Novi Sad J. Math.
Vol. 34, No. 2, 2004, 109-117
Proc. Novi Sad Algebraic Conf. 2003
(eds. I. Dolinka, A. Tepavčević)

ON SUBDIRECT DECOMPOSITION AND VARIETIES OF SOME RINGS WITH INVOLUTION. II [1]

Igor Dolinka[2], **Nebojša Mudrinski**[1]

Abstract. We describe an effective algorithm which, for a given $n \geq 1$ constructs the lattice of all varieties of (involution) rings satisfying the 'Jacobson identity' $x^{n+1} = x$.

AMS Mathematics Subject Classification (2000):

Key words and phrases:

As it is clearly suggested by the title, this note is a continuation of [1]. In the latter paper, the authors start from the famous theorem of N. Jacobson which asserts that every ring satisfying the identity $x^{n+1} = x$ for some $n \geq 1$ must be commutative (though Jacobson's result is more general: the existence of a positive integer $n(a)$ for each $a \in R$ such that $a^{n(a)+1} = a$ suffices to conclude that the ring R is commutative). One way (which is, for obvious reasons, quite popular among universal algebraists) to see this is to determine, for a fixed n, the subdirectly irreducible rings with the identity $x^{n+1} = x$, e.g. as in [4, pp.175–178]. It turns out that these subdirectly irreducibles are precisely the finite fields $\mathbb{F}_{p^k}$ such that $(p^k - 1) \mid n$. Hence, every ring satisfying an identity of the form $x^{n+1} = x$ is a subdirect product of finite fields, and thus commutative.

Motivated by this approach, in [1] all subdirectly irreducible *involution rings* satisfying $x^{n+1} = x$ were determined. Recall that an involution ring is a structure $(R, ^*)$ such that R is a ring, and the unary operation * is an involutorial antiautomorphism of R, i.e. we have $(x + y)^* = x^* + y^*$, $(xy)^* = y^* x^*$ and $(x^*)^* = x$ (we refer e.g. to [2, 3, 6, 7] for an overview of involution rings). The result is as follows (the notation is slightly changed, but is still standard).

Theorem 1. [1, Theorem 2] *A ring with involution 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) $\mathbb{F}_{p^k}$, where the involution is the identity mapping,

[1] Supported by Grant No.1227 of the Ministry of Science, Technologies and Development of the Republic of Serbia.

[2] Department of Mathematics and Informatics, University of Novi Sad, Trg Dositeja Obradovića 4, 21000 Novi Sad, Serbia and Montenegro, dockie@im.ns.ac.yu, nmudrinski@im.ns.ac.yu

(2) $\mathbb{F}^*_{p^k}$*, with the involution defined by* $x^* = x^{p^m}$*, when* k *is even and* $k = 2m$*,*

(3) $Ex(\mathbb{F}_{p^k})$*.*

Of course, as we want to keep this note reasonably self-contained, we should explain what $Ex(R)$ is for a given ring R. Let R^{opp} denote the opposite ring of R (i.e. its anti-isomorphic copy). Define a unary operation * on the direct sum $R \bigoplus R^{opp}$ by $(a, b)^* = (b, a)$. It is easily verified that * is an involution of the considered direct sum, usually called the *exchange involution* [6]. The resulting involution ring is denoted by $Ex(R)$. Of course, if R is commutative (and this is the case e.g. when R is a field), $Ex(R)$ can be considered just as a direct sum of two copies of R, while the involution just reverses pairs.

In the second part of [1], an application of the above result is presented, namely, it is shown how to determine the lattice of all subvarieties of the involution ring variety determined by $x^7 = x$. This example is particularly interesting, because it contains all varieties of regular *-rings considered by Yamada [8]. It turned out that while the corresponding ring variety has 12 subvarieties, there are 90 varieties in the involutorial case. And then, the last sentence of [1] (not counting, of course, the *Acknowledgment*) reads as follows: "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."

