b$. Now, for each $x \in G$ consider the element

$$(x_0,1)(x,x),(x_0,1)^{-1}(x^{-1},x^{-1}) = (x_0xx_0^{-1}x^{-1},1).$$

Observe that this element belongs to S, and $x_0xx_0^{-1}x^{-1} \in H$, because G/H is commutative. By our contradictory assumption it follows that $x_0xx_0^{-1}x^{-1} = 1$ for each $x \in G$. The last equality means that x_0 belongs to the center of $\mathbf{G}$. However, by assumption of the theorem, $\mathbf{G}$ is centerless, hence $x_0 = 1$. We obtained a contradiction.

Since the subgroup **H** is functionally complete, the existence of an element $(x_1, x_2) \in S$ such that $x_1, x_2 \in H$, $x_1 \neq x_2$, entails that $H^2 \subseteq S$ by the observation after Proposition 6.5.

Now let $k \geqslant 3$, and let $\mathbf{S} \leqslant (\mathbf{G}^+)^k$ be non-diagonal. It is clear that $H^k \cap S$ is a subuniverse of $(\mathbf{H}^+)^k$. On the other hand, from what we have proved for $k = 2$, we see that for any $1 \leqslant i < j \leqslant k$, the 2-fold projection $(H^k \cap S)_{ij} = H^2$.

Since **H** is functionally complete, $\mathbf{H}^+$ has a majority term. In 1975, Baker and Pixley discovered that for a finite algebra **A** with a majority term, every subalgebra of $\mathbf{A}^k$ (with $k \geqslant 2$) is completely determined by all of its 2-fold projections ([2]). Observe that H^k is a subuniverse of $(\mathbf{H}^+)^k$ and $(H^k)_{ij} = H^2$ for all $1 \leqslant i < j \leqslant k$. Altogether, we conclude $H^k \cap S = H^k$, and thus $H^k \subseteq S$. □

Theorem 6.7. *Let* $\mathbf{H}_1$ *and* $\mathbf{H}_2$ *be finite simple non-abelian groups,* $\mathbf{A}$ *a finite abelian group and* $\mathbf{G}_1$ *and* $\mathbf{G}_2$ *extensions of* $\mathbf{H}_1$ *and* $\mathbf{H}_2$ *by* $\mathbf{A}$*, respectively. If* $\mathbf{G}_1$ *and* $\mathbf{G}_2$ *are centerless, then they are p-categorically equivalent.*

Proof. We apply Theorem 2.9 and show that the relation algebras $\mathcal{R}(\mathbf{G}_1^+)$ and $\mathcal{R}(\mathbf{G}_2^+)$ are isomorphic. The invariant relations of an algebra are the non-empty subuniverses of its finite direct powers, so for a group **G** with the required properties, we examine the subalgebras of $(\mathbf{G}^+)^k$ for any positive integer k. Let **H** be a simple non-abelian normal subgroup of **G** such that $\mathbf{G}/\mathbf{H} \simeq \mathbf{A}$.

By Lemma 6.6, H^k is contained in any non-diagonal subalgebra of $(\mathbf{G}^+)^k$. Since **H** is a normal subgroup of **G**, $\mathbf{H}^k$ is a normal subgroup of $\mathbf{G}^k$. By one of the classical isomorphism theorems, there is a natural bijection between the subgroups of $\mathbf{G}^k$ containing H^k and the subgroups of $\mathbf{G}^k/\mathbf{H}^k \simeq \mathbf{A}^k$. This bijection takes a subgroup $\mathbf{S} \leqslant \mathbf{G}^k$ containing a diagonal element $(a, \ldots, a)$, $a \in G$, to a subgroup $\mathbf{F}_S \leqslant \mathbf{G}^k/\mathbf{H}^k$ containing $(aH, \ldots, aH)$. Altogether we obtain a bijection between the non-diagonal subalgebras of $(\mathbf{G}^+)^k$ and the subalgebras of $(\mathbf{A}^+)^k$, i.e. the subgroups of $\mathbf{A}^k$, which contain all diagonal elements $(a, \ldots, a)$, $a \in A$.

Now we consider all subalgebras of $(\mathbf{G}^+)^k$.

Let $\kappa(\varepsilon)$ denote the number of equivalence classes of an equivalence relation ε on the set $\underline{k} = \{1, \ldots, k\}$. For each equivalence class of ε, we take the smallest number that occurs in this class. We obtain the $\kappa(\varepsilon)$-tuple $A_\varepsilon = (a_1, a_2, \ldots, a_{\kappa(\varepsilon)})$, where we additionally require $a_1 < a_2 < \ldots < a_{\kappa(\varepsilon)}$. Note that $a_1 = 1$. We also define a function f_ε on $\underline{k}$ as follows:

$$f_\varepsilon(i) = j \quad \Leftrightarrow \quad i \; \varepsilon \; a_j.$$

Take any subalgebra $\mathbf{S}$ of $(\mathbf{G}^+)^k$. Let ε_S be the equivalence relation on the set $\{1,\dots,k\}$ defined by

$$(i,j)\in\varepsilon_S \quad\Leftrightarrow\quad x_i = x_j \text{ for all } x=(x_1,\dots,x_k)\in S.$$

Now for the equivalence relation ε_S, take the tuple $A_{\varepsilon_S} = (a_1, a_2, \dots, a_{\kappa(\varepsilon_S)})$, and consider the set

$$c(S) = \{(x_{a_1}, x_{a_2}, \dots, x_{a_{\kappa(\varepsilon_S)}}) \mid (x_1, x_2, \dots, x_k)\in S\}.$$

This is the universe of a non-diagonal subalgebra of the algebra $(\mathbf{G}^+)^{\kappa(\varepsilon_S)}$. As discussed above, there is a subalgebra $\mathbf{F}_S = \mathbf{F}_{c(S)} \leqslant (\mathbf{A}^+)^{\kappa(\varepsilon_S)}$.

So we obtain a mapping

$$\varphi_k : \mathrm{Sub}(\mathbf{G}^+)^k \to \{(\varepsilon,\mathbf{B}) \mid \varepsilon\in \mathrm{Eq}\,\underline{k},\ \mathbf{B}\in\mathrm{Sub}(\mathbf{A}^+)^{\kappa(\varepsilon)}\}$$

defined by $\varphi_k(\mathbf{S}) = (\varepsilon_S, \mathbf{F}_S)$. This is actually a bijective mapping. To see this, we take an equivalence relation ε on $\underline{k}$ and a subalgebra $\mathbf{F}$ of $(\mathbf{A}^+)^{\kappa(\varepsilon)}$, to which uniquely corresponds some non-diagonal subalgebra $\mathbf{S}'$ of $(\mathbf{G}^+)^{\kappa(\varepsilon)}$. We define

$$S = \{(s_1,\dots,s_k) \mid \exists (s'_1,\dots,s'_{\kappa(\varepsilon)})\in S' : s_i = s'_{f_\varepsilon(i)},\ 1\leqslant i\leqslant k\}.$$

Then $\varepsilon = \varepsilon_S$, and $\mathbf{F} = \mathbf{F}_S$ since $S' = c(S)$.

Using this bijective mapping we can define in a natural way a bijection between the subalgebras of $(\mathbf{G}_1^+)^k$ and $(\mathbf{G}_2^+)^k$ for all $k\geqslant 1$. Let

$$\begin{aligned}
\varphi_{1_k} :&\quad \mathrm{Sub}(\mathbf{G}_1^+)^k \to \{(\varepsilon,\mathbf{B}) \mid \varepsilon\in \mathrm{Eq}\,\underline{k},\ \mathbf{B}\in\mathrm{Sub}(\mathbf{A}^+)^{\kappa(\varepsilon)}\},\\
\varphi_{2_k} :&\quad \mathrm{Sub}(\mathbf{G}_2^+)^k \to \{(\varepsilon,\mathbf{B}) \mid \varepsilon\in \mathrm{Eq}\,\underline{k},\ \mathbf{B}\in\mathrm{Sub}(\mathbf{A}^+)^{\kappa(\varepsilon)}\}
\end{aligned}$$

and let $\Phi = \varphi_{2_k}^{-1}\varphi_{1_k} : \mathrm{Sub}(\mathbf{G}_1^+)^k \to \mathrm{Sub}(\mathbf{G}_2^+)^k$. We verify that the bijection Φ induces an isomorphism between the algebras $\mathcal{R}(\mathbf{G}_1^+)$ and $\mathcal{R}(\mathbf{G}_2^+)$.

In the trivial case $k=1$, the only subalgebra of $\mathbf{G}_i^+$ $(i=1,2)$ is $\mathbf{G}_i^+$ itself. Thus there is only one unary invariant relation of $\mathbf{G}_i^+$, which we denote by 1_R. We have $\xi(1_R) = 1_R$, $\tau(1_R) = 1_R$, $\Delta(1_R) = 1_R$, and $1_R\circ\lambda = \lambda\circ 1_R = \lambda$ for any $\lambda\in\mathcal{R}(G_i^+)$, $i=1,2$.

