DOI 10.1007/s10469-018-9492-7
Algebra and Logic, Vol. 57, No. 3, July, 2018
(Russian Original Vol. 57, No. 3, May-June, 2018)

PROJECTIONS OF FINITE COMMUTATIVE RINGS WITH IDENTITY

S. S. Korobkov

UDC 512.552

Keywords: *finite commutative rings with identity, subring lattices, lattice isomorphisms of rings.*

Associative rings R and R' are said to be lattice-isomorphic if their subring lattices $L(R)$ and $L(R')$ are isomorphic. An isomorphism of the lattice $L(R)$ onto the lattice $L(R')$ is called a projection (or a lattice isomorphism) of the ring R onto the ring R'. A ring R' is called the projective image of a ring R. We study lattice isomorphisms of finite commutative rings with identity. The objective is to specify sufficient conditions subject to which rings under lattice homomorphisms preserve the following properties: to be a commutative ring, to be a ring with identity, to be decomposable into a direct sum of ideals. We look into the question about the projective image of the Jacobson radical of a ring. In the first part, the previously obtained results on projections of finite commutative semiprime rings are supplemented with new information. Lattice isomorphisms of finite commutative rings decomposable into direct sums of fields and nilpotent ideals are taken up in the second part. Rings definable by their subring lattices are exemplified. Projections of finite commutative rings decomposable into direct sums of Galois rings and nilpotent ideals are considered in the third part. It is proved that the presence in a ring of a direct summand definable by its subring lattice (i.e., the Galois ring $GR(p^n, m)$, where $n > 1$ and $m > 1$) leads to strong connections between the properties of R and R'.

INTRODUCTION

Associative rings R and R' are said to be *lattice-isomorphic* if their subring lattices $L(R)$ and $L(R')$ are isomorphic. An isomorphism of the lattice $L(R)$ onto the lattice $L(R')$ is denoted φ and

Ural State Pedagogical University, ul. K. Libknekhta 9, Yekaterinburg, 620065 Russia; ser1948@gmail.com.
Translated from *Algebra i Logika*, Vol. 57, No. 3, pp. 285-305, May-June, 2018. Original article submitted November 22, 2016.

is called a *lattice isomorphism* (or a *projection*) of the ring R onto the ring R'. For convenience, a ring R' is denoted R^φ and is called the *projective image* of a ring R.

Let R be a finite commutative ring with identity and φ a lattice isomorphism of R onto R^φ. There are examples showing that the projective image R^φ is not always commutative. The objective of our research is to specify sufficient conditions subject to which rings under lattice homomorphisms preserve the following properties: to be a commutative ring, to be a ring with identity, to be decomposable into a direct sum of ideals. Of importance is the question about the projective image of the Jacobson radical of a ring R. This is explained by the fact that whenever the equality $(\operatorname{Rad} R)^\varphi = \operatorname{Rad} R^\varphi$ holds, the factor rings $\overline{R} = R/\operatorname{Rad} R$ and $\overline{R^\varphi} = R^\varphi/\operatorname{Rad} R^\varphi$ are lattice-isomorphic, and so their common properties, in particular, commutativity, follow from the previously obtained results [1].

The projective image of a ring R is not always a ring with identity [1, Lemma 1.2]. However, if R and R^φ contain identity elements (e.g., e and e', resp.), then the question arises whether it is true that

$$\langle e\rangle^\varphi = \langle e'\rangle, \tag{1}$$

where $\langle e\rangle$ and $\langle e'\rangle$ are subrings generated by the elements e and e'. The satisfiability of (1) is closely connected with another question: Will projective images of direct summands of a ring R be direct summands in R^φ?

Yet another important problem in studying projections of rings is searching for lattice-definable rings, i.e, rings isomorpic to their projective images. Such rings being unique objects are interesting in their own right.

The study of lattice isomorphisms of finite commutative rings with identity was started in [1] and continued in [2, 3]. According to [1, Prop. 3.1], the projective image of a ring decomposable into a direct sum of finite fields, which is not isomorphic to the sum $GF(p) \oplus GF(p)$, is a commutative ring. Furthermore, in [1, Thm. 4.1], necessary and sufficient conditions were found under which projective images of direct sums of finite fields are direct sums of projective images of summands. However, whether (1) is satisfiable was not explored in that case. In [2], it was proved that the Galois ring $GR(p^n, m)$ is lattice-definable for $n > 1$ and $m > 1$. Lattice isomorphisms of finite rings decomposable into direct sums of Galois rings of different types were dealt with in [3]. The results obtained in [2, 3] imply that the projective image of a finite ring with identity which is decomposable into a direct sum of Galois rings is (with some exceptions) a commutative ring with identity.

The basic content of the paper is presented in three sections. In Sec. 1, the previously obtained results on projections of finite commutative semiprime rings are supplemented with new information. Lattice isomorphisms of finite commutative rings decomposable into direct sums of fields and nilpotent ideals are taken up in Sec. 2. The presence in R of a proper nilpotent ideal leads to a more close relationship between the rings R and R^φ: both R and R^φ have equal characteristics, $(\operatorname{Rad} R)^\varphi = \operatorname{Rad} R^\varphi$, Eq. (1) is satisfied, decomposability into a direct sum of ideals

is preserved (Thm. 4), while the commutative property may fail to be respected (Example 2). Lemma 3 and Theorem 3 contain examples of rings definable by their subring lattices. Projections of finite commutative rings decomposable into direct sums of Galois rings and nilpotent ideals are considered in Sec. 3. The presence in a ring of a direct summand definable by its subring lattice (namely, the Galois ring $GR(p^n, m)$, where $n > 1$ and $m > 1$) also leads to strong connections between the properties of R and R^φ. This is confirmed by Theorem 5.

We specify the notation used in the paper. Let S and T be subgroups of the additive group R^+ of a ring R. The situation where $R = \{s + t \mid s \in S \text{ and } t \in T\}$ is denoted $R = S + T$. We write $R = S \dot{+} T$ whenever $R = S + T$ and $S \cap T = \{0\}$. The equality $R = S \oplus T$ signifies that $R = S \dot{+} T$ 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. By $M(R)$ we denote the intersection of all maximal subrings of a finite ring R. Other designations are standard: $S \vee T$ is a subring generated by subrings S and T in R; $\operatorname{Rad} R$ is the Jacobson radical of a ring R; $GR(p^n, m)$ is a Galois ring; $GF(p^m) = GR(p, m)$ is a Galois field; $\mathbb{Z}$ and $\mathbb{N}$ are the sets of integers and natural numbers, 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, i.e., $(r) = \left\{ \alpha r + br + rc + \sum\limits_{i=1}^{n} x_i r y_i \;\middle|\; \alpha \in \mathbb{Z}, b, c, x_i, y_i \in R \right\}$; $o(r)$ 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 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 where the projective image of a ring generated by an element r is a one-generated ring, $\langle r\rangle^\varphi$ is denoted by $\langle r'\rangle$; in particular, $\langle 0\rangle^\varphi = \langle 0'\rangle$.

