

# On Subdirect Decomposition and Varieties of Some Rings with Involution

Siniša Crvenković    Igor Dolinka    Milovan Vinčić

*Institute of Mathematics, Faculty of Science, University of Novi Sad  
Trg Dositeja Obradovića 4, 21000 Novi Sad, Yugoslavia  
e-mail: sima@eunet.yu    e-mail: dockie@unsim.ns.ac.yu*

*Department of Mathematics, Faculty of Mechanical Engineering  
University of Banja Luka  
Danka Mitrova 10, 78000 Banja Luka, Bosnia and Herzegovina*

**Abstract.** We give a complete description of subdirectly irreducible rings with involution satisfying  $x^{n+1} = x$  for some positive integer  $n$ . We also discuss ways to apply this result for constructing lattices of varieties of rings with involution obeying an identity of the given type.

MSC 2000: 16W10, 08B26, 08B15

Keywords: ring with involution, field, subdirectly irreducible, variety

## 1. Introduction

A well-known (or better to say, famous) theorem of N. Jacobson states that every ring satisfying the identity  $x^{n+1} = x$  for some  $n \geq 1$  is commutative. In more detail, every subdirectly irreducible ring obeying such an identity is a finite field, so that every ring with  $x^{n+1} = x$  decomposes into a subdirect product of finite fields.

The main purpose of this note is to obtain the involutorial analogue of Jacobson's theorem. Recall that a *ring with involution* is an algebraic system  $(R, +, \cdot, -, 0, *)$  of similarity type  $(2, 2, 1, 0, 1)$  such that

- (1)  $(R, +, \cdot, -, 0)$  is a ring,
- (2) the following identities hold:

$$(x + y)^* = x^* + y^*, \quad (xy)^* = y^*x^*, \quad (x^*)^* = x.$$

Throughout the paper, we are working within the variety of all involution rings, defined by these identities and the ring axioms. Also, all involution ring varieties, referred to in the sequel, are assumed to be of the above similarity type. Therefore, the involution  $*$  is considered as a fundamental operation, and thus all universal-algebraic constructions on rings with involution must respect this operation. For example, by an involution ring congruence we mean a congruence of the underlying ring which also preserves the corresponding involutorial operation (occasionally, we use the term  $*$ -congruence only for emphasis). Consequently, by adopting this universal-algebraic approach, we have that a ring with involution is subdirectly irreducible if the intersection of all of its nonidentical  $*$ -congruences is nonidentical. Hence, there may exist involution rings which are subdirectly irreducible, but whose ring reducts are not subdirectly irreducible as rings. However, this will not cause any confusion, because the variety in which the notion of subdirect irreducibility is considered will be always clear from the context.

With this view at hand, it turns out that finite fields with involution are not the only subdirectly irreducibles among the involution rings in which  $x^{n+1} = x$  holds, so that the result, cited above, is no longer true. Aside from the ‘internal’ phenomenon of an involution on a field, we are going to encounter another type of involution, an ‘external’ kind, as described below.

Let  $R$  be a ring, and let  $R^{op}$  be its opposite ring (i.e. its anti-isomorphic copy). Consider the direct sum  $R \oplus R^{op}$ , and define a unary operation  $*$  on this sum such that for all  $r, s \in R$  we have

$$(r, s)^* = (s, r).$$

It is easy to verify that in the way just described,  $R \oplus R^{op}$  is given the structure of a ring with involution, and  $*$  defined as above is known as the *exchange involution*, cf. [8]. The resulting involution ring we denote by  $Ex(R)$ . We shall be concerned with the following typical situation: a ring with involution  $R$  possesses an ideal  $I$  such that  $R$  is a direct sum of  $I$  and  $I^* = \{a^* : a \in I\}$  (which is also an ideal in  $R$ ). Then  $R \cong Ex(I)$ . Here by an *ideal* we mean a ring ideal; ideals which are closed for the star operation we call  $*$ -ideals.

Investigations concerning rings with involution in which the involution is considered as a fundamental operation have been intensified in recent years (cf. Wiegandt [9] for an overview of this topic up to the early nineties). Particular emphasis has been put on the ideal and  $*$ -ideal structure, and a number of papers deal with the radical theory of involution rings, e.g. [2]. On the other hand, several universal-algebraic aspects were also studied, such as in [3], and our results aim to contribute to this latter direction.