Although it is true that [1] indeed gives a good grip on how the prescribed task should be done for a given n, the reader will probably agree with us in finding this unsatisfactory from the algorithmic point of view. Thus the goal of this note becomes apparent: to provide a description or a characterization of the lattice of (involution) ring varieties with the considered identity, clearly yielding an effective algorithm which, for a given n, constructs the required lattice. Of course, all the lattices in question are finite, as there are only finitely many subdirectly irreducible (involution) rings satisfying $x^{n+1} = x$ for a given n. So, our task is, in fact, in recognizing whether two sets of such subdirectly irreducibles generate the same variety.

In the following, let $\mathcal{F}$ denote the class of all finite fields, while $\mathcal{F}^*$ denotes the class of all subdirectly irreducible involution rings described in Theorem 1 above (that is, $\mathbb{F}_{p^k}, \mathbb{F}^*_{p^k}$ and $Ex(\mathbb{F}_{p^k})$ for all primes p and for all $k \geq 1$). By $\mathcal{F}_p$ and $\mathcal{F}^*_p$ we denote the members of $\mathcal{F}$ and $\mathcal{F}^*$, respectively, of characteristic p. Finally, let $\mathcal{F}_p(n) = \{\mathbb{F}_{p^k} : (p^k - 1) \mid n\}$, $\mathcal{F}^*_{p,k} = \{\mathbb{F}_{p^k}, \mathbb{F}^*_{p^k}, Ex(\mathbb{F}_{p^k})\}$ and $\mathcal{F}^*_p(n) = \bigcup_{(p^k-1)|n} \mathcal{F}^*_{p,k}$. Clearly, $\mathcal{F}_p(n)$ $(\mathcal{F}^*_p(n))$ contains precisely the subdirectly irreducible (involution) rings satisfying $x^{n+1} = x$ and having characteristic p. It is obvious (and recorded in Corollary 8 of [1]) that $\mathcal{F}_p(n)$ $(\mathcal{F}^*_p(n))$ contains nontrivial members if and only if $(p - 1) \mid n$.

Certainly, the first step towards calculating $L^{(n)}$, the lattice of all varieties of (involution) rings satisfying $x^{n+1} = x$, is the following fact.

Theorem 2. [1, Theorem 9] *Let n be a positive integer, and let $\{p_1, \ldots, p_k\}$ be the set of all prime numbers p_i such that $(p_i - 1) \mid n$. Further, let $L_p^{(n)}$ denote the sublattice of $L^{(n)}$ consisting only of varieties satisfying $px = 0$ (i.e. of varieties of characteristic p). Then $L^{(n)} \cong L_{p_1}^{(n)} \times \ldots \times L_{p_k}^{(n)}$.*

Therefore, to construct $L^{(n)}$, it suffices first to determine all primes p with $(p-1) \mid n$, and then to construct $L_p^{(n)}$ for every such p. In the sequel, we shall assume that p, the characteristic of rings we are working with, is fixed.

Let us notice here that in [1], the above theorem was proved by using some basic facts from universal algebra and elementary number-theoretical considerations. But it may be easily noted from that proof as well that the considered result on the direct decomposition of the subvariety lattice is in fact *not* a result on rings, since the additive abelian group (a left $\mathbb{Z}$-module) was the only part of the ring structure used there. We pause for a moment just to indicate how the above result follows from a much more general setting.