In the paper we use the concept of length for rings. We clarify it. A nonnegative integer n is called the *length of a lattice* L if L contains a chain of length n and the length of any chain in L does not exceed n. By the *length of a finite ring* R we mean the length of its subring lattice $L(R)$. The length of a ring R is denoted by $l(R)$.

A ring R is called a p-ring if its additive group R^+ is a p-group. It is well known that every finite ring decomposes into a finite direct sum of rings with primary additive groups, $R = R_{p_1} \oplus \cdots \oplus R_{p_n}$, and its subring lattice $L(R)$ decomposes into a direct product of lattices $L(R_{p_i})$, $L(R) \cong L(R_{p_1}) \times \cdots \times L(R_{p_n})$. Therefore, the study of projections of finite rings reduces to treating projections of rings with primary additive groups.

1. PRELIMINARIES

A subring $\langle e\rangle$ generated by an identity e of a ring R plays an important part in the paper. We give a description of rings that are lattice-isomorphic to the ring $\langle e\rangle$.

PROPOSITION 1 [4, Thm. 1.6]. Let $R = \langle e\rangle$, where $e^2 = e$ and $o(e) = p^n$, and φ be a projection of the ring R onto the ring R^φ. Then R^φ is isomorphic to one of the following rings:

$K_1 = \langle v\rangle$, where $v^2 = v$ and $o(v) = q^n$;

$K_2 = GF(p_1^{p_2^{n-1}})$;

$K_3 = \langle r \rangle$, where $r^2 \neq 0$, $r^3 = 0$, and $o(r) = q$;

$K_4 = \langle r \rangle$, where $r^2 = q^k r$, $k = \overline{1,n}$, and $o(r) = q^n$.

PROPOSITION 2. Let $R = \langle e_1 \rangle \oplus \cdots \oplus \langle e_n \rangle$, where $n \geqslant 2$, $e_i^2 = e_i$, $o(e_i) = p^{k_i}$, $i = \overline{1,n}$, and $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_n$, and any of the following two conditions be satisfied:

$k_1 = \ldots = k_n = 1$ and $n > 2$;

$k_1 > 1$.

Suppose also that φ is a projection of R onto R^φ. Then:

(a) $R^\varphi = \langle e'_1 \rangle \oplus \cdots \oplus \langle e'_n \rangle$, where $(e'_i)^2 = e'_i$ and $o(e'_i) = q^{k_i}$, $i = \overline{1,n}$;

(b) R^φ is a ring with identity;

(c) if $k_2 > 1$, then $R^\varphi \cong R$.

Proof. Statement (b) follows from (a), and (c) derives from [2, Thm. 2]. We prove statement (a). If $k_1 = \ldots = k_n = 1$ and $n > 2$, then (a) results from [1, Lemma 3].

Let $n \geqslant 2$, $k_1 > 1$, and $k_2 = \ldots = k_n = 1$. We use induction on the variable n. For $n = 2$, the truth of (a) follows from [2, Lemma 6]. Suppose that the statement is true for $n = m \geqslant 2$. Let $n = m + 1$. Consider a subring $V = \langle e_1 \rangle \oplus \cdots \oplus \langle e_m \rangle$ in R. By the induction hypothesis, $V^\varphi = \langle v'_1 \rangle \oplus \cdots \oplus \langle v'_m \rangle$, where $(v'_i)^2 = v'_i$ and $o(v'_i) = q^{k_i}$, $i = \overline{1,m}$. The element $v' = v'_1 + \cdots + v'_m$ is an identity in the ring V^φ. The ring V contains an idempotent element v such that $\langle v \rangle^\varphi = \langle v' \rangle$. Clearly, $o(v) = p^{k_1}$. In view of $k_1 > 1$ and [2, Lemma 6], we obtain $(\langle v \rangle \oplus \langle e_{m+1} \rangle)^\varphi = \langle v' \rangle \dot{+} \langle e'_{m+1} \rangle$, where $(e'_{m+1})^2 = e'_{m+1}$, and either $v'e'_{m+1} = e'_{m+1}v' = 0'$ or $v'e'_{m+1} = e'_{m+1}v' = e'_{m+1}$.

If $v'e'_{m+1} = 0'$, then $e'_i e'_{m+1} = (e'_i v')e'_{m+1} = e'_i(v'e'_{m+1}) = e'_i 0' = 0'$ hold for any $i = \overline{1,m}$. These equalities imply that $R^\varphi = \langle v'_1 \rangle \oplus \cdots \oplus \langle v'_m \rangle \oplus \langle e'_{m+1} \rangle$. If $v'e'_{m+1} = e'_{m+1}$, then there exists a number $j \in \{1, \ldots, m\}$ such that $v'_j e'_{m+1} = e'_{m+1}$. Consider an element $w'_j = (v' - e'_{m+1})v'_j = v'_j - e'_{m+1}$. Obviously, $(w'_j)^2 = w'_j$, $o(w'_j) = o(v'_j)$, and $w'_j e'_{m+1} = 0'$. In addition, if $i \in \{1, \ldots, m\}$ and $i \neq j$, then $w'_j v'_i = 0'$. Replacing the elements v'_j for which $v'_j e'_{m+1} \neq 0'$ by elements w'_j and denoting the remaining elements v'_i by w'_i, we obtain a system of orthogonal idempotent elements $w'_1, w'_2, \ldots, w'_{m+1}$, in which case $R^\varphi = \langle w'_1 \rangle \oplus \cdots \oplus \langle w'_{m+1} \rangle$.

Remark 1. If R satisfies the conditions of Proposition 2, then the rings R and R^φ contain identity elements e and e', respectively. However, as follows from [2, Lemmas 6, 8], Eq. (1) does not always hold.

[1, Prop. 2.1] gives rise to

PROPOSITION 3. Let $R \cong GF(p^n)$, $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the canonical decomposition of the number n, $k > 1$, and φ be a projection of the ring R onto the ring R^φ. Then R^φ is isomorphic to one of the following rings:

$K_5 = GF(q^{n'})$, where $n' = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$;

$K_6 = \langle e, r \rangle$, $e^2 = e$, $o(e) = q^2$, $o(r) = q$, $er = re = r$, $r^2 = \gamma q e$, and either $\gamma = 1$ or γ is not a square in $GF(q)$.

If $R^\varphi \cong K_6$, then the number n is a product of two distinct primes.

Remark 2. Let the rings R and R^φ be finite fields with identities e and e', respectively. Then Eq. (1) holds.

Indeed, the subrings $\langle e\rangle$ and $\langle e'\rangle$ are unique minimal subrings in R and R^φ, respectively; so $\langle e\rangle^\varphi = \langle e'\rangle$.