In the following section we prove that a ring with involution which obeys  $x^{n+1} = x$  for some integer  $n \geq 1$  is subdirectly irreducible if and only if it is either a finite field with involution (in which case all possible involutions will be discussed), or of the form  $Ex(F)$  for some finite field  $F$  in which the indicated identity holds. In the final section, we give some hints and an example of how this information can be applied in order to construct the lattice of subvarieties of the involution ring variety defined by  $x^{n+1} = x$  for a given  $n$ . Our example includes all varieties of  $*$ -regular rings with a special involution considered by Yamada in [10].

## 2. The main result

It is well-known that congruences and ideals of rings are in a one-to-one correspondence such that a congruence  $\theta$  of a ring  $R$  gives rise to an ideal  $I$  of  $R$  such that  $a \in I$  if and only if  $(0, a) \in \theta$ , and conversely, for each ideal  $I$  of  $R$ , we have a congruence  $\theta$  defined by  $(a, b) \in \theta$  if and only if  $a - b \in I$ . Note that a similar symmetry occurs in rings with involution concerning its  $*$ -congruences and  $*$ -ideals. Indeed, if  $\theta$  is a  $*$ -congruence of  $R$ , then the ideal  $I$  constructed as above is a  $*$ -ideal, since if  $a \in I$ , then  $(0, a) \in \theta$ , yielding  $(0, a^*) \in \theta$  (as we have  $0^* = 0$ ), and so  $a^* \in I$ . Conversely, if  $I$  is a  $*$ -ideal and  $\theta$  the corresponding congruence, then  $(a, b) \in \theta$  implies  $a - b \in I$ , so  $a^* - b^* = (a - b)^* \in I$ . Thus,  $(a^*, b^*) \in \theta$ . We record these observations as

**Lemma 1.** *Let  $R$  be a ring with involution. Then  $*$ -congruences and  $*$ -ideals of  $R$  are in a one-to-one correspondence, such that the ideal of  $R$  arising from its  $*$ -congruence is a  $*$ -ideal, and vice versa.*

Now define the  $*$ -heart  $H^*(R)$  of a ring with involution  $R$  to be the intersection of all of its nonzero  $*$ -ideals. According to the above lemma,  $R$  is subdirectly irreducible if and only if  $H^*(R)$  is nonzero. As we already mentioned, the subdirect irreducibility of  $R$  does not guarantee that the  $*$ -free reduct of  $R$  is subdirectly irreducible as a ring, which can be now easily seen from the example of  $Ex(R)$ , where  $R$  is a simple ring.

Our main objective in this note is to prove the following result, which provides an involutorial counterpart of Lemma 7 from [10].

**Theorem 2.** *A ring with involution  $R$  is subdirectly irreducible and obeys the identity  $x^{n+1} = x$  if and only if there is a prime number  $p$  and an integer  $k \geq 1$  satisfying  $(p^k - 1) \mid n$ , such that  $R$  is isomorphic to one of the following:*

- (1)  $GF(p^k)$  (the finite field with  $p^k$  elements), with the involution being the identity mapping,
- (2)  $GF(p^k)$  with the involution defined by  $x^* = x^{p^m}$  (this is going to be denoted by  $GF^*(p^k)$ ), when  $k = 2m$  for some  $m \geq 1$ , and
- (3)  $Ex(GF(p^k))$ .

First we collect some auxiliary results, which are the first steps towards our goal.

**Lemma 3.** *Let  $R$  be a simple ring such that  $R^2 = R$ , and let  $Z(R)$  denote the center of  $R$ . Then  $R$  has an identity element if and only if  $Z(R)$  is nonzero.*

*Proof.* Assume  $z \in Z(R)$ ,  $z \neq 0$ . Then  $zR = R$  and there exists  $e \in R$  such that  $z = ze$ . Let  $r \in R$ . We have  $zr = zer$ , and hence,  $z(r - er) = 0$ . However, since  $Ann(z) = 0$ , we obtain  $r = er$ , and similarly,  $r = re$ . So,  $e$  is the identity element in  $R$ . The converse is obvious.  $\square$

Rings with involution which are  $*$ -simple (in the sense of having no nontrivial  $*$ -ideals) are one of the topics dealt with by Birkenmeier, Groenewald and Heatherly in [1]. Their result is as follows.

