PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 34 (48), 1983, pp. 165–167

# ON RINGS WITH POLYNOMIAL IDENTITY $x^n - x = 0$

**Veselin Perić**

**Abstract**. If $R \neq 0$ is an associative ring with the polynomial identity $x^n - x = 0$, where $n > 1$ is a fixed natural number, then it is well known that $R$ is commutative. It is also known that any anti-inverse ring $R(\neq 0)$ satisfies the polynomial identity $x^3 - x = 0$ [**1**]. The structure of anti-inverse rings was described in [**2**]: they are exactly subdirect sums of $GF(2)$'s and $GF(3)$'s. In generalizing the last result, we prove here that a ring $R$ with the polynomial identity $x^n - x = 0$ ($> 1$) is a subdirect sum of $GF(p)$'s, where $p^r - 1$ divides $n - 1$. We also prove again some known results about commutative regular rings.

We consider here the associative rings $R \neq 0$. These rings need not be commutative and they can be without identity. In the polynomial identity $x^n - x = 0$ we assume $n$ to be a fixed natural number greater than 1.

Following B. Cerović [**1**], a ring $R$ is called an anti-inverse ring if every element $x$ in $R$ has an anti-inverse $x^*$ in $R: x^*xx^* = x$ and $xx^*x = x^*$. From this definition the following well known lemma is immediately inferred:

Lemma 1. ([**2**]). *In any anti-inverse ring $R$ the following identities are valid:* $x^2 = x^{*2} = (xx^*)^2 = (x^*x)^2$.

*Especially, any anti-inverse ring R satisfies the polynomial identity* $x^5 - x = 0$.

According to the well known Jacobson's Theorem, from the preceding lemma we have also the following well known lemma:

Lemma 2. *Every ring $R$ with the polynomial identity $x^n - x = 0$ is commutative. Especially, any anti-inverse ring $R$ is commutative.*

From the two preceding lemma we obtain the following proposition, already known in the literature:

---

*AMS Subject Classification* (1980): Primary 16 A 38.

*Key words and phrases*: Anti-inverse rings; polynomial identity $x^n - x = 0$; subdirect sum of $GF(p)$'s; commutative regular rings.

This research was supported by SIZ nauke SRBiH.

Proposition 1. ([**1**, prop. 2.2] and [**2**]) *A ring $R$ is an anti-inverse ring if and only if it satisfies the polynomial identity $x^3 - x = 0$.*

The anti-inverse rings were characterized in [**2**] in the following manner:

Proposition 2. ([**2**]) *The following are equivalent:*

(1) *$R$ is an anti-inverse ring;*

(2) *$R$ is a subdirect sum of $GF(2)$'s and $GF(3)$'s;*

(3) *$R$ satisfies the polynomial identity $x^3 - x = 0$*

In generalizing the part of this proposition asserting the equivalence between (2) and (3), we prove here the following theorem:

Theorem: *For a ring $R$ the following conditions are equivalent:*

(i) *$R$ is a ring with the polynomial identity $x^n - x = 0$;*

(ii) *$R$ is a subdirect of fields $GF(p^r)$, where $p^r - 1$ divides $n - 1$.*

For the proof of this theorem we need a certain preparation and we start with the following lemma:

Lemma 3. *Let $R$ be a subdirectly irreducible ring. Then $R$ is without proper zero divisors if and only if $R$ has no nonzero nilpotent elements.*

*Proof*. If $R$ is without proper zero divisors, then it is clear that $R$ has no nonzero nilpotent elements.

Conversely, let $R$ be without nonzero nilpotent elements. Then for any subset $S$ of $R$ the left annihilating set of $S$ coincides with the right annihilating set of $S$, and hence it is an ideal of $R$, the annihilating ideal $\mathrm{ann}_R(S)$ of $S$ in $R$. Suppose the set $A$ of all proper zero divisors in $R$ is not void. For any $a$ in $A$ the annihilating ideal $\mathrm{ann}_R(a)$ is a singular ideal in $R$ different from (0) and contains no regular elements $b$ in $R$. By hypothesis $a \notin \mathrm{ann}_R(a)$ for any $a$ in $A$, and hence $\cap_{a \in A} \mathrm{ann}_R(a) = (0)$. Consequently, $R$ would not be a subdirectly irreducible ring.

If $R$ is a ring with the polynomial identity $n^n - x = 0$, or a commutative regular ring (a ring with identity having for any $x$ in $R$ an element $x'$ in $R$ with $xx'x = x$), then surely $R$ has no nonzero nilpotent elements. If moreover such a ring is subdirectly irreducible, then $R$ is without proper zero divisors according to the preceding lemma. But in this case $R$ is a field, because it is a finite commutative ring having at most $n$ elements, or according to $x(x'x - 1) = 0$, a commutative ring in which any nonzero element $x$ is invertible.