THEOREM 1. Let $R = F_1 \oplus \cdots \oplus F_n$, where $n > 1$, and $F_i \cong GF(p^{l_i})$, $i = \overline{1,n}$. Suppose also that $l_i > 1$, $l_i = p_1^{\alpha_1}\cdots p_{k_i}^{\alpha_{k_i}}$, $i = \overline{1,n}$, and φ is a projection of the ring R onto the ring R^φ. Then $R^\varphi = F_1^\varphi \oplus \cdots \oplus F_n^\varphi$, where $F_i^\varphi \cong GF(q^{m_i})$ and $m_i = q_1^{\alpha_1}\cdots q_{k_i}^{\alpha_{k_i}}$, $i \leqslant n$, and if e and e' are identity elements of R and R^φ, respectively, then $\langle e\rangle^\varphi = \langle e'\rangle$.

Proof. The first part of the conclusion of the theorem was proved in [1, Thm. 4.2]. We argue for the satisfiability of Eq. (1).

Let e_i and e_i' be identities of the fields F_i and F_i^φ, $i = \overline{1,n}$, respectively. Then $e = e_1 + \cdots + e_n$ and $e' = e_1' + \cdots + e_n'$ are identity elements in the rings R and R^φ, respectively. By Remark 2, the equality

$$\langle e_i\rangle^\varphi = \langle e_i'\rangle \tag{2}$$

holds for all $i = \overline{1,n}$. We use induction on the number n. For $n = 2$, the subrings $\langle e_1\rangle$, $\langle e_2\rangle$, and $\langle e_1 + e_2\rangle$ are unique minimal subrings in R. Similarly, $\langle e_1'\rangle$, $\langle e_2'\rangle$, and $\langle e_1' + e_2'\rangle$ are unique minimal subrings in R^φ. With Eq. (2) in mind, we conclude that $\langle e_1 + e_2\rangle^\varphi = \langle e_1' + e_2'\rangle$.

Suppose that Eq. (1) holds for $n = k \geqslant 2$. Let $n = k + 1$. Put $v = e_1 + \cdots + e_n$ and $v' = e_1' + \cdots + e_n'$. By the induction hypothesis, $\langle v\rangle^\varphi = \langle v'\rangle$. The subring $\langle v\rangle \oplus \langle e_n\rangle$ contains no more than three proper subrings: $\langle v\rangle$, $\langle e_n\rangle$, and $\langle v + e_n\rangle$. Since $\langle v\rangle^\varphi = \langle v'\rangle$ and $\langle e_n\rangle^\varphi = \langle e_n'\rangle$, we have $\langle v + e_n\rangle^\varphi = \langle v' + e_n'\rangle$. The theorem is proved.

2. PROJECTIONS OF RINGS CONTAINING FINITE FIELDS

In this section we consider lattice isomorphisms of finite commutative rings with identity that are decomposable into direct sums of fields and nilpotent ideals.

LEMMA 1. Let R be a p-nil-ring containing more than four elements, and let the lattice $L(R)$ not be a chain. Suppose that φ is a lattice isomorphism of the ring R onto the ring R^φ. Then R^φ is a p-ring, and if it is commutative then it is also a nil-ring.

Proof. By hypothesis, R contains more than four elements and is therefore not a direct sum of two nilpotent rings of order 2. Furthermore, $L(R)$ is not a chain. Applying [5, Thm. 1] to a subring of R, we see that R^φ is a p-ring. If R^φ is commutative, then it is a nil-ring; otherwise, in view of [5, Thm. 1], R^φ would contain elements e' and s' for which $e's' \neq s'e'$.

LEMMA 2. Let a finite commutative ring R of prime characteristic p be defined thus: $R = \langle e\rangle \dotplus N$, where e is an identity element of the ring R, N is a nil-ring of order greater than 4, and the lattice $L(N)$ is not a chain. Then the following statements hold:

(a) $R^\varphi = \langle e\rangle^\varphi \dotplus N^\varphi$;

(b) $\langle e\rangle^\varphi = \langle e'\rangle$, $o(e') = q$, and $(e')^2 = e'$ for $q = p$;

(c) N^φ is a p-nil-ring;

(d) either e' is the identity in R^φ and then $q = p$, or the equalitites $e'r' = r'e' = 0'$ hold for any element $r' \in N^\varphi$.

Proof. According to [6, Thm. 1], the subring lattice $L(R)$ decomposes into a direct product of lattices, and $L(R) \cong L(\langle e\rangle) \times L(N)$ holds by virtue of [6, Cor. 6]. Hence $L(R^\varphi) \cong L(\langle e\rangle^\varphi) \times L(N^\varphi)$ with $o(e') = p$, and by [6, Cor. 6], one of the subrings $\langle e\rangle^\varphi$ or N^φ does not contain nonzero nilpotent elements, while the other is a nil-ring. By Lemma 1, N^φ is a p-ring. If N^φ is not a nil-ring, then it follows by [5, Thm. 1] that it contains nonzero idempotent and nilpotent elements, which is impossible. Consequently, N^φ is a p-nil-ring. Then the subring $\langle e\rangle^\varphi$ does not contain nonzero nilpotent elements; hence $\langle e\rangle^\varphi = \langle e'\rangle$, $(e')^2 = e'$, and $o(e') = q$. According to [6, Thm. 1], either e' is the identity in R^φ and then $q = p$, or $e'r' = r'e' = 0'$ for any element $r' \in N^\varphi$. The lemma is proved.

We give an example showing that for $|N| \leqslant 4$, not all statements of Lemma 2 hold.

Example 1. Consider a commutative ring $K_7 = \langle e\rangle \dotplus N$, where e is an identity element, $o(e) = 2$, and $N = \langle r_1\rangle \oplus \langle r_2\rangle$ is a ring with zero multiplication. The ring K_7 has 10 subrings and contains 8 elements: $0, e, r_1, r_2, e + r_1, e + r_2, r_1 + r_2, e + r_1 + r_2$. The diagram of the subring lattice of K_7 is presented in Fig. 1.

We define another commutative ring: $K_8 = \langle r\rangle \oplus \langle e_1\rangle \oplus \langle e_2\rangle$, where $r^2 = pr = 0$, $e_i^2 = e_i$, and $o(e_i) = p$, $i \leqslant 2$. The ring K_8 contains p^3 elements and has 10 subrings. The diagram of the subring lattice of K_8 is shown in Fig. 2.

Clearly, the rings K_7 and K_8 are lattice-isomorphic. In this case statements (b)-(d) of Lemma 3 do not hold. In addition, K_7 is not a one-generated ring, while K_8 for $p \neq 2$ is generated by one element $(r + e_1 - e_2)$.

LEMMA 3. Let a finite commutative ring R be defined thus: $R = F \dotplus N$, where $F \cong GF(p^n)$, $n > 1$, an identity element e of the field F is the identity in R, N is a principal ideal in R generated by a nonzero nilpotent element. Suppose φ is a lattice isomorphism of the ring R onto the ring R^φ.

