Journal of Algebra and Its Applications
Vol. 15, No. 8 (2016) 1650154 (12 pages)
© World Scientific Publishing Company
DOI: 10.1142/S0219498816501541

World Scientific
www.worldscientific.com

On categorical equivalence of finite rings

Kalle Kaarli* and Oleg Košik†
Institute of Mathematics, University of Tartu
50090 Tartu, Estonia
**kaarli@ut.ee*
†*oleg.koshik@ut.ee*

Tamás Waldhauser
Bolyai Institute, University of Szeged
Aradi vértanúk tere 1, 6720 Szeged, Hungary
twaldha@math.u-szeged.hu

Received 14 January 2015
Accepted 18 September 2015
Published 6 November 2015

Communicated by L. Bokut

We reduce the problem of categorical equivalence for finite 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.

Keywords: Categorical equivalence; ring; semisimple ring; characteristic of a ring.

Mathematics Subject Classification: 08C05

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 $\mathbf{R}$ is contained in every subring of $\mathbf{R}$.

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. Because of universal algebraic background of this research, we use the standard universal algebraic notation. That is, the algebraic structures are denoted by capital boldface letters and their underlying sets (universes) by corresponding usual capital letters. Thus, in particular, a ring $\mathbf{R}$ has the universe R.

Definition 1. Two algebras $\mathbf{A}$ and $\mathbf{B}$ are called *categorically equivalent*, denoted $\mathbf{A} \equiv_c \mathbf{B}$, if there is a categorical equivalence between the varieties they generate that sends $\mathbf{A}$ to $\mathbf{B}$.

Recall that the equivalence of categories was first used in algebra by Morita who in 1958 introduced the equivalence relation on the class of rings that now is known as Morita equivalence. By definition, two rings $\mathbf{R}$ and $\mathbf{S}$ are right Morita equivalent, if the categories of right modules over $\mathbf{R}$ and $\mathbf{S}$ are equivalent. We emphasize that the Morita equivalence of rings and the categorical equivalence of rings are incomparable notions. Indeed, it is well known that any field $\mathbf{K}$ is Morita equivalent to all rings $\mathrm{Mat}_n(\mathbf{K})$ but in view of our Theorem 18, if $\mathbf{K}$ is finite then $\mathbf{K} \equiv_c \mathrm{Mat}_n(\mathbf{K})$ holds only if $n = 1$. On the other hand, a result by Bergman and Berman (see Theorem 2) provides examples of categorically equivalent rings that are not Morita equivalent.

A special case of categorical equivalence is weak isomorphism. Recall that two algebras $\mathbf{A}$ and $\mathbf{B}$ are called *weakly isomorphic* if there exists a third algebra $\mathbf{C}$ that is isomorphic to $\mathbf{A}$ and term equivalent to $\mathbf{B}$. Clearly, weakly isomorphic algebras have the same cardinality. For example, every group (semigroup, ring) is accompanied by its anti-isomorphic copy which, as easily seen, is weakly isomorphic to the original group (semigroup, ring). Similarly, every lattice is weakly isomorphic to its dual.

All algebraic notions and properties that can be expressed in the language of category theory are preserved under categorical equivalence. The next theorem lists some of these properties specialized to rings, that we shall need in the sequel. Their proofs can be found in [3, Sec. 3].

Theorem 1. *Let* $\mathbf{R}$ *and* $\mathbf{S}$ *be categorically equivalent rings. Then*:

(1) *the automorphism groups of* $\mathbf{R}$ *and* $\mathbf{S}$ *are isomorphic*;
(2) *the subring lattices of* $\mathbf{R}$ *and* $\mathbf{S}$ *are isomorphic*;
(3) *the (two-sided) ideal lattices of* $\mathbf{R}$ *and* $\mathbf{S}$ *are isomorphic*;
(4) *for every positive integer* n, $\mathbf{R}^n \equiv_c \mathbf{S}^n$;
(5) $\mathbf{R}$ *is finite if and only if* $\mathbf{S}$ *is finite.*

The first studies on categorical equivalence in algebra involved general algebraic structures that did not belong to any well-known class. The fundamental example of this sort is the theorem of Hu [6] claiming that every two primal algebras are categorically equivalent to each other. 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. Thus, $\mathbb{Z}_p \equiv_c \mathbb{Z}_q$ for any primes p and q. This result was generalized by Bergman and Berman.

