This paper appeared in Communications in Algebra. **49** (2021), 1437–1450.

ON CATEGORICAL EQUIVALENCE OF FINITE p-RINGS

KALLE KAARLI AND TAMÁS WALDHAUSER

Abstract. We prove that finite categorically equivalent p-rings have isomorphic additive groups (in particular, they have the same cardinality) and that the number of generators is a categorical invariant for finite rings. We also classify rings of size p^3 up to categorical equivalence.

1. Introduction

This paper is a continuation of the paper [9]. Therefore, concerning the background and motivation, we refer to that paper.

Every finite ring can be represented as a direct product of p-rings for different primes p. In [9] we proved that finite rings $\mathbf{R}$ and $\mathbf{S}$ are categorically equivalent if and only if there is a bijection between their p-components such that the corresponding p-components are categorically equivalent. This reduces the problem of describing all categorical equivalences between finite rings to the case where $\mathbf{R}$ is a p-ring and $\mathbf{S}$ is a q-ring for possibly different primes p and q. The case $p \neq q$ was completely settled in [9] by the following theorem.

Theorem 1.1 ([9])**.** *Let $\mathbf{R}$ be a finite p-ring and let $\mathbf{S}$ be a finite q-ring for distinct primes p and q. Then $\mathbf{R}$ and $\mathbf{S}$ are categorically equivalent if and only if $\mathbf{R} \cong \mathrm{GF}(p^{k_1}) \times \cdots \times \mathrm{GF}(p^{k_t})$ and $\mathbf{S} \cong \mathrm{GF}(q^{k_1}) \times \cdots \times \mathrm{GF}(q^{k_t})$ for some positive integers $k_1, \ldots, k_t$.*

Now it remains to consider the case where $\mathbf{R}$ and $\mathbf{S}$ are both p-rings for the same prime p. We recall some results from [9] concerning this case.

Theorem 1.2 ([9])**.** *Categorically equivalent finite p-rings have the same characteristic.*

Theorem 1.3 ([9])**.** *Categorically equivalent finite semisimple p-rings are isomorphic.*

Theorem 1.4 ([9])**.** *Let $\mathbf{R}$ and $\mathbf{S}$ be finite categorically equivalent p-rings. If at least one of $\mathbf{R}$ and $\mathbf{S}$ is either simple (i.e., isomorphic to a full matrix ring over a finite field $\mathrm{GF}(p^k)$ for some $k \in \mathbb{N}$) or cyclic (i.e., isomorphic to $\mathbb{Z}_{p^k}$ for some $k \in \mathbb{N}$) or is of size p^2 (i.e., isomorphic to one of the rings $\mathbb{Z}_{p^2}$, $\mathrm{GF}(p^2)$, $\mathbb{Z}_p \times \mathbb{Z}_p$, $\mathbb{Z}_p[x]/(x^2)$ by [5]), then $\mathbf{R}$ and $\mathbf{S}$ are isomorphic.*

Thus, trying to understand when can two finite non-isomorphic p-rings $\mathbf{R}$ and $\mathbf{S}$ be categorically equivalent, we may restrict to non-semisimple p-rings of the same characteristic.

Let us describe the structure of the paper. Section 3 that comes after Preliminaries, has a technical nature but its content is crucial for the rest of the paper. It is well known that categorically equivalent algebras always have isomorphic congruence lattices. Hence, categorically isomorphic rings have isomorphic ideal lattices. In our approach, if $\mathbf{S}$ is a subring of $\mathbf{R}$ then it is assumed that $1_{\mathbf{R}} \in S$. However, it is also useful to consider so-called *subrngs* of $\mathbf{R}$, that is, the subgroups of the additive group of $\mathbf{R}$ that are closed with respect to multiplication (but need not contain $1_{\mathbf{R}}$). Since every subrng of $\mathbf{R}$ is an ideal of some subring of $\mathbf{R}$, it turns out that categorically equivalent rings have isomorphic subrng lattices. This is important because it allows

2010 *Mathematics Subject Classification.* Primary 08C05; Secondary 16B50.

Key words and phrases. Categorical equivalence, ring, p-ring, additive group of a ring, one-generated ring, relational clone.

us to apply the methods and results of Korobkov [11, 12, 13] who has extensively studied rngs with isomorphic subrng lattices.

In Section 4 one of the main results of the paper is proved: categorically equivalent finite p-rings (for the same prime p) have isomorphic additive groups. In Section 5 the rings of order p^3 are classified in the sense of categorical equivalence. It turns out that most of the non-isomorphic rings of order p^3 are categorically non-equivalent. There is a single pair of non-isomorphic but categorically equivalent (actually weakly isomorphic) rings of order p^3.

Recall that in [9] we conjectured that if two finite p-rings of the same characteristic are categorically equivalent then they must be either isomorphic or anti-isomorphic. The new results show that this conjecture does not hold but is not too far from the truth. Indeed, on one hand categorically equivalent finite p-rings have isomorphic additive groups just as isomorphic or anti-isomorphic rings. On the other hand, the pair of rings of order p^3 above are not anti-isomorphic because they are commutative. Our new conjecture is that two categorically equivalent p-rings for the same p are necessarily weakly isomorphic.

In Section 6 it is proved that the number of generators is a categorical invariant for finite rings. We first reduce the problem to p-rings and then prove that in that case the property to be one-generated is categorical. This proof is relatively complicated, Korobkov's methods play an essential role in it. The step from one generator to any finite number of generators is easy. An interesting corollary from this result is that freedom is a categorical property, too, i.e., if a functor F witnesses a categorical equivalence between p-rings $\mathbf{R}$ and $\mathbf{S}$ then F maps free rings of the variety $\mathrm{HSP}(\mathbf{R})$ to free rings of the variety $\mathrm{HSP}(\mathbf{S})$.

2. Preliminaries

2.1. **Rings.** In this paper, by a *ring* we always mean a finite associative ring with identity. The identity element of the ring $\mathbf{R}$ is denoted by $1_{\mathbf{R}}$; the subscript will be sometimes omitted, if there is no risk of ambiguity. We will sometimes also consider rings that do not necessarily have an identity; following Jacobson [8], we call such structures *rngs*, and these will be also assumed to be finite without further mention. As a notational convention, we will use boldface letters for rings and normal letters for rngs. Using this terminology, if $\mathbf{R}$ is a r(i)ng and $S \subseteq R$ is a nonempty subset that is closed under addition, additive inverses and multiplication, then we say that S is a *subrng* of $\mathbf{R}$. If $\mathbf{R}$ is a ring and $\mathbf{S}$ is a subrng of $\mathbf{R}$ such that $1_{\mathbf{R}} \in S$, then we say that $\mathbf{S}$ is a *subring* of $\mathbf{R}$, and we denote this by $\mathbf{S} \leq \mathbf{R}$. Let $\mathrm{Subrng}(\mathbf{R})$ and $\mathrm{Subring}(\mathbf{R})$ denote the lattice of all subrngs and the lattice of all subrings of $\mathbf{R}$, respectively. The smallest subrng containing a nonempty set $H \subseteq R$ is denoted by $\langle H \rangle$, and the smallest subring containing $H \subseteq R$ is denoted by $\langle H \rangle_1$, i.e., $\langle H \rangle_1 = \langle H \cup \{1_{\mathbf{R}}\} \rangle$. Note that if I is an ideal of $\mathbf{R}$ (notation: $I \lhd \mathbf{R}$), then we have $\langle I \rangle = I$ and $\langle I \rangle_1 = I + \langle 1_{\mathbf{R}} \rangle = I + \langle 1_{\mathbf{R}} \rangle_1$, and $\langle 1_{\mathbf{R}} \rangle_1 \cong \mathbb{Z}_c$, where c is the characteristic of $\mathbf{R}$. The principal ideal in the ring $\mathbf{R}$ generated by an element $r \in R$ is denoted by (r).

The *Galois ring* $\mathrm{GR}(p^n, m)$ is defined as the quotient ring $\mathbb{Z}_{p^n}[x]/(f)$, where $f \in \mathbb{Z}_{p^n}[x]$ is a polynomial of degree m, such that f is irreducible over $\mathbb{Z}_p$. This ring is determined up to isomorphism by p, n and m. We have the special cases $\mathrm{GR}(p^n, 1) \cong \mathbb{Z}_{p^n}$ and $\mathrm{GR}(p, m) = \mathrm{GF}(p^m)$.