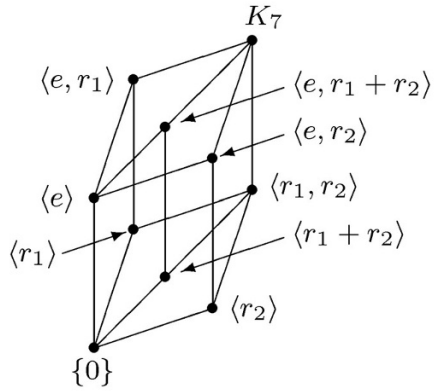

Fig. 1.

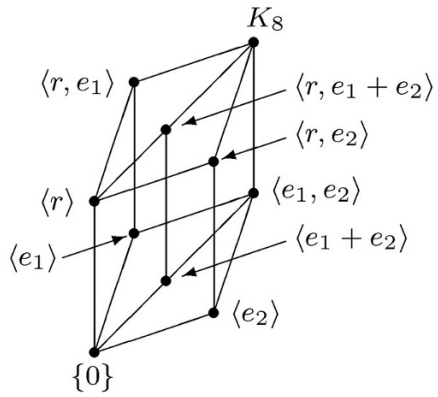

Fig. 2.

Then the following statements hold:

(a) $R^\varphi = F^\varphi \dotplus N^\varphi$;

(b) $F^\varphi \cong F$ and $N^\varphi \cong N$;

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

(d) $\langle e\rangle^\varphi = \langle e'\rangle$, where e' is the identity element in R^φ;

(e) $R^\varphi \cong R$.

Proof. In view of [3, Prop. 2], the ring R is one-generated. An identity of the field F is the identity in R, so R is a ring of prime characteristic p. Let $F = \langle x\rangle$, $N = (r)$, and $\operatorname{ind} r = m$. Since R is a commutative ring with identity, we have $N = \{sr \mid s \in R\}$, in which case N is additively generated by elements of the form $x^i r^j$, where $i = \overline{0, n-1}$ and $j = \overline{1, m-1}$. Clearly, these elements are linearly independent over $GF(p)$, and so $|N| = p^{n(m-1)}$. It is easy to see that $|N| \geqslant 4$ and $N = \operatorname{Rad} R$. Thus the ring R is uniquely defined by specifying three natural numbers p, n, and m.

Consider separately the case where $|N| = 4$. Then $p = n = m = 2$, and so the ring R consists of 16 elements. According to [7, Table 3, ring R_{14}], the maximal subrings of R are two subrings: F and $\langle e\rangle \dotplus (\langle r\rangle \oplus \langle xr\rangle)$. In addition, $F \cong GF(2^2)$ and $\langle e\rangle \dotplus (\langle r\rangle \oplus \langle xr\rangle) \cong\cong K_7$. The diagram of the subring lattice of R is presented in Fig. 3.

We now turn to examine a projective image R^φ. Since the lattice $L(F)$ is a chain, a projective image F^φ is generated by one element. Let $F^\varphi = \langle x'\rangle$, $\langle e\rangle^\varphi = \langle e'\rangle$, $\langle r\rangle^\varphi = \langle r'\rangle$, $o(e') = q_1$, and $o(r') = q_2$. If $q_1 \neq q_2$, then, in view of the equality $R^\varphi = F^\varphi \vee \langle r'\rangle$, we obtain $L(R^\varphi) \cong L(F') \times L(\langle r'\rangle)$, whence $L(R^\varphi) \ncong L(R)$. Consequently, the additive group $(R^\varphi)^+$ is primary with respect to some prime number q_1. It is clear that $\langle e, r\rangle^\varphi = \langle e', r'\rangle$, and so the subring $\langle e', r'\rangle$ contains no more than two proper subrings. Hence one of the elements e' and r' is idempotent, while the other is nilpotent. Below we use the description of finite rings having exactly two maximal subrings [7, Thm. 3] and the description of their maximal subrings [7, Table 3]. First note that the ring R itself does not contain Galois subrings of the form $GR(p^k, q^l)$, where $k, l \in \mathbb{N}$, $k > 1$, which are lattice-definable according to [2, Thm. 3]. Therefore, the ring R^φ cannot be isomorphic to the

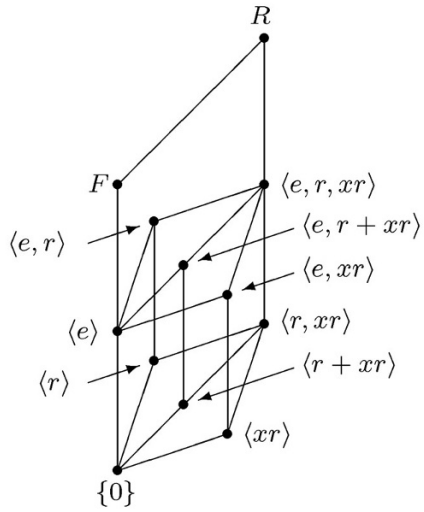

Fig. 3.

rings $R_7, R_{10}, R_{11}, R_{13}$ in the list of rings R_5-R_{14} contained in [7, Thm. 3], since these rings contain Galois subrings of the specified type. We will exclude from further consideration the rings R_9 and R_{12}, for they do not contain nonzero nilpotent elements, while the ring R^φ contains such. Using [7, Table 3], in the remaining rings R_5, R_6, R_8, R_{14} we distinguish those one of the two maximal subrings of which has a subring lattice, a chain of length 2, and the other has order q_1^3. These conditions are satisfied only by one ring, namely, the ring $R_{14} \cong GF(q^{p_1}) + (s_1)$, where p_1 is some prime number, s_1 is a nilpotent element, and $q_1 s_1 = s_1^2 = 0$. Clearly, $\operatorname{Rad} R^\varphi \cong (s_1)$, and so $(s_1) \cong \langle r, xr\rangle^\varphi$. This implies that $q_1 = p$ and $p_1 = 2$. Hence $R^\varphi \cong R$ and statements (a)-(d) of the present lemma hold as well.

Let $|N| > 4$. The subring lattice $L(N)$ is not a chain since, for instance, $\langle xr^{m-1}\rangle \cap \langle r^{m-1}\rangle = \{0\}$. The subring $T = \langle e\rangle \dotplus N$ satisfies the conditions of Lemma 2, so N^φ is a p-nil-ring, $\langle e\rangle^\varphi = \langle e'\rangle$, and e' is an idempotent element. Since $r \in N$, and $\langle r\rangle^\varphi = \langle r'\rangle$ by [5, Remark 1], r' is a nilpotent element. In view of Lemma 2, one of the following holds:

$$e'r' = r'e' = r', \tag{3}$$

$$e'r' = r'e' = 0'. \tag{4}$$

Consider the projective image F^φ of a field F. Applying Propositions 1 and 3 and keeping in mind that $\langle e'\rangle$ is the unique minimal subring in the ring F^φ, we conclude that F^φ is a finite field. If (4) holds, then $R^\varphi = F^\varphi \oplus \langle r'\rangle^\varphi$, whence $N^\varphi \subseteq \langle r'\rangle$, which clashes with $\langle r\rangle$ being a proper subring of N. Hence (3) holds true. Then F^φ is a field of characteristic p and e' is the identity in the ring R^φ. Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the canonical decomposition of the number n. By Proposition 3, $F^\varphi \cong GF(p^{n'})$ and $n' = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$.