Let $\mathcal{V}_1, \ldots, \mathcal{V}_m$ be varieties of the same similarity type. These varieties are *independent* if there is a term $t(x_1, \ldots, x_m)$ such that for each i, $1 \leq i \leq m$, the variety $\mathcal{V}_i$ satisfies $t(x_1, \ldots, x_m) = x_i$. Further, if for a variety $\mathcal{V}$ we have $\mathcal{V} = \mathcal{V}_1 \vee \ldots \vee \mathcal{V}_m$ and the subvarieties $\mathcal{V}_1, \ldots, \mathcal{V}_m$ are independent, then $\mathcal{V}$ is said to be the *varietal product of* $\mathcal{V}_1, \ldots, \mathcal{V}_m$, written as $\mathcal{V} = \mathcal{V}_1 \otimes \ldots \otimes \mathcal{V}_m$. In such a case each algebra $\mathbf{A} \in \mathcal{V}$ is a direct product $\mathbf{A} \cong \mathbf{A}_1 \times \ldots \times \mathbf{A}_m$, where $\mathbf{A}_i \in \mathcal{V}_i$ for all $1 \leq i \leq m$, and the factors $\mathbf{A}_i$ are unique up to an isomorphism (see p.12 of [5]). A quite straightforward consequence of the latter fact is that

$$L(\mathcal{V}) \cong L(\mathcal{V}_1) \times \ldots \times L(\mathcal{V}_m),$$

where $L(\mathcal{U})$ denotes the lattice of all subvarieties of a variety $\mathcal{U}$.

Now assume that a variety $\mathcal{V}$ has a term definable structure of a left $\mathbb{Z}$-module, which means that there is a binary term $f(x,y)$ and unary terms $g_a(x)$, $a \in \mathbb{Z}$, in the language of $\mathcal{V}$, such that for each algebra $\mathbf{A} \in \mathcal{V}$, $\mathbf{A} = (A, F)$, the algebra $(A, f^{\mathbf{A}}, g_a^{\mathbf{A}})_{a \in \mathbb{Z}}$ is a left $\mathbb{Z}$-module (this is trivially the case in any variety of rings, involution rings, abelian groups, etc.). For a prime p, let $\mathcal{V}_p$ denote the subvariety of $\mathcal{V}$ determined by the identity $g_p(x) = 0$. Then for any finite sequence of mutually distinct primes $p_1, \ldots, p_k$, the varieties $\mathcal{V}_{p_1}, \ldots, \mathcal{V}_{p_k}$ are independent. Indeed, define, as in [1], $q_i = p_1 \ldots p_{i-1} p_{i+1} \ldots p_k$. Since $(p_i, q_i) = 1$, we have $\alpha_i p_i + \beta_i q_i = 1$ for some $\alpha_i, \beta_i \in \mathbb{Z}$ and for all $1 \leq i \leq k$. Consider the term

$$t(x_1, \ldots, x_k) = \beta_1 q_1 x_1 + \ldots + \beta_k q_k x_k,$$

where $x + y$ means $f(x,y)$, and ax means $g_a(x)$ ($a \in \mathbb{Z}$). Since $p_i \mid q_j$ if $i \neq j$, and $\mathcal{V}_{p_i}$ satisfies $p_i x_i = 0$, we have that

$$t(x_1, \ldots, x_k) = \beta_i q_i x_i = (1 - \alpha_i p_i) x_i = x_i$$

holds in $\mathcal{V}_{p_i}$. Hence, $\mathcal{V}_{p_1} \vee \ldots \vee \mathcal{V}_{p_k} = \mathcal{V}_{p_1} \otimes \ldots \otimes \mathcal{V}_{p_k}$, which immediately implies Theorem 2. It is not hard to see that the above considerations can be generalized for varieties having term definable K-module structures, where K is an arbitrary commutative ring with an identity element.

Turning back to our aim, write $R \hookrightarrow S$ for (involution) rings R, S if R embeds into S. This relation turns immediately $\mathcal{F}_p$ and $\mathcal{F}_p^*$ into partially ordered sets. Note that since $\mathbb{F}_{p^k} \hookrightarrow \mathbb{F}_{p^\ell}$ if and only if $k \mid \ell$, we have $(\mathcal{F}_p, \hookrightarrow) \cong (\mathbb{N}, |)$. Our main result is now as follows.

