P. Jedlička

The rings which are Boolean. II.

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 53 (2012), No. 1, 73--75

THE RINGS WHICH ARE BOOLEAN II

PŘEMYSL JEDLIČKA

Praha

Received October 22, 2011

Revised November 16, 2011

In this article we answer the following question: if one has a ring R of characteristics 2 satisfying $x^p = x$, for some p; which values of p imply the identity $x^2 = x$?

If we have a boolean algebra A, there is a classical way how to define a ring structure on A, namely

$$x + y = (x \wedge y') \vee (x' \wedge y), \qquad x \cdot y = x \wedge y.$$

Such a ring is *boolean*, that means unitary (with 1 as the multiplicative unit), of characteristic 2 and satisfying the identity $x^2 = x$. On the other hand, whenever one has a boolean ring, defining

$$x \vee y = x + y + xy, \qquad x \wedge y = x \cdot y, \qquad x' = 1 + x$$

we obtain a boolean algebra.

Ivan Chajda and Filip Švrček were considering a more general situation. Suppose, that our unitary ring of characteristic 2 satisfies the identity $x^p = x$, for some $p > 2$. Is there a lattice (or lattice-like) structure on the ring that enables one to reconstruct the ring operations? And they managed to find a structure satisfying all the lattice axioms but the absorption [1].

To make their result more complete, the authors of [1] needed to know whether the identity $x^p = x$ implies already $x^2 = x$ (and hence the ring is already boolean and the solution is trivial) or there exist non-boolean examples. They tackled the problems using elementary methods obtaining some partial results [2].

Department of Mathematics, Faculty of Engineering, Czech University of Life Sciences, Kamýcká 129, 165 21, Prague 6 – Suchdol.

2000 Mathematics Subject Classification. 06E20; 16R40

Key words and phrases. Boolean ring, unitary ring, characteristic 2

E-mail address: jedlickap@tf.czu.cz

In this paper we use structural properties of one-generated rings to answer the question completely. It turns out that the only fundamental examples of rings, that one has to consider, are finite fields.

Acknowledgement: The author would like to thank the unknown referee for simplifying one of the proofs.

Solution

We would like to find whether the identity $x^p = x$, for a given p, implies $x^2 = x$, in a unitary ring of characteristic 2. Since it is an identity of a single variable, it suffices to consider one-generated (sub)rings, more precisely, we are going to construct the free one-generated ring of characteristic 2 with respect to $x^p = x$.

The free one-generated ring of characteristic 2 is $\mathbb{Z}_2[x]$. Since our ring satisfies $x^p = x$, we have to factor over this identity, i.e. over the ideal generated by the polynomial $x^p - x$. However, this is not sufficient, we have to consider all the possible identities $f^p = f$, for every $f \in \mathbb{Z}_2[x]$, and therefore the free ring of $x^p = x$ is $\mathbb{Z}_2[x]/I$ where I is the ideal generated by all the polynomials $f^p - f$ for all $f \in \mathbb{Z}_2[x]$.

The ring $\mathbb{Z}_2[x]$ is a principal ideal domain and therefore I is generated by a single polynomial, namely by the greatest common divisor of I. And this generator is square-free:

Lemma 1 *Let d be a common divisor of all the polynomials $f^p - f$, for all $f \in$ $\in \mathbb{Z}_2[x]$. Then d is not divisible by the square of a non-trivial polynomial.*

Proof. Let $f \in \mathbb{Z}_2[x]$; we want to prove $f^2 \nmid d$. Since d is a divisor of $f^p - f$, it suffice to prove $f^2 \nmid (f^p - f)$. This follows from the fact that $f^2 | f^p$ and $f^2 \nmid f$. $\square$

The preceding lemma holds in fact in each characteristic and for all identities in one variable with invertible linear coefficient—the proof remains the same.

Proposition 2 *Any one-generated unitary ring of characteristic 2 satisfying the identity $x^p = x$ is a product of finite fields.*

Proof. Any such one-generated ring is a factor of $\mathbb{Z}_2[x]$ over some ideal I. This ideal has to contain all the polynomials $f^p - f$. Hence I is generated by a common divisor of $f^p - f$, we denote it by d, and such d is square-free, according to Lemma 1 Hence $d = d_1 \cdots d_k$, where all the d_i are irreducible and pairwise distinct. By the Chinese remainder theorem,

$$\mathbb{Z}_2[x]/I \cong \mathbb{Z}_2[x]/d_1 \times \cdots \times \mathbb{Z}_2[x]/d_k$$

and since all the d_i are irreducible, they generate maximal ideals and $\mathbb{Z}_2[x]/d_i$ is a (finite) field. $\square$

It is very likely that Proposition 2 is already known to some extent; however we were not able to find a suitable reference. This is why we decided to include it in the paper.

With this proposition at hand, we are able to decide when $x^p = x$ enforces $x^2 = x$.

Theorem 3 *There exists a non-boolean unitary ring of characteristics* 2 *satisfying the identity* $x^p = x$*, for some* $p \geq 1$*, if and only if* $p = l \cdot (2^k - 1) + 1$*, for some* $l \geq 0$ *and* $k \geq 2$*.*

Proof. "$\Leftarrow$" An example is the 2^k-element field. Since the multiplication group has $2^k - 1$ elements, all the non-zero elements satisty $x^{l\cdot(2^k-1)} = 1$.
"$\Rightarrow$" Let R be a ring of characteristics 2 satisfying $x^p = x$ and take $a \in R$ satisfying $a^2 \neq a$. The subring $\langle a \rangle$ is a product of fields, according to Proposition 2. As $\langle a \rangle$ is not a product of 2-element fields, there must exist a larger field in the product. But, a 2^k-element field satisfies the identity $x^p = x$ if and only if $(p-1) \mid (2^k - 1)$, since the multiplication group is cyclic of order $2^k - 1$ and an element x satisfies $x^{p-1} = 1$ only if its order divides the order of the group. $\square$

References

[1] Chajda, I., Svrček, F.: *Lattice-like structures derived from rings*, Contributions to General Algebra **20**, Proc. of Salzburg Conference (AAA81), J. Hayn, Klagenfurt 2011, to appear.

[2] Chajda, I., Svrček, F.: *The rings which are boolean*, to appear in Discussiones Mathem., General Algebra and Appl.