DOI 10.1007/s10469-024-09750-5
Algebra and Logic, Vol. 62, No. 4, September, 2023
(Russian Original Vol. 62, No. 4, July-August, 2023)

PROJECTIONS OF FINITE RINGS

S. S. Korobkov

UDC 512.552

Keywords: *one-generated finite rings, matrix rings, lattice isomorphisms of associative rings.*

Let R and R^{φ} be associative rings with isomorphic subring lattices, and φ be a lattice isomorphism (or else a projection) of the ring R onto the ring R^{φ}. We call R^{φ} the projective image of a ring R and call R itself the projective preimage of a ring R^{φ}. The main result of the first part of the paper is Theorem 5, which proves that the projective image R^{φ} of a one-generated finite p-ring R is also one-generated if R^{φ} at the same time is itself a p-ring. In the second part, we continue studying projections of matrix rings. The main result of this part is Theorems 6 and 7, which prove that if $R = M_n(K)$ is the ring of all square matrices of order n over a finite ring K with identity, and φ is a projection of the ring R onto the ring R^{φ}, then $R^{\varphi} = M_n(K')$, where K' is a ring with identity, lattice-isomorphic to the ring K.

INTRODUCTION

Associative rings are considered. The lattice of all subrings of an arbitrary ring R is denoted by $L(R)$. Two rings R and R' are said to be *lattice-isomorphic* if their subring lattices $L(R)$ and $L(R')$, respectively, are isomorpic. A lattice isomorphism (or else a *projection*) $L(R) \cong L(R')$ is denoted by the letter φ and the ring R' is denoted as R^{φ}. We call R^{φ} the *projective image* of a ring R and call R itself the *projective preimage* of a ring R^{φ}. If the lattice isomorphism $L(R) \cong L(R^{\varphi})$ implies an isomorphism $R \cong R^{\varphi}$, then we say that the ring R is *lattice definable*. We say that some class of rings $\mathcal{K}$ is lattice definable if the projective images of rings in the class $\mathcal{K}$ also belong to $\mathcal{K}$. In studying lattice isomorphisms of rings, we consider the problems of lattice definability of classes of rings and of lattice definability of rings.

Ural State Pedagogical University, Yekaterinburg, Russia; ser1948@gmail.com. Translated from *Algebra i Logika*, Vol. 62, No. 4, pp. 524-551, July-August, 2023. Russian DOI: 10.33048/alglog.2023.62.405. Original article submitted January 19, 2023; accepted July 19, 2024.

Let k be a natural number. A finite ring R is said to be *k-generated* if any of its minimal sets of generators consists of k elements. For $k = 1$, R will be referred to as a *one-generated* ring. In [1, 2], it was proved that the property of being one-generated for rings is preserved under projections of nilpotent rings and finite fields. Lattice definability of Galois rings was stated in [3] (for a definition of a Galois ring, see [3, Def. 1]). However, one-generatedness of rings is not always preserved under projections [4, Example 2]. It is worth noting that the problem of preserving the property of being k-generated under lattice isomorphisms is important as for proving the lattice definability of rings as well as for constructing examples [5, Lemma 3, Example 2]. Let $\mathcal{K}_p$ be a class of rings whose additive groups are p-groups. The main results of the first part of the paper are Theorem 5 and Corollary 1, which prove that the property of being k-generated for a finite ring is preserved under projections in the class $\mathcal{K}_p$. The relevance of these statements is strengthened by the fact that projective images of rings in $\mathcal{K}_p$ not infrequently themselves belong to $\mathcal{K}_p$, which is confirmed in the second part of the paper devoted to projections of matrix rings.

Lattice isomorphisms of matrix algebras were first considered by D. W. Barnes [6], who proved that an algebra lattice-isomorphic to an algebra $M_n(\Delta)$, where $n \geqslant 2$ and Δ is a finite-dimensional division algebra, is also a matrix algebra $M_n(D)$ considered over some division algebra D lattice-isomorphic to Δ. A. V. Yagzhev [7] generalized Barnes's result by lifting the restriction on the dimension of the algebra Δ. That matrix rings treated over different types of Galois rings are lattice definable was proved in [8, 9]. Lattice isomorphisms of matrix rings, when considered over finite local rings, were dealt with in [10]. The main results of the second part of this paper are Theorems 6 and 7, which prove that if $R = M_n(K)$ is the ring of all square matrices of order n over a finite ring K with identity, and φ is a projection of the ring R onto the ring R^φ, then $R^\varphi = M_n(K')$, where K' is a ring with identity, lattice-isomorphic to the ring K. The question whether the ring R is lattice definable remains open.

We specify the notation used in the paper. Let S and T be subgroups in the additive group R^+ of a ring R. If $R = \{s+t \mid s \in S \wedge t \in T\}$, then we use the notation $R = S+T$. And use $R = S \dotplus T$ whenever $R = S + T$ and $S \cap T = \{0\}$. The equality $R = S \oplus T$ will mean that $R = S \dotplus T$ and S and T are two-sided ideals in R. In this case we say that a ring R is decomposable into a direct sum of rings S and T. Other designations are standard: $S \vee T$ is a subring generated by subrings S and T in a ring R; $\operatorname{Rad} R$ is the Jacobson radical of a ring R; $L(R)$ is the subring lattice of a ring R; $l(R)$ is the length of a ring R, i.e., the length of its subring lattice $L(R)$, where by the length of a finite lattice L is meant the greatest of the lengths of the chains in L; $\operatorname{char} R$ is the characteristic of a ring R; $\mathbb{N}$ and $\mathbb{Z}$ are the sets of natural numbers and integers, respectively; $\langle a_1, a_2, \ldots, a_n\rangle$ is a ring generated by elements $a_1, a_2, \ldots, a_n$; (r) is a principal ideal generated by an element r in R; $o(r)$ is the additive order of an element r; $\operatorname{ind} r$ is the nilpotency index of an element r; the letters k, l, m, n, p, q with or without indices stand for natural numbers, and p and q also stand for prime numbers. Lower-case Greek letters, except φ, denote integers. The letter φ is used to denote a lattice isomorphism of the ring R onto the ring R^φ. In the cases when the projective image of a ring R generated by an element r is a one-generated ring, we denote $\langle r\rangle^{\varphi}$ as $\langle r'\rangle$, in particular $\langle 0\rangle^{\varphi} = \langle 0'\rangle$.

1. PRELIMINARY INFORMATION

By a p-ring R we mean a ring whose additive group is a p-group. By an algebraic ring we mean a ring in which every element is a root of some primitive polynomial in the ring $x\mathbb{Z}[x]$. In proving a series of statements, we use a description of p-rings whose subring lattices are decomposable into direct products of lattices. For the reader's convenience, we give this description.

THEOREM 1 [11, Thm. 1]. The subring lattice of a p-ring R is decomposable into a direct product of lattices if and only if R is an algebraic ring isomorphic to one of the rings

$$Q_1 = N \oplus P,\ L(Q_1) \cong L(N) \times L(P),$$
$$Q_2 = (N \oplus S) \dotplus \langle e\rangle,\ L(Q_2) \cong L(N) \times L(S \dotplus \langle e\rangle),$$
$$Q_3 = Q_2 \oplus P,\ L(Q_3) \cong L(N) \times L((S \dotplus \langle e\rangle) \oplus P);$$

here N, P are nonzero rings, N is a nil ring, P is a ring without nilpotent elements other than zero, $S = \{0\}$ or S is a ring without nilpotent elements other than zero, and e is the identity element of order p in the ring Q_2.

As a criterion for one-generatedness of a finite commutative ring we use the following:

THEOREM 2 [4, Prop. 2]. Let a finite commutative p-ring R be representable as $R = S + (r)$, where S is a subring decomposable into a direct sum of Galois rings and r is a nilpotent element. The ring R is generated by a single element if and only if the subring S is generated by a single element.

To study projective images of finite one-generated p-rings, we need a description of rings whose subring lattices are finite chains. We give this description.

THEOREM 3 [12, Thm. 1.6]. The subring lattice of a ring R is a finite chain if and only if R is isomorphic to one of the rings

$$C_1 = \langle r\rangle,\ \text{where } o(r) = p^n,\ r^2 = p^k r,\ k = \overline{1, n},$$
$$C_2 = \langle r\rangle,\ \text{where } o(r) = p,\ \operatorname{ind} r = 3,$$
$$C_3 = \langle e\rangle,\ \text{where } o(e) = p^n,\ e^2 = e,$$
$$C_4 = GF(p^{q^n}).$$

2. PROJECTIONS OF k-GENERATED FINITE RINGS

Recall that by $\mathcal{K}_p$ we denoted a class of p-rings. Let $k \in \mathbb{N}$. It is easy to see that the property of a ring to be k-generated is preserved under projections in the class $\mathcal{K}_p$ if it is preserved for $k = 1$. Therefore, in this section we mainly focus on the projections of one-generated finite p-rings.

PROPOSITION 1. Let R be a one-generated nilpotent ring of order p^n, and let φ be a lattice isomorphism of the ring R onto the ring R^φ. Then R^φ is a one-generated ring. If $L(R)$ is not a chain, then R^φ is a nilpotent ring of order p^n; if, in addition, $\operatorname{char} R = \operatorname{char} R^\varphi = p$, then $R \cong R^\varphi$.

Proof. Let $R = \langle r\rangle$ The ring R is finite and contains a unique maximal subring $M = pR + R^2$, so R^φ is a one-generated ring. Let $R^\varphi = \langle r'\rangle$.

Suppose that the lattice $L(R)$ is not a chain. According to [1, Thm. 1], R^φ is a nilpotent p-ring. By [1, Lemma 7], $|R^\varphi| = |R|$. If $\operatorname{char} R = \operatorname{char} R^\varphi = p$, then R and R^φ are lattice-isomorphic finite-dimensional nilpotent algebras over a finite prime field $GF(p)$. For finite-dimensional nilpotent algebras, the dimension of an algebra coincides with the length of its subalgebra lattice [6, p. 107]. Then $\operatorname{ind} R^\varphi - 1 = \dim R^\varphi = l(R^\varphi) = l(R) = \dim R = \operatorname{ind} R - 1$, whence $\operatorname{ind} R^\varphi = \operatorname{ind} R$. It is clear that $\operatorname{ind} r = \operatorname{ind} R = \operatorname{ind} R^\varphi = \operatorname{ind} r'$, and so $\langle r\rangle \cong \langle r'\rangle$. The proposition is proved.