2.2. **Categorical equivalence.** Algebras $\mathbf{A}$ and $\mathbf{B}$ are said to be *categorically equivalent*, denoted by $\mathbf{A} \equiv_c \mathbf{B}$, if there is a categorical equivalence functor $F\colon \mathrm{HSP}(\mathbf{A}) \to \mathrm{HSP}(\mathbf{B})$ between the varieties generated by $\mathbf{A}$ and $\mathbf{B}$ such that $F(\mathbf{A}) = \mathbf{B}$. Categorical equivalence of finite algebras has been characterized by R. McKenzie [15] in terms of matrix powers and by K. Denecke and O. Lüders [4] in terms of relational clones. In the following we briefly explain the latter characterization.

If $\rho \in \mathrm{SP}_{\mathrm{fin}}(\mathbf{A})$ is (the underlying set of) a subalgebra of a finite direct power of $\mathbf{A}$, then ρ is said to be an *invariant relation* of $\mathbf{A}$. The set of all invariant relations of $\mathbf{A}$ is the *relational clone* of $\mathbf{A}$, which is equipped with the operations of direct product,

diagonalization and projection, which we shall define next. The *direct product* of $\rho \leq \mathbf{A}^k$ and $\sigma \leq \mathbf{A}^m$ is defined by

$$\rho \times \sigma = \{(x_1, \ldots, x_{k+m}) : (x_1, \ldots, x_k) \in \rho \text{ and } (x_{k+1}, \ldots, x_{k+m}) \in \sigma\} \leq \mathbf{A}^{k+m}.$$

If $\rho \leq \mathbf{A}^k$ and ε is an equivalence relation on $\{1, \ldots, k\}$, then the *diagonalization* of ρ with respect to ε is the invariant relation

$$\Delta_\varepsilon(\rho) = \{(x_1, \ldots, x_k) : (x_1, \ldots, x_k) \in \rho \text{ and } i \varepsilon j \implies x_i = x_j\} \leq \mathbf{A}^k.$$

The *projection* $\mathrm{pr}_{i_1,\ldots,i_m}(\rho)$ of ρ to the coordinates $i_1, \ldots, i_m \in \{1, \ldots, k\}$ is defined by

$$\mathrm{pr}_{i_1,\ldots,i_m}(\rho) = \{(x_{i_1}, \ldots, x_{i_m}) : (x_1, \ldots, x_k) \in \rho\} \leq \mathbf{A}^m.$$

Note that the indices $i_1, \ldots, i_m$ are not assumed to be in increasing order, hence the projection operator can be used to permute coordinates. Observe also that intersections of relations of the same arity and the usual relational product of binary relations can be expressed with the above defined three operations.

If $F\colon \mathrm{HSP}(\mathbf{A}) \to \mathrm{HSP}(\mathbf{B})$ is a categorical equivalence between the varieties generated by the algebras $\mathbf{A}$ and $\mathbf{B}$ such that $F(\mathbf{A}) = \mathbf{B}$, then the restriction of F to $\mathrm{SP}_{\mathrm{fin}}(\mathbf{A})$ gives an isomorphism between the relational clones of $\mathbf{A}$ and $\mathbf{B}$, i.e., F is a bijection $F\colon \mathrm{SP}_{\mathrm{fin}}(\mathbf{A}) \to \mathrm{SP}_{\mathrm{fin}}(\mathbf{B})$ that commutes with direct products, diagonalizations and projections [3]. Conversely, every isomorphism between the relational clones $\mathrm{SP}_{\mathrm{fin}}(\mathbf{A})$ and $\mathrm{SP}_{\mathrm{fin}}(\mathbf{B})$ extends to a categorical equivalence of the varieties of $\mathbf{A}$ and $\mathbf{B}$ [4]. Therefore, $\mathbf{A} \equiv_c \mathbf{B}$ holds if and only if $\mathbf{A}$ and $\mathbf{B}$ have isomorphic relational clones. We summarize this characterization of categorical equivalence in the following theorem.

Theorem 2.1 ([3, 4])**.** *Let $\mathbf{A}$ and $\mathbf{B}$ be finite algebras, and let $F\colon \mathrm{HSP}(\mathbf{A}) \to \mathrm{HSP}(\mathbf{B})$ be a categorical equivalence with $F(\mathbf{A}) = \mathbf{B}$. Then F provides an isomorphism between the relational clones of $\mathbf{A}$ and $\mathbf{B}$, i.e., $F\colon \mathrm{SP}_{\mathrm{fin}}(\mathbf{A}) \to \mathrm{SP}_{\mathrm{fin}}(\mathbf{B})$ is a bijection, and the following hold:*

(i) *if $\rho \leq \mathbf{A}^k$ and $\sigma \leq \mathbf{A}^m$, then $F(\rho \times \sigma) = F(\rho) \times F(\sigma)$;*
(ii) *if $\rho \leq \mathbf{A}^k$ and ε is an equivalence relation on $\{1, \ldots, k\}$, then $F(\Delta_\varepsilon(\rho)) = \Delta_\varepsilon(F(\rho))$;*
(iii) *if $\rho \leq \mathbf{A}^k$ and $i_1, \ldots, i_m \in \{1, \ldots, k\}$, then $F\left(\mathrm{pr}_{i_1,\ldots,i_m}(\rho)\right) = \mathrm{pr}_{i_1,\ldots,i_m}(F(\rho))$.*

Conversely, if $\mathbf{A}$ and $\mathbf{B}$ are finite algebras and $F\colon \mathrm{SP}_{\mathrm{fin}}(\mathbf{A}) \to \mathrm{SP}_{\mathrm{fin}}(\mathbf{B})$ is a bijection satisfying the above three properties, then F extends to a categorical equivalence between $\mathrm{HSP}(\mathbf{A})$ and $\mathrm{HSP}(\mathbf{B})$ such that $F(\mathbf{A}) = \mathbf{B}$.

Note that the above theorem implies that a categorical equivalence functor witnessing $\mathbf{A} \equiv_c \mathbf{B}$ yields an isomorphism between the subalgebra lattices of $\mathbf{A}$ and $\mathbf{B}$, and the corresponding subalgebras are categorically equivalent. Similarly, categorically equivalent algebras have isomorphic congruence lattices, and the corresponding quotient algebras are categorically equivalent. Regarding automorphisms (endomorphisms) as binary invariant relations, we can also conclude that categorically equivalent algebras have isomorphic automorphism groups (endomorphism monoids).

Algebras $\mathbf{A}$ and $\mathbf{B}$ are said to be *term equivalent*, if they have the same clone of term operations (this requires, of course, that the two algebras have the same underlying set). In this case $\mathbf{A}$ and $\mathbf{B}$ are categorically equivalent by Theorem 2.1, since they have the very same relational clone. If $\mathbf{A}$ is term equivalent to an isomorphic copy of $\mathbf{B}$, then we say that $\mathbf{A}$ and $\mathbf{B}$ are *weakly isomorphic*. Weakly isomorphic algebras are necessarily categorically equivalent, and, in light of the above considerations, we can regard weak isomorphism as a trivial case of categorical equivalence.

3. Ideals under categorical equivalence

Let us now turn our attention to rings. Congruences of rings correspond to ideals, hence one can define the image $F(I)$ of an ideal $I \lhd \mathbf{R}$ under a categorical equivalence functor F. In this section we work out the technical details concerning the definition of $F(I)$, and we prove some auxiliary results about the behavior of ideals under

categorical equivalence. We will use properties (i), (ii) and (iii) of Theorem 2.1 without further mention.

For an arbitrary ring $\mathbf{R}$ and $I \lhd \mathbf{R}$, let ϑ_I denote the congruence relation of $\mathbf{R}$ that corresponds to I:

$$\vartheta_I := \left\{(a,b) \in R^2 \colon a - b \in I\right\} \leq \mathbf{R}^2.$$

If $F\colon \mathrm{HSP}(\mathbf{R}) \to \mathrm{HSP}(\mathbf{S})$ is a categorical equivalence such that $F(\mathbf{R}) = \mathbf{S}$, then $F(\vartheta_I) \leq \mathbf{S}^2$ is a congruence on $\mathbf{S}$, and we shall denote the ideal of $\mathbf{S}$ corresponding to $F(\vartheta_I)$ simply by $F(I)$. Now, if $\mathbf{T}$ is a subring of $\mathbf{R}$ containing I, then I is also an ideal of $\mathbf{T}$, hence one could interpret $F(I)$ as the ideal of $F(\mathbf{T})$ that corresponds to the congruence $F\left(\vartheta_I \cap T^2\right)$. However, since $F\left(\vartheta_I \cap T^2\right) = F(\vartheta_I) \cap F(T)^2$, we see that $F\left(\vartheta_I \cap T^2\right)$ is the restriction of $F(\vartheta_I)$ to $F(T)^2$, and this means that the ideal of $F(\mathbf{T})$ corresponding to the congruence $F\left(\vartheta_I \cap T^2\right)$ is the same as the ideal of $\mathbf{S}$ corresponding to the congruence $F(\vartheta_I)$. Thus the meaning of $F(I)$ does not depend on whether we regard I as an ideal of $\mathbf{R}$ or as an ideal of $\mathbf{T}$.