**Proposition 4.** [1, Proposition 2.1] *Let  $R$  be a  $*$ -simple ring. Then either  $R$  is simple as a ring, or  $R \cong Ex(K)$ , where  $K$  is a maximal ideal of  $R$ ,  $K$  is simple,  $R^2 \neq 0$ , and  $K$  and  $K^*$  are the only nontrivial ideals of  $R$ .*

**Lemma 5.** *Let  $R$  be a subdirectly irreducible semiprime PI-ring with involution. Then  $R$  is  $*$ -simple and has an identity element.*

*Proof.* Consider the  $*$ -heart  $H^*(R)$  of  $R$ . Of course,  $H^*(R)$  is  $*$ -simple (we have  $H^*(R) \neq 0$  by our assumptions and the remarks following Lemma 1). By the above proposition, either  $H^*(R)$  is simple as a ring, or  $H^*(R) \cong Ex(K)$ , where  $K$  is a simple ring. From [7] and Lemma 3,  $H^*(R)$  has an identity element  $e$ . Hence, we have a ring decomposition  $R = eR \oplus A$ , where  $H^*(R) = eR$  and  $A$  is the annihilator of  $H^*(R)$ . Since  $H^*(R)$  is a  $*$ -ideal, so is  $A$ . Therefore,  $R = eR = H^*(R)$ , implying that  $R$  is  $*$ -simple.  $\square$

Using the above lemma, we move substantially closer to our aim.

**Lemma 6.** *Let  $R$  be a subdirectly irreducible ring with involution satisfying the identity  $x^{n+1} = x$  for some  $n \geq 1$ . Then either  $R$  is a finite field with involution, or  $R \cong Ex(F)$  for some finite field  $F$ .*

*Proof.* By the given assumptions and Lemma 5,  $R$  is  $*$ -simple and has an identity element. Of course,  $R$  is commutative. If  $R$  is simple as a ring, then it must be a field, in addition, a finite one, as all of its elements are roots of the polynomial  $x^{n+1} - x$ .

On the other hand, assume that  $R \cong Ex(K)$ , with  $K$  as described in Proposition 4. Then there exists  $e, f \in K$  such that

$$1 = e + f^*.$$

Now for an arbitrary  $a \in K$  we have

$$a = ae + af^* = ae,$$

since  $af^* = 0$ , and  $e$  is the identity element in  $K$ . As  $K$  is simple (and commutative),  $K$  is a field, and the lemma is proved.  $\square$

*Proof of Theorem 2.* Of course, it is clear that a finite field  $GF(p^k)$  satisfies the identity  $x^{n+1} = x$  if and only if  $(p^k - 1) \mid n$ . Therefore, if  $R \cong Ex(F)$ , we obtain precisely the involution rings described by (3).

On the other hand, assume that  $R$  is a field with involution. It is well-known from the theory of fields that the group of automorphisms of the finite field  $GF(p^k)$  is a cyclic group of  $k$  elements, and its members are the mappings  $x \mapsto x^{p^m}$ ,  $1 \leq m \leq k$ . Now we should select which of these are involutions, i.e. the automorphisms of order two. This is obtained from the condition

$$x = (x^{p^m})^{p^m} = x^{p^{2m}},$$

or equivalently,

$$x \neq 0 \Rightarrow x^{p^{2m}-1} = 1.$$

Since the multiplicative group of every finite field is cyclic, the above condition will be satisfied if and only if  $(p^k - 1) \mid (p^{2m} - 1)$ , i.e.  $k \mid 2m$ . As  $2m \leq 2k$ , we have two possibilities: either  $2m = 2k$ , that is  $m = k$ , and the corresponding involution is the identity mapping (when we have the case (1)), or  $2m = k$  (yielding the situation described in (2)).

The converse implication is easy, as it is obvious that all the listed rings with involution are  $*$ -simple, and thus subdirectly irreducible.  $\square$

Note that it was proved in [3] that the ring reduct of a subdirectly irreducible ring with involution is either subdirectly irreducible as a ring, or a subdirect sum of two subdirectly irreducible rings. However, they presented an example which shows that in the latter case, the subdirect product in question need not to be direct, even in the commutative case. Yet, Theorem 2 shows that the constraint  $x^{n+1} = x$  suffices to obtain a direct decomposition of ring reducts of subdirectly irreducible involution rings into subdirectly irreducible rings.