In view of [5, Cor. 3], $\langle r'\rangle \cong \langle r\rangle$. Hence $\operatorname{ind} r' = \operatorname{ind} r = m$. Clearly, $\operatorname{Rad} R^\varphi = (r') = N^\varphi$. According to [5, Lemma 7], $|\operatorname{Rad} R| = |\operatorname{Rad} R^\varphi| = p^{n(m-1)}$. This implies that $|F^\varphi| = |F| = p^n$

and $F^\varphi \cong F$. As noted above, the ring R is uniquely defined by specifying numbers p, n, and m. Therefore, $R^\varphi \cong R$.

THEOREM 2. Let a finite commutative ring R be defined thus: $R = F \dot{+} N$, where $F \cong GF(p^n)$ $(n > 1)$, an identity element e of the field F is the identity in R, and N is a nonzero nilpotent ideal. Suppose also that φ is a lattice isomorphism of the ring R onto the ring R^φ. Then the following statements hold:

(a) $R^\varphi = F^\varphi \dot{+} N^\varphi$;

(b) $F^\varphi \cong F$;

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

(d) $\langle e\rangle^\varphi = \langle e'\rangle$, where e' is the identity element in R^φ;

(e) R^φ is commutative if and only if N^φ is commutative.

Proof. Consider the subring N^φ. Obviously, $|N| \geqslant 4$ and $L(N)$ is not a chain. By virtue of [5, Thm. 1], N^φ is a p-ring. Suppose N^φ is not a nil-ring and take in it a nonzero idempotent element u'. Let $u \in N$ and $\langle u\rangle^\varphi = \langle u'\rangle$. Applying Lemma 3 to a subring $S = F \dot{+} (u)$, we conclude that $(u)^\varphi$ is a nil-ring, a contradiction. Therefore, N^φ is a p-nil-ring.

Let r' be an arbitrary nonzero element in N^φ, $r \in N$, and $\langle r\rangle^\varphi = \langle r'\rangle$. Applying Lemma 3 to a subring $T = F \dot{+} (r)$, where (r) is a principal ideal in T generated by the element r, we conclude that N^φ is a two-sided ideal in the ring R^φ. Statements (a), (b), and (d) of the present theorem follow from Lemma 3. Since $R^\varphi/N^\varphi \cong F^\varphi \cong F$, we have $\operatorname{Rad} R^\varphi = N^\varphi = (\operatorname{Rad} R)^\varphi$, and so statement (c) holds as well.

Suppose that N^φ is a commutative subring and w'_1 and w'_2 are arbitrary elements of the ring R^φ. Let $w'_i = x'_i + r'_i$, where $x'_i \in F^\varphi$ and $r'_i \in N^\varphi$ $(i = 1, 2)$. Then $w'_1 w'_2 = (x'_1 + r'_1)(x'_2 + r'_2) = x'_1x'_2 + x'_1r'_2 + r'_1x'_2 + r'_1r'_2 = x'_2x'_1 + r'_2x'_1 + x'_2r'_1 + r'_2r'_1 = w'_2w'_1$. If the ring R^φ is commutative, then the subring N^φ is commutative. Consequently, statement (d) holds true.

Below is an example showing that the presence of an identity in a commutative ring is not sufficient for a projective image to be commutative.

Example 2. First we define two lattice-isomorphic nilpotent rings N and N' of prime characteristic $p > 2$ by setting $N = \langle r_1\rangle \oplus \langle r_2\rangle$, $\operatorname{ind} r_1 = 3$, $\operatorname{ind} r_2 = 2$; $N' = \langle r'_1\rangle \dot{+} \langle r'_2\rangle$, $\operatorname{ind} r'_1 = \operatorname{ind} r'_2 = 3$, $(r'_2)^2 = (r'_1)^2$, $r'_1r'_2 = -(r'_1)^2$, $r'_2r'_1 = 0'$. Both rings N and N' have order p^3. The diagrams of the subring lattices of N and N' are shown in Fig. 4. The letters α and β used in the designations in Fig. 4 assume the following values: $\alpha = \overline{0, p-1}$, $\beta = \overline{0, p-2}$. It is easy to see that $L(N) \cong L(N')$.

Now we define two rings R and R' by setting $R = \langle e\rangle \dot{+} N$ and $R' = \langle e'\rangle \dot{+} N'$, where e and e' are identity elements in the rings R and R', respectively. According to [6, Thm. 1], the subring lattices $L(R)$ and $L(R')$ are isomorphic to direct products of their subring lattices $L(\langle e\rangle)$, $L(N)$ and $L(\langle e'\rangle)$, $L(N')$, respectively. Since $L(N) \cong L(N')$ and $L(\langle e\rangle) \cong L(\langle e'\rangle)$, we have $L(R) \cong L(R')$. In this case R is commutative, whereas R' is not commutative.

THEOREM 3. Let a finite commutative ring R be defined as follows: $R = F \dot{+} N$, where

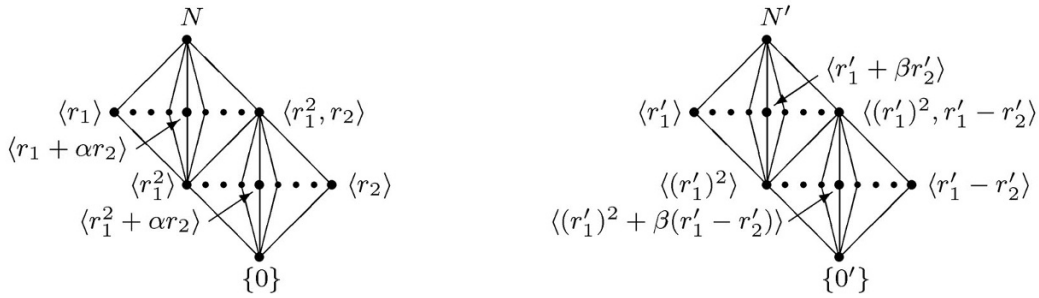

Fig. 4.

$F \cong GF(p^n)$, $n > 1$, an identity element e of the field F is the identity in R, and N is a nilpotent ideal of nilpotency index 2. Suppose φ is a lattice isomorphism of the ring R onto the ring R^φ. Then $R^\varphi \cong R$.