Theorem 2 ([2, 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 in other well-studied varieties the finite categorically equivalent members have been proved to be weakly isomorphic, hence of the same size. For finite groups this fact was obtained by Zádori [12]. Recently

Behrisch and Waldhauser announced that the similar result is true in case of finite semigroups [1]. Even stronger result holds in case of lattices. Košik [10] proved that two lattices (not necessarily finite) are categorically equivalent if and only if they are isomorphic or dually isomorphic.

In the present paper 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.

2. Reduction to p-Rings

A ring whose additive group is a p-group will be called a *p-ring.*[a] 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 $\mathrm{char}(\mathbf{R})$, 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.

We shall make use of the notion of independence introduced by Foster in [5] and developed further by Hu and Kelenson in [7]. The algebras $\mathbf{A}_1, \ldots, \mathbf{A}_n$ of the same type are called *independent* if there exists an n-ary term $t(x_1, \ldots, x_n)$ such that in the algebra $\mathbf{A}_i$ the identity $t(x_1, \ldots, x_n) \approx x_i$ holds, $i = 1, \ldots, n$. Corollary 2.9 of [7] essentially states that algebras $\mathbf{A}_1, \ldots, \mathbf{A}_n$ 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 [7].

Proposition 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 [7] 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

[a]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.

where W is some variety of rings then the system $F(\mathbf{R}_1), \dots, F(\mathbf{R}_n)$ is independent, too.

Corollary 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 1(5). Suppose that $\mathbf{S}$ is not a q-ring for some prime q. Then it is a direct product of two independent rings. Since $\mathbf{R} \equiv_c \mathbf{S}$, the same must hold for $\mathbf{R}$, a contradiction. □

Theorem 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 $\mathbf{R}_i$, $i = 1, \dots, n$, are the p-components of $\mathbf{R}$, then $\mathbf{S}$ is the direct product of $F(\mathbf{R}_1), \dots, F(\mathbf{R}_n)$. Obviously, $\mathbf{R}_i \equiv_c F(\mathbf{R}_i)$, $i = 1, \dots, n$. Thus, we have to show that $F(\mathbf{R}_1), \dots, F(\mathbf{R}_n)$ are the p-components of $\mathbf{S}$. By Corollary 4, there exist primes q_i such that the characteristic of $F(\mathbf{R}_i)$ is a power of q_i, $i = 1, \dots, n$. It remains to show that $q_i \neq q_j$ if $i \neq j$. But this easily follows from Proposition 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 $\mathbf{S}_i$, $i = 1, \dots, n$. Then F_i induces an isomorphism between skeletons of the categories $\mathrm{Var}(\mathbf{R}_i)$ and $\mathrm{Var}(\mathbf{S}_i)$, $i = 1, \dots, n$. By [7, Theorem 2.6], 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, and the similar statement holds 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, our main problem splits into 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 paper 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.

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 2 by showing that a finite field $\mathbf{F}_{p^k}$ can be categorically equivalent only to $\mathbf{F}_{q^k}$.

Theorem 6. *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 1 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 $n \geq 2$ and consider the automorphism groups of $\mathbf{F}_{p^k}$ and $\mathbf{R}$. It is well known that the first of them is cyclic while the other is non-abelian. Thus, $n = 1$, that is, $\mathbf{R} \simeq \mathbf{F}$. Now our claim follows from Theorem 2. □

Corollary 7. *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 8. *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 $\mathbb{Z}_{p^k} \equiv_c \mathbb{Z}_{q^l}$. Since categorically equivalent algebras have isomorphic congruence lattices, we immediately have $k = l$. Assume $k \geq 2$. Then the ring $\mathbb{Z}_{p^2}$, being a homomorphic image of $\mathbb{Z}_{p^k}$, is categorically equivalent to some of the homomorphic images of $\mathbb{Z}_{q^k}$. Counting the congruences, we conclude $\mathbb{Z}_{p^2} \equiv_c \mathbb{Z}_{q^2}$ which implies $\mathbb{Z}^2_{p^2} \equiv_c \mathbb{Z}^2_{q^2}$. Consequently, there is a one-to-one correspondence between subrings of $\mathbb{Z}^2_{p^2}$ and $\mathbb{Z}^2_{q^2}$ under which the corresponding subrings are categorically equivalent.