It is clear that F commutes with intersections and sums of ideals (it gives an isomorphism between the ideal lattices of $\mathbf{R}$ and $\mathbf{S}$), and similarly for subrings. In the following lemma we consider the intersection and sum of an ideal $I \lhd \mathbf{R}$ and a subring $\mathbf{T} \leq \mathbf{R}$. Clearly $I + T \leq \mathbf{R}$, but in general $I \cap T$ is neither an ideal nor a subring of $\mathbf{R}$. However, $I \cap T$ is an ideal of $\mathbf{T}$, hence $F(I \cap T)$ can be defined.

Lemma 3.1. *Let $\mathbf{R}$ and $\mathbf{S}$ be finite rings, and let $F\colon \mathrm{HSP}(\mathbf{R}) \to \mathrm{HSP}(\mathbf{S})$ be a categorical equivalence with $F(\mathbf{R}) = \mathbf{S}$. If $I \lhd \mathbf{R}$ and $\mathbf{T} \leq \mathbf{R}$, then*

$$F(I \cap T) = F(I) \cap F(T) \text{ and } F(I + T) = F(I) + F(T).$$

In particular, we have $F(\langle I\rangle_1) = \langle F(I)\rangle_1$.

Proof. As mentioned above, $I \cap T$ is understood as an ideal of $\mathbf{T}$, thus $F(I \cap T)$ is the ideal of $F(\mathbf{T})$ that corresponds to the congruence $F\left(\vartheta_I \cap T^2\right) = F(\vartheta_I) \cap F(T)^2$ of $F(\mathbf{T})$, and this ideal is clearly $F(I) \cap F(T)$.

For the second statement, we only need to observe that the subring $I + T$ consists of those elements x of $\mathbf{R}$ for which there exists $t \in T$ such that $x \vartheta_I t$. Thus $I + T$ can be expressed from the invariant relations $\vartheta_I \leq \mathbf{R}^2$ and $\mathbf{T} \leq \mathbf{R}$ using the relational clone operations: $I + T = \mathrm{pr}_1(\Delta_\varepsilon(\vartheta_I \times T))$, where ε is the equivalence relation on $\{1,2,3\}$ corresponding to the partition $\{\{1\},\{2,3\}\}$. Since F is an isomorphism of relational clones, it follows that

$$F(I + T) = F(\mathrm{pr}_1(\Delta_\varepsilon(\vartheta_I \times T))) = \mathrm{pr}_1(\Delta_\varepsilon(F(\vartheta_I) \times F(T))) = F(I) + F(T).$$

Setting $\mathbf{T} = \langle 1_{\mathbf{R}}\rangle_1$, we obtain

$$F(\langle I\rangle_1) = F(I + \langle 1_{\mathbf{R}}\rangle_1) = F(I) + F(\langle 1_{\mathbf{R}}\rangle_1) = F(I) + \langle 1_{\mathbf{S}}\rangle_1 = \langle F(I)\rangle_1,$$

because $F(\langle 1_{\mathbf{R}}\rangle_1) = \langle 1_{\mathbf{S}}\rangle_1$, as $\langle 1_{\mathbf{R}}\rangle_1$ and $\langle 1_{\mathbf{S}}\rangle_1$ are the smallest subrings of $\mathbf{R}$ and $\mathbf{S}$, respectively. □

Lemma 3.2. *Subrngs are exactly the ideals of subrings:*

$$\mathrm{Subrng}(\mathbf{R}) = \{I \subseteq R : \exists \mathbf{T} \leq \mathbf{R} \text{ such that } I \lhd \mathbf{T}\}.$$

Proof. It is straightforward to verify that if I is a subrng, then the subring generated by I is $\langle I\rangle_1 = I + \langle 1\rangle_1$, and I is an ideal of $\langle I\rangle_1$. Conversely, it is obvious that ideals of subrings are subrngs. □

Lemma 3.3. *Let $\mathbf{R}$ and $\mathbf{S}$ be finite p-rings, and let $F\colon \mathrm{HSP}(\mathbf{R}) \to \mathrm{HSP}(\mathbf{S})$ be a categorical equivalence with $F(\mathbf{R}) = \mathbf{S}$. Then F induces a lattice isomorphism from* $\mathrm{Subrng}(\mathbf{R})$ *to* $\mathrm{Subrng}(\mathbf{S})$

Proof. Lemma 3.2 implies that $F(I)$ is a subrng of $\mathbf{S}$ whenever I is a subrng of $\mathbf{R}$, since $I \lhd \mathbf{T} \leq \mathbf{R}$ implies that $F(I) \lhd F(\mathbf{T}) \leq F(\mathbf{R})$. Conversely, every subrng of $\mathbf{R}$ is the image of some subrng of $\mathbf{S}$ under F^{-1}. Thus F and F^{-1} induce maps between the sets $\mathrm{Subrng}(\mathbf{R})$ and $\mathrm{Subrng}(\mathbf{S})$, and these two maps are the inverses of

each other, thus both of them are bijections. It remains to prove that both maps are order-preserving. We prove it only for F; the proof for F^{-1} is similar.

Assume that $I, J \in \mathrm{Subrng}(\mathbf{R})$ and $I \subseteq J$. It is easy to see that the subrngs I and $\langle I\rangle_1 \cap J$ generate the same subring $\mathbf{T} \leq \mathbf{R}$, hence they both are ideals of the ring $\mathbf{T}$. Since $I \subseteq \langle I\rangle_1 \cap J$, we have $F(I) \subseteq F(\langle I\rangle_1 \cap J)$ and, in view of Lemma 3.1, $F(\langle I\rangle_1 \cap J) = F(\langle I\rangle_1) \cap F(J)$. Thus, $F(I) \subseteq F(J)$. □

Lemma 3.3 allows us to apply results of Korobkov [11, 12, 13] about rngs with isomorphic subrng lattices. In particular, in the next proposition we determine p-rings that are categorically equivalent to a Galois p-ring.

Proposition 3.4. *If a p-ring $\mathbf{R}$ is categorically equivalent to a Galois ring $\mathrm{GR}(p^n, m)$, then $\mathbf{R} \cong \mathrm{GR}(p^n, m)$.*

Proof. If $\mathbf{R}$ is categorically equivalent to $\mathrm{GR}(p^n, m)$, then Lemma 3.3 implies that $\mathrm{Subrng}(\mathbf{R}) \cong \mathrm{Subrng}(\mathrm{GR}(p^n, m))$. Theorem 4 of [12] then shows that $\mathbf{R} \cong \mathrm{GR}(p^n, m)$ if $n > 1$ and $m > 1$. If $n = 1$, then we have $\mathrm{GR}(p^n, m) = \mathrm{GF}(p^m)$, and if $m = 1$, then we have $\mathrm{GR}(p^n, m) = \mathbb{Z}_{p^n}$, and in both cases Theorem 1.4 gives $\mathbf{R} \cong \mathrm{GR}(p^n, m)$. □

In the following lemma we prove that categorical equivalences commute with commutators of ideals.

Lemma 3.5. *Let $\mathbf{R}$ and $\mathbf{S}$ be finite rings, and let $F\colon \mathrm{HSP}(\mathbf{R}) \to \mathrm{HSP}(\mathbf{S})$ be a categorical equivalence with $F(\mathbf{R}) = \mathbf{S}$. If I and J are ideals of $\mathbf{R}$, then $F([I, J]) = [F(I), F(J)]$, where $[I, J] = I \cdot J + J \cdot I$ is the commutator of the ideals I and J. In particular, if I is a nilpotent subrng of $\mathbf{R}$, then $F(I)$ is a nilpotent subrng of $\mathbf{S}$.*

Proof. The commutator of ideals corresponds to the commutator of congruences. For congruence modular varieties, the commutator is a categorical notion, as it is shown by the following characterization [6]. If ϑ, ψ and α are congruences of an algebra $\mathbf{A}$ belonging to a congruence modular variety $\mathcal{V}$, then $\alpha \geq [\vartheta, \psi]$ if and only if there exists $\mathbf{B} \in \mathcal{V}$, a surjective homomorphism $f\colon \mathbf{B} \to \mathbf{A}$ and congruences σ, τ on $\mathbf{B}$ such that

(1) $\sigma \vee f^{-1}(\alpha) \geq f^{-1}(\psi)$;
(2) $\tau \vee f^{-1}(\alpha) \geq f^{-1}(\vartheta)$;
(3) $f^{-1}(\alpha) \geq \sigma \wedge \tau$.