Now consider the general case $k\neq 1$. For a centerless extension $\mathbf{G}$ of a finite simple non-abelian group $\mathbf{H}$ by $\mathbf{A}$, any invariant relation $\theta\in\mathcal{R}(\mathbf{G}^+)$, as a subuniverse of some direct power of $\mathbf{G}^+$, is mapped bijectively to the pair $(\varepsilon_\theta, F_\theta)$, where F_θ is a subuniverse of $(\mathbf{A}^+)^{\kappa(\varepsilon_\theta)}$, as defined above. We describe how the basic operations of $\mathcal{R}(\mathbf{G}^+)$ act on the pair $(\varepsilon_\theta, F_\theta)$. Since this description is valid for both $\mathbf{G}=\mathbf{G}_1$ and $\mathbf{G}=\mathbf{G}_2$, the isomorphism follows immediately.

First, take the operation $\delta^{\{1;2,3\}}$. We have $\varepsilon_{\delta^{\{1;2,3\}}} = \{\{1\},\{2,3\}\}$ and $F_{\delta^{\{1;2,3\}}} = A^2$.

Now let $\theta \in \mathcal{R}(\mathbf{G}^+)$ be k-ary, $k \geqslant 2$.

Take the operation τ. The equivalence relation $\varepsilon_{\tau(\theta)}$ is obtained from ε_θ by exchanging $1 \leftrightarrow 2$. If $(1,2) \in \varepsilon_\theta$, then $F_{\tau(\theta)} = F_\theta$, otherwise

$$F_{\tau(\theta)} = \{(g_2, g_1, g_3, \dots, g_{\kappa(\varepsilon)}) \mid (g_1, g_2, \dots, g_{\kappa(\varepsilon)}) \in F_\theta\}.$$

Take the operation ξ. The equivalence relation $\varepsilon_{\xi(\theta)}$ is obtained from ε_θ by the substitution $2 \to 1, 3 \to 2, \dots, k \to (k-1), 1 \to k$. To describe $F_{\xi(\theta)}$, consider two cases.

Case 1. Number 1 is the only element in its equivalence class in ε_θ. Then

$$F_{\xi(\theta)} = \{(g_2, g_3, \dots, g_{\kappa(\varepsilon)}, g_1) \mid (g_1, g_2, \dots, g_{\kappa(\varepsilon)}) \in F_\theta\}.$$

Case 2. There is $j \neq 1$ such that $(1, j) \in \varepsilon_\theta$. Let $q := f_{\varepsilon_{\xi(\theta)}}(k)$. Then

$$F_{\tau(\theta)} = \{(g_2, g_3, \dots, g_q, g_1, g_{q+1}, \dots, g_{\kappa(\varepsilon)}) \mid (g_1, g_2, \dots, g_{\kappa(\varepsilon)}) \in F_\theta\}.$$

Take the operation Δ. We define

$$\begin{array}{rcl} \varepsilon'_\theta & = & \{(i-1, j-1) \mid (i,j) \in \varepsilon_\theta,\ 2 \leqslant i, j\}, \\ \varepsilon' & = & \{(i-1, j-1) \mid (1,i) \in \varepsilon_\theta \ \&\ (2,j) \in \varepsilon_\theta,\ 2 \leqslant i, j\}, \\ \breve{\varepsilon}' & = & \{(i,j) \mid (j,i) \in \varepsilon'\}. \end{array}$$

The relation $\varepsilon_{\Delta(\theta)}$ is the equivalence relation on the set $\{1, \dots, k-1\}$:

$$\varepsilon_{\Delta(\theta)} = \varepsilon'_\theta \cup \varepsilon' \cup \breve{\varepsilon}',$$

where $\varepsilon' \cup \breve{\varepsilon}'$ stands for joining the equivalence classes of 1 and 2; when $(1,2) \in \varepsilon_\theta$, it is just the subset of ε'_θ.

To describe $F_{\Delta(\theta)}$, consider two cases.

Case 1. $(1,2) \in \varepsilon_\theta$. Then $F_{\Delta(\theta)} = F_\theta$.

Case 2. $(1,2) \notin \varepsilon_\theta$. Then

$$F_{\Delta(\theta)} = \{(g_1, \dots, g_{\kappa(\varepsilon_\theta)-1}) \mid (g_1, g_1, \dots, g_{\kappa(\varepsilon_\theta)-1}) \in F_\theta\}.$$

Finally, let $\theta, \lambda \in \mathcal{R}(\mathbf{G}^+)$, where θ is k-ary and λ is l-ary, $k, l \geqslant 2$, and consider the operation $\circ$. We define

$$\begin{array}{rcl} \varepsilon'_\theta & = & \{(i,j) \mid (i,j) \in \varepsilon_\theta,\ i, j \leqslant k-1\}, \\ \varepsilon'_\lambda & = & \{(i+k-2, j+k-2) \mid (i,j) \in \varepsilon_\lambda,\ 2 \leqslant i, j\}, \\ \varepsilon' & = & \{(i, j+k-2) \mid (i,k) \in \varepsilon_\theta \ \&\ (1,j) \in \varepsilon_\lambda,\ i \leqslant k-1,\ 2 \leqslant j\}, \\ \breve{\varepsilon}' & = & \{(i,j) \mid (j,i) \in \varepsilon'\}. \end{array}$$

The relation $\varepsilon_{\theta\circ\lambda}$ is the equivalence relation on the set $\{1,\dots,k+l-2\}$:

$$\varepsilon_{\theta\circ\lambda} = \varepsilon'_\theta \cup \varepsilon'_\lambda \cup \varepsilon' \cup \breve{\varepsilon}',$$

where $\varepsilon' \cup \breve{\varepsilon}'$ stands for joining the equivalence classes of k in ε_θ and of 1 in ε_λ. For $F_{\theta\circ\lambda}$, there are three cases.
Case 1. Number k is the only element in its equivalence class in ε_θ, and 1 is the only element in its equivalence class in ε_λ. In this case

$$\begin{aligned} F_{\theta\circ\lambda} &= \{(g_1,g_2,\dots,g_{\kappa(\varepsilon)+\kappa(\lambda)-2}) \mid \exists g \in A\ (g_1,\dots,g_{\kappa(\varepsilon)-1},g) \in F_\theta \\ &\quad \&\ (g,g_{\kappa(\varepsilon)},\dots,g_{\kappa(\varepsilon)+\kappa(\lambda)-2}) \in F_\lambda\}. \end{aligned}$$

Case 2. Number k is the only element in its equivalence class in ε_θ, and there is $j \neq 1$ such that $(1,j) \in \varepsilon_\lambda$. Let $q := f_{\varepsilon_{\theta\circ\lambda}}(j+k-2)$, i.e. q is the position of the equivalence class of 1 from ε_λ in the combined equivalence relation. We get

$$\begin{aligned} F_{\theta\circ\lambda} &= \{(g_1,g_2,\dots,g_{\kappa(\varepsilon)+\kappa(\lambda)-1}) \mid (g_1,g_2,\dots,g_{\kappa(\varepsilon)-1},g_q) \in F_\theta \\ &\quad \&\ (g_q,g_{\kappa(\varepsilon)},\dots,g_{q-1},g_{q+1},\dots,g_{\kappa(\varepsilon)+\kappa(\lambda)-1}) \in F_\lambda\}. \end{aligned}$$

Case 3. Number k is not the only element in its equivalence class in ε_θ. Let $q := f_{\varepsilon_\theta}(k)$. We get

$$\begin{aligned} F_{\theta\circ\lambda} &= \{(g_1,g_2,\dots,g_{\kappa(\varepsilon)+\kappa(\lambda)-1}) \mid (g_1,g_2,\dots,g_{\kappa(\varepsilon)}) \in F_\theta \\ &\quad \&\ (g_q,g_{\kappa(\varepsilon)+1},\dots,g_{\kappa(\varepsilon)+\kappa(\lambda)-1}) \in F_\lambda\}. \end{aligned}$$

□

The following simple proposition can be found in any group theory textbook, e.g. [38].

Proposition 6.8. *Let* $\mathbf{G}$ *be a group,* $\mathbf{H}_1$ *and* $\mathbf{H}_2$ *its normal subgroups,* $G = H_1H_2$ *and* $H_1 \cap H_2 = \{1\}$*. Then* $\mathbf{G} \simeq \mathbf{H}_1 \times \mathbf{H}_2$*.*

We call an extension $\mathbf{G}$ of $\mathbf{H}$ by $\mathbf{A}$ *direct*, if $\mathbf{G} \simeq \mathbf{H} \times \mathbf{A}$.