We move on to examining projections of one-generated nonnilpotent rings. Projections of one-generated finite rings with identity were studied in detail in [4], where sufficient conditions were found under which the projective image of a finite one-generated ring with identity likewise is a one-generated ring.

LEMMA 1. Let R be a finite nonnilpotent commutative ring without identity. The ring R is one-generated if and only if R is representable as

$$R = \langle t\rangle \oplus \langle r\rangle, \tag{1}$$

where $\langle t\rangle$ is a subring with identity, decomposable into a finite direct sum of rings $T_i = S_i + (r_i)$, $i = \overline{1, n}$; moreover, $S_i \cong GR(p^{n_i}, m_i)$, r_i is a nilpotent element, and the identity element of the subring S_i is also one in T_i, and r is a nonzero nilpotent element.

Proof. Necessity. Let R be one-generated. Since R is not a nil ring, it contains at least one nonzero idempotent element and, hence, contains a maximal orthogonal system of idempotents $e_1, \dots, e_n$. Using the Peirce decomposition of R with respect to idempotents e_i, $i = \overline{1, n}$, we represent R as $R = T \oplus N$, where $T = e_1R \oplus \cdots \oplus e_nR$ is a subring with identity and N is a nilpotent subring. As shown in [4, Lemma 1], if the ring R is one-generated, then so are its direct summands T and N: $T = \langle t\rangle$ and $N = \langle r\rangle$, where $t, r \in R$. Consequently, equality (1) holds. The structure of finite one-generated rings with identity is described in [4, Thm. 1]. According to that description, the ring $\langle t\rangle$ is decomposable into a finite direct sum of rings $T_i = S_i + (r_i)$, $i = \overline{1, n}$, in which case $S_i \cong GR(p^{n_i}, m_i)$, r_i is a nilpotent element, the identity of the subring S_i is also one in T_i.

Sufficiency. Let R be representable in form (1). Denote by e an identity element of the subring $\langle t\rangle$ and represent e as a polynomial in t, setting $e = f(t)$, where $f(x) \in x\mathbb{Z}[x]$. Let $v = t + r$. Then $f(v) = e + f(r)$. Let $r^k = 0$. Then $(f(v))^k = e$, and so $e \in \langle v\rangle$, whence $\langle v\rangle = R$. The lemma is proved.

As follows from Lemma 1, the simplest one-generated rings not containing an identity are rings decomposable into a direct sum of two subrings, of which one is generated by an idempotent and the other, by a nilpotent element. A description of projective images of such rings is given in

PROPOSITION 2. Let φ be a lattice homomorphism of the p-ring $R = \langle e\rangle \oplus \langle r\rangle$, where $o(e) = p^n$, $e^2 = e$, and r is a nonzero nilpotent element, onto the ring R^φ. Then R^φ is a one-generated ring and the following conditions are satisfied:

(1) if $n = 1$ and $\langle r\rangle \cong C_i$, $i = 1, 2$ (cf. Theorem 3), then $R^\varphi \cong P_1$ or $R^\varphi \cong P_2$, where $P_1 = \langle s'\rangle \oplus \langle t'\rangle$, $o(s') = p_1$, $\langle t'\rangle$ is a p_2-ring, p_1, p_2 are primes, $\langle t'\rangle \cong C_j$, and also either

(a) $(s')^2 = 0'$ or $(s')^2 = s'$ and $j = \overline{1,4}$, $p_2 \neq p_1$, or

(b) $(s')^2 = 0'$ and $j = 3, 4$, $p_2 = p_1$, or

(c) $(s')^2 = s'$ and $j = 1, 2$, $p_2 = p_1$;

$P_2 = \langle s'\rangle \dotplus \langle t'\rangle$, $o(s') = p_1$, $\langle t'\rangle \cong C_j$, $j = 1, 2$, s' is the identity of P_2;

(2) if $n = 1$ and the lattice $L(\langle r\rangle)$ is not a chain, then $R^\varphi = \langle e\rangle^\varphi \dotplus \langle r\rangle^\varphi$, $\langle r\rangle^\varphi = \langle r'\rangle$ is a nilpotent p-subring, $\langle e\rangle^\varphi = \langle s'\rangle$, $o(s') = q$ (q is a prime), and also

(a) for $q = p$, it is true that $(s')^2 = s'$, $s'r' = r's' = 0'$ or s' is the identity of the ring R^φ;

(b) for $q \neq p$, it is true that $s'r' = r's' = 0'$, $(s')^2 = 0'$ or $(s')^2 = s'$;

(3) if $n > 1$, then R^φ is a q-ring, $\langle e\rangle^\varphi = \langle e'\rangle$, $(e')^2 = e'$, $o(e') = q^n$, $\langle r\rangle^\varphi = \langle r'\rangle$, r' is a nilpotent element, and one of the following holds:

(a) $R^\varphi = \langle e'\rangle \dotplus \langle r'\rangle$, where e' is an identity, $q = p$;

(b) $R^\varphi = \langle e'\rangle \oplus \langle v'\rangle$, where v' is a nilpotent element, $q = p$;

(c) $R^\varphi \cong GF(q^{q_1}) \oplus GF(q)$, and also $n = 2$, $p = 2$, q_1 is a prime.

Proof. The ring R satisfies the hypotheses of Theorem 3 in [13] and, therefore, contains exactly two maximal subrings. This means that the ring R itself and its projective image R^φ are one-generated. There are three cases to consider.

Case 1. Let $n = 1$ and $\langle r\rangle \cong C_i$, $i = 1, 2$. According to Theorem 1, $L(R) \cong L(\langle e\rangle) \times L(\langle r\rangle)$. Let $\langle e\rangle^\varphi = \langle s'\rangle$ and $\langle r\rangle^\varphi = \langle t'\rangle$. By Theorem 3, $o(s') = p_1$ and $(s')^2 = 0'$ or $(s')^2 = s'$, $\langle t'\rangle$ is a p_2-ring, and $\langle t'\rangle \cong C_j$, $j = \overline{1,4}$, p_1, p_2 are some primes. If $p_2 \neq p_1$, then $R^\varphi \cong P_1$ by [11, Thm. 2], and condition (1a) holds. Let $p_2 = p_1$. If R^φ does not contain an identity, then $R^\varphi \cong P_1$ by Theorem 1, and condition (1b) or (1c) holds, and if R^φ is a ring with identity, then $R^\varphi \cong P_2$.

Case 2. Let $n = 1$ and the lattice $L(\langle r\rangle)$ not be a chain. In view of Proposition 1, $\langle r\rangle^\varphi = \langle r'\rangle$ is a nilpotent p-subring. According to Theorem 1, $L(R)$ is decomposable into a direct product of lattices $L(\langle e\rangle)$ and $L(\langle r\rangle)$. The subring $\langle e\rangle$ is an atom in the lattice $L(R)$, so $\langle e\rangle^\varphi = \langle s'\rangle$, where $s' \in R^\varphi$ and $o(s') = q$ for some prime q.

Suppose $q = p$. Since $L(R^\varphi) \cong L(\langle s'\rangle) \times L(\langle r'\rangle)$, and the subring $\langle r'\rangle$ is nilpotent, the subring $\langle e\rangle^\varphi$ does not contain nonzero nilpotent elements, and we may therefore assume that $(s')^2 = s'$. Applying Theorem 1, we conclude that either $s'r' = r's' = 0'$ or s' is the identity in the ring R^φ. In the latter case, it is obvious that $o(r') = p$. If $q \neq p$, then $s'r' = r's' = 0'$, and either $(s')^2 = 0'$ or $(s')^2 = s'$. Conditions (2a) and (2b) hold.

Case 3. Let $n > 1$. If the subring $\langle r\rangle$ contains just p elements, then conditions (3a)-(3c) hold in view of [3, Lemma 7]. Therefore, below we assume that $|\langle r\rangle| > p$. Then a nilpotent subring

$S = \langle pe\rangle \oplus \langle r\rangle$ contains more than p^2 elements. Furthermore, its subring lattice is not a chain, and hence the projective image S^φ is a p-ring, as follows by [1, Thm. 1]. Recall that R^φ is a commutative ring. Applying again [1, Thm. 1] to the subring S, we conclude that S^φ is a p-nil ring. This fact and Proposition 1 imply that $\langle r\rangle^\varphi = \langle r'\rangle$ is a nilpotent subring. In addition, R^φ is a p-ring because all minimal subrings of R^φ are contained in the subring S^φ. Since $L(\langle e\rangle)$ is a finite chain, it follows by Theorem 3 that the ring $\langle e\rangle^\varphi$ either is a finite field or is generated by a nilpotent or idempotent element. The ring $\langle e\rangle^\varphi$ cannot be a finite field since $\langle e\rangle^\varphi \cap S^\varphi = \langle pe\rangle^\varphi$ is a nonzero nil ring. Suppose that $\langle e\rangle^\varphi = \langle s'\rangle$, where s' is a nilpotent element. Then the ring R^φ is generated by two nilpotent elements s' and r', and R^φ being commutative implies that it will be nilpotent. We have arrived at a contradiction with [13, Lemma 2], which says that a finite p-ring that contains exactly two maximal subrings will contain a nonzero idempotent element. Hence $\langle e\rangle^\varphi = \langle e'\rangle$, where $(e')^2 = e'$ and $o(e') = p^n$. Thus the ring R^φ is generated by elements e', r' and contains exactly two maximal subrings. If the element e' is an identity in the ring R^φ, then condition (3a) holds.