A categorical equivalence functor induces an isomorphism of congruence lattices of the corresponding algebras, and surjectivity of homomorphisms is also a categorical property [2, 15], hence the first statement of the lemma follows from the above characterization of the commutator. For the second claim, recall that if I is a subrng of $\mathbf{R}$, then I is an ideal of some subring $\mathbf{T} \leq \mathbf{R}$ by Lemma 3.2, hence $F(I)$ is an ideal of $F(\mathbf{T})$. Assuming $I^n = 0$ and viewing I^n as the n-fold commutator of I by itself, we see that $F(I)^n = 0$. □

Next we investigate the images of annihilators under categorical equivalence functors. Let us denote by $\mathrm{Ann}_{\mathbf{R}}(I)$ the two-sided annihilator of the ideal $I \lhd \mathbf{R}$, i.e., let $\mathrm{Ann}_{\mathbf{R}}(I) = \{r \in R\colon r \cdot I = 0 \text{ and } I \cdot r = 0\}$.

Lemma 3.6. *Let $\mathbf{R}$ and $\mathbf{S}$ be finite rings, and let $F\colon \mathrm{HSP}(\mathbf{R}) \to \mathrm{HSP}(\mathbf{S})$ be a categorical equivalence with $F(\mathbf{R}) = \mathbf{S}$. If I is an ideal of $\mathbf{R}$, then $F(\mathrm{Ann}_{\mathbf{R}}(I)) = \mathrm{Ann}_{\mathbf{S}}(F(I))$.*

Proof. This follows immediately from Lemma 3.5, since $\mathrm{Ann}_{\mathbf{R}}(I)$ is the join of all ideals $X \lhd \mathbf{R}$ satisfying $[X, I] = 0$. □

In our last two lemmas we consider the relationship between the size of an ideal and the subring generated by that ideal.

Lemma 3.7. *If $\mathbf{R}$ is a finite ring and $I \lhd \mathbf{R}$, then we have $|\langle I\rangle_1| = |I| \cdot \mathrm{char}(\mathbf{R}/I)$.*

Proof. Let us assume for notational simplicity that $\langle 1_{\mathbf{R}} \rangle_1 = \mathbb{Z}_c$, where $c = \operatorname{char}(\mathbf{R})$. Since $\langle I \rangle_1 = I + \langle 1_{\mathbf{R}} \rangle_1 = I + \mathbb{Z}_c$, the first isomorphism theorem yields $\langle I \rangle_1 / I \cong \mathbb{Z}_c / (I \cap \mathbb{Z}_c)$. The intersection $I \cap \mathbb{Z}_c$ is an ideal in $\mathbb{Z}_c$, thus it is of the form $d \cdot \mathbb{Z}_c$ for some divisor d of c, hence $\langle I \rangle_1 / I \cong \mathbb{Z}_c / (d \cdot \mathbb{Z}_c) \cong \mathbb{Z}_d$. It remains to verify that $\operatorname{char}(\mathbf{R}/I) = d$, but this is clear: for every positive integer m, we have

$$m \cdot 1_{\mathbf{R}} \in I \iff m \cdot 1_{\mathbf{R}} \in d \cdot \mathbb{Z}_c \iff d \mid m. \qquad \square$$

Lemma 3.8. *Let $\mathbf{R}$ and $\mathbf{S}$ be finite p-rings for some prime number p, and let us assume that $F\colon \operatorname{HSP}(\mathbf{R}) \to \operatorname{HSP}(\mathbf{S})$ is a categorical equivalence with $F(\mathbf{R}) = \mathbf{S}$. If $I \lhd \mathbf{R}$, then $|F(\langle I \rangle_1)| = |F(I)| \cdot \operatorname{char}(\mathbf{R}/I)$.*

Proof. By Lemma 3.1, we have $F(\langle I \rangle_1) = \langle F(I) \rangle_1$, and Lemma 3.7 gives $|\langle F(I) \rangle_1| = |F(I)| \cdot \operatorname{char}(\mathbf{S}/F(I))$. The rings $\mathbf{S}/F(I) = F(\mathbf{R})/F(I) = F(\mathbf{R}/I)$ and $\mathbf{R}/I$ are categorically equivalent p-rings, hence they have the same characteristic by Theorem 1.2, and this completes the proof. $\square$

4. Additive groups of categorically equivalent p-rings

In this section we prove the main result of the paper: categorically equivalent finite p-rings have isomorphic additive groups. The key step is to verify that $\mathbf{R} \equiv_c \mathbf{S}$ implies $|R| = |S|$ for arbitrary finite p-rings $\mathbf{R}$ and $\mathbf{S}$. We will prove this by induction on the size of $\mathbf{R}$, namely we will apply the induction hypothesis to the rings $\langle I \rangle_1$ and $\mathbf{R}/I$ for a suitably chosen ideal $I \lhd \mathbf{R}$. For this we need that both $\langle I \rangle_1$ and $\mathbf{R}/I$ are strictly smaller than $\mathbf{R}$, i.e., $\langle I \rangle_1 \neq \mathbf{R}$ and $I \neq 0$. Such an ideal need not always exist, so our first task is to compile the list of those "bad" rings for which there is no such ideal. We shall do this in Proposition 4.2, whose proof requires the following technical lemma proof of which we will leave to the reader.

Lemma 4.1. *If I is an ideal of the ring $\mathbf{R}$ such that $I^2 = 0$ and $\langle I \rangle_1 = \mathbf{R}$, then every additive subgroup of I is an ideal of $\mathbf{R}$.*

Proposition 4.2. *For every finite ring $\mathbf{R}$, the following two conditions are equivalent:*

(i) *for every nonzero ideal $I \lhd \mathbf{R}$, we have $\langle I \rangle_1 = \mathbf{R}$;*
(ii) *$\mathbf{R}$ is either simple (i.e., isomorphic to a full matrix ring over a finite field) or cyclic (i.e., isomorphic to $\mathbb{Z}_m$ for some positive integer m) or $\mathbf{R}$ has size p^2 for some prime number p (i.e., isomorphic to one of the rings $\mathbb{Z}_{p^2}$, $\mathrm{GF}(p^2)$, $\mathbb{Z}_p \times \mathbb{Z}_p$, $\mathbb{Z}_p[x]/(x^2)$ by [5]).*

Proof. It is easy to check that (ii) implies (i). For the other implication, we consider an arbitrary finite ring $\mathbf{R}$, and we prove that it has a nonzero ideal I with $\langle I \rangle_1 \neq \mathbf{R}$ unless $\mathbf{R}$ is isomorphic to one of the rings listed in (ii).

Assume first that $\mathbf{R}$ is directly decomposable: $\mathbf{R} = \mathbf{R}_1 \times \mathbf{R}_2$, where $\mathbf{R}_1$ and $\mathbf{R}_2$ are nontrivial rings. If $\mathbf{R}_1 \neq \langle 1_{\mathbf{R}_1} \rangle_1$, then $I = 0_{\mathbf{R}_1} \times \mathbf{R}_2$ is a nonzero ideal of $\mathbf{R}$ with $\langle I \rangle_1 \neq \mathbf{R}$, since I is contained in the subring $\langle 1_{\mathbf{R}_1} \rangle_1 \times \mathbf{R}_2 < \mathbf{R}$. A similar argument works if $\mathbf{R}_2 \neq \langle 1_{\mathbf{R}_2} \rangle_1$. If $\mathbf{R}_1 = \langle 1_{\mathbf{R}_1} \rangle_1$ and $\mathbf{R}_2 = \langle 1_{\mathbf{R}_2} \rangle_1$, then $\mathbf{R} \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ for some integers $m_1, m_2 \geq 2$. If m_1 and m_2 have a common prime divisor p, then the ideal $I = p \cdot \mathbb{Z}_{m_1} \times p \cdot \mathbb{Z}_{m_2}$ satisfies $\langle I \rangle_1 \neq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$, since for every $(a_1, a_2) \in \langle I \rangle_1$ we have $a_1 \equiv a_2 \pmod{p}$. Moreover, if at least one of m_1 and m_2 is different from p, then $I \neq 0$ (otherwise we have $\mathbf{R} \cong \mathbb{Z}_p \times \mathbb{Z}_p$). Finally, if $\mathbf{R} \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$, where m_1 and m_2 are relatively prime, then $\mathbf{R} \cong \mathbb{Z}_{m_1 m_2}$.

