ON AUTOMORPHISM GROUPS OF NON-ASSOCIATIVE
BOOLEAN RINGS

Sin-Min Lee

Abstract. The present paper is concerned with the study of Aut \( (B(n)) \) the automorphism group of a non-associative Boolean rings \( B(n) \), where \( (B(n), +) \) is a free 2-group on \( n \) generators \( \{x_i\} \ i = 1, \ldots, n \), subject with \( X_i \circ X_j = X_i + X_j \) for \( i \neq j \). It is shown that for \( n \) even, \( Aut \ (B(n)) = S_{n+1} \) and for \( n \) odd, \( Aut \ (B(n)) = S_n \). An example of a non-associative Boolean ring \( R \) of order 8 is provided which shows that in general \( Aut \ (R) \) is not a symmetric group.

1. Introduction. All rings considered below will be assumed non-associative. A ring \( (R; +, 0) \) is said to be Boolean if \( x \circ x = x \) for all \( x \) in \( R \). A Boolean ring is always commutative and of characteristic two ([1], [3]).

If \( Aut \ (R) \) is the group of automorphisms of a Boolean associative ring, it is well known that [2, p. 60] \( Aut \ (R) \) always either infinite, or else it is isomorphic to a symmetric group. However, for non-associative finite Boolean rings, the automorphism groups need not be symmetric.

We exhibit a Boolean ring of order 8 whose automorphism group has 21 elements in section 2.

In general, it is difficult to determine the structure of the automorphism groups of a ring. We confine our attention on a special class of Boolean rings \( B(n) \) which were introduced in [4]. The additive group of \( B(n) \) is a free 2-group generated by \( \{x_1, \ldots, x_n\} \) and multiplication subject to the following properties:

\[
x_i \circ x_j = \begin{cases} x_i, & \text{if } i = j \\ x_i + x_j, & \text{otherwise} \end{cases}
\]

The Boolean ring \( B(n) \) is simple if \( n \) is even. For \( n \) is odd, \( B(n) \) is subdirectly irreducible whose lattice ideals is isomorphic to a 3-element chain [4].

We show that \( Aut \ (B(n)) \) is isomorphic to the symmetric group \( S_n \) of \( n \) symbols if \( n \) is odd and \( Aut \ (B(n)) = S_{n+1} \), if \( n \) is even.

AMS Subject Classification (1980): Primary 17A36
2. A Boolean ring \( R \) whose \( \text{Aut}(R) \) is non-symmetric. Let \( R = \text{GF}(2^9) \) be the Galois field of order 8. Assume \( x = 001, y = 010, z = 100, x + z = 101, x + y + z = 111, x + y = 011, y + z = 110 \). Let \( y \) be the primitive element of \( \text{GF}(2^9) \); then for any \( a \in \text{GF}(2^9) \setminus \{0\} \) there exist a unique integer \( t \) with \( 0 \leq t \leq 6 \) such that \( a = y^t \). We define \( \text{ind}(a) = t \). Thus we assume