Assume that e' is not an identity in R^φ and consider the Peirce decomposition: $R^\varphi = e'R^\varphi \oplus (1-e')R^\varphi$. According to [13, Lemma 4], the subrings $e'R^\varphi$ and $(1-e')^\varphi R$ each contains one maximal subring. The ring $e'R^\varphi$ contains a nonzero idempotent element e' of nonprime order. By [13, Thm. 1], one of the following two cases holds: either $e'R^\varphi = \langle e'\rangle$ or $e'R^\varphi \cong GR(p^n, q_2^m)$, where q_2 is a prime. If the second case holds, then [3, Thm. 3] says that the subring R contains a subring isomorphic to the ring $GR(p^n, q_2^m)$. The ring R does not have such subrings since any subring of R containing an idempotent element e has the form $\langle e\rangle \oplus T$, where $T \subseteq \langle r\rangle$, and cannot be isomorphic to $GR(p^n, q_2^m)$. Hence $e'R^\varphi = \langle e'\rangle$. If the subring $(1-e')^\varphi R$ is nonnilpotent, then it contains a nonzero idempotent element e_1', and hence the ring R^φ will have two orthogonal idempotent elements e' and e_1'. By virtue of [3, Lemmas 6, 8], the projective image of a subring $\langle e'\rangle \oplus \langle e_1'\rangle$ should also contain two nonzero orthogonal idempotent elements. Clearly, the ring R lacks such idempotent elements. Consequently, the subring $(1-e')R^\varphi$ is generated by a nilpotent element. Let $(1-e')R^\varphi = \langle v'\rangle$. Then $R^\varphi = \langle e'\rangle \oplus \langle v'\rangle$, and condition (3b) holds. Proposition 2 is proved.

LEMMA 2. Let a finite one-generated p-ring $R = S + (r)$ be given, where $S = GR(p^n, m)$, $m, n \in \mathbb{N}$, r is a nilpotent element. Suppose also that φ is a projection from the ring R to the ring R^φ. Then R^φ is a one-generated ring.

Proof. Let $r = 0$. If, in addition, $m = 1$, then $R = GR(p^n, 1)$ is a ring generated by an idempotent and $L(R)$ is a finite chain. That the statement of the lemma is true in this case follows from Theorem 3. If $n = 1$ and $m > 1$, then $R = GR(p, m)$ is a field of order p^m. In this case the statement of the lemma is true in virtue of [2, Thm. 2.1]. For $n > 1$ and $m > 1$, $R \cong R^\varphi$ according to [3, Thm. 4], and hence R^φ is one-generated.

Let $r \neq 0$. Further we assume that $m > 1$ since $R = GR(p^n, 1) \oplus \langle r\rangle$ for $m = 1$, and according to Proposition 2, the ring R^φ is one-generated.

Let e be an identity element of a ring S. By [4, Lemma 14], e is the unique nonzero idempotent element of the ring R. Suppose R is a ring with identity. Then e is the identity element in R. If $n > 1$, then [4, Lemma 17] implies that the statement of the lemma is true. Let $n = 1$. Then $S \cong GF(p^m)$, and by [5, Lemma 3], $R^\varphi \cong R$. Hence the ring R^φ is generated by a single element.

Let R be a ring without identity. Consider the Peirce decomposition of R with respect to an idempotent e: $R = eR \oplus (1-e)R$. The subring $(1-e)R$ is nilpotent since e is the unique nonzero idempotent element of the ring R. Let $r = s_1 + r_1$, where $s_1 \in S$ and $r_1 \in (1-e)R$. Since $R = S \vee \langle r\rangle = S \vee \langle r_1\rangle = S \oplus \langle r_1\rangle$, there is no loss of generality in assuming that $er = 0$, and so $R = S \oplus \langle r\rangle$. There are two cases to consider.

Case 1. Let $n = 1$. Then $S = GF(p^m)$. By Theorem 1, the subring lattice $L(R)$ is decomposable into a direct product of lattices: $L(R) \cong L(S) \times L(\langle r\rangle)$. Consequently, $L(R^\varphi) \cong L(S^\varphi) \times L(\langle r\rangle^\varphi)$. In view of [2, Thm. 2.1], combined with Proposition 1, S^φ and $\langle r\rangle^\varphi$ are one-generated rings. Let $S^\varphi = \langle s'\rangle$ and $\langle r\rangle^\varphi = \langle r'\rangle$. The rings $\langle s'\rangle$ and $\langle r'\rangle$ have primary additive groups since their subring lattices are not decomposable into direct products of lattices. Let $\langle s'\rangle$ be a p_1-ring and $\langle r'\rangle$ a p_2-ring, where p_1 and p_2 are primes. If $p_1 \neq p_2$ then $\langle s' + r'\rangle = \langle s'\rangle \oplus \langle r'\rangle = R^\varphi$. Let $p_1 = p_2$. The rings S^φ and $\langle r\rangle^\varphi$ are one-generated, and by Theorem 1, R^φ is a commutative ring, and the set of its nilpotent elements is an ideal. Hence R^φ satisfies the hypotheses of Theorem 2 and is therefore one-generated.

Case 2. Let $n > 1$. By [3, Thm. 4], $S^\varphi \cong S$, and by [4, Cor. 2], R^φ is a p-ring. Let a number m have the following canonical decomposition: $m = q_1^{m_1} \dots q_k^{m_k}$, where $q_1, \dots, q_k$ are primes. According to [14, Lemma XVI.7], the ring S contains subrings $G_i = GR(p^n, q_i^{m_i})$, $i = \overline{1,k}$. By [14, Thm. XVI.8], $S = G_1 \vee G_2 \vee \dots \vee G_k$. In view of [13, Thm. 3], the ring $S_i = G_i \oplus \langle r\rangle$, $i = \overline{1,k}$, contains exactly two maximal subrings; hence the subring $S_i^\varphi = G_i^\varphi \vee \langle r\rangle^\varphi$, $i = \overline{1,k}$, is commutative, and so therefore is the ring R^φ itself. In accordance with Theorem 2, R^φ is a one-generated ring. The lemma is proved.

It is well known that direct sums of Galois rings play an important role in finite ring theory. Projective images of finite rings decomposable into direct sums of different types of Galois rings were dealt with in [4]. The structure of projective images of one-generated finite rings decomposable into direct sums of Galois rings are described in the following:

THEOREM 4. Let R be a finite one-generated p-ring decomposable into a direct sum of n Galois rings. Suppose also that φ is a projection of the ring R onto the p-ring R^φ. Then R^φ is a one-generated ring, and if $n > 1$ and $R \not\cong GF(2^q) \oplus GF(2)$, then R^φ is also decomposable into a direct sum of n Galois rings.

Proof. By hypothesis, R is a ring with identity. We represent R as follows: $R = R_1 \oplus R_2 \oplus R_3$, where $R_1 = \{0\}$ or $R_1 = GR(p^{k_1}, \alpha_1) \oplus \dots \oplus GR(p^{k_l}, \alpha_l)$ and $(\forall i = \overline{1,l})\,(k_i > 1, \alpha_i > 1)$; $R_2 = \{0\}$ or $R_2 = GF(p^{m_1}) \oplus \dots \oplus GF(p^{m_s})$ and $(\forall j = \overline{1,s})\,(m_j > 1)$; $R_3 = \{0\}$ or $R_3 = \langle v_1\rangle \oplus \dots \oplus \langle v_n\rangle$, $v_i^2 = v_i$, $i = \overline{1,n}$. By hypothesis, the ring R is one-generated, and so are the subrings R_1, R_2, R_3 by [4, Lemma 1]. We prove that projective images of these subrings are one-generated.

Consider the ring R_1. According to [4, Thm. 9], $R_1^\varphi = (GR(p^{k_1}, \alpha_1))^\varphi \oplus \dots \oplus (GR(p^{k_l}, \alpha_l))^\varphi$ and

$(\forall i = \overline{1,l})\,(GR(p^{k_i}, \alpha_i))^\varphi \cong GR(p^{k_i}, \alpha_i))$. Consequently, $R_1^\varphi \cong R_1$, and so R_1^φ is a one-generated ring.

Consider the ring R_2. If $s = 1$, then R_2 is a finite field, and by [2, Thm. 2.1], R_2^φ is a one-generated ring. Let $s > 1$ and

$$R_2 = \underbrace{GF(p^{m_1}) \oplus \cdots \oplus GF(p^{m_1})}_{n_1} \oplus \cdots \oplus \underbrace{GF(p^{m_s}) \oplus \cdots \oplus GF(p^{m_s})}_{n_s}.$$

In view of [4, Thm. 6],

$$\begin{aligned} R_2^\varphi = {} & \underbrace{(GF(p^{m_1}))^\varphi \oplus \cdots \oplus (GF(p^{m_1}))^\varphi}_{n_1} \oplus \cdots \\ & \oplus \underbrace{(GF(p^{m_s}))^\varphi \oplus \cdots \oplus (GF(p^{m_s}))^\varphi}_{n_s}, \end{aligned}$$

with $\big(\forall i = \overline{1,s}\big)\,\Big((GF(p^{m_i}))^\varphi \cong GF(p^{m_i'})\Big)$, and if $n_i > 1$, then $m_i' = m_i$ by virtue of [4, Lemma 7]. The subring R_2 is generated by a single element, and according to [4, Prop. 1], for all $i = \overline{1,s}$ the following condition is satisfied:

$$n_i \leqslant N_p(m_i), \tag{2}$$

where $N_p(m_i)$ is the number of all normed irreducible polynomials of degree m_i over the field $GF(p)$. Applying [4, Prop. 1] to R_2^φ, we conclude that R_2^φ is one-generated.

Consider the ring R_3. If $R_3 = \langle v_1 \rangle$, then $L(R_3)$ is a chain, and so R_3^φ is a one-generated ring. Let $R_3 = \langle v_1 \rangle \oplus \langle v_2 \rangle$. If $o(v_1) = o(v_2) = p$, then, in view of R_3 being one-generated, we conclude that $p \neq 2$. By hypothesis, R^φ is a p-ring. If we apply [6, Lemma 6] we conclude that $R_3^\varphi \cong R_3$. In all other cases, to R_3 we can apply [5, Prop. 2], according to which $R_3^\varphi \cong R_3$. The above argument implies that the theorem that we are proving is true if some two summands in the sum $R = R_1 \oplus R_2 \oplus R_3$ equal zero.