Proof. Recall that the Frattini subring $\Phi(K)$ of an arbitrary ring K is the intersection of all maximal right ideals in K. If K is a nilpotent ring, then the subring $\Phi(K)$ coincides with the intersection of all maximal subrings in K. According to [8, Assert. 4.1.3], if K is a nilpotent p-ring, then $\Phi(K) = K^2 + pK$. As applied to the ring N, this means that $\Phi(N) = \{0\}$. Passing to a projective image N^φ, which is a nilpotent p-ring by Theorem 2, we derive $(N^\varphi)^2 = pN^\varphi = \{0'\}$. Thus N and N^φ are lattice-isomorphic finite rings of characteristic p with zero multiplication. According to [5, Lemma 7], we have $|N^\varphi| = |N|$, whence $N^\varphi \cong N$. In view of Theorem 2, we obtain $F^\varphi \cong F$, and hence $R^\varphi \cong R$.

THEOREM 4. Let a finite commutative ring R with identity be decomposable into a direct sum of rings T_i, $i = \overline{1,k}$, satisfying the following conditions: $T_i = F_i \dotplus N_i$, $F_i \cong GF(p^{n_i})$, $n_i > 1$, N_i is a nonzero nilpotent ideal of T_i, and an identity e_i of the field F_i is the identity in T_i, $i = \overline{1,k}$. Suppose also that φ is a lattice isomorphism of the ring R onto the ring R^φ. Then:

(a) $R^\varphi = T_1^\varphi \oplus \cdots \oplus T_k^\varphi$;

(b) $T_i^\varphi = F_i^\varphi \dotplus N_i^\varphi$, $F_i^\varphi \cong F_i$, $\langle e_i\rangle^\varphi = \langle e_i'\rangle$, e_i' is the identity element in the ring T_i^φ, and N_i^φ is a nonzero nilpotent ideal of T_i^φ, $i = \overline{1,k}$;

(c) $\langle e\rangle^\varphi = \langle e'\rangle$, where e and e' are identity elements of R and R^φ, respectively;

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

(e) the ring R^φ is commutative if and only if every subring N_i^φ, $i = \overline{1,k}$, is commutative.

Proof. Statement (b) follows from Theorem 2. Applying (b) and Theorem 1 to a subring $F = F_1 \oplus \cdots \oplus F_k$, we derive (a) and (c). Statement (e) results from Theorem 2. It is clear that $\operatorname{Rad} R = N_1 \oplus \cdots \oplus N_k$. The equality $(N_1 \oplus \cdots \oplus N_k)^\varphi = N_1^\varphi \oplus \cdots \oplus N_k^\varphi$ follows from (a). Statements (a) and (b) imply that $\operatorname{Rad} R^\varphi = N_1^\varphi \oplus \cdots \oplus N_k^\varphi$. Consequently, (d) holds true. The theorem is proved.

3. PROJECTIONS OF RINGS CONTAINING GALOIS RINGS

LEMMA 4. Let a finite p-ring R be defined as follows: $R = \langle e\rangle \dot{+} \langle r\rangle$, where e is an identity element of R, $o(e) = p^n$, $n \geqslant 2$, r is a nonzero nilpotent element, and $|\langle r\rangle| > 2$. Suppose also that φ is a lattice isomorphism of the ring R onto the ring R^φ. Then:

(a) R^φ is a p-ring;

(b) $\langle r\rangle^\varphi = \langle r'\rangle$ is a nil-ring;

(c) $\langle e\rangle^\varphi = \langle e'\rangle$, $(e')^2 = e'$, and $o(e') = p^n$;

(d) $R^\varphi = \langle e'\rangle \dot{+} \langle r'\rangle$, and either $e'r' = r'e' = r'$ or $e'r' = r'e' = \alpha pe'$, where $\alpha \in \mathbb{Z}$.

Proof. (a), (b) According to [7, Thm. 3], R contains exactly two maximal subrings, and hence R^φ is generated by one element and is therefore commutative. Obviously, the subring lattice of a ring $T = \langle pe\rangle \dot{+} \langle r\rangle$ is not a chain. In addition, $|T| > 4$ since $o(e) \geqslant p^2$. By Lemma 1, T^φ is a p-nil-ring, and hence R^φ is a p-ring.

(c) In the subring $\langle r\rangle$, we choose an element r_1 such that $r_1^2 = pr_1 = 0$. Applying [2, Lemma 7] to a subring $S = \langle e\rangle \dot{+} \langle r_1\rangle$ and keeping in mind that $\langle r_1\rangle^\varphi$ is a nil-ring, we obtain $S^\varphi = \langle e'\rangle \dot{+} \langle r_1'\rangle$, where $(e')^2 = e'$. The subring lattices of rings $\langle e\rangle$ and $\langle e'\rangle$ are the unique chains of maximal length in the lattices $L(S)$ and $L(S^\varphi)$, respectively.

(d) Suppose that the element e' is not an identity in R^φ and consider the Pierce decomposition $R^\varphi = e'R^\varphi \oplus (1 - e')R^\varphi$. According to [7, Lemma 4], the subrings $e'R^\varphi$ and $(1 - e')^\varphi R$ each contains one maximal subring. The ring $e'R^\varphi$ has a nonzero idempotent element e' whose order is not prime. By [7, Thm. 1], only one of the following two cases is possible: $e'R^\varphi = \langle e'\rangle$ or $e'R^\varphi \cong GR(p^n, q^m)$. If the second case holds, then it follows by [2, Thm. 3] that R contains a subring isomorphic to a ring $GR(p^n, q^m)$. The ring R has no such subrings since any subring in R containing an idempotent element e has the form $\langle e\rangle \oplus N$, where $N \subseteq \langle r\rangle$, and cannot be isomorphic to $GR(p^n, q^m)$. Hence $e'R^\varphi = \langle e'\rangle$. If the subring $(1 - e')^\varphi R$ is not nilpotent, then it contains a nonzero idempotent element e_1', and consequently R^φ has two orthogonal idempotent elements e' and e_1'. By [2, Lemmas 6, 8], the projective preimage of a subring $\langle e'\rangle \oplus \langle e_1'\rangle$ should also contain two nonzero orthogonal idempotent elements. It is easy to see that the ring R does not contain such idempotent elements. Hence the subring $(1 - e')R^\varphi$ is generated by a nilpotent element. Let $(1 - e')R^\varphi = \langle v'\rangle$. Then $R^\varphi = \langle e'\rangle \oplus \langle v'\rangle$. We express an element r' via generating elements e' and v' by setting $r' = \beta e' + w'$, where $\beta \in \mathbb{Z}$ and $w' \in \langle v'\rangle$. Since r' is a nilpotent element, β should be divisible by p. Let $\beta = \alpha p$, where $\alpha \in \mathbb{Z}$. Then $r' = \alpha pe' + w'$. Multiplying both parts of the last equality by e', we obtain $e'r' = \alpha pe'$. The lemma is proved.