From now on we assume that $\mathbf{R}$ is directly indecomposable; in particular, $\mathbf{R}$ is a p-ring for some prime p, hence $\operatorname{char}(\mathbf{R}) = p^n$ for some positive integer n. We deal with the cases $n \geq 2$ and $n = 1$ separately.

If $n \geq 2$, then we let I be the principal ideal $I = p^{n-1} \cdot \mathbf{R}$. Since $n \geq 2$, we have $I^2 = p^{2n-2} \cdot \mathbf{R} = 0$. Then the conditions of Lemma 4.1 are satisfied, therefore for every additive subgroup A of I, we have $A \lhd \mathbf{R}$. In particular, $A = p^{n-1} \cdot \langle 1_{\mathbf{R}} \rangle$ is an ideal of $\mathbf{R}$. But then $\mathbf{R} = \langle A \rangle_1 = \langle 1_{\mathbf{R}} \rangle_1$, that is, $\mathbf{R} \cong \mathbb{Z}_{p^n}$.

Let now $n = 1$ and suppose first that $\mathbf{R}$ is semisimple. Then, due to direct indecomposability, it is simple and we are done. Let now $\mathbf{R}$ be non-semisimple. Then it

has a nonzero nilpotent ideal, hence also a nonzero ideal I with zero multiplication. By Lemma 4.1, we may take I of cardinality p. Since $R = I + \langle 1_{\mathbf{R}} \rangle_1$, we conclude $|R| \leq p^2$. This proves the proposition. □

Now we are ready to perform the induction argument outlined at the beginning of this section. Luckily, rings categorically equivalent to any of the "bad" rings listed in item (ii) of the above proposition have been completely determined in [9] (see Theorem 1.4).

Theorem 4.3. *If* $\mathbf{R}$ *and* $\mathbf{S}$ *are finite categorically equivalent p-rings, then* $|\mathbf{R}| = |\mathbf{S}|$.

Proof. We prove the theorem by induction on the size of $\mathbf{R}$. If $|\mathbf{R}| = p$, then $\mathbf{R} \cong \mathbb{Z}_p$, and then $\mathbf{S} \cong \mathbb{Z}_p$ follows from Theorem 1.4.

Now let $|\mathbf{R}| > p$, and assume that the theorem holds for all p-rings of size less than $|\mathbf{R}|$. Let $F\colon \mathrm{HSP}(\mathbf{R}) \to \mathrm{HSP}(\mathbf{S})$ be a categorical equivalence with $F(\mathbf{R}) = \mathbf{S}$. If $\mathbf{R}$ is one of the rings listed in item (ii) of Proposition 4.2, then we can use again Theorem 1.4 to see that $\mathbf{R} \cong \mathbf{S}$. Otherwise $\mathbf{R}$ has a nonzero ideal I such that $\langle I \rangle_1 \neq \mathbf{R}$. Then both $\mathbf{R}/I$ and $\langle I \rangle_1$ are p-rings that are smaller than $\mathbf{R}$, so the induction hypothesis implies that $|\mathbf{R}/I| = |F(\mathbf{R}/I)|$ and $|\langle I \rangle_1| = |F(\langle I \rangle_1)|$. The first equality shows that $|\mathbf{R}/I| = |F(\mathbf{R})/F(I)| = |\mathbf{S}/F(I)|$. The second equality together with Lemmas 3.7 and 3.8 yields

$$|I| \cdot \mathrm{char}(\mathbf{R}/I) = |\langle I \rangle_1| = |F(\langle I \rangle_1)| = |F(I)| \cdot \mathrm{char}(\mathbf{R}/I),$$

from which $|I| = |F(I)|$ follows. Now we can conclude that $|\mathbf{R}| = |\mathbf{R}/I| \cdot |I| = |\mathbf{S}/F(I)| \cdot |F(I)| = |\mathbf{S}|$. □

Corollary 4.4. *If* $\mathbf{R}$ *and* $\mathbf{S}$ *are finite p-rings and* $F\colon \mathrm{HSP}(\mathbf{R}) \to \mathrm{HSP}(\mathbf{S})$ *is a categorical equivalence with* $F(\mathbf{R}) = \mathbf{S}$*, then we have* $|F(I)| = |I|$ *for all subrngs (in particular, for all ideals)* I *of* $\mathbf{R}$.

Proof. First, let $I \lhd \mathbf{R}$. Then:

$$|F(I)| = \frac{|F(\mathbf{R})|}{|F(\mathbf{R})/F(I)|} = \frac{|F(\mathbf{R})|}{|F(\mathbf{R}/I)|} = \frac{|\mathbf{R}|}{|\mathbf{R}/I|} = |I|. \qquad \square$$

The general case now follows from Lemma 3.2.

For proving one of the central results of the present paper we need the following lemma.

Lemma 4.5. *Let* A *be a finite abelian group of exponent* p^n*. Then the sizes of subgroups* $p^k \cdot A$ *(*$k = 1, \ldots, n$*) determine the group* A *up to isomorphism.*

Proof. This fact should be well known but since we could not find a good reference, we provide a hint of proof. Let $p^{a_k} = \left|p^{k-1} \cdot A\right|$ and let b_k be the number cyclic direct summands of order p^k in the canonical decomposition of A, $k = 1, \ldots, n$. Then it is easy to see that

$$a_k = b_k + 2b_{k+1} + \cdots + (n-k+1)b_n, \qquad (k = 1, \ldots, n).$$

Obviously, this system of linear equations uniquely determines the integers $b_1, \ldots, b_n$. □

Theorem 4.6. *If* $\mathbf{R}$ *and* $\mathbf{S}$ *are finite categorically equivalent p-rings, then* $\mathbf{R}$ *and* $\mathbf{S}$ *have isomorphic additive groups.*

Proof. Assume that $F\colon \mathrm{HSP}(\mathbf{R}) \to \mathrm{HSP}(\mathbf{S})$ is a categorical equivalence functor that maps $\mathbf{R}$ to $\mathbf{S}$. Then $\mathbf{R}$ and $\mathbf{S}$ have the same characteristic by Theorem 1.2: let $\mathrm{char}\,\mathbf{R} = \mathrm{char}\,\mathbf{S} = p^n$.

One can characterize $p^k \cdot R$ by the property that it is the least ideal $I \lhd \mathbf{R}$ such that the characteristic of $\mathbf{R}/I$ is at most p^k (cf. the proof of Lemma 3.7). Since F preserves quotients and characteristics (by Theorem 1.2), we have that $F\left(p^k \cdot R\right)$ is the least ideal of $\mathbf{S}$ such that the characteristic of the corresponding quotient ring is at most p^k, hence $F\left(p^k \cdot R\right) = p^k \cdot S$. Thus, in view of Corollary 4.4, we have $\left|p^k \cdot R\right| = \left|p^k \cdot S\right|$. It remains to apply Lemma 4.5. □

5. Rings of order p^3

In [9] we described categorical equivalence for rings of order p^2. The next step is naturally the case of rings of order p^3. By Theorem 4.3, if $|R| = p^3$ and $\mathbf{R} \equiv_c \mathbf{S}$, then $|S| = p^3$, therefore it suffices to determine categorical equivalences among rings of order p^3. Let us recall the list of these rings from [16].