Let $R_3 = \{0\}$ and R_1, R_2 be nonzero subrings. Then

$$R = \underbrace{GR(p^{k_1}, m_1) \oplus \cdots \oplus GR(p^{k_l}, m_l)}_{R_1} \oplus \underbrace{GF(p^{m_{l+1}}) \oplus \cdots \oplus GF(p^{m_{l+s}})}_{R_2}. \tag{3}$$

If among the positive integers $m_1, \ldots, m_{l+s}$ there are repetitions, then we number them anew, assigning all equal ones the same number. Let γ be the amount of the resulting numbers. Denote by n_i the amount of positive integers in the sequence $m_1, \ldots, m_{l+s}$ equal to m_i, $1 \leqslant i \leqslant \gamma$. Taking into account that $GF(p^m) = GR(p, m)$, we rewrite equality (3) in the following form:

$$R = (R_{11} \oplus \cdots \oplus R_{1n_1}) \oplus \cdots \oplus (R_{\gamma 1} \oplus \cdots \oplus R_{\gamma n_\gamma}), \tag{4}$$

where $R_{ij} \cong GR(p^{k_i}, m_i)$, $i = \overline{1,\gamma}$, $j = \overline{1,n_i}$, and $m_1, \ldots, m_\gamma$ are pairwise distinct positive integers. The ring R is one-generated, and [4, Prop. 1] says that the positive integers n_i, $i = \overline{1,\gamma}$, satisfy equality (2). By [4, Thm. 11],

$$R^\varphi = (R_{11}^\varphi \oplus \cdots \oplus R_{1n_1}^\varphi) \oplus \cdots \oplus (R_{\gamma 1}^\varphi \oplus \cdots \oplus R_{\gamma n_\gamma}^\varphi), \tag{5}$$

with $R_{ij}^{\varphi} \cong R_{ij}$ or $R_{ij}^{\varphi} \cong GF(p^{m'_j})$ for all $i = \overline{1, \gamma}$ and all $j = \overline{1, n_i}$. Consider an arbitrary summand $T_i = (R_{i1} \oplus \cdots \oplus R_{in_i})$ in the right part of (4) and its projective image $T_i^{\varphi} = (R_{i1}^{\varphi} \oplus \cdots \oplus R_{in_i}^{\varphi})$. Minimal polynomials of elements generating subrings R_{ij} $(j = \overline{1, n_i})$ have the same degree equal to m_i. If $n_i > 1$, then [4, Lemma 7, Thm. 9, Lemma 13] says that minimal polynomials of elements generating subrings R_{ij}^{φ} $(j = \overline{1, n_i})$ have the same degree m_i. If $n_i = 1$, then the degrees m_i and m'_i of minimal polynomials of elements generating rings T_i and T_i^{φ}, respectively, may differ; however, $m_i \neq m_k$ for $i \neq k$, and so $m'_i \neq m'_k$, $i, k = \overline{1, \gamma}$. Consequently, inequality (2) for the ring R^{φ} holds, and by [4, Prop. 1], R^{φ} is a one-generated ring.

Let $R_2 = \{0\}$ and R_1, R_3 be nonzero subrings. Then

$$R = \underbrace{GR(p^{k_1}, m_1) \oplus \cdots \oplus GR(p^{k_l}, m_l)}_{R_1} \oplus \underbrace{\langle v_1 \rangle \oplus \cdots \oplus \langle v_n \rangle}_{R_3}, \tag{6}$$

where $v_1, \ldots, v_n$ are nonzero idempotent elements. Let e_i be the identity element of the ring $GR(p^{k_i}, m_i)$, $i = \overline{1, l}$. By [3, property 9], $\langle e_i \rangle^{\varphi} = \langle e'_i \rangle$ and e'_i is the identity element in the ring $GR(p^{k_i}, m_i)^{\varphi}$. Consider a subring $W = \langle e_1 \rangle \oplus \cdots \oplus \langle e_l \rangle \oplus \langle v_1 \rangle \oplus \cdots \oplus \langle v_n \rangle$. By hypothesis, $o(e_1) = p^{k_1}$ and $k_1 > 1$. To the subring W, therefore, we can apply [5, Prop. 2], which says that $W^{\varphi} \cong W$. Let $W^{\varphi} = \langle e'_1 \rangle \oplus \cdots \oplus \langle e'_l \rangle \oplus \langle v'_1 \rangle \oplus \cdots \oplus \langle v'_n \rangle$, where $(v'_j)^2 = v'_j$, $j = \overline{1, n}$. At the beginning of the proof, it was noted that $R_1^{\varphi} \cong R_1$, so

$$R^{\varphi} = \underbrace{(GR(p^{k_1}, m_1))^{\varphi} \oplus \cdots \oplus (GR(p^{k_l}, m_l))^{\varphi}}_{R_1^{\varphi}} \oplus \underbrace{\langle v'_1 \rangle \oplus \cdots \oplus \langle v'_n \rangle}_{R_3^{\varphi}} \cong R.$$

Consequently, being one-generated for R implies being one-generated for R^{φ}.

Let $R_1 = \{0\}$ and R_2, R_3 be nonzero subrings. Then

$$R = \underbrace{GF(p^{m_1}) \oplus \cdots \oplus GF(p^{m_s})}_{R_2} \oplus \underbrace{\langle v_1 \rangle \oplus \cdots \oplus \langle v_n \rangle}_{R_3}, \tag{7}$$

where $v_1, \ldots, v_n$ are nonzero idempotent elements. We rewrite (7) in the form

$$\begin{aligned} R = {} & \underbrace{GF(p^{m_1}) \oplus \cdots \oplus GF(p^{m_1})}_{n_1} \oplus \cdots \oplus \underbrace{GF(p^{m_s}) \oplus \cdots \oplus GF(p^{m_s})}_{n_s} \\ & \oplus \langle v_1 \rangle \oplus \cdots \oplus \langle v_n \rangle, \end{aligned} \tag{8}$$

where, as above, n_i is the number of direct summands in the right part of (8) which are defined by a minimal polynomial of degree m_i, $i = \overline{1, s}$. Consider several versions.

(a) Let $s = n_1 = n = 1$, $R = GF(p^{m_1}) \oplus \langle v_1 \rangle$, and $o(v_1) = p$. If $l(GF(p^{m_1})) = 2$, then it follows by [13, Thm. 3] that the ring R contains only two maximal subrings, and so both the rings R and R^{φ} are one-generated. If $l(GF(p^{m_1})) > 2$, then $l(R) > 3$, and by [2, Cors. 3.1, 3.2]. the projective image R^{φ} is decomposable into a direct sum of two finite fields F'_1 and F'_2 of characteristic p. In view of [5, Lemma 7], the fields F'_1 and F'_2 are not isomorphic, and hence the ring R^{φ} satisfies the hypotheses of [4, Prop. 1] and is therefore one-generated.

(b) Let $s = n_1 = n = 1$, $R = GF(p^{m_1}) \oplus \langle v_1 \rangle$, $o(v_1) = p^k$, and $k > 1$. According to [4, Lemma 8, Remark 1], the rings R and R^φ are one-generated, with R^φ decomposable into a direct sum of two Galois rings.

(c) Let $s = n_1 = 1$, $n > 1$, $R = GF(p^{m_1}) \oplus \langle v_1 \rangle \oplus \dots \oplus \langle v_n \rangle$, and $o(v_i) = p$ $(i = \overline{1,n})$. In this case [2, Cor. 3.1] implies that the ring R^φ is decomposable into a direct sum of $n+1$ fields in characteristic p. Among these fields, only $(GF(p^{m_1}))^\varphi$ is not a prime field, and the other n fields are isomorphic to $GF(p)$. If the ring R is one-generated, then it satisfies [4, Cor. 1], and so $n < p$. This means that the ring R^φ satisfies the hypotheses of [4, Prop. 1] and is therefore also one-generated.

(d) Let $s = n_1 = 1$, $n > 1$, $R = GF(p^{m_1}) \oplus \langle v_1 \rangle \oplus \dots \oplus \langle v_n \rangle$, $o(v_i) = p^{k_i}$, $k_i > 1$, $i = \overline{1,t}$, and $1 < t \leqslant n$. In this case, by [4, Lemma 9; 3, Lemma 6], $R^\varphi = GF(p^{m_1'}) \oplus \langle v_1' \rangle \oplus \dots \oplus \langle v_n' \rangle$, where $\langle v_i' \rangle \cong \langle v_i \rangle$, $i = \overline{1,n}$. By [4, Prop. 1], the rings R and R^φ are one-generated for $n < p$.

(e) Let $s > 1$. Suppose also that $\beta = n_1 + \dots + n_s$. In view of [4, Thm. 6],

$$R_2^\varphi = \underbrace{GF(p^{m_1'}) \oplus \dots \oplus GF(p^{m_1'}) \oplus \dots \oplus GF(p^{m_s'}) \oplus \dots \oplus GF(p^{m_s'})}_{\beta},$$

where $GF(p^{m_i'}) = (GF(p^{m_i}))^\varphi$, $i = \overline{1,\beta}$; moreover, in view of [4, Lemma 7], $m_i' = m_i$, for $n_i > 1$, and $m_i' \neq m_k'$ for $n_i = 1$ and $i \neq k$. Let e_i be the identity of a field $GF(p^{m_i})$, $i = \overline{1,\beta}$, and $\langle e_i \rangle^\varphi = \langle e_i' \rangle$. Then e_i' is an identity of the field $GF(p^{m_i'})$, and $e_1', \dots, e_\beta'$ is an orthogonal system of idempotents. Consider a subring $U = \langle e_1 \rangle \oplus \dots \oplus \langle e_\beta \rangle \oplus \langle v_1 \rangle \oplus \dots \oplus \langle v_n \rangle$. Since $\beta + n > 2$, and R^φ is a p-ring, it follows by [5, Prop. 2] that R^φ contains idempotents v_i', $i = \overline{1,n}$, satisfying the following conditions: $o(v_i') = o(v_i)$ $(i = \overline{1,n})$ and $U^\varphi = \langle e_1' \rangle \oplus \dots \oplus \langle e_\beta' \rangle \oplus \langle v_1' \rangle \oplus \dots \oplus \langle v_n' \rangle$. Consequently,

$$R^\varphi = \underbrace{GF(p^{m_1'}) \oplus \dots \oplus GF(p^{m_1'})}_{n_1} \oplus \dots \oplus \underbrace{GF(p^{m_s'}) \oplus \dots \oplus GF(p^{m_s'})}_{n_s}$$
$$\oplus \langle v_1' \rangle \oplus \dots \oplus \langle v_n' \rangle.$$

Numbers n_i, $i = \overline{1,s}$, satisfy $n_i \leqslant N_p(m_i')$ and $n < p$, and by Theorem 2, R^φ is a one-generated subring.