### 3. Applications

A ring with involution is said to have a *special involution* if it satisfies the identity

$$x = xx^*x.$$

In other words, these are regular rings in which  $a^*$  is always an inverse (in the sense of von Neumann) of  $a$ . Such rings with involution were studied by Yamada [10]. He proved that these are precisely the involution rings whose multiplicative semigroups are inverse (and one can replace the term ‘inverse’ by ‘Clifford’). The characteristic of every such ring is a divisor of 6, which follows from the fact that every specially involutive ring can be represented as a direct sum of its  $*$ -ideals  $R_2$  and  $R_3$  formed by its 2-torsion and 3-torsion elements, respectively. Moreover,  $R_2$  satisfies  $x^4 = x$ , while  $R_3$  satisfies  $x^3 = x$ , so that every specially involutive ring satisfies  $x^7 = x$ . The lattice of all varieties of rings with involution satisfying  $x^7 = x$  will be presented in this section. The varieties with special involution will be indicated within this broader lattice.

Yamada proved that the only subdirectly irreducible specially involutive rings are those which we denoted by  $GF(2)$ ,  $GF(3)$  and  $GF^*(4)$ . This result is now easily deducible from our Theorem 2. Since we are concerned with involution rings satisfying  $x^7 = x$ , it suffices to look after prime numbers  $p$  and positive integers  $k$  such that  $(p^k - 1) \mid 6$  and by inspection we find  $p = 2, 3, 7$  for  $k = 1$  and  $p = 2$  for  $k = 2$ . Therefore, we have nine subdirectly irreducibles in the considered variety (two for each of the cases with  $k = 1$  and three for  $k = 2$ ). Now we can easily select those satisfying the identity  $x = xx^*x$ , as listed above. Note that the three considered fields with involution are the only ones covered by Theorem 2 in which the involution coincides with the multiplicative group inverse (completed with  $0^* = 0$ ). Therefore, we obtain the following result.

**Corollary 7.** *A ring with involution satisfies  $x = xx^*x$  if and only if it is a subdirect product of fields with inverse involution ( $a^* = a^{-1}$  for all  $a \neq 0$ , and  $0^* = 0$ ).*

Now we turn our attention to some methods which enable us to construct, given a positive integer  $n$ , the lattice of all varieties of rings with involution satisfying  $x^{n+1} = x$ . It is important to note that all rings with involution listed in Theorem 2 have a prime characteristic,

and that there are only a finite number of possible characteristics for subdirectly irreducible rings (with involution) satisfying  $x^{n+1} = x$ . In more detail, we have

**Corollary 8.** *Let  $R$  be a subdirectly irreducible ring with involution satisfying  $x^{n+1} = x$ . Then the characteristic of  $R$  is a prime number  $p$  such that  $(p - 1) \mid n$ .*

Therefore, the involution rings produced by Theorem 2 naturally split into several groups according to their characteristics. It is quite reasonable to hypothesize that such a classification must have some impact on the structure of the considered lattice of varieties, even if we consider ordinary rings without involution. The exact strength of this impact is shown in the following result.

**Theorem 9.** *Let  $n$  be a positive integer, and let  $\{p_1, \dots, p_k\}$  be the set of all prime numbers  $p_i$  such that  $(p_i - 1) \mid n$ . Further, let  $L$  denote the lattice of all varieties of rings (with involution) satisfying  $x^{n+1} = x$ , and let  $L_{p_i}$  denote the sublattice of  $L$  consisting only of those varieties satisfying  $p_i x = 0$  (i.e. varieties of characteristic  $p_i$ ). Then  $L \cong L_{p_1} \times \dots \times L_{p_k}$ .*

*Proof.* It is not difficult to see that it suffices to prove the following assertion: let  $\mathcal{V}_1, \dots, \mathcal{V}_k$  be varieties of rings (with involution) satisfying  $x^{n+1} = x$ , such that  $\mathcal{V}_i$  is of characteristic  $p_i$ ,  $1 \leq i \leq k$ , and let  $R$  be a subdirectly irreducible member of the join  $\mathcal{V}_1 \vee \dots \vee \mathcal{V}_k$ ; then  $R$  belongs to one of  $\mathcal{V}_i$ ,  $1 \leq i \leq k$ . More generally, we are going to show that if  $\text{char}(R) = p_i$  and  $R \in \mathcal{V}_1 \vee \dots \vee \mathcal{V}_k$ , then  $R \in \mathcal{V}_i$  even without the assumption of the subdirect irreducibility of  $R$ .