LEMMA 5. Let a finite p-ring R be defined as follows: $R = \langle e\rangle \dot{+} N$, where e is an identity element of R, $o(e) = p^n$, $n \geqslant 2$, N is a nilpotent ring, the lattice $L(N)$ is not a chain, and $|N| \neq 4$. Suppose also that φ is a lattice isomorphism of the ring R onto the ring R^φ. Then:

(a) R^φ is a p-ring;

(b) $\langle e\rangle^\varphi = \langle e'\rangle$, $(e')^2 = e'$, and $o(e') = p^n$;

(c) N^φ is a nilpotent ring;

(d) $R^{\varphi} = \langle e' \rangle \dotplus N^{\varphi}$, and either e' is the identity in R^{φ} or there exists an integer α such that $e'r' = r'e' = \alpha pe'$ for every element r' in N^{φ}.

Proof. (a), (b) The subring lattice of a ring $\langle e \rangle$ is a chain of length n. Suppose that the projective image $\langle e \rangle^{\varphi}$ is not generated by an idempotent element. Let $u' \in N^{\varphi}$, $l(\langle u' \rangle) = 1$, $u \in N$, and $\langle u \rangle^{\varphi} = \langle u' \rangle$. Obviously, $u^2 = pu = 0$, and so the subring $S = \langle e \rangle \dotplus \langle u \rangle$ satisfies the hypotheses of [2, Lemma 7]. Then $\langle e \rangle^{\varphi} = F'$ is a field of length 2, $(u')^2 = u'$, and $p = 2 = n$. This implies that the ring N^{φ} does not contain nonzero nilpotent elements and is therefore decomposable into a finite direct sum of finite fields, $N^{\varphi} = F'_1 \oplus \cdots \oplus F'_k$. According to [2, Lemma 7], all fields F'_i, $i = \overline{1,k}$, have the same characteristic as the field F'. The subring lattice of a finite field is distributive [4, Thm. 1.2], and a distributive lattice of any p-nil-ring is a chain [4, Thm. 1.1]. Therefore, the subring lattices of all fields F'_i, $i = \overline{1,k}$, will be finite chains. Applying [5, Thm. 1] to a subring N, we conclude that either $L(N)$ is a chain or $|N| = 4$. In each of the two cases we arrive at a contradiction with the hypothesis. Thus the assumption that the projective image $\langle e \rangle^{\varphi}$ is not generated by an idempotent element is invalid.

Let $\langle e \rangle^{\varphi} = \langle e' \rangle$, where $(e')^2 = e'$. Applying again [2, Lemma 7] to a subring S, we conclude that $o(e') = o(e) = p^n$, $(u')^2 = pu' = 0'$, and either e' is the identity in the ring S^{φ} or there exists an element w' such that $(w')^2 = pw' = 0'$ and $S^{\varphi} = \langle e \rangle^{\varphi} \oplus \langle w' \rangle$. According to [6, Thm. 1], the subring lattice of a ring R is not decomposable into a direct product of lattices, and so the additive group of a ring R^{φ} is primary with respect to a prime number p.

(c) Suppose that N^{φ} is not a nilpotent ring, and let v' be a nonzero idempotent element in N^{φ}. The subring lattice of a ring $\langle v' \rangle$ is a chain, so the ring N contains a nilpotent element v such that $\langle v \rangle^{\varphi} = \langle v' \rangle$. The above argument implies that $l(\langle v \rangle) > 1$. Applying Lemma 4 to a subring $T = \langle e \rangle \dotplus \langle v \rangle$, we conclude that $\langle v' \rangle$ is a nil-ring, which contradicts the assumption.

(d) Let r' be an arbitrary element of the ring N^{φ}, $r \in N$, and $\langle r \rangle^{\varphi} = \langle r' \rangle$. If $l(\langle r' \rangle) = 1$, then by [2, Lemma 7] (and if $l(\langle r' \rangle) > 1$ then by Lemma 4) one of the following options is true:

$$e'r' = r'e' = r', \tag{5}$$

$$e'r' = r'e' = \alpha pe', \tag{6}$$

where $\alpha \in \mathbb{Z}$.

Suppose that there exist two nonzero elements r'_1 and r'_2 in N^{φ} having the properties

$$e'r'_1 = r'_1 \quad \text{and} \quad e'r'_2 = \alpha pe'. \tag{7}$$

Then $e'(r'_1 + r'_2) = r'_1 + \alpha pe'$. The equality $r'_1 + \alpha pe' = r'_1 + r'_2$ should follow from (5), and (6) must give rise to $r'_1 + \alpha pe' = \beta pe$ for some integer β. It is easy to see that the last two equalities lead to a contradiction. Consequently, (5) or (6) holds for all elements $r' \in N^{\varphi}$.

LEMMA 6. Let a finite commutative p-ring R with identity e be defined thus: $R = S + N$, where $S \cong GR(p^n, m)$, $n > 1$, $m > 1$, and N is a nonzero nilpotent ideal of R. Suppose also that φ is a lattice isomorphism of the ring R onto the ring R^{φ}. Then the following statements hold:

(a) R^φ is a p-ring;

(b) $S^\varphi \cong S$;

(c) $\langle e\rangle^\varphi = \langle e'\rangle$, $(e')^2 = e'$, and $o(e') = o(e)$;

(d) N^φ is a nilpotent subring;

(e) $R^\varphi = S^\varphi + N'$, where N' is a two-sided nilpotent ideal of R^φ generated by the subring N^φ, e' is the identity in R^φ, and $s'r' = r's'$ for all $s' \in S^\varphi$ and all $r' \in N'$;

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

(g) the ring R^φ is commutative if and only if the ring N^φ is commutative.

Proof. (a), (b) According to [3, Cor. 2], the projective image of a p-ring containing a Galois ring $GR(p^n, m)$, where $n > 1$ and $m > 1$, is a p-ring. Consequently, (a) holds true. The truth of (b) follows from the property of being lattice-definable for a Galois ring [2, Thm. 3].

(c) By [3, Lemma 14], the identity e of the ring R belongs to a subring S. In view of [2, Property 9], $\langle e\rangle^\varphi = \langle e'\rangle$ and e' is the identity in the ring S^φ. The isomorphism $S^\varphi \cong S$ implies $o(e') = o(e)$.

(d) Suppose that the ring N^φ is not a nil-ring and choose in it a nonzero idempotent element v'. The subring N contains an element v such that $\langle v\rangle = \langle v'\rangle$. Consider a subring $V = S + (v)$, where (v) is a principal ideal in V generated by the element v. According to [3, Prop. 2], the subring V is generated by one element, and by [3, Lemma 17], the element v' is nilpotent, which contradicts the assumption. Consequently, N^φ is a nil-ring, and hence it is a nilpotent ring.