Let $R = R_1 \oplus R_2 \oplus R_3$ and $R_i \neq \{0\}$, $i = \overline{1,3}$. Consider a subring

$$K = \underbrace{GR(p^{k_1}, m_1) \oplus \dots \oplus GR(p^{k_l}, m_l)}_{R_1} \oplus \underbrace{GF(p^{m_{l+1}}) \oplus \dots \oplus GF(p^{m_{l+s}})}_{R_2}.$$

According to [4, Thm. 11],

$$K^\varphi = \underbrace{(GR(p^{k_1}, m_1))^\varphi \oplus \dots \oplus (GR(p^{k_l}, m_l))^\varphi}_{R_1^\varphi}$$
$$\oplus \underbrace{(GF(p^{m_{l+1}}))^\varphi \oplus \dots \oplus (GF(p^{m_{l+s}}))^\varphi}_{R_2^\varphi}.$$

Let e_i be an identity of the ring $GR(p^{k_i}, m_i)$, $i = \overline{1, l}$, and e_{l+j} be one of the field $GF(p^{m_{l+j}})$, $j = \overline{1, s}$. Consider a subring $E = \langle e_1 \rangle \oplus \cdots \oplus \langle e_{l+s} \rangle \oplus \langle v_1 \rangle \oplus \cdots \oplus \langle v_n \rangle$. Since R^φ is a p-ring, $E^\varphi \cong E$ by virtue of [5, Prop. 2]. Consequently, there exist idempotent elements $v'_i \in R^\varphi$, $i = \overline{1, n}$, for which $R^\varphi = K^\varphi \oplus \langle v'_1 \rangle \oplus \cdots \oplus \langle v'_n \rangle$. Rewriting the ring K in form (4) and applying equality (5), we obtain

$$R^\varphi = (R^\varphi_{11} \oplus \cdots \oplus R^\varphi_{1n_1}) \oplus \cdots \oplus (R^\varphi_{\gamma 1} \oplus \cdots \oplus R^\varphi_{\gamma n_\gamma}) \oplus \langle v'_1 \rangle \oplus \cdots \oplus \langle v'_n \rangle. \tag{9}$$

Numbers n_i, $i = \overline{1, \gamma}$, in (9) satisfy the condition $n_i \leqslant N_p(m'_i)$, and the inequality $n < p$ holds likewise. By [4, Prop. 1], R^φ is a one-generated ring. The theorem is proved.

One of the basic results of the paper is the following:

THEOREM 5. Let φ be a projection of a finite one-generated p-ring R onto a p-ring R^φ. Then R^φ is a one-generated ring.

The **proof** is divided into two parts.

Part 1. Let R be a ring with identity. By [15, Thm. II.5], R is decomposable into a direct sum of n local rings R_i, $i = \overline{1, n}$. In view of [4, Lemma 1], every subring R_i, $i = \overline{1, n}$, is one-generated and is therefore representable as $R_i = S_i + (r_i)$, where $S_i = GR(p^{k_i}, m_i)$, r_i is a nilpotent element, and the identity e_i of the subring S_i is also one in R_i. Let $S = S_1 \oplus \cdots \oplus S_n$ and $r = r_1 + \cdots + r_n$. Then $R = S + (r)$.

That the theorem that we are proving is true for $n = 1$ follows from Lemma 2.

Let $n > 1$. By Theorem 4, the subring S^φ is one-generated, and if $r = 0$, then we are done.

Let $r \neq 0$. Consider the particular case where $n = 2$, $S_1 \cong GF(2^q)$, and $S_2 \cong GF(2)$. Then $R = (S_1 \oplus S_2) + (r)$. We prove that the ring $(S_1 \oplus S_2)^\varphi$ does not contain nonzero nilpotent elements. Assume the contrary. The subring $S_1 \oplus S_2$ satisfies [3, Lemma 7]. Consequently, $(S_1 \oplus S_2)^\varphi$ contains nonzero nilpotent elements iff S_1^φ is generated by an idempotent element of order 2^2. If $e_1 r = 0$, then $S_1 r = \{0\}$, and by Theorem 1, $L(S_1 \oplus \langle r \rangle) \cong L(S_1) \times L(\langle r \rangle)$. In view of Theorem 1, a p-ring whose subring lattice decomposes into a direct product of lattices does not contain idempotent elements of nonprime additive order. If $e_1 r \neq 0$, then $S_1 + (e_1 r)$ is a local ring. According to [5, Lemma 3], $(S_1 + (e_1 r))^\varphi \cong S_1 + (e_1 r)$. This argument implies that the subring $(S_1 \oplus S_2)^\varphi$ contains no nonzero nilpotent elements and, therefore, decomposes into a direct sum of two finite fields.

Coming back to the general case and applying Theorem 4 to a subring S, we conclude that S^φ is a one-generated ring decomposable into a direct sum of n Galois rings.

Let $(\forall i = \overline{1, n})$ $S_i^\varphi = S'_i$. The ring S^φ is one-generated, so $(\forall i, j = \overline{1, n})$ $S'_i S'_j = S'_j S'_i$. Proposition 1 implies that $\langle r \rangle^\varphi = \langle r' \rangle$, where $r' \in R^\varphi$. Then $R^\varphi = S'_1 \vee \cdots \vee S'_n \vee \langle r' \rangle$. If we apply Lemma 2 to a subring $S_i + (r)$ for every $i = \overline{1, n}$ we conclude that $S'_i \vee \langle r' \rangle$ is a one-generated subring. Consequently, the ring R^φ is commutative.

By hypothesis, R is a ring with identity. Obviously, an identity in R is the element $e = e_1 + \cdots + e_n$. Since $er = r \neq 0$, there exists an index $i \in \{1, \ldots, n\}$ with which $e_i r = r_i \neq 0$. Without loss of generality, we may assume that $i = 1$. Let $\langle r_1 \rangle^\varphi = \langle r'_1 \rangle$. We prove that r'_1 is a nilpotent element. Consider a subring $H = \langle e_1, r_1 \rangle \oplus \langle e_2 \rangle$. By [13, Thm. 3], the subrings $H_1 = \langle e_1, r_1 \rangle$ and

$H_2 = \langle e_2\rangle \oplus \langle r_1\rangle$ each contains two maximal subrings, while $H_3 = \langle e_1\rangle \oplus \langle e_2\rangle$, in view of [3, Lemma 4], contains three maximal subrings. Let $\langle e_i\rangle^{\varphi} = \langle e_i'\rangle$, $i = 1, 2$. If $o(e_1) > p$ or $o(e_2) > p$, then $H_3^{\varphi} \cong H_3$ by virtue of [3, Lemmas 6, 8]; so e_i' are nonzero idempotents, and r_1' is a nonzero nilpotent element by virtue of [13, Thm. 3]. Suppose $o(e_1) = o(e_2) = p$. Then $o(r_1) = p$, and so $pH = \{0\}$. According to Theorem 1, $L(H) \cong L(H_3) \times L(\langle r_1\rangle)$. Consequently, $L(H^{\varphi}) \cong L(H_3^{\varphi}) \times L(\langle r_1\rangle^{\varphi}))$. In view of [11, Cor, 6], one of the subrings H_3^{φ} or $\langle r_1\rangle^{\varphi}$ is nilpotent and the other, on the contrary, contains no nonzero nilpotent elements. If the subring H_3^{φ} is nilpotent, then $p = 2$ and $\langle r_1\rangle^{\varphi}$ is a chain of length at most two. By Theorem 3, either $\langle r_1\rangle^{\varphi} = GF(2)$ or $\langle r_1\rangle^{\varphi} = GF(2^q)$. According to [4, Cor. 4], the ring H is not generated by one element in either case. Therefore, $R \neq H$. Hence two cases are possible.

Case (1). Let $o(e_1) = o(e_2) = p$ and $l(S_1) + l(S_2) > 2$. Suppose $l(S_1) > 1$. Then the subring S_1 is a field, and $S_1 \dotplus \langle r_1\rangle$ is a local subring. In view of [16, Thm. 3], the subring $\langle r_1\rangle^{\varphi}$ is nilpotent, which contradicts the assumption. If $l(S_2) > 2$, then the subring S_2 is a field. If we apply [2, Cor. 3.1] to a subring $S_1 \oplus S_2$ we conclude that S_2 is a field of length 2. By Theorem 1, $L(\langle e_1, r_1\rangle \oplus S_2) \cong L(\langle e_1\rangle \oplus S_2) \times L(\langle r_1\rangle)$. The subrings $\langle e_1\rangle^{\varphi}$ and $\langle e_2\rangle^{\varphi}$ being nilpotent implies that so is S_2^{φ}. Consequently, the subring $(\langle e_1\rangle \oplus S_2)^{\varphi}$, too, is nilpotent. However, $(\langle e_1\rangle \oplus S_2)$ satisfies the hypotheses of [3, Lemma 7] and cannot be lattice-isomorphic to a nilpotent ring, a contradiction. Hence Case (1) is impossible.

Case (2). Let $n > 2$. Consider a subring $D = H \oplus \langle e_3\rangle$, where e_3 is the identity of the subring S_3. Let $E = \langle e_1\rangle \oplus \langle e_2\rangle \oplus \langle e_3\rangle$. By Theorem 1, $L(H \oplus \langle e_3\rangle) \cong L(E) \times L(\langle r_1\rangle)$. According to [2, Lemma 3.1], $E^{\varphi} \cong E$, and hence the assumption that the subring H_3^{φ} is nilpotent is untrue. Consequently, nilpotent is the subring $\langle r_1\rangle^{\varphi}$. Thus the element r_1' is nilpotent, as also are all elements r_i' $(i = \overline{1,n})$.

Let $\langle r\rangle^{\varphi} = \langle r'\rangle$ and $\langle r_i\rangle^{\varphi} = \langle r_i'\rangle$, $i = \overline{1,n}$. Since $r \in \langle r_1, \ldots, r_n\rangle$, we have $r' \in \langle r_1', \ldots, r_n'\rangle$, The ring R^{φ} is commutative, so the ring $\langle r_1', \ldots, r_n'\rangle$ is nilpotent. This implies that r' is a nilpotent element. It is clear that $R^{\varphi} = S^{\varphi} + (r')$, and since S^{φ} is a one-generated subring, R^{φ} is a one-generated ring, as follows by Theorem 2.