We claim that both $\mathbb{Z}^2_{p^2}$ and $\mathbb{Z}^2_{q^2}$ have precisely three subrings. It is easy to check this directly but we prefer the universal algebraic approach. Since 1 is a nullary basic operation and every $\mathbb{Z}_n$ is generated by 1, it follows that every subuniverse of $\mathbb{Z}^2_n$, is reflexive, that is, contains the diagonal relation $\{(x, x) \mid x \in \mathbb{Z}_n\}$. It is well known that the only reflexive subuniverses of the direct square of an algebra $\mathbf{A}$ in a congruence permutable variety are the congruences of $\mathbf{A}$ (See [8, Theorem 1.2.13]). Now our claim becomes obvious because $\mathbb{Z}_{p^2}$ has precisely three ideals: $\{0\}$, $p\mathbb{Z}_{p^2}$ and $\mathbb{Z}_{p^2}$.

Let $\mathbf{A}_p$ be the subring of $\mathbb{Z}^2_{p^2}$ whose universe A_p is the congruence of $\mathbb{Z}_{p^2}$ that corresponds to the ideal $p\mathbb{Z}_{p^2}$. Note that

$$A_p = \{(x, y) \in \mathbb{Z}^2_{p^2} \mid px = py\}$$

and $|A_p| = p^3$. By what we mentioned above, we have $\mathbf{A}_p \equiv_c \mathbf{A}_q$, hence the congruence lattices of $\mathbf{A}_p$ and $\mathbf{A}_q$ are isomorphic. We are going to show that $\mathbf{A}_p$ has exactly $p+1$ minimal ideals which will yield $p = q$.

Let $I_k = \{(px, kpx) \mid x \in \mathbb{Z}_{p^2}\}$, $k = 0, 1, \ldots, p-1$ and $I = \{(0, px) \mid x \in \mathbb{Z}_{p^2}\}$. It is easy to check that $I, I_0, \ldots, I_{p-1}$ are pairwise different ideals of the ring $\mathbf{A}_p$. Moreover, they all are of order p, thus they are minimal ideals $\mathbf{A}_p$. We show that every non-zero ideal J of $\mathbf{A}_p$ contains one of the selected $p+1$ ideals proving so that $\mathbf{A}_p$ has no other minimal ideals. Indeed, if (x, y) is a non-zero element of J then either (x, y) or (px, py) is a non-zero element of one of the ideals $I, I_0, \ldots, I_{p-1}$. □

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 9. *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 and Lemma 8. □

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 9.

Corollary 10. *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 $\mathrm{char}(\mathbf{S}) = q$.*

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 13, 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 14 and 18.

From [4] it follows 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 another simple lemma.

Lemma 11. *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 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. □

Corollary 12. *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* $\mathbf{S}$.

Theorem 13. *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 6 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 7 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 9 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 1 (5)) and by Corollary 10 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 $I = \{a\varepsilon \mid a \in \mathbb{Z}_p\}$. 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 7 implies that $\mathbf{S}/J$ is isomorphic to $\mathbb{Z}_q$. Corollary 12 gives that J is the radical of $\mathbf{S}$ and $J \neq 0$ because by Lemma 11 semisimplicity is a categorical property.

We next show that $|J| = q$. It is well known that a radical of a finite ring $\mathbf{S}$, if non-zero, 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 13 and Corollary 10. It shows, in essence, that a finite non-semisimple p-ring can be categorically equivalent only to a ring of the same characteristic.

Theorem 14. *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 10 $\mathrm{char}(\mathbf{R}) = p$ and $\mathrm{char}(\mathbf{S}) = q$ where q is a prime different from p. Since $\mathbf{R}$ is not semisimple, there exists a non-zero nilpotent element $a \in R$, say $a^n = 0$ but $a^{n-1} \neq 0$. Let $e = a^{n-1}$, then we have $e^2 = 0$ and $e \neq 0$.

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 13, we have $\mathbf{R}_1 \simeq \mathbf{S}_1$, implying $p = q$. This contradiction proves the theorem. □

Corollary 15. *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 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 14 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. 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.