Lemma 6.9. *Let* $\mathbf{H}$ *be a simple non-abelian group and* $\mathbf{A}$ *a simple abelian group (i.e. a cyclic group of prime order). Then any non-direct extension of* $\mathbf{H}$ *by* $\mathbf{A}$ *is centerless.*

Proof. Let $\mathbf{G}$ be a non-direct extension of $\mathbf{H}$ by $\mathbf{A}$. The center $\mathbb{Z}(\mathbf{G})$ is a normal subgroup of $\mathbf{G}$. Therefore $\mathbf{H} \cap \mathbb{Z}(\mathbf{G})$ and $\mathbf{H} \cdot \mathbb{Z}(\mathbf{G})$ are normal subgroups of $\mathbf{G}$, too. Since $\mathbf{H}$ is a minimal normal subgroup of $\mathbf{G}$ and it is abelian, we have $H \cap Z(\mathbf{G}) = \{1\}$. Now, if $Z(\mathbf{G}) \neq \{1\}$ then $Z(\mathbf{G}) \not\subseteq H$ and simplicity of $\mathbf{G}/\mathbf{H}$ implies $H \cdot Z(\mathbf{G}) = \mathbf{G}$. Thus, by Proposition 6.8, we have $\mathbf{G} \simeq \mathbb{Z}(\mathbf{G}) \times \mathbf{H}$ and $\mathbb{Z}(\mathbf{G}) \simeq \mathbf{G}/H \simeq \mathbf{A}$. □

Theorem 6.7 and Lemma 6.9 imply the following corollary.

Corollary 6.10. *Let* $\mathbf{H}_1$ *and* $\mathbf{H}_2$ *be finite simple non-abelian groups and* $\mathbf{A}$ *a finite simple abelian group. Then non-direct extensions of* $\mathbf{H}_1$ *and* $\mathbf{H}_2$ *by* $\mathbf{A}$ *are p-categorically equivalent.*

Corollary 6.11. *Symmetric groups* $\mathcal{S}_m$ *and* $\mathcal{S}_n$*, where* $m, n \geqslant 5$*, are p-categorically equivalent.*

Proof. For $n \geqslant 5$, the symmetric group $\mathcal{S}_n$ is an extension of the alternating group $\mathcal{A}_n$ by $\mathbb{Z}_2$, but $\mathcal{S}_n \not\simeq \mathcal{A}_n \times \mathbb{Z}_2$. □

Remark 6.12. It is easy to see that a non-direct extension $\mathbf{G}$ of a finite simple non-abelian group $\mathbf{H}$ by a finite simple abelian group $\mathbf{A}$ cannot be p-categorically equivalent to the direct extension of $\mathbf{H}$ by $\mathbf{A}$. The direct product $\mathbf{H} \times \mathbf{A}$ has two non-trivial normal subgroups, isomorphic to $\mathbf{H}$ and $\mathbf{A}$, while the only non-trivial normal subgroup of $\mathbf{G}$ is $\mathbf{H}$. If there were any other non-trivial normal subgroup, say $\mathbf{H}'$, then $H \cap H' = \{1\}$ and $G = HH'$, because $\mathbf{H}$ and $\mathbf{A}$ are simple. Proposition 6.8 would imply $\mathbf{G} \simeq \mathbf{H} \times \mathbf{H}'$ yielding $\mathbf{H}' \simeq \mathbf{G}/\mathbf{H} \simeq \mathbf{A}$.

6.4 Arithmetical varieties

An algebra is called *arithmetical* if it is congruence distributive and congruence permutable. A variety is *arithmetical* if each of its members is arithmetical. An algebra $\mathbf{A}$ is called *congruence primal* if every congruence compatible operation on A is a term operation of $\mathbf{A}$, and *affine complete* if every congruence compatible operation on A is a polynomial operation of $\mathbf{A}$. Again, a variety is *affine complete* if each of its members is affine complete.

For example, a variety of rings is arithmetical iff it is generated by a finite number of finite fields ([22], p. 33). An important example of an affine complete variety is the variety of Boolean algebras ([22], p. 157). This variety is also arithmetical ([22], p. 33).

Theorem 6.13 ([5, Cor. 4.5],[7, Cor. 2.4])**.** *Let* $\mathbf{A}$ *be a finite arithmetical congruence primal algebra and* $\mathbf{B}$ *any algebra. Then* $\mathbf{A} \equiv_c \mathbf{B}$ *if and only if* $\mathbf{B}$ *is finite arithmetical congruence primal and* $\operatorname{Con}\mathbf{A} \simeq \operatorname{Con}\mathbf{B}$.

An algebra $\mathbf{A}$ is called *strictly locally affine complete* if any congruence compatible finite partial function on A is a restriction of a polynomial function of $\mathbf{A}$. A variety, all of whose members have this property, is called by the same name.

We need the following important facts about strictly locally affine complete algebras and varieties (see [22], Section 3.4.3).

Theorem 6.14. *A finite algebra is strictly locally affine complete if and only if it is arithmetical and affine complete. A variety is strictly locally affine complete if and only if it is arithmetical.*

Observe that an algebra $\mathbf{A}$ is affine complete iff $\mathbf{A}^+$ is congruence primal, and that $\mathbf{A}$ is arithmetical iff so is $\mathbf{A}^+$.

Now we apply Theorem 6.13 to get the following result.

Theorem 6.15. *Let* $\mathbf{A}$ *be a finite strictly locally affine complete algebra and* $\mathbf{B}$ *any algebra. Then* $\mathbf{A} \equiv_p \mathbf{B}$ *if and only if* $\mathbf{B}$ *is finite strictly locally affine complete and* $\operatorname{Con}\mathbf{A} \simeq \operatorname{Con}\mathbf{B}$.

Proof. Assume first that $\mathbf{A} \equiv_p \mathbf{B}$, hence $\mathbf{A}^+ \equiv_c \mathbf{B}^+$. By Theorem 6.14, the algebra $\mathbf{A}$ is affine complete, implying that $\mathbf{A}^+$ is congruence primal. Now, Theorem 6.13 implies that the algebra $\mathbf{B}^+$ is finite, arithmetical and congruence primal, and $\operatorname{Con}\mathbf{A} \simeq \operatorname{Con}\mathbf{B}$. Applying again Theorem 6.14, we conclude that $\mathbf{B}$ is strictly locally affine complete.

For the converse, assume that a finite algebra $\mathbf{B}$ is strictly locally affine complete and $\operatorname{Con}\mathbf{A} \simeq \operatorname{Con}\mathbf{B}$. Then by Theorem 6.14, the algebras $\mathbf{A}$ and $\mathbf{B}$ are affine complete and arithmetical. Hence, $\mathbf{A}^+$ and $\mathbf{B}^+$ are congruence primal and Theorem 6.13 applies to conclude that $\mathbf{A} \equiv_p \mathbf{B}$ □

Corollary 6.16. *Let* $\mathbf{A}$ *and* $\mathbf{B}$ *be finite algebras generating arithmetical varieties. Then* $\mathbf{A} \equiv_p \mathbf{B}$ *if and only if* $\operatorname{Con}\mathbf{A} \simeq \operatorname{Con}\mathbf{B}$.

6.5 Sublattices of the direct square

Next we are going to consider p-categorical equivalence of lattices. Before that we make one general observation about sublattices of the direct square of a lattice, that will be useful later.

A *tolerance* of an algebra $\mathbf{A}$ is a binary relation on A that is reflexive, symmetric and compatible with all basic operations.

For a lattice $\mathbf{L}$, a tolerance is a subuniverse of $\mathbf{L}^2$ which is reflexive and symmetric as a binary relation. The set $\operatorname{Tol}\mathbf{L}$ of all tolerances of a lattice $\mathbf{L}$ is a lattice under set theoretic inclusion.

The following notion and its basic properties are taken from [21].

By *an adjunction* between two (partially) ordered sets $\mathbf{A} = (A, \leqslant)$ and $\mathbf{B} = (B, \leqslant)$ we call a Galois connection between these two sets, i.e. a pair of mappings $\varphi : A \to B$, $\psi : B \to A$, such that

$$a \leqslant \psi(b) \iff \varphi(a) \leqslant b \tag{6.1}$$

for all $a \in A$, $b \in B$.

An adjunction between $(A, \leqslant)$ and $(A, \leqslant)$ is called a *self-adjunction* of $(A, \leqslant)$.

If (φ, ψ) is an adjunction between complete lattices $\mathbf{K}$ and $\mathbf{M}$, then φ preserves all (also infinite) joins and ψ preserves all meets. It follows that φ and ψ are order preserving.

Moreover, given any join preserving mapping $\varphi : \mathbf{K} \to \mathbf{M}$ (meet preserving mapping $\psi : \mathbf{M} \to \mathbf{K}$), there exists a unique mapping $\psi : \mathbf{M} \to \mathbf{K}$ ($\varphi : \mathbf{K} \to \mathbf{M}$) such that the pair (φ, ψ) is an adjunction between $\mathbf{K}$ and $\mathbf{M}$.