Part 2. Let R be a ring without identity. If R is nilpotent, then the result follows from Prop. 1.

Let R be nonnilpotent. By Lemma 1, the ring R is representable as $R = \langle t\rangle \oplus \langle r\rangle$, where $\langle t\rangle$ is a nonzero subring with identity, decomposable into a finite direct sum of rings $T_i = S_i + (r_i)$, $i = \overline{1,n}$, in which case $S_i \cong GR(p^{n_i}, m_i)$, r_i is a nilpotent element, an identity element of a subring S_i is one in T_i, and r is a nonzero nilpotent element. The first part of the proof implies that the projective image of a subring $\langle t\rangle$ is one-generated. Let $\langle t\rangle^{\varphi} = \langle t'\rangle$. In view of Proposition 1, $\langle r\rangle^{\varphi} = \langle r'\rangle$ for some element $r' \in R^{\varphi}$. Consequently, $R^{\varphi} = \langle t'\rangle \vee \langle r'\rangle$.

We prove that R^{φ} is a commutative ring. Consider a subring $W_i = T_i \oplus \langle r\rangle = (S_i + (r_i)) \oplus \langle r\rangle = S_i + (w_i)$, where $w_i = r_i + r$, $i = \overline{1,n}$. Obviously, w_i is a nilpotent element. By hypothesis, every subring S_i, $i = \overline{1,n}$, is one-generated, and so is the ring W_i in virtue of Theorem 2. By Lemma 2, the ring W_i^{φ} is also one-generated. Since $(\forall i = \overline{1,n})\,(W_i^{\varphi} = T_i^{\varphi} \vee \langle r'\rangle$ and $T_1^{\varphi} \vee \cdots \vee T_n^{\varphi} = \langle t'\rangle)$, we have $r't' = t'r'$, and hence R^φ is commutative.

Let $w = r_1 + \cdots + r_n + r$. Then w is a nilpotent element, and $R = S + (w)$, where $S = S_1 \oplus \cdots \oplus S_n$. By hypothesis, the ring R is one-generated, and so is the ring S in virtue of Theorem 2. Since w is a nilpotent element, $\langle w\rangle^\varphi$ is a one-generated ring. Let $\langle w\rangle^\varphi = \langle w'\rangle$. By Theorem 4, the ring S^φ is one-generated. If w' is a nilpotent element, then $R^\varphi = S^\varphi + (w')$, and R^φ is a one-generated ring by Theorem 2.

Let $N = \langle r_1\rangle \oplus \cdots \oplus \langle r_n\rangle \oplus \langle r\rangle$. It is clear that $w \in N$. There are three cases to consider.

Case (a). Suppose $(\forall i = \overline{1,n})\,(r_i = 0)$. Then $N = \langle r\rangle$ and $R = S \oplus \langle r\rangle$. By Lemma 2, R^φ is a one-generated ring for $n = 1$.

Let $n = 2$ and $S \cong GF(2^q) \oplus GF(2)$. According to Theorem 1, $L(S \oplus \langle r\rangle) \cong L(S) \times L(\langle r\rangle)$. By [11, Cor. 6], one of the subrings S^φ or $\langle r\rangle^\varphi$ is nilpotent and the other contains no nonzero nilpotent elements. In view of [3, Lemma 7], no nil ring can be lattice-isomorphic to a ring S. Therefore, the subring $\langle r\rangle^\varphi$ is nilpotent, and hence r' is a nilpotent element. If $n \geqslant 2$ and $S \ncong GF(2^q) \oplus GF(2)$, then it follows by Theorem 4 that S^φ is decomposable into a direct sum of n Galois rings, and so S^φ contains an orthogonal system of n nonzero idempotents. If the ring N^φ is nonnilpotent, then R^φ will contain an orthogonal system of $n+1$ nonzero idempotents. Since $n + 1 \geqslant 3$, it follows by [5, Prop. 2] that such an orthogonal system of idempotents should also be in R. Obviously, in the ring $R = S_1 \oplus \cdots \oplus S_n \oplus \langle r\rangle$ any orthogonal system of nonzero idempotents consists of not more than n elements. Thus if $n > 1$ and $(\forall i = \overline{1,n})\,(r_i = 0)$, then the subring $N^\varphi = \langle r\rangle^\varphi = \langle r'\rangle$ is nilpotent, and hence, as shown above, R^φ is a one-generated ring.

Case (b). Let $(\exists i, j \in \{1, \ldots, n\})\,(i \neq j, r_i \neq 0, r_j \neq 0)$. By [1, Thm. 1], N^φ is a nil ring, and hence, as above, R^φ is a one-generated ring.

Case (c). Let $(\exists i \in \{1, \ldots, n\})\,(r_i \neq 0)$ and $(\forall j \in \{1, \ldots, n\} \setminus \{i\})\,(r_j = 0)$. There is no loss of generality in assuming that $i = 1$. Then $R = (S_1 \dotplus \langle r_1\rangle) \oplus \cdots \oplus S_n \oplus \langle r\rangle$. For $n = 1$, $R = (S_1 \dotplus \langle r_1\rangle) \oplus \langle r\rangle = S_1 + (w)$, where $w = r_1 + r$. By Lemma 2, R^φ is one-generated. Let $n > 1$. If we treat the subring $R_1 = S_1 \oplus \cdots \oplus S_n \oplus \langle r\rangle$ and apply to it the argument from Case (a) we conclude that r' is a nilpotent element. Then the ring N^φ contains a nonzero nilpotent element r', and by [1, Thm. 1], N^φ is a nil ring. Since $w' \in N^\varphi$, the ring $R^\varphi = S^\varphi + (w')$ is one-generated by Theorem 2. The theorem is proved.

Using Theorem 5 as the base of induction on a variable k, we derive

COROLLARY 1. Let φ be a projection of a k-generated finite p-ring R onto a p-ring R^φ. Then R^φ is a finite k-generated ring.

3. PROJECTIONS OF MATRIX RINGS

The theorem below likewise pertains to the basic results of the paper. Its proof relies essentially on the results and methods in [8-10].

THEOREM 6. Let $R = M_n(K)$, where K is a finite p-ring with identity, $n \geqslant 2$. Let φ be a lattice isomorphism of the ring R onto the ring R^φ. The following statements are valid:

(1) $R^\varphi = M_n(K')$, where K' is a finite p-ring with identity;

(2) $\langle u\rangle^\varphi = \langle u'\rangle$, where u and u' are the identity elements of the rings R and R^φ, respectively;

(3) $\operatorname{char} R^\varphi = \operatorname{char} R$;

(4) the projective image Y^φ of a nilpotent ring $Y \subset R$ is a nilpotent ring;

(5) $(\operatorname{Rad} R)^\varphi = \operatorname{Rad} R^\varphi$;

(6) $|\operatorname{Rad} R^\varphi| = |\operatorname{Rad} R|$;

(7) if K is a semiprime ring then $R^\varphi \cong R$;

(8) $|R^\varphi| = |R|$;

(9) $(e_{ii}Re_{ii})^\varphi = e'_{ii}R^\varphi e'_{ii}$, where e_{ii} are diagonal matrix units in R, and $\langle e_{ii}\rangle^\varphi = \langle e'_{ii}\rangle$, $i = \overline{1,n}$;

(10) the ring K' is matrix isomorphic to the ring K.

Proof. Let $R = M_n(K)$, where $n > 1$, and K be a finite p-ring with identity e. Suppose also that $o(e) = p^k$. Let φ be a projection of R onto R^φ. Consider a subring $S = M_n(\langle e\rangle)$. By [8, Thm. 1.2], $S^\varphi \cong S$. This, in particular, implies that the subring S^φ and hence the ring R^φ itself will be p-rings. Consequently, φ is a projection of the p-ring R onto the p-ring R^φ. According to Theorem 5, the projective image of any one-generated subring in R will be a one-generated subring in R^φ, and conversely, the projective preimage of any one-generated subring in R^φ will be a one-generated subring in R. In what follows, these facts will be used without further comments.

Let e_{ij} $(i, j = \overline{1,n})$ be a system of matrix units in a ring S and $u = e_{11} + \cdots + e_{nn}$ be an identity in the ring R. By [10, Lemma 6], $\left(\forall i = \overline{1,n}\,\right)(\exists\, e'_{ii} \in R^\varphi)\,(\langle e_{ii}\rangle^\varphi = \langle e'_{ii}\rangle \cong \langle e_{ii}\rangle)$; $e'_{11}, e'_{22}, \ldots, e'_{nn}$ is an orthogonal system of idempotents; $u' = e'_{11} + e'_{22} + \cdots + e'_{nn}$ is an identity of the ring S^φ, and

$$\langle u\rangle^\varphi = \langle u'\rangle. \tag{10}$$

By [10, Thm. 3], the system of idempotents $e'_{11}, e'_{22}, \ldots, e'_{nn}$ can be complemented to a full system of matrix units e'_{ij}, $i, j = 1, n$ in the ring S^φ.

We prove that u' is the identity in the ring R^φ. Assume the contrary and consider a two-sided Peirce decomposition of R^φ with respect to an idempotent u':

$$R^\varphi = u'R^\varphi u' \dotplus u'R^\varphi(1-u') \dotplus (1-u')R^\varphi u' \dotplus (1-u')R^\varphi(1-u'). \tag{11}$$

Note that $S^\varphi \subseteq u'R^\varphi u'$ since $u'R^\varphi u'$ is the greatest subring of R^φ in which the element u' is an identity. In addition, the subring $u'R^\varphi u'$ contains a system of matrix units e'_{ij}, $i, j = \overline{1,n}$, and according to [17, Prop. 6], $u'R^\varphi u' = M_n(K')$, where K' is a subring of $u'R^\varphi u'$ consisting of all elements commuting with all e'_{ij}, $i, j = \overline{1,n}$. The projective preimage of the ring $u'R^\varphi u'$ contains a subring S; hence it contains an identity element and a system of matrix units and is therefore also the complete matrix ring over some subring B of K. Let $T = M_n(B)$ and $T^\varphi = u'R^\varphi u'$. By [10, Lemma 5], the ring T contains as a subring the Galois ring $T_1 = GR(p^k, n)$. If $k = 1$, then $T_1 = GF(p^n)$, and since the unique minimal subring of the field T_1 is the subring $\langle u\rangle$, with equality (10) in mind, we conclude that $u' \in T_1^\varphi$. Projective images of finite fields were taken up in [2]. According to [2, Thm. 2.1], T_1^φ is a field. If $k > 1$, then $T_1^\varphi \cong T_1$ in view of [3, Thm. 4].