Lemma 16. *Let* $\mathbf{K}$ *be a finite field and* $n \geq 2$ *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* $\operatorname{PSL}(n, \mathbf{K})$*.*

Proof. It is well known (see, for example, [9, Chapter I, Theorem 3.1]) that every automorphism of the full matrix ring $\operatorname{Mat}_n(\mathbf{K})$ over a field $\mathbf{K}$ is a composition of an outer automorphism (a fixed automorphism of $\mathbf{K}$ is applied to all entries of all matrices) and an inner automorphism (mapping of the form $X \mapsto C^{-1}XC$ where C is a fixed non-singular matrix). It is easily seen that all inner automorphisms of the ring $\operatorname{Mat}_n(\mathbf{K})$ form a normal subgroup (denoted by $\operatorname{Inn}\operatorname{Mat}_n(\mathbf{K})$) of the full automorphism group $\operatorname{Aut}\operatorname{Mat}_n(\mathbf{K})$ while the outer automorphisms of $\operatorname{Mat}_n(\mathbf{K})$ form just a subgroup of $\operatorname{Aut}\operatorname{Mat}_n(\mathbf{K})$, isomorphic to $\operatorname{Aut}(\mathbf{K})$. Moreover, obviously

$$\operatorname{Aut}\operatorname{Mat}_n(\mathbf{K}) \simeq \operatorname{Inn}\operatorname{Mat}_n(\mathbf{K}) \rtimes \operatorname{Aut}\mathbf{K}, \tag{1}$$

where $\rtimes$ denotes semidirect product of groups. Therefore, since the automorphism group of a finite field is cyclic, the solvability of $\operatorname{Aut}\operatorname{Mat}_n(\mathbf{K})$ is equivalent to that of $\operatorname{Inn}\operatorname{Mat}_n(\mathbf{K})$. Further, since $\operatorname{Inn}\operatorname{Mat}_n(\mathbf{K})$ is isomorphic to the quotient group of $\operatorname{GL}(n, \mathbf{K})$ over its center, the solvability of $\operatorname{Inn}\operatorname{Mat}_n(\mathbf{K})$ is equivalent to that of $\operatorname{GL}(n, \mathbf{K})$. Now our claim follows from a classical fact of group theory: the group $\operatorname{GL}(n, \mathbf{K})$ with $n \geq 2$ is solvable if and only if $n = 2$ and $|\mathbf{K}|$ is 2 or 3, and in all other cases the only non-abelian composition factor of $\operatorname{GL}(n, \mathbf{K})$ is $\operatorname{PSL}(n, \mathbf{K})$.

□

Lemma 17. *Every atom in the lattice of subrings of* $\operatorname{Mat}_2(\mathbb{Z}_p)$ *has cardinality* p^2*.*

Proof. Since $\mathbb{Z}_p$ is a prime field, every subring of $\operatorname{Mat}_2(\mathbb{Z}_p)$ 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 $\mathbf{S} \leq \operatorname{Mat}_2(\mathbb{Z}_p)$ is a three-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 18. *Let* $\mathbf{K}_1$ *and* $\mathbf{K}_2$ *be finite fields and* $n_1, n_2 \geq 2$ *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 $\operatorname{Aut}\mathrm{Mat}_{n_1}(\mathbf{K}_1) \simeq \operatorname{Aut}\mathrm{Mat}_{n_2}(\mathbf{K}_2)$.