Assume to the contrary: that  $R$  is of prime characteristic  $p_i$ , but  $R \notin \mathcal{V}_i$ . From universal algebra (see [6]) it is known that  $R$  is a homomorphic image of a subdirect product of members of  $\mathcal{V}_1, \dots, \mathcal{V}_k$  (note that all factors also have prime characteristics). Let  $S$  be that subdirect product (so that  $R = \psi(S)$  for some homomorphism  $\psi$ ); then  $S$  is a subring of a direct product of the form  $R_1 \times \dots \times R_k$ , where for all  $1 \leq i \leq k$ ,  $R_i \in \mathcal{V}_i$ .

Clearly, every element  $a \in S$  can be written in the form

$$a = a_1 + \dots + a_k,$$

such that  $p_i a_i = 0$  (i.e.  $a_i$  is  $p_i$ -torsion) – it suffices to choose

$$a_i = (0, \dots, 0, \pi_i(a), 0, \dots, 0),$$

where  $\pi_i$  is the  $i$ th canonical projection of the considered direct product and  $\pi_i(a)$  occurs in the  $i$ th coordinate. Now denote

$$q_i = p_1 \dots p_{i-1} p_{i+1} \dots p_k.$$

Since  $(p_i, q_i) = 1$ , there exists an integer  $\ell_i$  such that  $q_i \ell_i \equiv 1 \pmod{p_i}$ . Obviously,  $q_i \ell_i a \in S$ . However, we also have  $q_i a_j = 0$  for all  $j \neq i$ , yielding  $q_i \ell_i a = q_i \ell_i a_i = a_i$ . Thus,  $a_i \in S$ . But since  $\pi_i(S) = R_i$  for all  $1 \leq i \leq k$ , it easily follows that  $S = R_1 \times \dots \times R_k$ .

Now  $\psi(S)$  is of characteristic  $p_i$ . Therefore, for each  $a \in S$ , we have  $p_i \psi(a) = 0$ . By Chinese Remainder Theorem, and since  $(p_i, p_j) = 1$  for  $j \neq i$ , one can find an integer  $\ell$  such that it satisfies the system of linear congruences

$$p_i \ell \equiv 1 \pmod{p_j}, \quad 1 \leq j \leq k, \quad j \neq i.$$

For such a choice of  $\ell$ , it follows that (with respect to the above decomposition of  $a$ )  $p_i \ell a_i = 0$  and  $p_i \ell a_j = a_j$  for all  $j \neq i$ , so that

$$0 = p_i \ell \psi(a) = \psi(p_i \ell a) = \psi(a - a_i) = \psi(a) - \psi(a_i),$$

whence  $\psi(a) = \psi(a_i)$ . Thus,  $R = \psi(S)$  can be represented as a homomorphic image of  $R_i$ , implying  $R \in \mathcal{V}_i$ , as desired.  $\square$

Hence, the task of finding the lattice of varieties of rings (with involution) satisfying  $x^{n+1} = x$  reduces to the determination of the structure of lattices of varieties satisfying  $x^{n+1} = x$  and  $px = 0$ , where  $(p - 1) \mid n$ . In the example that we aim to present we have  $n = 6$ , so that  $p \in \{2, 3, 7\}$ . When we consider ordinary rings, without involution, the situation is more or less clear: for  $p = 2$  we have two subdirectly irreducibles,  $GF(2)$  and  $GF(4)$ , where  $GF(2)$  embeds into  $GF(4)$ ; for  $p = 3$  we have  $GF(3)$ , and for  $p = 7$  we have  $GF(7)$ . Thus, it is easy (using the above theorem) to verify that there are 12 ring varieties satisfying  $x^7 = x$ , and their inclusion diagram is given in Figure 1, with indicated positions of the fields just listed.

