PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 41 (55), 1987, pp. 49–52

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 $\langle B(n), +\rangle$ is a free 2-group on n generators $\{x_i\}$ $i = 1, \dots, n$, 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 $\langle R; +, 0\rangle$ 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 ([l], [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 automorhism group 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 $\{x_1, \dots, x_n\}$ and multiplication subject to the following properties:

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

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 simbols 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 Aut (R) is non-symmetric. Let $R = GF(2^3)$ 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 $GF(2^3)$; then for any $a \in GF(2^3) \setminus \{0\}$ there exist a unique integer t with $0 \leq t \leq 6$ such that $a = y^t$. We define $\operatorname{ind}(a) = t$. Thus we assume

a	x	y	z	$x+z$	$x+y+z$	$x+y$	$x+z$
$\operatorname{ind}(a)$	0	1	2	3	4	5	6

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

Now we define a binary operation $*$: $GF(8) \times GF(8) \to GF(8)$ as follows: $a * b = a^4 \circ b^4$.

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

$*$	0	x	y	z	$x+y$	$x+z$	$y+z$	$x+y+z$
0	0	0	0	0	0	0	0	0
x		x	$x+y+z$	y	$y+z$	$x+y$	$x+z$	z
y			y	$x+y$	$x+z$	z	x	$y+z$
z				z	x	$y+z$	$x+y+z$	$x+z$
$x+y$					$x+y$	$x+y+z$	z	y
$x+z$						$x+z$	y	x
$y+z$							$y+z$	$x+y$
$x+y+z$								$x+y+z$

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

If we represent the elements of R by the following numbers:

0	x	y	z	$x+z$	$x+z$	$y+z$	$x+y+z$
0	1	2	3	4	5	6	7

then an automorphism φ 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 $\operatorname{Aut}(\langle R; +, *\rangle)$ contains the following elements:

(1) (1 2 3 4 5 6 7)	(2) (1 3 7 5 6 4 2)	(3) (1 7 2 6 4 5 3)
(4) (2 4 3 1 6 7 5)	(5) (2 3 5 6 7 1 4)	(6) (2 5 4 7 1 6 3)
(7) (3 6 5 2 1 4 7)	(8) (3 5 7 1 4 2 6)	(9) (3 7 6 4 2 1 5)
(10) (4 1 3 2 7 5 6)	(11) (4 6 1 5 2 7 3)	(12) (4 3 6 7 5 2 1)
(13) (5 4 1 6 3 2 7)	(14) (5 1 7 3 2 6 4)	(15) (5 7 4 2 6 3 1)
(16) (6 1 2 7 3 4 5)	(17) (6 5 1 4 7 3 2)	(18) (6 2 5 3 4 7 1)
(19) (7 2 4 5 3 1 6)	(20) (7 6 2 1 5 3 4)	(21) (7 4 6 3 1 5 2)

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 $D = X\S(u)$ is non-empty and $u \circ X^+ = C^+$. Therefore $X^+ \in T(B(n))$. □

Remark. If n is odd then $X^+ \in T(B))$. 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 $X_k \in X\S(u)$; we see that $u \circ (u + X_k) = u + u \circ X_k ==$ $u + u \circ X_k = u + u = 0$. 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*

$$T(B(n)) = \begin{cases} X \cup \{X^+\} & \textit{if } n \textit{ is even} \\ X, & \textit{if } n \textit{ is odd.} \end{cases}$$

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 $\mathrm{Aut}\,(B(n))$, $f(X) = f(T(B(n))) = T(B(n)) = X$. Thus $\mathrm{Aut}\, B(n) \cong S_n$.

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 $\mathrm{Aut}\,(B(n)) \cong S_{n+1}$.

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

[1] G. Birkoff and G.D. Birkhoff, *Distributive postulates for systems like Boolean algebras*, Trans. Amer. Math. Soc. **60**(1946), 3–11. g

[2] B. Jonson, *Topics in Universal Algebra*, Lecture Notes in Maths. No. 250, Springer-Verlag, New York, 1972.

[3] Sin-Min Lee, *A construction of simple non-associative Boolean rings*, Bull. Malaysian Math. Soc. **7**(1984), 35–37.

[4] Sin-Min Lee, *A construction of a class of simple nonassociative Boolean rings*, Abstracts Amer. Math. Soc., Vol. 4, No. 6, Oct. 1983, 83T–17–394.

[5] R. Lidl and H. Neidereiter, *Finite fields*, in Encyclopedia of Maths. and its Applications, Vol. 20, Addison-Wesley, Reading, Massachusets, 1983.

Dept. of Maths. and Computer Science
San Jose State University
San Jose, California 95192
U. S. A.

(Received 07 05 1986)
(Revised 24 12 1986)