Theorem 6.17 ([21])**.** *Let* $\mathbf{L}$ *be a subdirect product of two finite lattices* $\mathbf{K}$ *and* $\mathbf{M}$*. Then there exist join preserving mappings* $\varphi : \mathbf{K} \to \mathbf{M}$*,* $\alpha : \mathbf{M} \to \mathbf{K}$ *and meet preserving mappings* $\psi : \mathbf{M} \to \mathbf{K}$*,* $\beta : \mathbf{K} \to \mathbf{M}$ *such that*

$$\{(x, y) \mid \varphi(x) \leqslant y \leqslant \beta(x)\} = L = \{(x, y) \mid \alpha(y) \leqslant x \leqslant \psi(y)\}, \tag{6.2}$$

where (φ, ψ) *and* (α, β) *are adjunctions.*

For a lattice $\mathbf{K}$, we call a sublattice of $\mathbf{K}^2$ *diagonal*, if it is reflexive as a binary relation on K. We call a function $f : \mathbf{K} \to \mathbf{K}$ decreasing if $f(x) \leqslant x$ for every $x \in K$. If in Theorem 6.17 we take $\mathbf{K} = \mathbf{M}$ and assume that $\mathbf{L}$ is diagonal, we immediately obtain that α and φ must be decreasing.

Furthermore, keeping in mind that (φ, ψ) and (α, β) are adjunctions, we obtain the following result for the diagonal sublattices of a finite lattice.

Theorem 6.18. *Let* $\mathbf{K}$ *be a finite lattice and* $\mathbf{L}$ *be a diagonal sublattice of* $\mathbf{K}^2$*. Then there exist join preserving decreasing mappings* $\varphi, \alpha : \mathbf{K} \to \mathbf{K}$*, such that*

$$L = \{(x, y) \mid \varphi(x) \leqslant y,\ \alpha(y) \leqslant x\}. \tag{6.3}$$

We denote the set of all join preserving decreasing mappings on K by $\operatorname{Fun}\mathbf{K}$. Clearly, the set $\operatorname{Fun}\mathbf{K}$ is a lattice with respect to pointwise order.

Theorem 6.19 ([21])**.** *The tolerances of a finite lattice* $\mathbf{K}$ *are precisely the sublattices of* $\mathbf{K} \times \mathbf{K}$ *of the form*

$$T = \{(x, y) \mid \varphi(x) \leqslant y \leqslant \psi(x)\} = \{(x, y) \mid \varphi(x) \leqslant y,\ \varphi(y) \leqslant x\}. \tag{6.4}$$

where (φ, ψ) *is a self-adjunction of* $\mathbf{K}$ *with the function* φ *decreasing.*

We will observe in the next lemma that this correspondence between tolerances and join preserving decreasing mappings is an anti-isomorphism of lattices.

By $S_{2d}(\mathbf{K})$ we denote the lattice of all diagonal sublattices of $\mathbf{K}^2$ with respect to inclusion.

Lemma 6.20. *For any finite lattice* $\mathbf{K}$, $S_{2d}(\mathbf{K}) \simeq_d (\mathrm{Fun}\,\mathbf{K})^2$ *and* $\mathrm{Tol}\,\mathbf{K} \simeq_d \mathrm{Fun}\,\mathbf{K}$.

Proof. For both statements we show that there is an order reversing bijection between corresponding lattices.

In the first case, we define, for any $(\varphi, \alpha) \in (\mathrm{Fun}\,\mathbf{K})^2$, a diagonal sublattice of $\mathbf{K}^2$ by

$$L_{(\varphi,\alpha)} = \{(x, y) \mid \varphi(x) \leqslant y,\ \alpha(y) \leqslant x\}. \tag{6.5}$$

Since φ and α are join preserving, it is straightforward to verify that this is a sublattice of $\mathbf{K}^2$. Since φ and α are decreasing, it is diagonal.

By Theorem 6.18, this correspondence is surjective. We verify that it is order reversing, this will also imply injectivity.

Let $\varphi_1, \alpha_1, \varphi_2, \alpha_2 \in \mathrm{Fun}\,\mathbf{K}$ and

$$L_1 = L_{(\varphi_1,\alpha_1)}, \qquad L_2 = L_{(\varphi_2,\alpha_2)}$$

Then

$$L_1 \subseteq L_2 \iff \big(\varphi_1(x) \leqslant y,\ \alpha_1(y) \leqslant x \Rightarrow \varphi_2(x) \leqslant y,\ \alpha_2(y) \leqslant x\big). \tag{6.6}$$

Since φ_1 and α_1 are decreasing, $(x, \varphi_1(x)) \in L_1$, as well as $(\alpha_1(x), x) \in L_1$, for any $x \in K$. Hence $L_1 \subseteq L_2$ implies that $\varphi_2(x) \leqslant \varphi_1(x))$ and $\alpha_2(x) \leqslant \alpha_1(x))$ for any $x \in K$. On the other hand, if $\varphi_2 \leqslant \varphi_1$ and $\alpha_2 \leqslant \alpha_1$, then the right hand side of (6.6) is fulfilled, hence $L_1 \subseteq L_2$.

Finally, if $L_{(\varphi_1,\alpha_1)} = L_{(\varphi_2,\alpha_2)}$, then $(\varphi_1, \alpha_1) \leqslant (\varphi_2, \alpha_2)$ and $(\varphi_2, \alpha_2) \leqslant (\varphi_1, \alpha_1)$ hold simultaneously, hence $(\varphi_1, \alpha_1) = (\varphi_2, \alpha_2)$.

For the second anti-isomorphism, for any $\varphi \in \mathrm{Fun}\,\mathbf{K}$, we define a tolerance of $\mathbf{K}$ by

$$T_\varphi = \{(x, y) \mid \varphi(x) \leqslant y,\ \varphi(y) \leqslant x\}. \tag{6.7}$$

By this definition, T_φ is actually a diagonal sublattice of $\mathbf{K}^2$ defined by (φ, φ), that is, $T_\varphi = L_{(\varphi,\varphi)}$. It is clear from definition that T_φ is also symmetric.

By Theorem 6.19, this correspondence is surjective. We show that it is also order reversing and injective.

Let $\varphi_1, \varphi_2 \in \operatorname{Fun}\mathbf{K}$ and

$$T_1 = L_{(\varphi_1,\varphi_1)}, \qquad T_2 = L_{(\varphi_2,\varphi_2)}.$$

Then

$$T_1 \subseteq T_2 \iff (\varphi_1,\varphi_1) \geqslant (\varphi_2,\varphi_2) \iff \varphi_1 \geqslant \varphi_2,$$

and if $T_{\varphi_1} = T_{\varphi_2}$, then $\varphi_1 \geqslant \varphi_2$ and $\varphi_1 \leqslant \varphi_2$ hold simultaneously, hence $\varphi_1 = \varphi_2$. □

The following theorem is a direct corollary of Lemma 6.20.

Theorem 6.21. *For any finite lattice* $\mathbf{K}$*,* $S_{2d}(\mathbf{K}) \simeq (\operatorname{Tol}\mathbf{K})^2$.

Remark 6.22. Theorem 6.17 and Theorem 6.19 were actually proved in [21] for complete lattices and complete tolerances of a complete lattice. The results we obtained in this section, Theorem 6.18, Lemma 6.20 and Theorem 6.21, hold also for complete diagonal sublattices and complete tolerances of a complete lattice. However, for finite lattices these results have a stronger form, and in the following section we will use them just for finite lattices.

6.6 Strictly locally order affine complete lattices

In Chapter 3, we showed that two lattices are categorically equivalent if and only if they are isomorphic or dually isomorphic. For p-categorical equivalence of lattices, we will obtain a result similar to Theorem 6.15, which will give us a series of non-trivial examples.

Actually, there are no strictly locally affine complete lattices, so we cannot apply Theorem 6.15 directly. But we can modify the requirements for the compatible functions.

We call a lattice $\mathbf{L}$ *strictly locally order affine complete* if, for any m and every finite subuniverse X of $(L^m; \wedge)$, every congruence compatible order preserving function from X to L is a restriction of a polynomial function of $\mathbf{L}$. This notion was first introduced and investigated in [23]. For example, all relatively complemented lattices are strictly locally order affine complete (by [23], this containment is strict).

Proposition 6.23. *Let* $\mathbf{L}$ *be a strictly locally order affine complete lattice. Then:*

(1) $\mathbf{L}$ *is congruence permutable ([22], Theorem 5.3.32)*

(2) *every tolerance of* $\mathbf{L}$ *is a congruence ([22], Theorem 5.3.30).*

Corollary 6.24. *Let T_1 and T_2 be tolerances of a strictly locally order affine complete lattice* $\mathbf{L}$. *Then* $T_1 \circ T_2 = T_1 \vee T_2$ *(join in the lattice* $\operatorname{Tol}\mathbf{L}$*).*

In [22], Section 5.3.3, the following two binary relations on a lattice are defined. Let S and T be two tolerances of a lattice $\mathbf{K}$:

$$S_{\leqslant} = \{(a,b) \in S \mid a \leqslant b\};$$

$$S * T = \{(a,c) \in K^2 \mid (a \vee c, a \wedge c) \in S \circ T\}.$$

Binary relation $S * T$ is a tolerance of $\mathbf{K}$ itself.

Lemma 6.25 ([22, Lemma 5.3.17])**.** *If S and T are tolerances of a lattice, then they are equal iff $S_{\leqslant} = T_{\leqslant}$.*

Lemma 6.26 ([22, p. 268])**.** *If S and T are tolerances of a lattice, then* $(S * T)_{\leqslant} = (S \circ T)_{\leqslant}$.