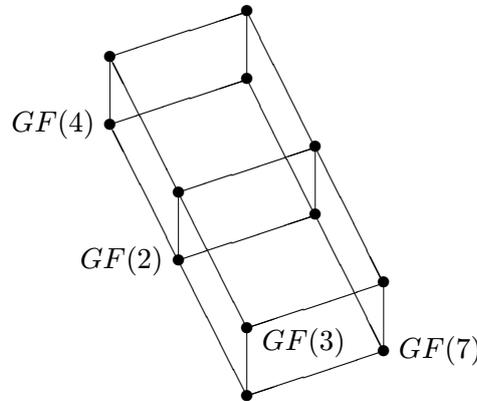


Figure 1. All varieties of rings satisfying  $x^7 = x$

However, the situation with involution rings obeying  $x^7 = x$  is somewhat more complicated. The complication arises mostly from the rings of characteristic 2, since there are five such which are subdirectly irreducible. The characteristic 3 and 7 rings are much easier to deal with. The following lemma solves, in particular, the latter two cases.

**Lemma 10.** *Both  $GF(p^k)$  and  $GF^*(p^k)$  (provided the latter exists) can be embedded into  $Ex(GF(p^k))$ .*

*Proof.* Consider the set of all elements of  $Ex(GF(p^k))$  which are fixed by the involution. These are all elements of the form  $(a, a)$ ,  $a \in GF(p^k)$ , and 0. It is an easy exercise to show that these elements form a subring of  $Ex(GF(p^k))$ , endowed with an identical involution, which is isomorphic to  $GF(p^k)$ .

On the other hand, assume that  $k = 2m$  and set  $r = p^m$  for short. Consider the zero of  $Ex(GF(p^k))$  and its elements of the form  $(a, a^r)$ ,  $a \in GF(p^k)$ . This set is obviously closed under multiplication and

$$(a, a^r)^* = (a^r, a) = (a^r, a^{r^2}) = (a, a^r)^r.$$

Finally,

$$(a, a^r) + (b, b^r) = (a + b, a^r + b^r).$$

However, since we are working with characteristic  $p$ , by a repeated use of ‘Freshmen’s Dream’  $(a + b)^p = a^p + b^p$  we have  $a^r + b^r = (a + b)^r$ , and the lemma is proved.  $\square$

From the above lemma it follows that the lattices of varieties of rings with involution satisfying  $x^7 = x$  and  $px = 0$  are isomorphic to the three-element chain both for  $p = 3$  and  $p = 7$ . Now it remains to settle the case  $p = 2$ , which is somewhat more involved.

**Lemma 11.** *The lattice of varieties of rings with involution satisfying  $x^7 = x$  and  $2x = 0$  is the one given by Figure 2, with the indicated positions of the subdirectly irreducibles.*

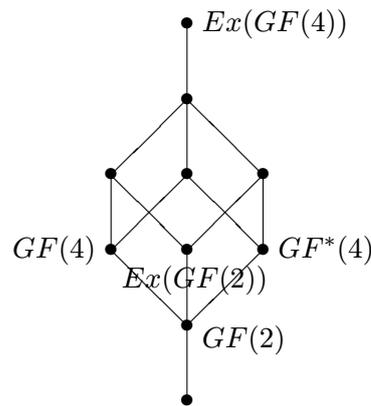


Figure 2. All varieties of rings with involution satisfying  $x^7 = x$  and  $2x = 0$

*Proof.* From Theorem 2 it follows that there are exactly five subdirectly irreducible rings with involution of characteristic 2 which satisfy  $x^7 = x$ ; these are:  $GF(2)$ ,  $Ex(GF(2))$ ,  $GF(4)$ ,  $GF^*(4)$  and  $Ex(GF(4))$ . Note that all of them obey  $x^4 = x$ ; thus, we may work with this simpler identity.

First of all,  $GF(2)$  embeds in each of the four other rings with involution from the above list, so that it generates the unique minimal subvariety in the required lattice.

To prove that the ‘middle part’ of Figure 2 indeed should be the three-dimensional cube, it suffices to prove that for each of  $Ex(GF(2))$ ,  $GF(4)$  and  $GF^*(4)$  one can find an identity which fails in the considered algebra, but holds in the other two. Consider the following identities:

$$(x^3)^* = x^3, \tag{1}$$

$$(x^3 + x)^* = x^3 + x^2, \tag{2}$$

$$(x^3 + x)^* = x^3 + x. \tag{3}$$

In  $GF(2)$  we have  $x^3 = x^2 = x$ , so (1) fails in  $Ex(GF(2))$ , since the latter has a nonidentical involution. On the other hand, (1) is true both in  $GF(4)$  and  $GF^*(4)$ , because for each  $a$ ,  $a^3 \in \{0, 1\}$  and so,  $a^3$  is fixed by the involution. Further, (2) is obviously false in  $GF(4)$ ,