Theorem 5.1 ([16])**.** *For every odd prime p, there are* 12 *rings with identity of size p^3, and there are* 11 *rings with identity of size 2^3 up to isomorphism (type* (xii) *is missing in the case $p = 2$, since there is no quadratic nonresidue modulo* 2*):*

(i) $\mathbf{R}_1 = \mathbb{Z}_{p^3}$;

(ii) $\mathbf{R}_2 = \mathrm{GF}(p^3)$;

(iii) $\mathbf{R}_3 = \mathbb{Z}_{p^2} \times \mathbb{Z}_p$;

(iv) $\mathbf{R}_4 = \mathrm{GF}(p^2) \times \mathbb{Z}_p$;

(v) $\mathbf{R}_5 = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$;

(vi) $\mathbf{R}_6 = \mathbb{Z}_p \times \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{Z}_p \right\}$;

(vii) $\mathbf{R}_7 = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} : a, b, c \in \mathbb{Z}_p \right\}$;

(viii) $\mathbf{R}_8 = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} : a, b, c \in \mathbb{Z}_p \right\}$;

(ix) $\mathbf{R}_9 = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z}_p \right\}$ *(this is the only noncommutative one);*

(x) $\mathbf{R}_{10} = \mathbb{Z}_{p^2}[x] / (x^2, px)$;

(xi) $\mathbf{R}_{11} = \mathbb{Z}_{p^2}[x] / (x^2 - up, px)$, *where $u \in \mathbb{Z}_p^*$ is a quadratic residue modulo p;*

(xii) $\mathbf{R}_{12} = \mathbb{Z}_{p^2}[x] / (x^2 - up, px)$, *where $u \in \mathbb{Z}_p^*$ is a quadratic nonresidue modulo p.*

Remark 5.2. The rings $\mathbf{R}_7$ and $\mathbf{R}_8$ can be given by polynomials as follows:

$$\mathbf{R}_7 \cong \mathbb{Z}_p[x] / (x^3), \quad \mathbf{R}_8 \cong \mathbb{Z}_p[x, y] / (x^2, y^2, xy, yx).$$

Lemma 5.3. *The only nontrivial categorical equivalences between rings of size p^3 can be between rings of types* (xi) *and* (xii)*.*

Proof. Taking direct decompositions, Theorem 1.2 and Theorem 1.4 into account, we see that the only possible categorical equivalences can be within the sets $\{\mathbf{R}_7, \mathbf{R}_8, \mathbf{R}_9\}$ and $\{\mathbf{R}_{10}, \mathbf{R}_{11}, \mathbf{R}_{12}\}$.

We show, by comparing their radicals, that the three rings in the first set cannot be categorically equivalent. By Corollary 12 of [9] and by Corollary 4.4, the radicals of categorically equivalent finite p-rings must have the same size. It is easy to see that the radicals of the rings $\mathbf{R}_7, \mathbf{R}_8$ and $\mathbf{R}_9$ consist precisely of matrices

$$\begin{pmatrix} 0 & b & c \\ 0 & 0 & b \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & b & c \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \quad (b, c \in \mathbb{Z}_p),$$

respectively. Hence, neither $\mathbf{R}_7$ nor $\mathbf{R}_8$ can be categorically equivalent to $\mathbf{R}_9$. That $\mathbf{R}_7$ and $\mathbf{R}_8$ are not categorically equivalent, follows from Lemma 3.6. Indeed, the radical of $\mathbf{R}_8$ is square-zero, i.e., it annihilates itself while the radical of $\mathbf{R}_7$ is not.

Also, we can see that neither $\mathbf{R}_{11}$ nor $\mathbf{R}_{12}$ can be categorically equivalent to $\mathbf{R}_{10}$, by looking at the ideal lattices. Let us write $\mathbf{R}_{11}$ and $\mathbf{R}_{12}$ as $\{a + b\vartheta : a \in \mathbb{Z}_{p^2}, b \in \mathbb{Z}_p\}$,

where $p\vartheta = 0$ and $\vartheta^2 = pu$. The ideal lattices of these rings are four-element chains regardless of the value of u (as long as u is not congruent to 0 modulo p):

$$(0) \subset \left(\vartheta^2\right) = (p) \subset (\vartheta) \subset (1).$$

On the other hand, the ideal lattice of $\mathbf{R}_{10}$ is not a chain. Indeed, we can represent $\mathbf{R}_{10}$ in the form $\mathbf{R}_{10} = \left\{a + b\varepsilon : a \in \mathbb{Z}_{p^2}, b \in \mathbb{Z}_p\right\}$ with $\varepsilon^2 = p\varepsilon = 0$, and, for instance, the ideals (p) and (ε) are incomparable. □

Next we prove that $\mathbf{R}_{11} \equiv_c \mathbf{R}_{12}$ for every odd prime p. In fact, we shall see that these two rings are weakly isomorphic. Using the notation introduced in the proof of the previous lemma, let $\mathbf{R}_u = \left\{a + b\vartheta : a \in \mathbb{Z}_{p^2}, b \in \mathbb{Z}_p\right\}$ with $p\vartheta = 0$ and $\vartheta^2 = pu$, where $u \in \mathbb{Z}_p^*$. Thus the multiplication of $\mathbf{R}_u$ is given by

$$(a + b\vartheta) \cdot (c + d\vartheta) = (ac + pubd) + (ad + bc)\vartheta.$$

We need to prove that $\mathbf{R}_u$ and $\mathbf{R}_v$ are term equivalent for all $u, v \in \mathbb{Z}_p^*$ (we will not use the fact that the rings $\mathbf{R}_u$ can fall into only two isomorphism classes depending on the quadratic character of u modulo p). Since the addition operations of the two rings are the same, it suffices to express the multiplication of one ring as a term operation of the other.

Lemma 5.4. *Let $f(x) = (x^p - x)^2$. Then $f(a + b\vartheta) = pub^2$ for all $a + b\vartheta \in \mathbf{R}_u$.*

Proof. From $p\vartheta = 0$ and $\vartheta^2 = pu$ it follows that $\vartheta^3 = \vartheta pu = 0$. Therefore, we can ignore all terms involving ϑ^i $(i \geq 3)$ from the binomial expansion of $(a + b\vartheta)^p$:

$$(a + b\vartheta)^p = a^p + p \cdot a^{p-1}b\vartheta + p \cdot \frac{p-1}{2} \cdot a^{p-2}b^2\vartheta^2.$$

The last two terms also disappear, since $p\vartheta = 0$, hence we have $(a + b\vartheta)^p = a^p$. Now we can compute $f(a + b\vartheta)$:

$$f(a + b\vartheta) = ((a^p - a) - b\vartheta)^2 = (a^p - a)^2 - 2(a^p - a)b\vartheta + b^2\vartheta^2.$$

By Fermat's theorem, $a^p - a$ is divisible by p, so $(a^p - a)^2 \equiv 0 \pmod{p^2}$ and $(a^p - a)\vartheta = 0$ (as $p\vartheta = 0$). We can conclude that $f(a + b\vartheta) = b^2\vartheta^2 = pub^2$. □

Theorem 5.5. *The rings $\mathbf{R}_u$ and $\mathbf{R}_v$ are term equivalent for all $u, v \in \mathbb{Z}_p^*$.*

Proof. As noted above, it suffices to represent the multiplication of $\mathbf{R}_v$ by a term operation of $\mathbf{R}_u$, i.e., we need to find a binary term $t(x, y)$ of $\mathbf{R}_u$ such that

$$t(a + b\vartheta, c + d\vartheta) = (ac + pvbd) + (ad + bc)\vartheta.$$

Let $g(x, y) = 2^{-1} \cdot (f(x + y) - f(x) - f(y))$, where 2^{-1} denotes the multiplicative inverse of 2 modulo p (e.g., one can put $2^{-1} = (p + 1)/2$). Using Lemma 5.4, we obtain

$$g(a + b\vartheta, c + d\vartheta) = 2^{-1} \cdot \left(pu(b + d)^2 - pub^2 - pud^2\right) = 2^{-1} \cdot pu \cdot 2bd = pubd.$$

Now let $t(x, y) = xy + \left(u^{-1}v - 1\right) \cdot g(x, y)$ where u^{-1} is the multiplicative inverse of u modulo p. By the above calculations, we have

$$\begin{aligned} t(a + b\vartheta, c + d\vartheta) &= (ac + pubd) + (ad + bc)\vartheta + \left(u^{-1}v - 1\right) \cdot pubd \\ &= (ac + pvbd) + (ad + bc)\vartheta. \end{aligned}$$

□

Corollary 5.6. *If $\mathbf{R}$ is a ring of order p^3 and $\mathbf{S}$ is a finite p-ring, then $\mathbf{R} \equiv_c \mathbf{S}$ if and only if either $\mathbf{R} \cong \mathbf{S}$ or $\mathbf{R} \cong \mathbb{Z}_{p^2}[x] / \left(x^2 - up, px\right)$ and $\mathbf{S} \cong \mathbb{Z}_{p^2}[x] / \left(x^2 - vp, px\right)$, where one of $u, v \in \mathbb{Z}_p^*$ is a quadratic residue modulo p and the other one is a quadratic nonresidue.*

6. The number of generators

In this section we prove that the number of generators is a categorical invariant in case of finite rings, i.e., if $\mathbf{R} \equiv_c \mathbf{S}$ and $\mathbf{R}$ is n-generated for some natural number n then $\mathbf{S}$ is n-generated, too. The crucial part of the proof is to handle the case $n = 1$, i.e., to show that "one-generatedness" is a categorical property for finite rings. We say that $\mathbf{R}$ is one-generated if there exists an element $r \in R$ such that $\mathbf{R} = \langle r \rangle_1$. Observe that a finite ring is one-generated if and only if its p-components are one-generated, therefore we can assume without loss of generality that $\mathbf{R}$ is a p-ring. We will build on studies of Korobkov [13] about one-generated rings; however, the definition of one-generatedness in [13] is different from ours: it requires the existence of an element $r \in R$ with $\mathbf{R} = \langle r \rangle$. Nevertheless, only minor modifications are needed in order to adapt the results of [13] to our situation.