Lemma 6.27. *In a strictly locally order affine complete lattice, $S * T = S \circ T$ for any tolerances S and T.*

Proof. Let S and T be tolerances of a strictly locally order affine complete lattice $\mathbf{L}$. Then $S * T$ is a tolerance of $\mathbf{L}$ and by Proposition 6.23, $S \circ T$ is a tolerance of $\mathbf{L}$, too. Now, the equality $S * T = S \circ T$ follows from the two previous lemmas. □

Let $\mathbf{K}$ be any lattice. By φ_T we denote the join preserving decreasing function on K corresponding to a tolerance T in the anti-isomorphism (6.7). From (6.7) it is easy to note that

$$\varphi_T(x) = \bigwedge\{y \in K \mid (x,y) \in T\}.$$

Lemma 6.28 ([22, Lemma 5.3.26])**.** *Let* $\mathbf{K}$ *be a lattice of finite height and S, T be tolerances of* $\mathbf{K}$. *Then* $\varphi_{S*T} = \varphi_T \varphi_S$.

Lemma 6.29. *Let* $\mathbf{K}$ *be a strictly locally order affine complete lattice of finite height. Then* $\varphi_1\varphi_2 = \varphi_1 \wedge \varphi_2$ *for any* $\varphi_1, \varphi_2 \in \operatorname{Fun}\mathbf{K}$.

Proof. Let $\varphi_1 = \varphi_{T_1}$ and $\varphi_2 = \varphi_{T_2}$. Then by Lemma 6.28, Lemma 6.27, Corollary 6.24, and Lemma 6.20,

$$\varphi_1\varphi_2 = \varphi_{T_1}\varphi_{T_2} = \varphi_{T_2 * T_1} = \varphi_{T_2 \circ T_1} = \varphi_{T_1 \vee T_2} = \varphi_{T_1} \wedge \varphi_{T_2} = \varphi_1 \wedge \varphi_2.$$

□

Now we prove the main result of this section.

Theorem 6.30. *Let* $\mathbf{K}_1$ *be a finite strictly locally order affine complete lattice and* $\mathbf{K}_2$ *any lattice. Then* $\mathbf{K}_1 \equiv_p \mathbf{K}_2$ *iff* $\mathbf{K}_2$ *is finite strictly locally order affine complete and* $\operatorname{Con}\mathbf{K}_1 \simeq \operatorname{Con}\mathbf{K}_2$.

Proof. Let $\mathbf{K}_1 \equiv_p \mathbf{K}_2$. Then, by Theorem 2.6, $\mathbf{K}_2$ is finite and $\operatorname{Con}\mathbf{K}_1 \simeq \operatorname{Con}\mathbf{K}_2$. Also $\operatorname{Tol}\mathbf{K}_1 \simeq \operatorname{Tol}\mathbf{K}_2$. The last isomorphism follows in general case from the proof of the Proposition 3.1 in [11], but in our finite case it is also a direct corollary from Theorem 2.10 and Theorem 6.21. By Proposition 6.23, for strictly locally order affine complete lattices every tolerance is a congruence. Hence $\mathbf{K}_2$ is also strictly locally order affine complete.

Now assume that $\mathbf{K}_1$ and $\mathbf{K}_2$ are finite strictly locally order affine complete lattices and there is a lattice isomorphism $\Phi : \operatorname{Con}\mathbf{K}_1 \to \operatorname{Con}\mathbf{K}_2$. Since lattices are majority algebras, we apply Theorem 2.10 and show that $\mathcal{S}(\mathbf{K}_1^+)$ and $\mathcal{S}(\mathbf{K}_2^+)$ are isomorphic. Note that for any lattice $\mathbf{K}$, $\operatorname{Sub}(\mathbf{K}_1^+)^2 = S_{2d}(\mathbf{K}_1) \cup \{\varnothing\}$. We will actually show that

$$(\operatorname{Sub}(\mathbf{K}_1^+)^2; \cap, \circ, ^{\smile}, \triangle, \nabla) \simeq (\operatorname{Sub}(\mathbf{K}_2^+)^2; \cap, \circ, ^{\smile}, \triangle, \nabla),$$

the isomorphism $\mathcal{S}(\mathbf{K}_1^+) \simeq \mathcal{S}(\mathbf{K}_2^+)$ follows immediately from this.

We define a bijection between $\operatorname{Sub}(\mathbf{K}_1^+)^2$ and $\operatorname{Sub}(\mathbf{K}_2^+)^2$ via the isomorphisms of lattices

$$\begin{aligned} S_{2d}(\mathbf{K}_1) &\simeq_d (\operatorname{Fun}\mathbf{K}_1)^2 \simeq_d (\operatorname{Tol}\mathbf{K}_1)^2 = (\operatorname{Con}\mathbf{K}_1)^2 \simeq \\ &\simeq (\operatorname{Con}\mathbf{K}_2)^2 = (\operatorname{Tol}\mathbf{K}_2)^2 \simeq_d (\operatorname{Fun}\mathbf{K}_2)^2 \simeq_d S_{2d}(\mathbf{K}_2), \end{aligned} \tag{6.8}$$

and the empty subuniverse is mapped to the empty subuniverse.

Compatibility with $\triangle, \nabla$ and $\cap$ is trivial. Compatibility with $\circ$ is trivial, too, if we show that $\circ$ actually coincides with the lattice operation $\vee$ in $S_2(\mathbf{K}_i^+)$, $i = 1, 2$. Let $L_1, L_2 \in S_2(\mathbf{K}_1^+)$ and let $L_i = L_{(\varphi_i, \alpha_i)}$, $i = 1, 2$.

Since L_1 and L_2 are diagonal, $L_2 \subseteq L_1 \circ L_2$ and $L_1 \subseteq L_1 \circ L_2$. Hence $L_1 \vee L_2 \subseteq L_1 \circ L_2$. On the other hand, by Lemmas 6.29 and 6.20,

$$\begin{aligned} L_1 \circ L_2 &= \{(x,y) \mid \exists z \in K : (x,z) \in L_1,\ (z,y) \in L_2\} \\ &= \{(x,y) \mid \exists z \in K : \varphi_1(x) \leqslant z,\ \varphi_2(z) \leqslant y,\ \alpha_1(z) \leqslant x,\ \alpha_2(y) \leqslant z\} \\ &\subseteq \{(x,y) \mid \varphi_2\varphi_1(x) \leqslant y,\ \alpha_1\alpha_2(y) \leqslant x\} \\ &= \{(x,y) \mid (\varphi_1 \wedge \varphi_2)(x) \leqslant y,\ (\alpha_1 \wedge \alpha_2)(y) \leqslant x\} \\ &= L_{(\varphi_1 \wedge \varphi_2, \alpha_1 \wedge \alpha_2)} = L_{(\varphi_1,\alpha_1) \wedge (\varphi_2,\alpha_2)} \\ &= L_{(\varphi_1,\alpha_1)} \vee L_{(\varphi_2,\alpha_2)} = L_1 \vee L_2. \end{aligned}$$

It remains to prove compatibility with $^{\smile}$. This actually follows from two observations. First, if the composite mapping (6.8) maps $L_{(\varphi_1,\alpha_1)} \in S_2(\mathbf{K}_1^+)$ to $L_{(\varphi_2,\alpha_2)} \in S_2(\mathbf{K}_2^+)$ then $(\Phi(T_{\varphi_1}), \phi(T_{\alpha_1})) = (T_{\varphi_2}, T_{\alpha_2})$. Second, if $L = L_{(\varphi_1,\alpha_1)} \in S_2(\mathbf{K}_1^+)$ then $L^{\smile} = L_{(\alpha_1,\varphi_1)}$. □

Now we draw some corollaries from Theorem 6.30.

In [23] it is shown that a finite modular lattice is strictly locally order affine complete iff it is relatively complemented. It is well known that a bounded modular lattice is relatively complemented iff it is complemented (see, for instance, [17], Lemma 99). Hence, in particular, every Boolean lattice is strictly locally order affine complete. On the other hand, the congruence lattice of a finite modular lattice is Boolean ([17], Theorem 357). We obtain the following result.

Corollary 6.31. *A finite modular lattice is p-categorically equivalent to some Boolean lattice iff it is complemented.*

Furthermore, if a finite lattice $\mathbf{B}$ is Boolean, then $\mathbf{B} \simeq \operatorname{Con}\mathbf{B}$. This implies an interesting observation.

Corollary 6.32. *For every finite complemented modular lattice* $\mathbf{L}$*, the lattices* $\mathbf{L}$ *and* $\operatorname{Con}\mathbf{L}$ *are p-categorically equivalent.*

A lattice $\mathbf{L}$ is called *order functionally complete*, if all order preserving functions on $\mathbf{L}$ are polynomial functions. A finite lattice $\mathbf{L}$ is order functionally complete iff L^2 and $\triangle_L$ are the only tolerances of $\mathbf{L}$ ([22], Theorem 5.3.40). Hence, finite order functionally complete lattices are strictly locally order affine complete. Since two-element chain is order functionally complete, we get the following corollary.

