The Rings Which Can Be Recovered by Means of the Difference

Ivan CHAJDA\textsuperscript{a}, Filip ŠVRČEK\textsuperscript{b}

Department of Algebra and Geometry, Faculty of Science, Palacký University
17. listopadu 12, 771 46 Olomouc, Czech Republic
\textsuperscript{a}e-mail: ivan.chajda@upol.cz
\textsuperscript{b}e-mail: filip.svrcek@upol.cz

(Received May 29, 2012)

Abstract

It is well known that to every Boolean ring $R$ can be assigned a Boolean algebra $B$ whose operations are term operations of $R$. Then a symmetric difference of $B$ together with the meet operation recover the original ring operations of $R$. The aim of this paper is to show for what a ring $R$ a similar construction is possible. Of course, we do not construct a Boolean algebra but only so-called lattice-like structure which was introduced and treated by the authors in a previous paper. In particular, we reached interesting results if the characteristic of the ring $R$ is either an odd natural number or a power of 2.

Key words: Boolean ring, commutative ring, lattice-like structure, difference

2000 Mathematics Subject Classification: 06E20, 06E30, 13B25, 13A99

Having a Boolean ring $R = (R; +, \cdot, 0, 1)$ the induced Boolean algebra $B(R) = (R; \lor, \land, ', 0, 1)$ can be established by

\[ x \lor y = x + y + xy, \quad x \land y = xy, \quad x' = 1 + x, \]

see [1]. Also conversely, having a Boolean algebra $B = (B; \lor, \land, ', 0, 1)$ we can define the so-called symmetric difference $x + y = (x \land y') \lor (x' \land y)$ and, using this, the induced Boolean ring $R(B) = (B; +, \cdot, 0, 1)$ can be recovered as follows:

- $x + y$ in $R(B)$ is equal to the symmetrical difference of $B$;
- $x \cdot y$ in $R(B)$ is equal to the meet operation $\land$ of $B$.

\textsuperscript{*}Supported by the project Algebraic Methods in Quantum Logic, CZ.1.07/2.3.00/20.0051.
It was already shown by several authors that a similar construction can be derived also for orthomodular lattices (see [6, 7, 8, 9, 10, 11, 12]), for ortholattices (see [2, 3]), or for pseudocomplemented semilattices, [4]. The construction was generalized for bounded lattices with an antitone involution in [12]. However, the ring-like structures induced by these lattices are rather far from rings.

Hence, we involved another approach in [5] in order to establish a certain lattice-like structure to a given ring such that the original ring can be recovered by means of the difference. Of course, this is not possible for every ring but it appeared in [5] that the construction works for commutative unitary rings of characteristic 2 satisfying the identity $x^{p+2} = x^p$ for a natural number $p$ (if $p = 1$, then the ring is Boolean and the assigned lattice-like structure is a Boolean algebra).

The aim of this paper is to extend this approach to a broader class of rings which contains some rings of residue classes and rings of characteristic different from 2.

All the rings considered in the paper are commutative (i.e. satisfying the identity $x \cdot y = y \cdot x$) and unitary (i.e. having an element 1 with $x \cdot 1 = x$).

Let $p$ be a given natural number and $R = (R; +, 0, 1)$ a ring. Let us agree in the following notation:

- $x' = 1 + x$;
- $x^* = 1 - x$;
- $x \land y = x \cdot y$;
- $x \lor y = x + y + x^p \cdot y^p$.

The induced algebra $\mathcal{L}(R) = (R; \lor, \land, ', *, 0, 1)$ will be referred to as a lattice-like structure induced by $R$ and the term operation

- $x \oplus y = (x \land y') \lor (x^* \land y)$

as a difference. We will not use the name symmetric difference because $x \oplus y$ need not be equal to $y \oplus x$ in general. However, if $R$ is recovered by the induced lattice-like structure, i.e. $x + y = x \oplus y$, then $x \oplus y = y \oplus x$, and hence it is symmetric.

In contrast to [5], we are not interested in the properties of the induced lattice-like structure $\mathcal{L}(R)$ but only in the case when $R$ can be recovered from $\mathcal{L}(R)$ by means of the difference $\oplus$ (since the second operation “$\land$” coincides with “$\land$” of $\mathcal{L}(R)$). In other words, we search for rings where $x + y = x \oplus y$. To show that this is possible also for rings which are not Boolean, let us give the following.

**Example 1** Let $R = \{0, 1, 2, 3\}, +, \cdot$ be a ring whose operations are determined by the tables

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

| $\cdot$ | 0 | 1 | 2 | 3 |
|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 2 | 0 | 2 | 2 |
| 3 | 0 | 3 | 2 | 1 |
The rings which can be recovered by means of the difference

It is immediate that $\mathcal{R}$ is commutative, unitary and of characteristic $2$. It satisfies the identity $x^4 = x^2$ since $0^4 = 0 = 0^2$, $1^4 = 1 = 1^2$, $2^4 = 0 = 2^2$ and $3^4 = 1 = 3^2$. Moreover, due to the foregoing definitions,

$$x \oplus y = (x \land y') \lor (x' \land y) = x + y$$

but $\mathcal{R}$ is not Boolean, because e.g. $2^2 = 0 \neq 2$. Let us note that this ring $\mathcal{R}$ is isomorphic to the polynomial ring $\mathbb{Z}_4[x]/(x^2)$, where $(x^2)$ is the principal ideal of $\mathbb{Z}_2[x]$ generated by $x^2$.

Now, we are focused on the rings of residue classes $\mathbb{Z}_p$.