Given any (universal) algebra $\mathbf{A}$, let $\Phi(\mathbf{A})$ be its *Frattini subalgebra*, that is, the intersection of all maximal subalgebras of $\mathbf{A}$. As usually, if $\mathbf{A}$ has no maximal subalgebras then $\Phi(\mathbf{A}) = \mathbf{A}$. It is well known that the elements of $\Phi(\mathbf{A})$ are the *non-generators* of $\mathbf{A}$, that is, such elements $a \in A$ that can be removed from any generating set of $\mathbf{A}$. In what follows, the Frattini subr(i)ng $\Phi(\mathbf{R})$ of a r(i)ng $\mathbf{R}$ is the intersection of all maximal subr(i)ngs of $\mathbf{R}$. However, we warn the reader that the same term has been used in a different meaning, as the name of the intersection of all maximal right ideals of a given r(i)ng.

We start with a very useful lemma that for rngs was proved in [13]. Only minor modifications are needed in the ring case.

Lemma 6.1. *If $\mathbf{R}$ is a finite p-r(i)ng then $pR \subseteq \Phi(\mathbf{R})$.*

Corollary 6.2. *A finite p-ring $\mathbf{R}$ is one-generated if and only if the quotient ring $\mathbf{R}/pR$ is one-generated.*

Let $\mathbf{R}$ be a finite ring of characteristic p with radical J. Then $\mathbf{R}$ is a finite dimensional algebra over $\mathrm{GF}(p)$, hence Wedderburn's theorem [7] applies. Therefore $\mathbf{R}$ contains a subring $\mathbf{G}$ such that $R = G \oplus J$ (direct sum of additive subgroups). Clearly $\mathbf{G} \cong \mathbf{R}/J$ and actually $\mathbf{G}$ is a maximal semisimple subring of $\mathbf{R}$. Obviously, if $\mathbf{R}$ is commutative then $\mathbf{G}$ is a direct sum of fields. Moreover, if $\mathbf{R}$ is commutative and local then $\mathbf{G}$ is a field.

Lemma 6.3. *Let $\mathbf{R}$ be a finite commutative local ring of characteristic p, let J be its radical and let $\mathbf{G}$ be a maximal semisimple subring of $\mathbf{R}$. Then the following are equivalent:*

1. *the ring $\mathbf{R}$ is one-generated;*
2. *J is a principal ideal of $\mathbf{R}$;*
3. *there is a nilpotent element $r \in R$ such that $\mathbf{R} = \langle G, r \rangle_1$ (equivalently, $\mathbf{R} = \langle G, \langle r \rangle \rangle_1$).*

Proof. (1) $\Rightarrow$ (2) Let $e \in G$ and $r \in J$ be such that $e + r$ generates the ring $\mathbf{R}$. Then, given any $s \in J$ there exists a polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(e + r) = s$. Since $\mathbf{R}$ is commutative, $s = f(e + r) = f(e) + s'$ where $s' \in (r)$. Since, $f(e) \in G$ and $s, s' \in J$, we conclude $s = s' \in (r)$. Thus, J is a principal ideal of $\mathbf{R}$ generated by r.

(2) $\Rightarrow$ (3) This is obvious because $R = G \oplus J$ and J is nilpotent.

(3) $\Rightarrow$ (1) Assume that $\mathbf{R} = \langle G, r \rangle_1$ where r is nilpotent. Note that in our situation $\mathbf{G}$ is a Galois field, hence it is one-generated. Let $e \in G$ be a generator for $\mathbf{G}$. Since $\mathrm{char}(\mathbf{R}) = p$ and the ring $\mathbf{R}$ is commutative, the mapping $x \mapsto x^p$ is an endomorphism of $\mathbf{R}$. Obviously, the restriction of this mapping to G is an automorphism of $\mathbf{G}$, thus, there is a positive integer k such that the k'th power of it is the identity mapping on G, in particular, $e^{p^k} = e$. We may choose k big enough to have $r^{p^k} = 0$. Then $e = (e + r)^{p^k} \in \langle e + r \rangle_1$ and also $r = e + r - e \in \langle e + r \rangle_1$. But then $\langle G, r \rangle_1 = \langle e, r \rangle_1 \subseteq \langle e + r \rangle_1$, hence $e + r$ generates the ring $\mathbf{R}$. □

Now we state a lemma about nilpotent rngs, which is mentioned as a remark and applied in [11]. For the sake of self-containedness, we include the proof of this lemma.

Lemma 6.4. *Let R and S be finite p-rngs with isomorphic subrng lattices. If there is a nilpotent element $r \in R$ such that $R = \langle r \rangle$, then there is an element $s \in S$ such that $S = \langle s \rangle$.*

Proof. If M is the Frattini subrng of R, then $M = R^2 + pR$ (see [14]). Clearly, M is an ideal of R, and R/M is a rng of characteristic p with zero multiplication. If $R = \langle r \rangle$, then $R/M = \langle r + M \rangle$, hence the additive group of R/M is cyclic; in fact, it must be a cyclic group of order p, as the characteristic of R/M is p. Thus M is a subrng of index p, therefore it is a maximal subrng. Since M is the intersection of all maximal subrngs, it follows that M is the only maximal subrng of R. Now since $\mathrm{Subrng}\,(R) \cong \mathrm{Subrng}\,(S)$, the rng S has a unique maximal subrng, and obviously $S = \langle s \rangle$ holds for every element s outside of this maximal subrng. □

Theorem 6.5. *Let $\mathbf{R}$ and $\mathbf{S}$ be finite categorically equivalent rings of characteristic p. If $\mathbf{R}$ is local and one-generated then $\mathbf{R} \cong \mathbf{S}$.*

Proof. Assume that $\mathbf{R}$ is local and one-generated. Since, $\mathbf{R}$ is one-generated, it is commutative. Thus, by Lemma 6.3, $\mathbf{R}$ is generated by a Galois subfield $\mathbf{G}$ and a subrng $\langle r \rangle$ where r is a nilpotent element of $\mathbf{R}$.

Let F be a categorical equivalence such that $F(\mathbf{R}) = \mathbf{S}$. Then by Lemma 3.3, $F(\mathbf{R})$ is generated by $F(\mathbf{G})$ and the subrng $F(\langle r \rangle)$. Note that by [1], $\mathbf{G} \cong F(\mathbf{G})$. By Lemma 3.3, the subrng lattices of rngs $\langle r \rangle$ and $F(\langle r \rangle)$ are isomorphic, thus by Lemma 6.4, there is $s \in S$ such that $F(\langle r \rangle) = \langle s \rangle$. Since $\mathbf{R}$ is commutative, the ideal (r) is nilpotent, thus contained in the radical of $\mathbf{R}$. Since F maps the radical of $\mathbf{R}$ to the radical of $\mathbf{S}$ and the radical of a finite ring is nilpotent, it follows that s is nilpotent.

Our next step is to prove that the ring $\mathbf{S}$ is commutative. Here we actually repeat Korobkov's argument in his proof of [13], Lemma 15. The ring $\mathbf{S}$ is obviously commutative if $r = 0$ or $\mathbf{G} = \mathrm{GF}(p)$. Thus, assume that $r \neq 0$ and $\mathbf{G} = \mathrm{GF}(p^m)$ where $m > 1$. Let first m be a prime power. Then $\mathbf{R}$ is the ring of type $\mathbf{R}_{14}$ from Theorem 3 of [10]. Hence, $\mathbf{R}$ has exactly two maximal subrngs (which actually are subrings). Then, by Lemma 3.3, $\mathbf{S}$ also has exactly two maximal subrngs which implies that $\mathbf{S}$ is one-generated, hence commutative. (Indeed, if the maximal subrings are $\mathbf{M}_1$ and $\mathbf{M}_2$, then for any $m_1 \in M_1 \setminus M_2$, $m_2 \in M_2 \setminus M_1$we have $m_1 + m_2 \notin M_1 \cup M_2$, hence $m_1 + m_2$ generates $\mathbf{R}$.)