Corollary 6.33. *A lattice is p-categorically equivalent to the 2-element chain iff it is finite and order functionally complete.*

One example of p-categorically equivalent lattices is shown in Figure 6.1.

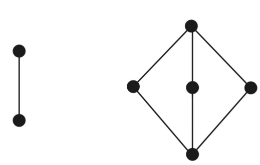

Figure 6.1: The lattices $\mathbf{C}_2$ and $\mathbf{M}_3$ are p-categorically equivalent.

Bibliography

[1] M. Auslander, D. A. Buchsbaum, *Groups, Rings, Modules*, Harper & Row Publishers, New York, 1974.

[2] K. Baker, A. Pixley, *Polynomial interpolation and the Chinese remainder theorem for algebraic systems*, Math. Z. (1975), 165–174.

[3] K. Baumgartner, *Bemerkungen zum Isomorphieproblem der Ringe*, Monatsh. Math. **70** (1966), 299–308.

[4] M. Behrisch, *Relational structure theory*, PhD thesis, TU Dresden, 2013.

[5] C. Bergman, J. Berman, *Morita equivalence of almost-primal clones*, J. Pure and Applied Algebra **108** (1996), 175–201.

[6] C. Bergman, J. Berman, *Algorithms for categorical equivalence*, Math. Struct. in Comp. Science **8** (1998), 1–15.

[7] C. Bergman, *Categorical equivalence of algebras with a majority term*, Algebra Univers. **40** (1998), 149–175.

[8] S. Burris, H. P. Sankappanavar, *A course in universal algebra*, Graduate Texts in Mathematics, 78, Springer-Verlag, 1981.

[9] A. H. Clifford, *Semigroups admitting relative inverses*, Ann. of Math. (2) **42** (1941), 1037–1049.

[10] A. H. Clifford, G. B. Preston, *The algebraic theory of semigroups*, Vol. I, American Mathematical Society, 1961.

[11] B. A. Davey and H. Werner, *Dualities and equivalences for varieties of algebras*, Contributions to lattice theory, Colloq. Math. Soc. János Bolyai, 33, North-Holland, Amsterdam, 1983, 101–275.

[12] K. Denecke, O. Lüders, *Categorical equivalence of varieties and invariant relations*, Algebra Univers. **46** (2001), 105–118.

[13] K. Denecke, S. L. Wismath, *Universal Algebra and Applications in Theoretical Computer Science*, Chapman & Hall/CRC, 2002.

[14] B. Fine, *Classification of finite rings of order p^2*, Math. Mag. **66** (1993), 248–252.

[15] A. L. Foster, *The identities of – and unique factorization within – classes of universal algebras*, Math. Z. **62** (1955), 171–188.

[16] J. A. Green, *On the structure of semigroups*, Annals of Math. **54** (1951), 163–172.

[17] G. Grätzer, *Lattice Theory: Foundation*, Birkhäuser, 2011.

[18] T.-K. Hu, *Stone duality for primal algebra theory*, Math. Z. **110** (1969), 180–198.

[19] T.-K. Hu, Ph. Kelenson, *Independence and direct factorization of universal algebras*, Math. Nachr. **51** (1971), 83–99.

[20] S. Izawa, *Composition of matrix products and categorical equivalence*, Algebra Univers. **69** (2013), 327–356.

[21] K. Kaarli, V. Kuchmei, S. E. Schmidt, *Sublattices of the direct product*, Algebra Univers. **59** (2008), 85–95.

[22] K. Kaarli, A. F. Pixley, *Polynomial Completeness of Algebraic Systems*, Chapman & Hall/CRC, 2001.

[23] K. Kaarli, K. Täht, *Strictly locally order affine complete lattices*, Order **10** (1993), 261–270.

[24] K. A. Kearnes, Á. Szendrei, *Groups with identical subgroup lattices in all powers*, J. Group Theory **7** (2004), 385–402.

[25] N. Kimura, *The structure of idempotent semigroups (I)*, Pacific J. Math. **8** (1958), 257–275.

[26] O. Košik, *Categorical equivalence of some algebras*, Acta Comment. Univ. Tartu. Math. **16** (2012), 233–239.

[27] E. Lukacs, P. P. Palfy, *Modularity of the subgroup lattice of a direct square*, Arch. Math (Basel) **46** (1986), 18–19.

[28] W. D. Maurer, J. L. Rhodes, *A property of finite simple non-abelian groups*, Proc. Amer. Math. Soci. **16** (1965), 552–554.

[29] S. Mac Lane, *Categories for the Working Mathematician*, Springer-Verlag, 1998.

[30] R. N. McKenzie, *An algebraic version of categorical equivalence for varieties and more general algebraic categories*, Lecture Notes in Pure and Applied Mathematics, 180, Marcel Dekker, New York, 1996, 211–243.

[31] R. N. McKenzie, G. F. McNulty, W. F. Taylor, *Algebras, Lattices, Varieties*, Vol. I, Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, California, 1987.

[32] K. Morita, *Duality for modules and its applications to the theory of rings with minimum condition*, Sci. Rep. Tokyo Kyoiku Daigaku Sect. A **6** (1958), 83–142.

[33] T. Nipkow, *Unification in primal algebras, their powers and their varieties*, J. Assoc. Comput. Mach. **37** (1990), 742–776.

[34] V. P. Platonov, V. I. Yanchevskii, *Finite-Dimensional Division Algebras.* In: A. I. Kostrikin, I. R. Shafarevich (eds.) *Algebra IX*, 121–239, Springer-Verlag Berlin-Heidelberg, 1995.

[35] D. Rees, *On semi-groups*, Proc. Cambridge Philos. Soc. **36** (1940), 387–400.

[36] B. M. Schein, *Bands with isomorphic endomorphism semigroups*, J. Algebra **96** (1985), 548–565.

[37] H. Schubert, *Kategorien I, II*, Springer-Verlag Berlin-Heidelberg, 1970.

[38] W. R. Scott, *Group Theory*, Dover Publications, Inc., New York, 1987.

[39] A. P. Street, *Subgroup-determining functions on groups*, Illinois J. Math. **12** (1968), 99–120.

[40] G. Takách, *Notes on sublattice-lattices*, Period. Math. Hungar. **35** (1997), 215–224.

[41] R. A. Wilson, *The finite simple groups*, Springer-Verlag London Limited, 2009.

[42] L. Zádori, *Categorical equivalence of finite groups*, Bull. Austral. Math. Soc. **56** (1997), 403–408.

[43] L. Zádori, *Relational sets and categorical equivalence of algebras*, Internat. J. Algebra Comput. **7** (1997), 561–576.

Kategoorne ekvivalents algebras

Kokkuvõte

Algebrate muutkonda saab vaadelda kategooriana loomulikul viisil: objektideks on muutkonna algebrad ja morfismideks nendevahelised homomorfismid. Kahte algebrat **A** ja **B** nimetatakse *kategoorselt ekvivalentseteks*, kui nende poolt tekitatud muutkonnad on ekvivalentsed kui kategooriad, ning kategoorse ekvivalentsi funktor kujutab algebra **A** algebraks **B**.

Esimeseks klassikaliseks algebrate kategoorse ekvivalentsi näiteks on T. K. Hu 1969. aastal tõestatud teoreem, mille kohaselt on iga primaalne algebra kategoorselt ekvivalentne kaheelemendilise Boole'i algebraga. (Lõplikku algebrat nimetatakse primaalseks, kui iga operatsioon tema põhihulgal on termfunktsioon, st, superpositsioon selle algebra tehetest ja projektsioonidest.)

Käesoleva väitekirja eesmärgiks on uurida algebrate kategoorset ekvivalentsi klassikaliste algebrate (rühmad, ringid, poolrühmad, võred) muutkondade piires. Väitekirja lähtekohtadena võib nimetada järgmisi tulemusi:

Teoreem 5.1. (C. Bergman, J. Bergman, 1996, [5]) Kahe algarvu p ja q korral on lõplikud korpused $\mathbf{F}_{p^m}$ ja $\mathbf{F}_{q^n}$ kategoorselt ekvivalentsed parajasti siis kui $m = n$.

Teoreem 2.11. (L. Zádori, 1997, [42]) Kaks lõplikku rühma on kategoorselt ekvivalentsed parajasti siis, kui nad on nõrgalt isomorfsed.

Teoreem 2.12. Kaks lõplikku poolrühma on kategoorselt ekvivalentsed parajasti siis, kui nad on nõrgalt isomorfsed. (Konverentsil ette kantud 2012. aastal M. Behrischi ja T. Waldhauseri poolt, kuid pole veel avaldatud.)

Väitekiri koosneb kuuest peatükist.

Esimene peatükk sisaldab lühiülevaadet probleemi ajaloost, väitekirja kokkuvõtet ning väitekirjas kasutatud tähistuste ja kokkulepete kirjeldust.