Theorem 3. *Let $n \geq 1$ be an integer and p a prime such that $(p-1) \mid n$. Then the lattice $L_p^{(n)}$ of all (involution) ring varieties satisfying $x^{n+1} = x$ and $px = 0$ is isomorphic to the lattice of all ideals of the ordered set $(\mathcal{F}_p(n), \hookrightarrow)$ (resp. $(\mathcal{F}_p^*(n), \hookrightarrow)$).*

Of course, the sets $\mathcal{F}_p(n)$ and $\mathcal{F}_p^*(n)$ can be effectively determined for each n. Moreover, we have (a quite easy) effective description of the relation $\hookrightarrow$ on $\mathcal{F}_p$, and so the (finite) poset $(\mathcal{F}_p(n), \hookrightarrow)$ can be effectively computed, along with all of its order ideals, which – in conjunction with the above theorem – establishes our goal for the ring case. To have the same situation with involution ring varieties, we need to determine $\hookrightarrow$ on $\mathcal{F}_p^*$.

Lemma 4. *Let $k, \ell \geq 1$ be integers.*

(1) $\mathbb{F}_{p^k} \hookrightarrow \mathbb{F}_{p^\ell}$ if and only if $k \mid \ell$.

(2) $\mathbb{F}_{p^k} \hookrightarrow \mathbb{F}^*_{p^\ell}$, $\ell = 2m$, if and only if $k \mid m$.

(3) $\mathbb{F}_{p^k} \hookrightarrow Ex(\mathbb{F}_{p^\ell})$ if and only if $k \mid \ell$.

(4) $\mathbb{F}^*_{p^k}$, $k = 2r$, does not embed into $\mathbb{F}_{p^\ell}$.

(5) $\mathbb{F}^*_{p^k} \hookrightarrow \mathbb{F}^*_{p^\ell}$, $k = 2r$, $\ell = 2m$, if and only if $r \mid m$ and $\frac{m}{r}$ is an odd number.

(6) $\mathbb{F}^*_{p^k} \hookrightarrow Ex(\mathbb{F}_{p^\ell})$, $k = 2r$, if and only if $k \mid \ell$.

(7) $Ex(\mathbb{F}_{p^k})$ does not embed into $\mathbb{F}_{p^\ell}$.

(8) $Ex(\mathbb{F}_{p^k})$ does not embed into $\mathbb{F}^*_{p^\ell}$, $\ell = 2m$.

(9) $Ex(\mathbb{F}_{p^k}) \hookrightarrow Ex(\mathbb{F}_{p^\ell})$ if and only if $k \mid \ell$.

Proof. (1) Since $\mathbb{F}_{p^k}$ and $\mathbb{F}_{p^\ell}$ both have the identity mapping as the involution, this follows from the classical result on finite field embeddings.

(2) Note that in $\mathbb{F}_{p^\ell}$, all fixed points of the involution satisfy the equation $x^{p^m} = x$. Therefore, they form a subfield isomorphic to $\mathbb{F}_{p^m}$. So, $\mathbb{F}_{p^k} \hookrightarrow \mathbb{F}^*_{p^\ell}$ if and only if $\mathbb{F}_{p^k} \hookrightarrow \mathbb{F}_{p^m}$.

(3) Similarly as in (2), consider the fixed points of the involution in $Ex(\mathbb{F}_{p^\ell})$: these are the pairs (a,a), $a \in \mathbb{F}_{p^\ell}$. They form a field, isomorphic to $\mathbb{F}_{p^\ell}$, and thus $\mathbb{F}_{p^k} \hookrightarrow Ex(\mathbb{F}_{p^\ell})$ if and only if $\mathbb{F}_{p^k} \hookrightarrow \mathbb{F}_{p^\ell}$.

(4) Since $x^* = x^{p^r}$ in $\mathbb{F}^*_{p^k}$, there is at least one element in this involution field which is not fixed by the involution (this is, e.g. the generator of the multiplicative cyclic group of the underlying field $\mathbb{F}_{p^k}$), and so the assertion follows.