Assume now that m is not a prime power. Then m is a product of prime powers $m_1, \ldots, m_k$ $(k > 1)$, for different primes, which implies that the ring $\mathbf{G}$ is generated by subfields $\mathbf{G}_i = \mathrm{GF}(p^{m_i})$ $(i = 1, \ldots, k)$. It follows that the set $X = G_1 \cup \cdots \cup G_k \cup \{s\}$ generates the ring $\mathbf{S}$. Thus, in order to prove commutativity of $\mathbf{S}$, it suffices to prove that arbitrary $x, y \in X$ permute. There are three possiblities: 1) if $x = y = s$ then obviously $xy = yx$, 2) if $x, y \in G_1 \cup \cdots \cup G_k$ then $xy = yx$ because $G_1 \cup \cdots \cup G_k$ is contained in the field $\mathbf{G}$, 3) if $x \in G_i$ for some i and $y = s$ then $xy = yx$ because the ring $\langle G_i, s \rangle$ is commutative by the previous part of the proof.

We have proved that $\mathbf{S}$ is commutative and generated by a Galois subfield and a nilpotent element. Thus, by Lemma 6.3 $\mathbf{S}$ is one-generated. It remains to observe that the rings $\mathbf{R}$ and $\mathbf{S}$ are isomorphic. Obviously, if $r^u = 0$ but $r^{u-1} \neq 0$ then $\mathbf{R} \cong \mathbf{G}[x]/(x^u)$. Similarly, if $s^v = 0$ but $s^{v-1} \neq 0$ then $\mathbf{S} \cong \mathbf{G}[x]/(x^v)$. Since by Theorem 4.3 $\mathbf{R}$ and $\mathbf{S}$ are of same size, we conclude $u = v$, hence $\mathbf{R} \cong \mathbf{S}$. □

Corollary 6.6. *Let $\mathbf{R}$ and $\mathbf{S}$ be finite categorically equivalent rings of characteristic p. If $\mathbf{R}$ is one-generated then $\mathbf{R} \cong \mathbf{S}$.*

Proof. This follows from the well-known fact that every finite commutative ring is isomorphic to a direct product of local rings. □

Corollary 6.7. *Let $\mathbf{R}$ and $\mathbf{S}$ be finite categorically equivalent p-rings. If $\mathbf{R}$ is one-generated then $\mathbf{S}$ is one-generated, too.*

Proof. If $\mathbf{R}$ is one-generated then so is $\mathbf{R}/pR$. The pR is the smallest ideal $I \lhd \mathbf{R}$ with the property that $\mathbf{R}/I$ is of characteristic p. Therefore $\mathbf{R} \equiv_c \mathbf{S}$ implies $\mathbf{R}/pR \equiv_c \mathbf{S}/pS$. Now Corollary 6.2 yields that $\mathbf{S}$ is one-generated. □

Corollary 6.8. *Let* $\mathbf{R}$ *and* $\mathbf{S}$ *be finite categorically equivalent p-rings. If* $\mathbf{R}$ *is n-generated then* $\mathbf{S}$ *is n-generated, too.*

Proof. Suppose $\mathbf{R}$ is n-generated. Then $\mathbf{R}$ has one-generated subrings $\mathbf{R}_1, \dots, \mathbf{R}_n$ such that $R = \langle R_1, \dots, R_n \rangle_1$. Let F be a categorical equivalence functor that takes $\mathbf{R}$ to $\mathbf{S}$ and let $F(\mathbf{R}_i) = \mathbf{S}_i$ $(i = 1, \dots, n)$. Then $\mathbf{S} = \langle S_1, \dots, S_n \rangle_1$. By Corollary 6.7, the rings $\mathbf{S}_1, \dots, \mathbf{S}_n$ are one-generated, hence the ring $\mathbf{S}$ is n-generated. □

Corollary 6.9. *Let* $\mathbf{R}$ *and* $\mathbf{S}$ *be finite categorically equivalent p-rings. If* $\mathbf{R}$ *is free in the variety it generates then* $\mathbf{S}$ *is free in the variety it generates, too.*

Proof. This follows from Corollary 6.8, Theorem 4.3 and the fact that in every finitely generated variety the free algebra in n generators is the largest n-generated algebra of that variety. □

7. Concluding remarks

Our results show that in the class of finite p-rings (for fixed p) the categorically equivalent rings have very similar structure though they need not be isomorphic. We conjecture that finite categorically equivalent p-rings are necessarily weakly isomorphic. Another important open question is whether the commutativity of finite rings is a categorical property. We plan to attack these problems in our further research work.

Acknowledgments

The authors would like to thank Gábor Czédli, Mária Szendrei, László Zádori and Gergő Gyenizse for helpful discussions. The research of the first author was partially supported by institutional research funding IUT20-57 of the Estonian Ministry of Education and Research and also by the Estonian Research Council grant PUT1519. The research of the second author was partially supported by the Hungarian Research, Development and Innovation Office grant K115518, and by grants 20391-3/2018/FEKUSTRAT and TUDFO/47138-1/2019-ITM of the Ministry for Innovation and Technology, Hungary. Mutual visits of the authors were made possible by the exchange agreement between the Estonian and the Hungarian Academies of Sciences.

References

[1] C. Bergman, J. Berman, *Morita equivalence of almost-primal clones,* J. Pure and Applied Algebra **108** (1996), 175–201.
[2] B. A. Davey, H. Werner, *Dualities and equivalences for varieties of algebras,* Contributions to lattice theory (Szeged, 1980), Colloq. Math. Soc. János Bolyai, vol. 33, North-Holland, Amsterdam, 1983, pp. 101–275.
[3] K. Denecke, O. Lüders, *Category equivalences and dualities of varieties and prevarieties generated by single preprimal algebras,* Acta Sci. Math. (Szeged) **58** (1993), 75–92.
[4] K. Denecke, O. Lüders, *Categorical equivalence of varieties and invariant relations,* Algebra Universalis **46** (2001), 105–118.
[5] B. Fine, *Classification of finite rings of order* p^2*,* Math. Mag. **66** (1993), 248–252. **38(86)** (1994), 45–48.
[6] J. Hagemann, C. Herrmann, *A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity,* Arch. Math. (Basel) **32** (1979), 234–245.
[7] N. Jacobson, *The theory of rings,* American Mathematical Society, New York, 1943.
[8] N. Jacobson, *Basic Algebra. I,* Second edition. W. H. Freeman and Company, New York, 1985.
[9] K. Kaarli, O. Košik, T. Waldhauser, *On categorical equivalence of finite rings,* J. Algebra Appl. **15** (2016), 1650154, 12 pp.
[10] S. S. Korobkov, *Finite rings with exactly two maximal subrings,* Izv. Vyssh. Uchebn. Zaved. Mat. (2011), no. 6, 55–62.
[11] S. S. Korobkov, *Projections of periodic nil-rings,* Izv. Vyssh. Uchebn. Zaved. Mat. (1980), no. 7, 30–38.

[12] S. S. Korobkov, *Projections of Galois rings,* Algebra Logic **54** (2015), 10–22.
[13] S. S. Korobkov, *Projections of finite one-generated rings with identity,* Algebra Logic **55** (2016), 128–145.
[14] R. L. Kruse, D. T. Price, *Nilpotent rings,* Gordon and Breach Science Publishers, New York-London-Paris, 1969.
[15] R. McKenzie, *An algebraic version of categorical equivalence for varieties and more general algebraic categories,* Logic and algebra (Pontignano, 1994), Lecture Notes in Pure and Appl. Math., vol. 180, Dekker, New York, 1996, pp. 211–243.
[16] R. Raghavendran, *Finite associative rings,* Compositio Math. **21** (1969), 195–229.

(K. Kaarli) Institute of Mathematics and Statistics, University of Tartu, 51009 Tartu, Estonia
Email address: kaarli@ut.ee

(T. Waldhauser) Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H–6720 Szeged, Hungary
Email address: twaldha@math.u-szeged.hu