Teises peatükis antakse ülevaade olulistest tulemustest, mida töös kasutatakse. Peatüki alguses defineeritakse kategoorne ekvivalents, termekvivalents ning tuuakse esimesed näited. Järgnevas loetletakse algebralised omadused, mis säilivad kategoorse ekvivalentsi korral, ning tutvustatakse erinevaid meetodeid kategoorse ekvivalentsi uurimiseks. Peatüki lõpus tutvustatakse tulemusi lõplike rühmade ja poolrühmade kohta, mis pakuvad motivatsiooni termekvivalentsete poolrühmade uurimiseks neljandas peatükis.

Kolmandas peatükis näidatakse, et kategoorsete ekvivalentsi tingimus on võrede ja (poolrühmade) normaalsete sidumite korral (ka lõpmatul juhul) väga tugev: kaks võret on kategoorselt ekvivalentsed siis ja ainult siis, kui nad on isomorfsed või duaalsed; kaks normaalset sidumit on kategoorselt ekvivalentsed siis ja ainult siis, kui nad on isomorfsed või antiisomorfsed. Järeldusena tuuakse välja, et kaks poolvõret on kategoorselt ekvivalentsed siis ja ainult siis, kui nad on isomorfsed.

Neljandas peatükis uuritakse poolrühmade termekvivalentsi. Leitakse palju poolrühmade omadusi, mis säilivad termekvivalentsi korral. Mõne poolrühmade klassi (näiteks kommutatiivsed poolrühmad või idempotentsed poolrühmad) on termekvivalents triviaalne: poolrühmad peavad olema identsed või duaalsed teineteisega. Üldjuhul leidub aga ka mittetriviaalse termekvivalentsi näiteid. Eraldi käsitletakse täielikult regulaarseid ja täielikult 0-lihtsaid poolrühmi.

Viiendas peatükis vaadeldakse lõplike ühikuga ringide kategoorset ekvivalentsi. Alguses taandatakse üldine probleem juhule, kus ringide karakteristika on algarvu aste. Näidatakse, et poollihtsus säilib kategoorse ekvivalentsi korral ning lahendatakse probleem täielikult kahe lõpliku poollihtsa ringi jaoks. Samuti näidatakse, et kui kahe ringi karakteristikad on ühistegurita, siis saavad nad olla kategoorselt ekvivalentsed ainult siis, kui nad on poollihtsad. Sama karakteristikaga ringide juht jääb lahtiseks.

Konstantide lisamine algebra põhitehetele võib anda huvitavaid mittetriviaalseid kategoorse ekvivalentsi näiteid. Kuuendas peatükis tuuakse sisse p-kategoorse ekvivalentsi mõiste. Öeldakse, et kaks algebrat on *p-kategoorselt ekvivalentsed*, kui algebrad, mis saadakse neist uute konstantsete tehete lisamisega iga elemendi jaoks, on kategoorselt ekvivalentsed. Tõestatakse, et kahe lõpliku lihtsa mittekommutatiivse rühma tsentrivabad laiendid lõpliku Abeli rühma abil on p-kategoorselt ekvivalentsed. Konkreetse näitena on kaks sümmeetrilist rühma $\mathcal{S}_m$ ja $\mathcal{S}_n$, kus $m, n > 4$, p-kategoorselt ekvivalentsed.

Samuti leitakse p-kategoorse ekvivalentsi tingimus lõplike rangelt lokaalselt afiinselt täielike algebrate ning lõplike rangelt lokaalselt järjestusafiinselt täielike võrede jaoks. Viimasest tulenevad mittetriviaalsed näited võrede p-kategoorse ekvivalentsi kohta.

Kolmanda peatüki aluseks on artikkel [26]. Neljas peatükk on sündinud koostöös Peter Mayriga Johannes Kepleri Ülikoolist (Linz, Austria). Viies peatükk on sündinud koostöös Kalle Kaarli ja Tamás Waldhauseriga Szegedi Ülikoolist (Ungari).

Curriculum vitae

NAME: Oleg Košik
DATE AND PLACE OF BIRTH: 12.09.1985, Odessa, Ukraine
NATIONALITY: Estonian
ADDRESS: Institute of Mathematics, J. Liivi 2, 50409 Tartu, Estonia
PHONE: +372 56916136
E-MAIL: oleg.koshik@ut.ee

EDUCATION:

1998–2003	Tallinna Tõnismäe Reaalkool
2003–2006	University of Tartu, bachelor studies in mathematics, B.Sc. in mathematics 2006
2006–2009	University of Tartu, master studies in fundamental physics, M.Sc. in theoretical physics 2009
2009–	University of Tartu, doctoral studies in mathematics

LANGUAGES: Estonian, English, Russian, German, Ukrainian

EMPLOYMENT:

09/2008–08/2010	The Gifted and Talented Development Centre, University of Tartu, senior specialist
01/2013–06/2015	University of Tartu, Institute of Mathematics, assistant

FIELDS OF SCIENTIFIC INTEREST:
Algebra – universal algebra
Theoretical physics – particle physics

Curriculum vitae

NIMI: Oleg Košik
SÜNNIAEG JA -KOHT: 12.09.1985, Odessa, Ukraina
KODAKONDSUS: Eesti Vabariik
AADRESS: TÜ matemaatika instituut, J. Liivi 2, 50409 Tartu, Eesti
TELEFON: +372 56916136
E-POST: oleg.koshik@ut.ee

HARIDUS:

1998–2003	Tallinna Tõnismäe Reaalkool
2003–2006	Tartu Ülikool, matemaatika bakalaureuseõpe, BSc matemaatikas 2006
2006–2009	Tartu Ülikool, fundamentaalfüüsika magistriõpe, MSc teoreetilises füüsikas 2009
2009–	Tartu Ülikool, matemaatika doktoriõpe

KEELTE OSKUS: eesti, inglise, vene, saksa, ukraina

TEENISTUSKÄIK:

09/2008–08/2010	Tartu Ülikool, teaduskool, peaspetsialist
01/2013–06/2015	Tartu Ülikool, matemaatika instituut, assistent

TEADUSLIKUD HUVID:
Algebra – universaalalgebra
Teoreetiline füüsika – elementaarosakeste füüsika

List of original publications

1. O. Košik, *Categorical equivalence of some algebras*, Acta Comment. Univ. Tartu. Math. **16** (2012), 233–239.
2. K. Kaarli, O. Košik, T. Waldhauser, *On categorical equivalence of finite rings*. Submitted, 2015.

DISSERTATIONES MATHEMATICAE UNIVERSITATIS TARTUENSIS

1. **Mati Heinloo.** The design of nonhomogeneous spherical vessels, cylindrical tubes and circular discs. Tartu, 1991, 23 p.
2. **Boris Komrakov.** Primitive actions and the Sophus Lie problem. Tartu, 1991, 14 p.
3. **Jaak Heinloo.** Phenomenological (continuum) theory of turbulence. Tartu, 1992, 47 p.
4. **Ants Tauts.** Infinite formulae in intuitionistic logic of higher order. Tartu, 1992, 15 p.
5. **Tarmo Soomere.** Kinetic theory of Rossby waves. Tartu, 1992, 32 p.
6. **Jüri Majak.** Optimization of plastic axisymmetric plates and shells in the case of Von Mises yield condition. Tartu, 1992, 32 p.
7. **Ants Aasma.** Matrix transformations of summability and absolute summability fields of matrix methods. Tartu, 1993, 32 p.
8. **Helle Hein.** Optimization of plastic axisymmetric plates and shells with piece-wise constant thickness. Tartu, 1993, 28 p.
9. **Toomas Kiho.** Study of optimality of iterated Lavrentiev method and its generalizations. Tartu, 1994, 23 p.
10. **Arne Kokk.** Joint spectral theory and extension of non-trivial multiplicative linear functionals. Tartu, 1995, 165 p.
11. **Toomas Lepikult.** Automated calculation of dynamically loaded rigid-plastic structures. Tartu, 1995, 93 p, (in Russian).
12. **Sander Hannus.** Parametrical optimization of the plastic cylindrical shells by taking into account geometrical and physical nonlinearities. Tartu, 1995, 74 p, (in Russian).
13. **Sergei Tupailo.** Hilbert's epsilon-symbol in predicative subsystems of analysis. Tartu, 1996, 134 p.
14. **Enno Saks.** Analysis and optimization of elastic-plastic shafts in torsion. Tartu, 1996, 96 p.
15. **Valdis Laan.** Pullbacks and flatness properties of acts. Tartu, 1999, 90 p.
16. **Märt Põldvere.** Subspaces of Banach spaces having Phelps' uniqueness property. Tartu, 1999, 74 p.
17. **Jelena Ausekle.** Compactness of operators in Lorentz and Orlicz sequence spaces. Tartu, 1999, 72 p.
18. **Krista Fischer.** Structural mean models for analyzing the effect of compliance in clinical trials. Tartu, 1999, 124 p.