(5) Clearly, since each involution ring embedding is at the same time an embedding of rings, if $\mathbb{F}^*_{p^k} \hookrightarrow \mathbb{F}^*_{p^\ell}$ then $k \mid \ell$. In that case, there is only one copy of $\mathbb{F}_{p^k}$ in $\mathbb{F}_{p^\ell}$ and it is formed by those elements of the latter field which are roots of $x^{p^k} - x = 0$. Of course, the involution in $\mathbb{F}^*_{p^\ell}$ is defined by $x^* = x^{p^m}$, but the required embedding will be possible if and only if for each root of the above polynomial we have $x^* = x^{p^r}$, i.e. if and only if the implication

$$x^{p^k} = x \;\Rightarrow\; x^{p^r} = x^{p^m}$$

holds (in the multiplicative group of $\mathbb{F}_{p^\ell}$). However, the latter condition is equivalent to $(p^k - 1) \mid (p^m - p^r)$. As $p^m - p^r = p^r(p^{m-r} - 1)$ and $k = 2r$, this will be true if and only if $2r \mid (m - r)$, i.e. $m = r(2s + 1)$ for some $s \geq 0$.

(6) By Lemma 10 of [1], $\mathbb{F}^*_{p^k}$ embeds in $Ex(\mathbb{F}_{p^k})$, and so if $k \mid \ell$, by (9) it follows that $\mathbb{F}_{p^k} \hookrightarrow Ex(\mathbb{F}_{p^\ell})$. On the other hand, each element of $Ex(\mathbb{F}_{p^\ell})$ satisfies $x^{p^\ell} = x$, and if $\mathbb{F}^*_{p^k} \hookrightarrow Ex(\mathbb{F}_{p^\ell})$, so must each element of $\mathbb{F}^*_{p^k}$, i.e. of the underlying field $\mathbb{F}_{p^k}$. This is, however, possible only if $k \mid \ell$.

(7) This is analogous to (4), since $Ex(\mathbb{F}_{p^k})$ has a nonidentical involution for each $k \geq 1$.

(8) This follows from the fact that $(a,0)^{p^m} = (a^{p^m}, 0) \neq (0,a) = (a,0)^*$ holds in $Ex(\mathbb{F}_{p^k})$ for any non-zero $a \in \mathbb{F}_{p^k}$.

(9) If $k \mid \ell$ and $\varphi : \mathbb{F}_{p^k} \to \mathbb{F}_{p^\ell}$ is an embedding, then it is easy to see that $\psi : Ex(\mathbb{F}_{p^k}) \to Ex(\mathbb{F}_{p^\ell})$, defined by $\psi((a,b)) = (\varphi(a), \varphi(b))$, is an embedding too, which preserves the exchange involution. On the other hand, if $Ex(\mathbb{F}_{p^k}) \hookrightarrow Ex(\mathbb{F}_{p^\ell})$, then by considering the identity $x^{p^\ell} = x$ one concludes, analogously as in (6), that $k \mid \ell$. □

Let us stop just for a minute to visualize the ordered set $(\mathcal{F}^*_p, \hookrightarrow)$. First of all, every integer $k \geq 1$ can be in a unique way decomposed as $k = 2^i j$, where j is an odd number. According to this decomposition, we attach some labels to involution rings in $\mathcal{F}^*_p$: $\mathbb{F}_{p^k}$ will be denoted by (a_i, j), $\mathbb{F}^*_{p^{2k}}$ by (b_i, j), and $Ex(\mathbb{F}_{p^k})$ by (c_i, j). Let $A = \{a_i : \ i \geq 0\} \cup \{b_i : \ i \geq 0\} \cup \{c_i : \ i \geq 0\}$, and define an ordering $\leq$ on A by:

(1) $a_i \leq \alpha$, $\alpha \in \{a_m, b_m, c_m\}$, if and only if $i \leq m$,

(2) $b_i \not\leq a_m$ for all $i, m \geq 0$,

(3) $b_i \leq b_m$ if and only if $i \leq m$,

(4) $b_i \leq c_m$ if and only if $i + 1 \leq m$,

(5) $c_i \not\leq \alpha$, $\alpha \in \{a_m, b_m\}$, for all $i, m \geq 0$,

(6) $c_i \leq c_m$ if and only if $i \leq m$.