<table>
<thead>
<tr>
<th>( a )</th>
<th>( x )</th>
<th>( y )</th>
<th>( z )</th>
<th>( x + y )</th>
<th>( x + z )</th>
<th>( x + y + z )</th>
<th>( y + z )</th>
<th>( x + y + z )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( x )</td>
<td>( x )</td>
<td>( x + y + z )</td>
<td>( y )</td>
<td>( y + z )</td>
<td>( x + y )</td>
<td>( x + z )</td>
<td>( z )</td>
<td>( x + y + z )</td>
</tr>
<tr>
<td>( y )</td>
<td>( y )</td>
<td>( x + y )</td>
<td>( x + z )</td>
<td>( z )</td>
<td>( y + z )</td>
<td>( x )</td>
<td>( y )</td>
<td>0</td>
</tr>
<tr>
<td>( z )</td>
<td>( z )</td>
<td>( x + y )</td>
<td>( y + z )</td>
<td>( x + y + z )</td>
<td>( z )</td>
<td>( y )</td>
<td>( x )</td>
<td>( x + y + z )</td>
</tr>
<tr>
<td>( x + y )</td>
<td>( x + y )</td>
<td>( x + y + z )</td>
<td>( z )</td>
<td>( y )</td>
<td>( x )</td>
<td>( y )</td>
<td>( x + z )</td>
<td>( x + y + z )</td>
</tr>
<tr>
<td>( x + z )</td>
<td>( x + z )</td>
<td>( y + z )</td>
<td>( x + y )</td>
<td>( x )</td>
<td>( y )</td>
<td>( x + y + z )</td>
<td>( x + y )</td>
<td>( x + y + z )</td>
</tr>
<tr>
<td>( y + z )</td>
<td>( y + z )</td>
<td>( y + z )</td>
<td>( y + z )</td>
<td>( y + z )</td>
<td>( y + z )</td>
<td>( x + y )</td>
<td>( x + y + z )</td>
<td>( x + y + z )</td>
</tr>
<tr>
<td>( x + y + z )</td>
<td>( x + y + z )</td>
<td>( x + y + z )</td>
<td>( x + y + z )</td>
<td>( x + y + z )</td>
<td>( x + y + z )</td>
<td>( x + y + z )</td>
<td>( x + y + z )</td>
<td>( x + y + z )</td>
</tr>
</tbody>
</table>

With the relation \( \text{ind}(a \circ b) \equiv \text{ind}(a) + \text{ind}(b) \) (mod 7). We can reconstruct the multiplication table for the Galois field \( \langle \text{GF}(8); +, 0 \rangle \) [5, pp. 541-546].

Now we define a binary operation \( *: \text{GF}(8) \times \text{GF}(8) \rightarrow \text{GF}(8) \) as follows: \( a \circ b = a^4 \circ b^4 \).

We observe that \(*\) is distributive with respect to \( + \) and \( a^6 a = a \) for all \( a \) in \( \text{GF}(8) \). Thus \( \langle R; +, * \rangle \) is a non-associative Boolean ring. Its multiplication table is given as follows:

The automorphism group \( \text{Aut}(\langle R; +, * \rangle) \) contains the Galois group of \( \text{GF}(8) \) over \( \text{GF}(2) \) as a subgroup.

If we represent the elements of \( R \) by the following numbers:

\[
\begin{array}{cccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
\end{array}
\]

then an automorphism \( \varphi \) of \( R \) is simply represented by \( (\varphi(1) \varphi(2) \varphi(3) \ldots \varphi(7)) \) for \( 0 \) is always fixed by the automorphism.

The automorphism group \( \text{Aut}(\langle R; +, * \rangle) \) contains the following elements:

\[
\begin{align*}
(1) & \quad (1234567) \quad (2) \quad (1375642) \quad (3) \quad (1726453) \\
(4) & \quad (2431675) \quad (5) \quad (2356714) \quad (6) \quad (2547163) \\
(7) & \quad (3652147) \quad (8) \quad (3571426) \quad (9) \quad (3764215) \\
(10) & \quad (4132756) \quad (11) \quad (4615273) \quad (12) \quad (4367521) \\
(13) & \quad (5416327) \quad (14) \quad (5173264) \quad (15) \quad (5742631) \\
(16) & \quad (6127345) \quad (17) \quad (6514732) \quad (18) \quad (6253471) \\
(19) & \quad (7245316) \quad (20) \quad (7621534) \quad (21) \quad (7463152)
\end{align*}
\]
3. Automorphism Group of $B(n)$. For $n = 1$, $B(1)$ is essentially the Galois field $GF(2)$, whose automorphism group is trivial. Hence we assume $n \geq 2$, and we have the following

**Theorem 1.** The automorphism group of $B(n)$ is

1. the symmetric group $S_{n+1}$, if $n$ is even
2. the symmetric group $S_n$, if $n$ is odd.