Suppose that $u'R^\varphi(1-u') \neq \{0'\}$ and choose a nonzero element $s' \in u'R^\varphi(1-u')$ of additive prime order. It is clear that $u's' = s'$, $s'u' = 0'$, and $(s')^2 = 0'$. For any integer α, therefore, the element $u' + \alpha s'$ is a nonzero idempotent, and hence a subring $U' = \langle u' \rangle \dotplus \langle s' \rangle$ contains exactly $p+1$ maximal subrings

$$\langle u' \rangle, \langle u' + s' \rangle, \ldots, \langle u' + (p-1)s' \rangle, p\langle u' \rangle \dotplus \langle s' \rangle.$$

The ring R contains an element s of additive prime order such that $\langle s \rangle^\varphi = \langle s' \rangle$. A subring $U = \langle u \rangle \dotplus \langle s \rangle$ is the projective preimage of the ring U' under the lattice isomorphism φ. The subring U is commutative and is not a nil ring. In addition, it is not a direct sum of prime fields if $k > 1$ and, obviously, $L(U)$ is not a chain. By virtue of [13, Thm. 4], the ring U contains a subring in which there are exactly two maximal subrings. In U' every commutative subring either is generated by an idempotent element or is a nil ring, and by [13, Thm. 4], also, it does not contain a subring having exactly two maximal subrings, a contradiction. Consequently, $u'R^\varphi(1-u') = \{0'\}$ for $k > 1$.

Let $k = 1$. Again we address the subring $T_1 = GF(p^n)$ and its projective image T_1^φ. Let $T_1^\varphi = \langle x' \rangle$. Then $x's', s'$ are linearly independent nilpotent elements. A subring $W' = \langle u', x's', s' \rangle$ has order p^3, and the length of its subring lattice equals three. The subring lattice of the projective preimage W of the ring W' also has length three. According to [2, Lemma 3.1], the ring W cannot be decomposed into a direct sum of three prime fields, and W, being generated by its subrings of order p, lacks subfields of length 2. Consequently, the ring W contains a nonzero nilpotent element y of nilpotency index 2 and additive order p. Clearly, a subring $\langle u, y \rangle$ contains exactly two proper subrings $\langle u \rangle$ and $\langle y \rangle$. By [13, Thm. 4], the ring W' does not contain a subring in which there would be only two proper subrings, a contradiction. Consequently, for $k = 1$, too, the equality $u'R^\varphi(1-u') = \{0'\}$ holds.

The equality $(1-u')R^\varphi u' = \{0'\}$ is proved in a similar way.

Suppose that $(1-u')R^\varphi(1-u') \neq \{0'\}$ and choose in $(1-u')R^\varphi(1-u')$ a nonzero element w'.

Let w' be a nilpotent element of characteristic p and nilpotency index 2 in the subring $(1-u')R^\varphi(1-u')$, $w \in R$, and $\langle w \rangle^\varphi = \langle w' \rangle$. Consider a subring $V' = T_1^\varphi \oplus \langle w' \rangle$ and its projective preimage $V = T_1 \dotplus \langle w \rangle$. If $k = 1$, then, as noted, T_1^φ is a nonprime field, and by Theorem 1, the subring lattice $L(V')$ decomposes into a direct product of lattices. It is not hard to see that a ring V does not satisfy the hypotheses of Theorem 1, and so the subring lattice $L(V)$ does not decompose into a direct product of lattices. If $k > 1$, then $T_1^\varphi \cong T_1 = GR(p^k, n)$, and Theorem 2 says that V' is a one-generated subring. Applying [4, Lemma 16] to the inverse projection φ^{-1}, we conclude that $V \cong V'$. We are led to a contradiction since the ring V contains the identity of R, while the ring V' has no identity element. Consequently, the ring $(1-u')R^\varphi(1-u')$ lacks nonzero nilpotent elements and, therefore, decomposes into a direct sum of fields.

Let y' be a nonzero idempotent in a subring $(1-u')R^\varphi(1-u')$, $y \in R$, and $\langle y \rangle^\varphi = \langle y' \rangle$. Applying [9, Thm. 4(2)] to a subring $Y' = S^\varphi \oplus \langle y' \rangle$ and the inverse projection φ^{-1}, we conclude that y

is a nonzero idempotent of characteristic p. According to [10, Lemma 5], a subring S^{φ} contains a Galois subring $G_1' = GR(p^k, n)$ which contains the identity element u' of the subring S^{φ}. If $k = 1$, then $G_1' \cong GR(p, n)$, i.e., G_1' is a field of length $n > 1$. In this case the projective preimage G_1 of G_1' is also a field since it cannot contain nonzero nilpotent elements in virtue of [10, Thm. 3(b)]. Furthermore, the field G_1 contains the identity of R, and so the subring $G_1 \vee \langle y \rangle$, in view of [2, Lemma 1.2, Cor. 3.1], cannot be lattice-isomorphic to ring $G_1' \oplus \langle y' \rangle$. If $k > 1$, then $G_1 \cong G_1'$ by [3, Thm. 4], and by [4, Lemma 12], the subring $G_1 \vee \langle y \rangle$ too cannot be lattice-isomorphic to $G_1' \oplus \langle y' \rangle$. Thus our supposition is invalid. Hence u' is an identity element in the ring R^{φ}, and so $R^{\varphi} = M_n(K')$. Statements (1) and (2) are proved.

The truth of statement (3) follows from statement (2).

(4) Let N be a nilpotent subring in the ring R. Consider a local subring $D = \langle u \rangle + N$ and its projective image $D^{\varphi} = \langle u' \rangle + N^{\varphi}$. The subring D and the projection φ of the ring D onto the ring D^{φ} satisfies the hypotheses of Lemma 4 in [10], which says that N^{φ} is a nilpotent subring.

(5) Let M be a maximal nilpotent subring in R. According to statement (4), M^{φ} is a nilpotent subring in R^{φ}. Suppose that the subring M^{φ} is not a maximal nilpotent subring in the ring R^{φ}. Let $M^{\varphi} \subset M_1'$, where M_1' is a nilpotent subring in R^{φ}. A subring $H' = \langle u' \rangle + M_1'$ is a local ring. The projective preimage of the ring H' is a ring $H = \langle u \rangle + M_1$, where M_1 is the projective preimage of the subring M_1'. Applying [10, Lemma 4] to a subring H' and the inverse projection φ^{-1}, we conclude that M_1 is a nilpotent subring. Since M is a proper subring of M_1, we arrive at a contradiction. Hence M^{φ} is a maximal nilpotent subring in R^{φ}. According to [18], $\operatorname{Rad} R$ is the intersection of all maximal nilpotent subrings in R. Consequently, $(\operatorname{Rad} R)^{\varphi} = \operatorname{Rad} R^{\varphi}$.

Statement (6) follows from [1, Lemma 7].

(7) Let K be a semiprime ring, and namely: $K = K_1 \oplus \cdots \oplus K_m$, where K_i is a finite prime ring, i.e., either $K_i = GF(p^{k_i})$ or $K_i = M_{n_i}(GF(p^{k_i}))$, with $n_i > 1$, $i = \overline{1, m}$. Then $R = M_n(K_1) \oplus \cdots \oplus M_n(K_m)$. By statement (1), $(M_n(K_i))^{\varphi} = M_n(K_i')$, where K_i' is a ring with identity, $i = \overline{1, m}$. Let e_i be an identity in a ring K_i, $i = \overline{1, m}$. Then $e = e_1 + \cdots + e_m$, and so $S = M_n(\langle e \rangle) = M_n(\langle e_1 \rangle) \oplus \cdots \oplus M_n(\langle e_m \rangle)$. In view of [10, Thm. 3.4] and statement (1), $S^{\varphi} = M_{n_1}(\langle e_1' \rangle) \oplus \cdots \oplus M_{n_m}(\langle e_m' \rangle)$, where e_i' is an identity element of a ring K_i', $i = \overline{1, m}$. This implies that $R^{\varphi} = M_n(K_1') \oplus \cdots \oplus M_n(K_m')$. Let $i \in \{1, \ldots, m\}$. For $K_i = GF(p^{k_i})$, the lattice definability of a ring $M_n(K_i)$ follows from [9, Thm. 1]. If $K_i = M_{n_i}(GF(p^{k_i}))$, then $M_n(K_i) = M_n(M_{n_i}(GF(p^{k_i})) = M_{nn_i}(GF(p^{k_i}))$, and so the lattice definability of $M_n(K_i)$ again follows from [9, Thm. 1]. Statement (7) is proved.

Statement (5) implies that the factor rings $\overline{R} = R/\operatorname{Rad} R$ and $\overline{R^{\varphi}} = R^{\varphi}/\operatorname{Rad} R^{\varphi}$ are lattice-isomorphic. In view of statement (7), $\overline{R} \cong \overline{R^{\varphi}}$, and in virtue of statement (6), $|\operatorname{Rad} R^{\varphi}| = |\operatorname{Rad} R|$. Hence $|R| = |\overline{R}| \cdot |\operatorname{Rad} R| = |\overline{R^{\varphi}}| \cdot |\operatorname{Rad} R^{\varphi}| = |R^{\varphi}|$. Statement (8) is proved.

(9) Let $|K| = p^{\kappa}$. We use induction on κ.

For $\kappa = 1$, $K = \langle e \rangle$, $o(e) = p$, and $R = M_n(\langle e \rangle)$. That statement (9) is true follows from [10, Thm. 3(d)].