It is easy to deduce from the above lemma that in $\mathcal{F}_p^*$ we have $(\alpha, j_1) \hookrightarrow (\beta, j_2)$ if and only $\alpha \leq \beta$ in A and $j_1 \mid j_2$. Hence, $(\mathcal{F}_p^*, \hookrightarrow)$ is isomorphic to the direct product of the lattice of all odd numbers with the divisibility order (which is, in turn, isomorphic to $(\mathbb{N}, |)$) and $(A, \leq)$. The latter order is depicted in Figure 1.

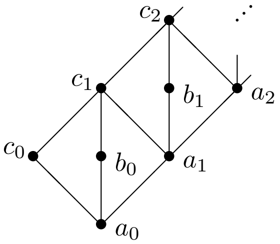

Figure 1. The partially ordered set $(A, \leq)$

Now it is fairly obvious that the relation $\hookrightarrow$ is defined effectively on $\mathcal{F}_p^*$, so that there is an algorithm which for each $n \geq 1$ computes the finite partial order $(\mathcal{F}_p^*(n), \hookrightarrow)$.

In the proof of our Theorem 3, we are going to use the following two lemmas. We recall that if $\mathcal{C}$ is a class of algebras (of a given similarity type), then $\mathcal{V}(\mathcal{C})$ denotes the variety *generated by* $\mathcal{C}$, the smallest variety containing $\mathcal{C}$.

Lemma 5. *Let R be an (involution) ring with no zero divisors. If*

$$R \in \mathcal{V}(R_1, \ldots, R_k)$$

for some (involution) rings $R_1, \ldots, R_k$, then $R \in \mathcal{V}(R_i)$ for some $1 \leq i \leq k$.

Proof. Assume that $R \notin \mathcal{V}(R_i)$ for all $1 \leq i \leq k$. This means that for each i, there is an identity

$$p_i(x_1, \ldots, x_{m_i}) = 0$$

which holds in R_i, but fails in R. Here p_i is an (involution) ring term, that is, a polynomial in non-commuting variables with coefficients from $\mathbb{Z}$, while in the involutorial case one must include also the stars of variables $x_1^*, x_2^*, \ldots$. So, there are elements $a_1^{(i)}, \ldots, a_{m_i}^{(i)} \in R$ such that

$$b_i = p_i(a_1^{(i)}, \ldots, a_{m_i}^{(i)}) \neq 0.$$

Now consider the identity

$$p_1(x_{1,1}, \ldots, x_{m_1,1}) p_2(x_{1,2}, \ldots, x_{m_2,2}) \ldots p_k(x_{1,k}, \ldots, x_{m_k,k}) = 0.$$

Clearly, this identity holds in each R_i, and thus in the variety $\mathcal{V}(R_1, \dots, R_k)$. On the other hand, in R we have

$$p_1(a_1^{(1)}, \dots, x_{m_1}^{(1)})p_2(x_1^{(2)}, \dots, x_{m_2}^{(2)}) \dots p_k(x_1^{(k)}, \dots, x_{m_k}^{(k)}) = b_1 b_2 \dots b_k \neq 0,$$

since R has no zero divisors. Hence, the considered identity is false in R, and so $R \notin \mathcal{V}(R_1, \dots, R_k)$. □

Remark 6. If R has zero divisors, but we can find terms $p_i(x_1, \dots, x_{m_i})$ and elements $a_j^{(i)} \in R$ as in the above proof, such that $b_1, \dots, b_k$ are *not* zero divisors, then we obtain the same conclusion as in the lemma just proved. This fact will be used later, in dealing with involution rings of the form $Ex(\mathbb{F})$, where $\mathbb{F}$ is a finite field.