(e) Let $r' \in N^\varphi$, $r \in N$, and $\langle r\rangle^\varphi = \langle r'\rangle$. Consider a subring $T = S + (r)$, where (r) is a principal ideal in T generated by the element r. By [3, Prop. 2], the subring T is generated by one element, and by virtue of [3, Lemma 17], T^φ is a one-generated ring. Therefore,

$$(\forall s' \in S^\varphi)(\forall r' \in N^\varphi)(s'r' = r's'). \tag{8}$$

According to [3, Lemma 17], the element e' is an identity in the ring R^φ. Let N' be a two-sided ideal in R^φ generated by the subring N^φ. Since $R^\varphi = S^\varphi \vee N^\varphi$, we have $R^\varphi = S + N'$. The ideal N' is additively generated by elements of the form $s'r'$, where $r' \in N^\varphi$ and $s' \in S^\varphi$; so Eqs. (8) imply that the subring N' is nilpotent. It is also clear that Eqs. (8) hold for all $s' \in S^\varphi$ and all $r' \in N'$.

(f) Obviously, $\operatorname{Rad} R = pS + N$. In the ring R^φ, the set of all nilpotent elements is contained in the subring $pS^\varphi + N'$. In view of [2, Property 10], $(pS)^\varphi = pS^\varphi$ and $(\operatorname{Rad} R)^\varphi \subseteq pS^\varphi + N'$. The projective preimage W of the ring $pS^\varphi + N'$ is a nil-ring, since otherwise it would contain a nonzero idempotent element, namely, the identity e, which is impossible. Consequently, $W \subseteq pS + N$ and $(\operatorname{Rad} R)^\varphi = \operatorname{Rad} R^\varphi$.

(g) Follows from (e). The lemma is proved.

THEOREM 5. Let a finite commutative ring R with identity be decomposable into a direct sum of rings T_i, $i = \overline{1,k}$, satisfying the following conditions: $T_i = S_i + N_i$, $S_i \cong GR(p^{n_i}, m_i)$,

$n_i > 1$, $m_i > 1$, N_i, is a nonzero nilpotent ideal of T_i, an identity e_i of the ring S_i is the identity in T_i, $i = \overline{1,k}$. Suppose that φ is a lattice isomorphism of the ring R onto the ring R^φ. Then:

(a) $T_i^\varphi = S_i^\varphi + N_i'$, $S_i^\varphi \cong S_i$, $\langle e_i\rangle^\varphi = \langle e_i'\rangle$, e_i' is the identity element in the ring T_i^φ, N_i' is a two-sided nilpotent ideal of T_i^φ generated by the subring N_i^φ, and $s'r' = r's'$ for all $s' \in S_i^\varphi$ and all $r' \in N_i'$, $i = \overline{1,k}$;

(b) $R^\varphi = T_1^\varphi \oplus \cdots \oplus T_k^\varphi$;

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

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

(e) the ring R^φ is commutative if and only if every subring N_i^φ, $i = \overline{1,k}$, is commutative.

Proof. (a) Follows from Lemma 6.

(b) Consider a subring $R_1 = S_1 \oplus \cdots \oplus S_k$. By [2, Thm. 9],

$$R_1^\varphi = S_1^\varphi \oplus \cdots \oplus S_k^\varphi. \tag{9}$$

Since identity elements of subrings S_i^φ are identities in rings T_i^φ, $i = \overline{1,k}$, Eq. (9) implies $R^\varphi = T_1^\varphi \oplus \cdots \oplus T_k^\varphi$.

(c) The elements $e = e_1 + \cdots + e_k$ and $e' = e_1' + \cdots + e_k'$ are the identities in R and R^φ, respectively. The subring lattice $L(\langle e\rangle)$ is a chain, so $\langle e\rangle^\varphi = \langle u'\rangle$ for some element $u' \in R^\varphi$. We prove that $\langle u'\rangle = \langle e'\rangle$. Let $E = \langle e_1\rangle \oplus \cdots \oplus \langle e_k\rangle$. Equalities $\langle e_i\rangle^\varphi = \langle e_i'\rangle$, $i = \overline{1,k}$, combined with (9), imply that $E^\varphi = \langle e_1'\rangle \oplus \cdots \oplus \langle e_k'\rangle$. Clearly, $u' \in E^\varphi$. By hypothesis, $L(\langle e_1'\rangle)$ is a finite chain of length greater than 1. The ring E^φ contains no fields, and by [7, Thm. 1], the element u' may be thought of as being either nilpotent or idempotent. For any number $i \in \{1, \ldots, k\}$, $o(e) \geqslant o(e_i)$, and in view of $o(u') = o(e)$, it is clear that u' is an element of maximal additive order in the ring E^φ. Every nilpotent element in E^φ belongs to a subring pE^φ and cannot have maximal additive order in E^φ. Therefore, u' is an idempotent element. Let $u' = e_{i_1}' + \cdots + e_{i_l}'$. If $l \neq k$, then $u' \in S_{i_1}^\varphi \oplus \cdots \oplus S_{i_l}^\varphi \neq S^\varphi$. Consequently, $e \in S_{i_1} \oplus \cdots \oplus S_{i_l}$, which is impossible. Hence $l = k$, and so $u' = e_1' + \cdots + e_k' = e'$ is the identity in R^φ.

(d) It is easy to see that $\operatorname{Rad} R = \operatorname{Rad} T_1 \oplus \cdots \oplus \operatorname{Rad} T_k = (pS_1 + N_1) \oplus \cdots \oplus (pS_k + N_k)$, whence $(\operatorname{Rad} R)^\varphi = (pS_1 + N_1)^\varphi \oplus \cdots \oplus (pS_k + N_k)^\varphi = (pS_1^\varphi + N_1') \oplus \cdots \oplus (pS_k^\varphi + N_k') = \operatorname{Rad} R^\varphi$.

(e) It follows from (a) that the ring R^φ is commutative iff every subring T_i^φ, $i = \overline{1,k}$, is commutative. By Lemma 6(g), the subring T_i^φ is commutative iff every subring N_i^φ, $i = \overline{1,k}$, is commutative. The theorem is proved.

Acknowledgments. I am grateful to an anonymous referee for important comments which helped me improve the text of the paper.

REFERENCES

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

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

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

4. P. A. Freidman and S. S. Korobkov, "Associative rings and their lattice of subrings," in *A Study of Algebraic Systems via Properties of Their Subsystems*, Ural State Ped. Univ., Yekaterinburg (1998), pp. 4-47.

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

6. S. S. Korobkov, "Periodic rings with subring lattices decomposable into a direct product," in *A Study of Algebraic Systems via Properties of Their Subsystems*, Ural State Ped. Univ., Yekaterinburg (1998), pp. 48-59.

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

8. R. L. Kruse and D. T. Price, *Nilpotent Rings*, Gordon and Breach, New-York (1969).