So, for commutative regular rings we have the following proposition:

Proposition 3. *A commutative regular ring $R$ is subdirectly irreducible if and only if it is a field.*

This proposition is implicitely contained in [**2**].

Proposition 4. *$R$ is a subdirectly irreducible ring with polynomial identity $x^n - x = 0$ if anf only if $R = GF(p^r)$, where $p^r - 1$ divides $n - 1$.*

*Proof*. Let $R = GF(p^r); p^r - 1$ divides $n - 1$. Then $R$ is surely a subdirectly irreducible ring. Moreover $(R, \cdot)$ is a cyclic group of order $p^r - 1$, and hence $x^{p^{r-1}} = 1 (x \in R)$. Since $p^r - 1$ divied $n - 1$ we have $x^{n-1} = 1 (x \in R)$, which means $x^n = x (x \in R)$.

Conversely, let $R$ be a subdirectly irreducible ring with polynomial identity $x^n - x = 0$. According to the remark following Lemma 3, R is a finite field having at most $n$ elements; hence, $R = GF(p^r)$. The generating element $g$ of the cyclic group $(R^\cdot)$ of order $p^r - 1$ has the same order, and because $g^n - g = 0$, i.e., $g^{n-1} = 1$, $p^r - 1$ must divide $n - 1$.

We can now prove our theorem.

(i) *implies* (ii): As it is known, $R$ is a subdirect sum of subdirectly irreducible rings $R_i (i \in I)$. The ring $R$ satisfies the polynomial identity $x^n - x = 0$, and since any $R_i$ is an epimorphic image of $R$, it satisfies that identity too. According to Proposition 4, any $R_i$ has form $GF(p^r)$, where $p^r - 1$ divides $n - 1$.

(ii) *implies* (i): According to Proposition 4, any of the rings $GF(p^r)$, where $p^r - 1$ divides $n - 1$ satisfies the polynomial identity $x^n - x = 0$; hence, the subdirect sum $R$ of these rings itself satisfies that identity.

As the implication "(i) implies (ii)" is proved using Proposition 4, we can prove again the following proposition using Proposition 3:

PROPOSITION 5. *Any commutative regular ring $R$ is a subdirect sum of fields.*

This proposition is not new and is implicitly contained in [**3**] (see leater). We observe that the converse of this proposition need not be true. Indeed, a subdirect sum of fields need not not have an identity (for instance the direct sum of infinitely many fields has no identity). But also when a subdirect sum of (infinitely many) fields has an identity, it need not be a (commutative) regular ring. Namely, if $f : R \to \prod_{t \in I} R_i$ is the monomorphism defining $R$ as a subdirect sum of the fields $R_i (i \in I)$ and $f(x) = (x_i)_{i \in I}$, then for $x'$ in $R$ with $x^2 x' = x$ we could have $f(x') = (x'_i)_{i \in I}$ where $x'_i = x_i^{-1}$ for $x_i \neq 0$. But, such an element $(x'_i)_{i \in I}$ need not belong to $f(R)$.

Moreover, it is well known that a commutative ring $R$ with identity is a subdirect sum of fields if and anly if the Jacobson radical of $R$ is equal to (0) ([**3**], Coroll. 2.11). But in such a ring any prime ideal need not be maximal, and hence such a ring need nor be a (commutative) regular) ring ([**3**, Prop. 2.2.3 and 2.2.4]).

We remark finally that hawing in mind Proposition 1 (whose proof as we have seen is simple), our theorem contains Proposition 2, as a special case. Indeed, for $n = 3$, from the condition $p^r - 1$ divides $n - 1$ it follows that $p - 2$, $r = 1$, or $p = 3$, $r = 1$, and conversely. Proposition 2, was proved by Tominaga [**2**] and it covers all results of [**1**] related to anti-inverse ring. Our theorem covers also these results of [**1**] related to the rings with polynomial identity $x^n - x = 0$.

REFERENCES

[1] B. Cerović, *Anti-inverse rings*, Publ. Inst. Math. (Beograd) (N.S.) **29** (**33**) (1981), 45–48.

[2] H. Tominaga, *On anti-inverse rings*, Publ. Inst. Math. (Beograd) (N.S) **33** (**47**) (1983), 225.

[3] J. Lamberk, *Lectures on Rings and Modules*, Waltham, Massachusetts-Toronto-London, 1966. (Russ. transl.:*Kol'ca i moduli*, Mir, Moskva, 1971).

Odsjek za matematiku
Prirodno-matematički fakultet
71000 Sarajevo
Jugoslavija

(Received 21 10 1982)