**Theorem 2** Let $\mathbb{Z}_p$ be the ring of residue classes modulo $p$ with $p = 2^k$ for some $k \in \mathbb{N}$. Then $x + y = x \oplus y$, i.e. $\mathbb{Z}_p$ can be recovered from the induced lattice-like structure.

**Proof** Since $x' = 1 + x$, $x^* = 1 - x$, $x \land y = x \cdot y$ and $x \lor y = x + y + x^p \cdot y^p$, we get

$$x \oplus y = (x \land y') \lor (x' \land y) = x \cdot (1 + y) + (1 - x) \cdot y + x^p \cdot (1 + y)^p \cdot (1 - x)^p \cdot y^p$$

$$= x + x \cdot y + y - x \cdot y + (x^p \cdot (1 - x)^p) \cdot (y^p \cdot (1 + y)^p)$$

$$= x + y + (x \cdot (1 - x))^p \cdot (y \cdot (1 + y))^p$$

However, for every $y \in \mathbb{Z}_p$ we have that $y \cdot (1 + y)$ is an even number (mod $p$), e.g. $y \cdot (1 + y) = 2a$. Since $p = 2^k$, we have $2^k \equiv 0 \mod p$. Thus

$$(y \cdot (1 + y))^p = (2a)^p = 2^p \cdot a^p = 2^k \cdot 2^{2^k - k} \cdot a^p \equiv 0 \cdot 2^{2^k - k} \cdot a^p \equiv 0 \mod p$$

where we used the fact that $k < 2^k$ for every $k \in \mathbb{N}$. Hence

$$(x \cdot (1 - x))^p \cdot (y \cdot (1 + y))^p = 0$$

for every $x, y \in \mathbb{Z}_p$ which implies $x + y = x \oplus y$.

If $p \neq 2^k$ for some $k \in \mathbb{N}$, then the addition in $\mathbb{Z}_p$ need not be equal to the difference, see the following.

**Example 3** Consider the ring $\mathbb{Z}_3$ of residue classes modulo 3. For $x = 2$ we have $(x \cdot (1 - x))^3 = (2 \cdot 2)^3 = 1^3 = 1$ and for $y = 1$ we have $(y \cdot (1 + y))^3 = (1 \cdot 2)^3 = 2^3 = 2$. Together we get $(x \cdot (1 - x))^p \cdot (y \cdot (1 + y))^p = 1 \cdot 2 = 2 \neq 0$.

The result of Example 3 can be extended for each ring of an odd characteristic.

**Theorem 4** Let $p$ be an odd natural number and $\mathcal{R} = (\mathbb{R}; +, \cdot, 0, 1)$ a ring of characteristic $p$. Then $x \oplus y \neq x + y$. 
Proof Assume that \( p \) is an odd natural number and let \( \text{char}(\mathcal{R}) = p \). Take \( x = -1 \) and \( y = 1 \). Since \( p \) is odd, we have \(-1 \neq 1\). Then for 
\[
x \oplus y = x + y + (x \cdot (1 - x))^p \cdot (y \cdot (1 + y))^p
\]
we have \((x \cdot (1 - x))^p \cdot (y \cdot (1 + y))^p = -4^p \neq 0\), thus \( x \oplus y \neq x + y \).

On the contrary, if the characteristic of \( \mathcal{R} \) is equal to 2, then we can easily characterize rings for which \( x \oplus y = x + y \).

Remark 5 Let us note that if \( \mathcal{R} \) is of characteristic 2, then
\[
x' = 1 - x = x^2,
\]
thus \( \oplus \) is defined formally in the same way as for Boolean rings.

Theorem 6 Let \( p = 2^k \) for some \( k \in \mathbb{N} \) and \( \mathcal{R} = (\mathcal{R}; +, \cdot, 0, 1) \) be a ring of characteristic 2. Then \( x \oplus y = x + y \) if and only if \( \mathcal{R} \) satisfies the identity
\[
(x^{2^p} + x^p)(y^{2^p} + y^p) = 0.
\]

Proof Since \( \text{char}(\mathcal{R}) = 2 \), we get \(-x = x\) for each \( x \in \mathcal{R} \). Thus
\[
x \oplus y = x + y + (x \cdot (1 + x))^p \cdot (y \cdot (1 + y))^p.
\]
Moreover, \( p = 2^k \), which implies \((1 + x)^p = 1 + x^p\). Altogether, \( x \oplus y = x + y \) if and only if
\[
x^p(1 + x^p)y^p(1 + y^p) = 0
\]
in \( \mathcal{R} \) which is if and only if \((x^{2^p} + x^p)(y^{2^p} + y^p) = 0\) in \( \mathcal{R} \).

Remark 7 If \( \mathcal{R} = (\mathcal{R}; +, \cdot, 0, 1) \) is of characteristic 2 and \( p = 2^k \), then the identity
\[
x^p(1 + x)^p = x^{2^p} + x^p = 0,
\]
i.e. \( x^{2^p} = x^p \), yields the identity of Theorem 6. It is a question if the identity of Theorem 6 can be replaced by this simpler one. The following example shows that this is not possible.

Example 8 Let \( \mathcal{R} = (\{0, 1, \ldots, 31\}, +, \cdot) \) be a ring whose operations are determined by the tables 1 and 2. This ring is of characteristic 2, clearly, it is not Boolean, moreover, it satisfies the identity
\[
(x^8 + x^4)(y^8 + y^4) = 0,
\]
but \( x^8 = x^4 \) does not hold in \( \mathcal{R} \) because e.g. \( 2^8 = 0 \neq 16 = 2^4 \).
The rings which can be recovered by means of the difference

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

Table 1
The rings which can be recovered by means of the difference

References