Let first $\operatorname{Aut}\mathrm{Mat}_{n_1}(\mathbf{K}_1)$ be non-solvable. Then, by Lemma 16, $\mathrm{PSL}(n_1, \mathbf{K}_1) \simeq \mathrm{PSL}(n_2, \mathbf{K}_2)$. 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 [11, Sec. 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 give $|\mathrm{GL}_2(\mathbf{F}_7)| = 48 \cdot 42$. Since the center of this group is of size 6 and $|\operatorname{Aut}(\mathbf{F}_7)| = 1$, the formula (1) gives $|\operatorname{Aut}\mathrm{Mat}_2(\mathbf{F}_7)| = (48 \cdot 42)/6 = 336$. On the other hand, $|\mathrm{GL}_3(\mathbf{F}_2)| = 7 \cdot 6 \cdot 4 = 168$, the center of this group is trivial and $|\operatorname{Aut}(\mathbf{F}_2)| = 1$, so the formula (1) gives $|\operatorname{Aut}\mathrm{Mat}_3(\mathbf{F}_2)| = 168$. Hence, $\operatorname{Aut}\mathrm{Mat}_2(\mathbf{F}_7) \not\simeq \operatorname{Aut}\mathrm{Mat}_3(\mathbf{F}_2)$ 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 $\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right)$ with $a, b \in \{0, 1\}$. Clearly, the size of $\mathbf{A}$ is 2^2, it is a ring of Type (4) in Sec. 4 and its only proper subring is the smallest subring of $\mathrm{Mat}_2(\mathbf{F}_4)$. On the other hand, by Lemma 17, every atom in the lattice of subrings of $\mathrm{Mat}_2(\mathbf{F}_5)$ has cardinality 5^2. Hence, by Theorem 13, none of the latter is categorically equivalent to $\mathbf{A}$.

It remains to consider the case when the group $\operatorname{Aut}\mathrm{Mat}_{n_1}(\mathbf{K}_1)$ is solvable. In view of Lemma 16, 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 2 holds for semisimple rings.

Theorem 19. *Let* $\mathbf{R}$ *and* $\mathbf{S}$ *be semisimple rings with p-components* $\mathbf{R}_1, \ldots, \mathbf{R}_n$ *and* $\mathbf{S}_1, \ldots, \mathbf{S}_n$*, 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* $i \in \{1, \ldots, n\}$*, 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* $k_1, \ldots, k_t$*.*

Proof. First, to prove the "only if" part, let us suppose that $\mathbf{R}$ and $\mathbf{S}$ are categorically equivalent. By Theorem 5, 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 $j = 1, \ldots, t$. By Theorems 6 and 18, 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 18, 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, 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 2, 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 2 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 $i = 1, \ldots, t$, and this implies

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

Acknowledgments

The authors express their sincere thanks to László Márki, Jenő Szigeti and Valdis Laan for valuable comments and suggestions. The research of the first two authors was partially supported by institutional research funding IUT20-57 of the Estonian Ministry of Education and Research. The research of the third author was partially supported by the Hungarian National Foundation for Scientific Research under Grants No. K83219 and K104251, and by the János Bolyai Research Scholarship. Mutual visits of the authors were made possible by the exchange agreement between the Estonian and the Hungarian Academies of Sciences.

References

[1] M. Behrisch and T. Waldhauser, Categorical equivalence of finite semigroups, Manuscript.

[2] C. Bergman and J. Berman, Morita equivalence of almost-primal clones, *J. Pure Appl. Algebra* **108** (1996) 175–201.
[3] B. A. Davey and H. Werner, Dualities and equivalences for varieties of algebras, in *Contributions to Lattice Theory*, Colloq. Math. Soc. János Bolyai, Vol. 33 (North-Holland, Amsterdam, 1983), pp. 101–275.
[4] B. Fine, Classification of finite rings of order p^2, *Math. Mag.* **66** (1993) 248–252.
[5] A. L. Foster, The identities of — and unique factorization within — classes of universal algebras, *Math. Z.* **62** (1955) 171–188.
[6] T.-K. Hu, Stone duality for primal algebra theory, *Math. Z.* **110** (1969) 180–198.
[7] T.-K. Hu and Ph. Kelenson, Independence and direct factorization of universal algebras, *Math. Nachr.* **51** (1971) 83–99.
[8] K. Kaarli and A. Pixley, *Polynomial Completeness in Algebraic Systems* (Chapman & Hall/CRC, Boca Raton, 2001).
[9] V. P. Platonov and V. I. Yanchevskii, Finite-dimensional division algebras, in *Algebra IX*, eds. A. I. Kostrikin and I. R. Shafarevich (Springer, Berlin, 1995), pp. 121–239.
[10] O. Košik, Categorical equivalence of some algebras, *Acta Comment. Univ. Tartu. Math.* **16** (2012) 233–239.
[11] R. A. Wilson, *The Finite Simple Groups* (Springer, 2009).
[12] L. Zádori, Categorical equivalence of finite groups, *Bull. Austral. Math. Soc.* **56** (1997) 403–408.