as  $x = x^2$  is not true in this field. Yet, in  $Ex(GF(2))$ , (2) holds because both sides always evaluate to zero, while in  $GF^*(4)$  we have

$$(x^3 + x)^* = (x^3 + x)^2 = x^6 + 2x^4 + x^2 = x^6 + x^2 = x^3 + x^2.$$

Finally, (3) is true in  $Ex(GF(2))$  for the same reason as above, and it trivially holds in  $GF(4)$ . However, in the above chain of identities we have just seen that it cannot be true in  $GF^*(4)$ .

Finally, the variety  $\mathcal{V}$  generated by the three algebras just considered is by Lemma 10 contained in the variety generated by  $Ex(GF(4))$ . That such an inclusion must be proper is verified by the identity

$$(x^2 + x)^* = x^2 + x,$$

which is true in  $\mathcal{V}$ , but fails in  $Ex(GF(4))$ , since we can take  $x$  to be an element of the first summand in  $Ex(GF(4))$  different from the zero and from the identity element of  $GF(4)$ , whence  $x^2 + x$  becomes the identity element of  $GF(4)$  – clearly not a fixed point of the involution. The lemma is proved.  $\square$

Summing up, we have constructed our example, as we have proved

**Proposition 12.** *The variety of rings with involution defined by  $x^7 = x$  has exactly 90 subvarieties, and they form a lattice isomorphic to the direct product of the lattice described in Lemma 11 and the square of the three-element chain.*

In particular, there are six varieties of rings with a special involution: these are varieties generated by  $GF(2)$ ,  $GF(3)$  and  $GF^*(4)$ , their joins, and the trivial variety. Their lattice is isomorphic to the direct product of the two-element and the three-element chain.

By similar methods as those presented in this section, one can apply our Theorem 2 (along with Theorem 9) for calculating the lattice of varieties of rings with involution satisfying  $x^{n+1} = x$  for an arbitrary (but fixed) positive integer  $n$ .

**Acknowledgement.** The authors are indebted a great deal to the referee for finding a substantial short-cut in the proof of Theorem 2. In particular, Lemmata 3 and 5 of the present paper were suggested by him/her.

## References

- [1] Birkenmeier, G. F.; Groenewald, N. J.; Heatherly, H. E.: *Minimal and maximal ideals in rings with involution*. Beitrage Algebra Geom. **38** (1997), 217–225. [Zbl 0884.16021](#)
- [2] Booth, G. L.; Groenewald, N. J.: *Lattices of radicals in involution rings*. Algebra Colloq. **7** (2000), 17–26. [Zbl 0968.16005](#)
- [3] Heatherly, H. E.; Lee, E. K. S.; Wiegandt, R.: *Involutions on universal algebras*. In: Saad, G. and Thomsen, M. J. (eds.), *Nearrings, Nearfields and K-Loops* (Hamburg 1995), 269–282, Kluwer 1997. [Zbl 0893.08003](#)
- [4] Herstein, I. N.: *Rings with Involution*. Chicago Lectures in Mathematics, University of Chicago Press, Chicago - London 1976. [Zbl 0343.16013](#)

- [5] Jacobson, N.: *Structure of Rings*. AMS Colloq. Publications **37**, Amer. Math. Soc., Providence 1956. [Zbl 0073.02002](#)
- [6] McKenzie, R.; McNulty, G.; Taylor, W.: *Algebras, Lattices, Varieties*. Vol. I, Wadsworth & Brooks/Cole, Monterey 1987. [Zbl 0611.08001](#)
- [7] Rowen, L. H.: *Some results on the center of a ring with polynomial identity*. Bull. Amer. Math. Soc. **79** (1973), 219–223. [Zbl 0252.16007](#)
- [8] Rowen, L. H.: *Ring Theory*. Vol. I, Academic Press, New York 1988. [Zbl 0651.16001](#)
- [9] Wiegandt, R.: *On the structure of involution rings with chain condition*. Vietnam J. Math. **21** (1993), 1–12. [Zbl 0940.16516](#)
- [10] Yamada, M.: *On the multiplicative semigroups of regular rings with special involution*. Simon Stevin **59** (1985), 51–57. [Zbl 0567.16007](#)

Received December 5, 200; revised version June 5, 2001