Lemma 7. *Let R, S be subdirectly irreducible (involution) rings form $\mathcal{F}_p$ ($\mathcal{F}_p^*$) such that $R \in \mathcal{V}(S)$. Then $R \hookrightarrow S$.*

Proof. While assuming that $R \not\hookrightarrow S$, we shall prove that there is an identity which holds in S and fails in R.

For the ring case, this is immediately clear, as $\mathbb{F}_{p^k} \not\hookrightarrow \mathbb{F}_{p^\ell}$ means that ℓ is not divisible by k, whence

$$x^{p^\ell} - x = 0$$

is the required identity. In the involutorial case, the above identity will work just fine (under the same non-divisibility assumption) for the cases

$$(R, S) \in \{(\mathbb{F}_{p^k}, \mathbb{F}_{p^\ell}), (\mathbb{F}_{p^k}, Ex(\mathbb{F}_{p^\ell})), (\mathbb{F}_{p^k}^*, Ex(\mathbb{F}_{p^\ell})), (Ex(\mathbb{F}_{p^k}), Ex(\mathbb{F}_{p^\ell}))\},$$

because $Ex(\mathbb{F}_{p^\ell})$ satisfies the above identity too (as its ring reduct is just a direct sum of two copies of $\mathbb{F}_{p^\ell}$). In fact, if R is a commutative ring, $Ex(R)$ satisfies the very same ring identities as R does.

Furthermore, it is obvious that the identity $x - x^* = 0$ will take care of the cases $(R, S) \in \{(\mathbb{F}_{p^k}^*, \mathbb{F}_{p^\ell}), (Ex(\mathbb{F}_{p^k}), \mathbb{F}_{p^\ell})\}$. So, consider the identity

$$x^{p^m} - x^* = 0.$$

By definition, this identity is true in $\mathbb{F}_{p^\ell}^*$, where $\ell = 2m$. On the other hand, if it holds in $\mathbb{F}_{p^k}$ then (since we have $x = x^*$ in the latter involution field) $k \mid m$, i.e. $\mathbb{F}_{p^k} \hookrightarrow \mathbb{F}_{p^\ell}^*$, by Lemma 4, (2). If the above identity holds in $\mathbb{F}_{p^k}^*$, $k = 2r$, then

$$0 = (x^{p^m})^* - x = (x^{p^m})^{p^r} - x = x^{p^{m+r}} - x$$

is satisfied as well, so $k \mid m + r$, and m is an odd multiple of r, as required in Lemma 4, (5). Finally, the above identity is false in $Ex(\mathbb{F}_{p^k})$, since

$$(a, 0)^{p^m} - (a, 0)^* = (a^{p^m}, 0) - (0, a) = (a^{p^m}, -a) \neq (0, 0)$$

for any non-zero $a \in \mathbb{F}_{p^k}$. □

Remark 8. In the above proof, in case when R is $Ex(\mathbb{F}_{p^k})$, the polynomials showing that $R \notin \mathcal{V}(S)$ are indeed constructed such that they have at least one value which is not a zero divisor in R (the zero divisors in $Ex(\mathbb{F}_{p^k})$ are of the form $(a,0)$ and $(0,a)$, $a \in \mathbb{F}_{p^k}$). Namely, this is explicitly shown for $x^{p^m} - x^*$ in the last displayed formula above. For $x - x^*$, it suffices to take $(a,0)$ for x, where $a \neq 0$, to obtain $(a,0) - (a,0)^* = (a,-a)$. Finally, evaluate x as (a,a), where $a \neq 0$ in $x^{p^\ell} - x$. Since the assumption is that k does not divide ℓ, we have $(a,a)^{p^\ell} - (a,a) = (a^{p^\ell} - a, a^{p^\ell} - a)$, and $a^{p^\ell} - a \neq 0$.