19. **Helger Lipmaa.** Secure and efficient time-stamping systems. Tartu, 1999, 56 p.
20. **Jüri Lember.** Consistency of empirical k-centres. Tartu, 1999, 148 p.
21. **Ella Puman.** Optimization of plastic conical shells. Tartu, 2000, 102 p.
22. **Kaili Müürisep.** Eesti keele arvutigrammatika: süntaks. Tartu, 2000, 107 lk.
23. **Varmo Vene.** Categorical programming with inductive and coinductive types. Tartu, 2000, 116 p.
24. **Olga Sokratova.** Ω-rings, their flat and projective acts with some applications. Tartu, 2000, 120 p.
25. **Maria Zeltser.** Investigation of double sequence spaces by soft and hard analitical methods. Tartu, 2001, 154 p.
26. **Ernst Tungel.** Optimization of plastic spherical shells. Tartu, 2001, 90 p.
27. **Tiina Puolakainen.** Eesti keele arvutigrammatika: morfoloogiline ühestamine. Tartu, 2001, 138 p.
28. **Rainis Haller.** *M(r,s)*-inequalities. Tartu, 2002, 78 p.
29. **Jan Villemson.** Size-efficient interval time stamps. Tartu, 2002, 82 p.
30. **Eno Tõnisson.** Solving of expession manipulation exercises in computer algebra systems. Tartu, 2002, 92 p.
31. **Mart Abel.** Structure of Gelfand-Mazur algebras. Tartu, 2003. 94 p.
32. **Vladimir Kuchmei.** Affine completeness of some ockham algebras. Tartu, 2003. 100 p.
33. **Olga Dunajeva.** Asymptotic matrix methods in statistical inference problems. Tartu 2003. 78 p.
34. **Mare Tarang.** Stability of the spline collocation method for volterra integro-differential equations. Tartu 2004. 90 p.
35. **Tatjana Nahtman.** Permutation invariance and reparameterizations in linear models. Tartu 2004. 91 p.
36. **Märt Möls.** Linear mixed models with equivalent predictors. Tartu 2004. 70 p.
37. **Kristiina Hakk.** Approximation methods for weakly singular integral equations with discontinuous coefficients. Tartu 2004, 137 p.
38. **Meelis Käärik.** Fitting sets to probability distributions. Tartu 2005, 90 p.
39. **Inga Parts.** Piecewise polynomial collocation methods for solving weakly singular integro-differential equations. Tartu 2005, 140 p.
40. **Natalia Saealle.** Convergence and summability with speed of functional series. Tartu 2005, 91 p.
41. **Tanel Kaart.** The reliability of linear mixed models in genetic studies. Tartu 2006, 124 p.
42. **Kadre Torn.** Shear and bending response of inelastic structures to dynamic load. Tartu 2006, 142 p.

43. **Kristel Mikkor.** Uniform factorisation for compact subsets of Banach spaces of operators. Tartu 2006, 72 p.
44. **Darja Saveljeva.** Quadratic and cubic spline collocation for Volterra integral equations. Tartu 2006, 117 p.
45. **Kristo Heero.** Path planning and learning strategies for mobile robots in dynamic partially unknown environments. Tartu 2006, 123 p.
46. **Annely Mürk.** Optimization of inelastic plates with cracks. Tartu 2006. 137 p.
47. **Annemai Raidjõe.** Sequence spaces defined by modulus functions and superposition operators. Tartu 2006, 97 p.
48. **Olga Panova.** Real Gelfand-Mazur algebras. Tartu 2006, 82 p.
49. **Härmel Nestra.** Iteratively defined transfinite trace semantics and program slicing with respect to them. Tartu 2006, 116 p.
50. **Margus Pihlak.** Approximation of multivariate distribution functions. Tartu 2007, 82 p.
51. **Ene Käärik.** Handling dropouts in repeated measurements using copulas. Tartu 2007, 99 p.
52. **Artur Sepp.** Affine models in mathematical finance: an analytical approach. Tartu 2007, 147 p.
53. **Marina Issakova.** Solving of linear equations, linear inequalities and systems of linear equations in interactive learning environment. Tartu 2007, 170 p.
54. **Kaja Sõstra.** Restriction estimator for domains. Tartu 2007, 104 p.
55. **Kaarel Kaljurand.** Attempto controlled English as a Semantic Web language. Tartu 2007, 162 p.
56. **Mart Anton.** Mechanical modeling of IPMC actuators at large deformations. Tartu 2008, 123 p.
57. **Evely Leetma.** Solution of smoothing problems with obstacles. Tartu 2009, 81 p.
58. **Ants Kaasik.** Estimating ruin probabilities in the Cramér-Lundberg model with heavy-tailed claims. Tartu 2009, 139 p.
59. **Reimo Palm.** Numerical Comparison of Regularization Algorithms for Solving Ill-Posed Problems. Tartu 2010, 105 p.
60. **Indrek Zolk.** The commuting bounded approximation property of Banach spaces. Tartu 2010, 107 p.
61. **Jüri Reimand.** Functional analysis of gene lists, networks and regulatory systems. Tartu 2010, 153 p.
62. **Ahti Peder.** Superpositional Graphs and Finding the Description of Structure by Counting Method. Tartu 2010, 87 p.
63. **Marek Kolk.** Piecewise Polynomial Collocation for Volterra Integral Equations with Singularities. Tartu 2010, 134 p.

64. **Vesal Vojdani.** Static Data Race Analysis of Heap-Manipulating C Programs. Tartu 2010, 137 p.
65. **Larissa Roots.** Free vibrations of stepped cylindrical shells containing cracks. Tartu 2010, 94 p.
66. **Mark Fišel.** Optimizing Statistical Machine Translation via Input Modification. Tartu 2011, 104 p.
67. **Margus Niitsoo**. Black-box Oracle Separation Techniques with Applications in Time-stamping. Tartu 2011, 174 p.
68. **Olga Liivapuu.** Graded q-differential algebras and algebraic models in noncommutative geometry. Tartu 2011, 112 p.
69. **Aleksei Lissitsin.** Convex approximation properties of Banach spaces. Tartu 2011, 107 p.
70. **Lauri Tart.** Morita equivalence of partially ordered semigroups. Tartu 2011, 101 p.
71. **Siim Karus.** Maintainability of XML Transformations. Tartu 2011, 142 p.
72. **Margus Treumuth.** A Framework for Asynchronous Dialogue Systems: Concepts, Issues and Design Aspects. Tartu 2011, 95 p.
73. **Dmitri Lepp.** Solving simplification problems in the domain of exponents, monomials and polynomials in interactive learning environment T-algebra. Tartu 2011, 202 p.
74. **Meelis Kull.** Statistical enrichment analysis in algorithms for studying gene regulation. Tartu 2011, 151 p.
75. **Nadežda Bazunova.** Differential calculus $d^3 = 0$ on binary and ternary associative algebras. Tartu 2011, 99 p.
76. **Natalja Lepik.** Estimation of domains under restrictions built upon generalized regression and synthetic estimators. Tartu 2011, 133 p.
77. **Bingsheng Zhang.** Efficient cryptographic protocols for secure and private remote databases. Tartu 2011, 206 p.
78. **Reina Uba.** Merging business process models. Tartu 2011, 166 p.
79. **Uuno Puus.** Structural performance as a success factor in software development projects – Estonian experience. Tartu 2012, 106 p.
80. **Marje Johanson.** $M(r, s)$-ideals of compact operators. Tartu 2012, 103 p.
81. **Georg Singer.** Web search engines and complex information needs. Tartu 2012, 218 p.
82. **Vitali Retšnoi.** Vector fields and Lie group representations. Tartu 2012, 108 p.
83. **Dan Bogdanov.** Sharemind: programmable secure computations with practical applications. Tartu 2013, 191 p.
84. **Jevgeni Kabanov.** Towards a more productive Java EE ecosystem. Tartu 2013, 151 p.
85. **Erge Ideon**. Rational spline collocation for boundary value problems. Tartu, 2013, 111 p.
86. **Esta Kägo**. Natural vibrations of elastic stepped plates with cracks. Tartu, 2013, 114 p.

87. **Margus Freudenthal.** Simpl: A toolkit for Domain-Specific Language development in enterprise information systems. Tartu, 2013, 151 p.
88. **Boriss Vlassov.** Optimization of stepped plates in the case of smooth yield surfaces. Tartu, 2013, 104 p.
89. **Elina Safiulina.** Parallel and semiparallel space-like submanifolds of low dimension in pseudo-Euclidean space. Tartu, 2013, 85 p.
90. **Raivo Kolde.** Methods for re-using public gene expression data. Tartu, 2014, 121 p.
91. **Vladimir Šor.** Statistical Approach for Memory Leak Detection in Java Applications. Tartu, 2014, 155 p.
92. **Naved Ahmed.** Deriving Security Requirements from Business Process Models. Tartu, 2014, 171 p.
93. **Kerli Orav-Puurand.** Central Part Interpolation Schemes for Weakly Singular Integral Equations. Tartu, 2014, 109 p.
94. **Liina Kamm.** Privacy-preserving statistical analysis using secure multi-party computation. Tartu, 2015, 201 p.
95. **Kaido Lätt.** Singular Fractional Differential Equations and Cordial Volterra Integral Operators. Tartu, 2015, 93 p.