Let $X = \{X_1, X_2, \ldots, X_n\}$ be the set of generators of $B(n)$. For $A \subseteq X$ with at least two elements we denote by $A^+$ the element $\sum_{x_i \in A} x_i$ in the free 2-group $F_2(X)$ generated by $X$.

If $0 \neq u \in F_2(X)$, then we let $S(u)$ be the set of all elements of $X$ which are summands in $u$.

We denote by $\|u\|$ the cardinal number of $S(u)$.

For a ring $R$, we denote its set of non zero-divisors by $T(R)$.

**Lemma 1.** For every $x \in X$ and $u \in B(n)$, we have

1. $x \circ u = u$ if $x \in S(u)$ and $\|u\|$ is odd or $x \notin S(u)$ and $\|u\|$ is even
2. $x \circ u = x + u$ if $x \in S(u)$ and $\|u\|$ is even or $x \notin S(u)$ and $\|u\|$ is odd.

**Proof.** Trivial. □

From Lemma 1, we conclude that $X \subseteq T(B(n))$.

**Lemma 2.** If $n$ is even then $X^+$ is not a zero-divisor in $B(n)$.

**Proof.** Let $u \in B(n)$ such that $1 < \|u\| < n$. By Lemma 1, if $\|u\|$ is even then $u \circ X^+ = u$. If $\|u\|$ is odd then $D = X \mathbb{Z}(u)$ is non-empty and $u \circ X^+ = C^+$. Therefore $X^+ \in T(B(n))$. □

**Remark.** If $n$ is odd then $X^+ \in T(B(n))$. In fact, $X^+ \circ u = 0$ for any $u$ such that $\|u\|$ is even.

**Lemma 3.** If $u \in B(n)$ and $1 < \|u\| < n$ then $u$ is a zero-divisor.

**Proof.** If $\|u\|$ is odd then $\|u\| \geq 3$. Pick $X_i, X_j$ in $S(u)$. We see that $(X_i + X_j) \circ u = 0$.

If $\|u\|$ is even then pick $X_k \in X \mathbb{Z}(u)$; we see that $u \circ (u + X_k) = u + u \circ X_k = u + u = 0$. Thus $u \notin T(B(n))$.

By virtue of Lemma 1, 2 and 3 we have

**Theorem 2.** The set of non-zero-divisors of $B(n)$ is

$$T(B(n)) = \begin{cases} X \cup \{X^+\} & \text{if } n \text{ is even} \\ X, & \text{if } n \text{ is odd} \end{cases}$$
Let $R$ be a ring and $f$ be an automorphism of $R$. If $\{X_1, \ldots, X_n\}$ is a generating set for $R$ then $f$ is completely determined by the values of $f(X_i)$, $1 \leq i \leq n$.

For any automorphism $f$ of $R$ and $u \in T(R)$ we have $f(u) \in T(R)$ since a one-to-one mapping of a finite set into itself is onto. Therefore we have $f(T(R)) = T(R)$.

Hence if $n$ is odd, by Theorem 2, we have for each $f$ in $\text{Aut}(B(n))$, $f(X) = f(T(B(n))) = T(B(n)) = X$. Thus $\text{Aut}(B(n)) \cong S_n$.

If $n$ is even then with the aid of Lemma 1 we see that every 1-1 mapping from $T(B(n))$ onto $T(B(n))$ induces an automorphism of $B(n)$. Conversely, every automorphism of $B(n)$ is an extension of some permutation of $T(B(n))$. Therefore $\text{Aut}(B(n)) \cong S_{n+1}$.

Acknowledgment. The author warmly thanks Professor Robert Gilman for pointing out a substantial simplification of the original argument and the referee for his helpful suggestions.

REFERENCES


Dept. of Maths. and Computer Science (Received 07 05 1986)
San Jose State University (Revised 24 12 1986)
San Jose, California 95192
U. S. A.