Therefore, by Remark 6, Lemma 5 holds also in the case when R is of the form $Ex(\mathbb{F}_{p^t})$, and $R_1, \ldots, R_k$ are from $\mathcal{F}_p^*$.

Proof of Theorem 3. Let $L_I(p,n)$ denote the lattice of order ideals of $(\mathcal{F}_p(n), \hookrightarrow)$ (of $(\mathcal{F}_p^*(n), \hookrightarrow)$) and define a mapping $f : L_I(p,n) \to L_p^{(n)}$ by

$$f(\mathcal{I}) = \mathcal{V}(\mathcal{I})$$

for each $\mathcal{I} \in L_I(p,n)$. We show that f is a lattice isomorphism. Indeed, f is onto, since each variety $\mathcal{V}$ from $L_p^{(n)}$ is generated by its set of subdirectly irreducible members $\mathcal{V}_{SI}$, which is an order ideal in $\mathcal{F}_p(n)$ $(\mathcal{F}_p^*(n))$. Thus, we need to prove that

$$\mathcal{I}_1 \subseteq \mathcal{I}_2 \text{ if and only if } \mathcal{V}(\mathcal{I}_1) \subseteq \mathcal{V}(\mathcal{I}_2).$$

The direct implication is obvious (and holds even if $\mathcal{I}_1, \mathcal{I}_2$ are arbitrary classes of algebras), so assume that $\mathcal{V}(\mathcal{I}_1) \subseteq \mathcal{V}(\mathcal{I}_2)$. Then for each (involution) ring $R \in \mathcal{I}_1$ we have $R \in \mathcal{V}(\mathcal{I}_2)$. By Lemma 5 and Remark 8, there is an $S \in \mathcal{I}_2$ such that $R \in \mathcal{V}(S)$, which by Lemma 7 implies $R \hookrightarrow S$, i.e. $R \in \mathcal{I}_2$. In other words, $\mathcal{I}_1 \subseteq \mathcal{I}_2$, as wanted. □

As already pointed out, the ordered sets $(\mathcal{F}_p(n), \hookrightarrow)$ and $(\mathcal{F}_p^*(n), \hookrightarrow)$ are effectively constructible (the latter by Lemma 4). Hence, the same is true for the lattices of their ideals, and, by Theorem 3, for $L_p^{(n)}$. Finally, it remains to use Theorem 2 to complete the construction of $L^{(n)}$.

References

[1] Crvenković, S., Dolinka, I., Vinčić, M., On subdirect decomposition and some varieties of rings with involution, Beiträge zur Algebra und Geometrie, 43(2002), 423–432.

[2] Heatherly, H. E., Lee, E. K. S., Wiegandt, R., Involutions on universal algebras, in (G. Saad and M.J. Thomsen, eds.) Nearrings, Nearfileds and K-Loops (Hamburg, 1995), pp.269–282, Kluwer, Dordrecht, 1997.

[3] Herstein, I. N., Rings with Involution, University of Chicago Press, 1976.

[4] McKenzie, R., McNulty, G., Taylor, W., Algebras, Lattices, Varieties, Vol. I, Wadsworth & Brooks/Cole, Monterey, CA, 1987.

[5] McKenzie, R., Valeriote, M., The Structure of Decidable Locally Finite Varieties, Birkhäuser, Boston, 1989.

[6] Rowen, L. H., Ring Theory, Academic Press, New York, 1988.

[7] Wiegandt, R., On the structure of involution rings with chain condition, Vietnam J. Math. 21 (1993), 1–12.

[8] Yamada, M., On the multiplicative semigroups of regular rings with special involution, Simon Stevin 59 (1985), 51–57.