Suppose statement (9) has been proven for all numbers $1 \leqslant \kappa < \nu$. Let $\kappa = \nu$. If $K = \langle e \rangle$, then the truth of statement (9) again follows from [10, Thm. 3(d)]. Let $K \neq \langle e\rangle$. Suppose that the ring K contains two distinct maximal subrings W_1 and W_2 containing an identity e. Let $T_i = M_n(W_i)$, $i = 1, 2$. By the induction hypothesis, the following equalities hold: $(e_{jj}T_ie_{jj})^{\varphi} = e'_{jj}T_i^{\varphi}e'_{jj}$ for $i = 1, 2$ and $j = \overline{1, n}$. It is obvious that

$$\begin{aligned}(e_{jj}T_1e_{jj}) \vee (e_{jj}T_2e_{jj}) &= e_{jj}(T_1 \vee T_2)e_{jj}\\ &= e_{jj}M_n(W_1 \vee W_2)e_{jj}\\ &= e_{jj}M_n(K)e_{jj}\\ &= e_{jj}Re_{jj}.\end{aligned}$$

Therefore,

$$\begin{aligned}(e_{jj}Re_{jj})^{\varphi} &= (e'_{jj}T_1^{\varphi}e'_{jj}) \vee (e'_{jj}T_2^{\varphi}e'_{jj})\\ &= e'_{jj}(T_1^{\varphi} \vee T_2^{\varphi})e'_{jj}\\ &= e'_{jj}M_n(W_1^{\varphi} \vee W_2^{\varphi})e'_{jj}\\ &= e'_{jj}M_n(K')e'_{jj}\\ &= e'_{jj}R^{\varphi}e'_{jj}.\end{aligned}$$

Let W be the unique maximal subring in K containing an identity e. Obviously, $(\forall v \in K \setminus W)\,(\langle e, v\rangle \nsubseteq W)$, and so $\langle e, v\rangle = K$. This implies that K is a commutative ring. It is well known that a finite commutative ring with identity either is local or is decomposable into a direct sum of local rings [15, Chap. 2, Thm. 5]. Let K be decomposable into a direct sum of local rings, i.e., $K = P_1 \oplus \cdots \oplus P_l$. Put $R_j = M_n(P_j)$ $(j = \overline{1, l})$. Then $e_{ii}Re_{ii} = e_{ii}R_1e_{ii} \oplus \cdots \oplus e_{ii}R_le_{ii}$. By [10, Thm. 3], $(\forall j = \overline{1, l})((e_{ii}R_je_{ii})^{\varphi} = e'_{ii}R_j^{\varphi}e'_{ii}$. By [10, Cor. 2], $R^{\varphi} = R_1^{\varphi} \oplus \cdots \oplus R_l^{\varphi}$. Hence $(\forall i = \overline{1, n})((e_{ii}Re_{ii})^{\varphi} = (e_{ii}R_1e_{ii})^{\varphi} \oplus \cdots \oplus (e_{ii}R_le_{ii})^{\varphi} = e'_{ii}R_1^{\varphi}e'_{ii} \oplus \cdots \oplus e'_{ii}R_l^{\varphi}e'_{ii} = e'_{ii}R^{\varphi}e'_{ii}$.

Thus statement (9) is true also for $\kappa = \nu$, and hence for all numbers κ.

(10) In view of [17, Prop. 6], there are isomorphisms $e_{11}Re_{11} \cong K$ and $e'_{11}R^{\varphi}e'_{11} \cong K'$. By virtue of statement (9), the rings $e_{11}Re_{11}$ and $e'_{11}R^{\varphi}e'_{11}$ are lattice-isomorphic, and so $L(K) \cong L(K')$. The theorem is proved.

THEOREM 7. Let $R = M_n(K)$, where K is a finite ring with identity, $n \geqslant 2$. Suppose also that φ is a lattice isomorphism of the ring R onto the ring R^{φ}. Then $R^{\varphi} = M_n(K')$, where K' is a finite ring with identity, lattice-isomorphic to the ring K.

Proof. Let $K = K_1 \oplus \cdots \oplus K_m$ be a decomposition of K into a direct sum of p_i-rings K_i taken over distinct prime numbers p_i, $i = \overline{1, m}$. Then $R = R_1 \oplus \cdots \oplus R_m$, where $R_i = M_n(K_i)$, $i = \overline{1, m}$, and $L(R) \cong L(R_1) \times \cdots \times L(R_m)$. Let φ be a lattice isomorphism of R onto R^{φ}. Clearly, $L(R^{\varphi}) \cong L(R_1^{\varphi}) \times \cdots \times L(R_m^{\varphi})$. By Theorem 6, $R_i^{\varphi} = M_n(K'_i)$, where K'_i is a p_i-ring with identity, lattice isomorphic to a ring K_i, $i = \overline{1, m}$. Since prime numbers p_i, $i = \overline{1, m}$, are pairwise distinct, we have $R^{\varphi} = R_1^{\varphi} \oplus \cdots \oplus R_m^{\varphi}$. Let $K' = K'_1 \oplus \cdots \oplus K'_m$. Then $R^{\varphi} = M_n(K')$ and K', in this case, is a ring with identity, lattice-isomorpic to the ring K. The theorem is proved.

THEOREM 8. Let $R = M_{n_1}(K_1) \oplus \cdots \oplus M_{n_l}(K_l)$, where K_i is a finite local p-ring, $|K_i/\mathrm{Rad}\, K_i| = p^{m_i}$, $i = \overline{1,l}$. Suppose that R is not isomorphic to the rings $GF(p^q) \oplus GF(p)$ (q is a prime) and $GF(p) \oplus GF(p)$. Let φ be a lattice isomorphism of the ring R onto the ring R^φ. Then the following statements hold:

(1) $R^\varphi = R_1^\varphi \dotplus \cdots \dotplus R_l^\varphi$ (group sum);

(2) $(\forall i = \overline{1,l})$ (R_i is a prime ring $\Rightarrow R_i^\varphi$ is a prime ring);

(3) if $n_i m_i > 1$ for all $i = \overline{1,l}$, then $R^\varphi = R_1^\varphi \oplus \cdots \oplus R_l^\varphi$, and also $(\mathrm{Rad}\, R)^\varphi = \mathrm{Rad}\, R^\varphi$.

Proof. Let $R_i = M_{n_i}(K_i)$, $i = \overline{1,l}$. According to [14, Thm. XIX.4], every local p-ring K_i, $i = \overline{1,l}$, contains as a subring the Galois ring $S_i = GR(p^{k_i}, m_i)$, $i = \overline{1,l}$. In R we consider a subring $T = T_1 \oplus \cdots \oplus T_l$, where $T_i = M_{n_i}(S_i)$. This subring satisfies the hypotheses of [9, Thm. 4], which implies that statements (1) and (2) are true.

Suppose that, for all $i \in \{1, \ldots, l\}$, the conditions that $n_i m_i > 1$ are satisfied. By [9, Thm. 4], $(\forall i, j = \overline{1,l})(i \neq j \Rightarrow (T_i \oplus T_j)^\varphi = T_i^\varphi \oplus T_j^\varphi)$. These equalities imply the equality

$$R^\varphi = R_1^\varphi \oplus \cdots \oplus R_l^\varphi. \tag{12}$$

It is clear that $\mathrm{Rad}\, R = \mathrm{Rad}\, R_1 \oplus \cdots \oplus \mathrm{Rad}\, R_l$. Let $i \in \{1, \ldots, l\}$. According to [17, Thm. 3], $\mathrm{Rad}\, R_i = M_{n_i}(\mathrm{Rad}\, K_i)$, $i = \overline{1,l}$. For $n_i = 1$, $R_i = K_i$, and since $m_i > 1$, in view of [16, Thm. 3] it is true that

$$(\mathrm{Rad}\, R_i)^\varphi = \mathrm{Rad}\, R_i^\varphi. \tag{13}$$

If $n_i > 1$ then, by [10, Thm. 3], equality (13) holds as well. The truth of statement (3) follows from equalities (12) and (13). The theorem is proved.

REFERENCES

1. S. S. Korobkov, "Projections of periodic nil-rings," *Izv. Vyssh. Uch. Zav., Mat.*, No. 7, 30-38 (1980).

2. S. S. Korobkov, "Lattice isomorphisms of finite rings without nilpotent elements," *Izv. Ural. Gos. Univ., Mat. Mekh. Komp. Nauki*, Iss. 4, No. 22, 81-93 (2002).

3. S. S. Korobkov, "Projections of Galois rings," *Algebra and Logic*, **54**, No. 1, 10-22 (2015).

4. S. S. Korobkov, "Projections of finite one-generated rings with identity," *Algebra and Logic*, **55**, No. 2, 128-145 (2016).

5. S. S. Korobkov, "Projections of finite commutative rings with identity," *Algebra and Logic*, **57**, No. 3, 186-200 (2018).

6. D. W. Barnes, "Lattice isomorphisms of associative algebras," *J. Aust. Math. Soc.*, **6**, No. 1, 106-121 (1966).

7. A. V. Yagzhev, "Lattice definability of certain matrix algebras," *Algebra and Logic*, **13**, No. 1, 57-65 (1974).

8. S. S. Korobkov, “Lattice definability of certain matrix rings,” *Mat. Sb.*, **208**, No. 1, 97-110 (2017).

9. S. S. Korobkov, “Projections of finite nonnilpotent rings,” *Algebra and Logic*, **58**, No. 1, 48-58 (2019).

10. S. S. Korobkov, “Projections of semilocal rings,” *Algebra and Logic*, **61**, No. 2, 125-138 (2022).

11. S. S. Korobkov, “Periodic rings with subring lattices decomposable into a direct product of subring lattices,” in *Studies of Algebraic Systems via Properties of Their Subsystems* [in Russian], Ural State Ped. Univ., Yekaterinburg (1998), pp. 48-59.

12. P. A. Freidman and S. S. Korobkov, “Associative rings and their lattice of subrings,” in *Studies of Algebraic Systems via Properties of Their Subsystems* [in Russian], Ural State Ped. Univ., Yekaterinburg (1998), pp. 4-45.

13. S. S. Korobkov, “Finite rings with exactly two maximal subrings,” *Izv. Vyssh. Uch. Zav., Mat.*, No. 6, 55-62 (2011).

14. B. R. McDonald, *Finite Rings with Identity*, Dekker, New York (1974).

15. V. P. Elizarov, *Finite Rings* [in Russian], Gelios, Moscow (2006).

16. S. S. Korobkov, “Lattice isomorphisms of finite local rings,” *Algebra and Logic*, **59**, No. 1, 59-70 (2020).

17. N. Jacobson, *Structure of Rings*, Am. Math. Soc., Providence, R.I. (1956).

18. D. W. Barnes, “On the radical of a ring with minimum condition,” *J. Aust. Math. Soc.*, **5**, 234-236 (1965).