ON THE BOOLEAN RINGS

By

JAU-SHYONG SHIUE* and WEN-MIN CHAO

(Received January 8, 1975)

I. Introduction. As a consequence of his theory of algebras, *N. Jacobson* ([2]) proved that if in a ring R there exists an integer $n>1$ such that for every a in R, $a^n=a$, then the ring is commutative.

R. Ayoub and *C. Ayoub* ([1]) proved the theorem in its simplest form for a certain class of exponents n without recourse to transfinite methods. Namely

Theorem A. *Let $n=p+1$, where p is a prime of the form 2^k+2^m-1. If R is an arbitrary ring in which $x^n=x$ for every x in R, then R is commutative.*

Theorem B. *If $n=2,3,4,5,7$, and $x^n=x$ for every x in R, then R is commutative.*

It is the object of the present note to prove that if m and q are two fixed positive integers, and

$x^{2q(m+1)}+2^m=x$ for all x in the ring R. Then R is a Boolean ring by using the elementary method.

2. Some preliminary lemmas.

Lemma 1. *If $x^k=x$ for some k in Z^+, then $x^r=x^s$ for all r, s in Z^+ with $r=s$ (mod $k-1$). In particular, x^{k-1} is an idempotent.*

Lemma 2. *Let R be a ring with the property that $x^2=0$ only if $x=0$. Then every idempotent is in the center of R.*

Proof. Let e be an idempotent of R, then for all x in R,

$$(ex-exe)^2=exex-exexe-exeex+exeexe=exex-exexe-exex+exexe=0$$

$$(xe-exe)^2=xexe-xeexe-exeexe+exeex=xexe-xexe-exexe+exexe=0\ .$$

Hence $ex=exe=xe$.

Lemma 3. *Let R be a ring such that for each x in R there is a positive*

---

* This paper was written while the first Author was an Alexander von Humboldt-Stiftung fellow visting the University of Köln and supported in part by the National Science Council, Taiwan, Republic of China.

The authors would like to thank Professor M. Orihara for his contribution to simplify Proposition 4.

integer k (dependent on x) with $x^k=x$, then R has the property that $x^2=0$ only for $x=0$.

Proof. If x is an element with $x^2=0$, then $x^{2(k-1)+1}=(x^2)^{k-1}x=0$. But $x^{2(k-1)+1}=(x^{k-1})^2x$ (by Lemma 1)

$=x.$

Hence $x=0$.

In particular, if k is a fixed positive integer such that $x^k=x$, for all x in the ring R, then x^{k-1} is a central idempotent (an idempotent in the center).

Lemma 4. *Let k be a fixed positive even integer and $x^k=x$ for all x in the ring R, then $2x=0$ for all x in R.*

Proof. $-x=(-x)^k=x^k=x$, hence $2x=0$ for all x in R.

3. The main results. Now let m and n be two positive integers with $n>m$. Let $k=2^n+2^m$.

Proposition 1. *Let R be a ring such that $x^{2^n+2^m}=x$ for all x in R. Then $x^{2^m+1}=x$ for all x in R.*

Proof. For x in R, we have

$$x+x^2=(x+x^2)^{2^n+2^m}=(x+x^2)^{2^n}(x+x^2)^{2^m}=(x^{2^n}+x^{2^{n+1}})(x^{2^m}+x^{2^{m+1}})$$

(by Lemma 4)

$$=x^{2^n+2^m}+x^{2^{n+1}+2^m}+x^{2^n+2^{m+1}}+x^{2(2^n+2^m)}$$
$$=x+x^{2^n+1}+x^{2^m+1}+x^2\ ,$$

hence we have,

$$x^{2^n+1}=x^{2^m+1},\quad\text{and}\quad x^{2^m+1}=x^{2^n+2^m}=x\ .$$

By proposition 1, we have the following result.

Proposition 2. *Let n be a positive integer and R be a ring such that $x^{2^{n+1}+2^n}=x$ for all x in R, then R is a Boolean ring.*

Proof. By proposition 1, and its proof, we have

$x^{2^n+1}=x$ and $x^{2^{n+1}+1}=x^{2^n+1}$ for all x in R. Hence,

$$x^2=x^{2^{n+1}+1}=x^{2^n+1},\ \text{and}\ x^{2^n+1}=x^2x^{2^n-1}=x^{2^n+1}x^{2^n-1}=x^{2^n+1}=x$$

for all x in R, then $x^2=x$, i.e. R is a Boolean ring.

Now we consider the case in Proposition 1 with $n>m$ and n is a multiple of $m+1$, i.e. there is a positive integer q such that $n=q(m+1)$. Then

$2^n-2^{m+1}=2^{q(m+1)}-2^{m+1}=0 \pmod{2^{m+1}-1}$. Since $x^{2^{m+1}}=x$ for all x in R, by Proposition 1, we have $x^{2^n+2^m}=x^{2^{m+1}+2^m}$, hence for all x in R, $x^{2^{m+1}+2}=x$, by Proposition 2, we conclude that R is a Boolean ring. This proves the following proposition:

Proposition 3. *Let m and q be two fixed positive integers and $x^{2^{q(m+1)}+2^m}=x$ for all x in the ring R. Then R is a Boolean ring.*

In general, if $n=q(m+1)+r$, where q and r are two positive integers with $o<r<m+1$. Then we have

$$2^n-2^{m+1+r}=2^r(2^{q(m+1)}-2^{m+1})\equiv 0 \pmod{2^{m+1}-1}\ ,$$

and then, $x^{2^n}=x^{2^{m+1+r}}$. Hence $x^{2^n+2^m}=x^{2^{m+1+r}+2^m}$ for all x in R. Now

Proposition 4. *Let m, q, r be fixed positive integers with $r<m+1$ and R be a ring such that $x^{2^{q(m+1)+r}+2^m}=x$ for all x in R, then $x^{2^{r+1}}=x$ for all x in R.*

Proof. By Proposition 1 we have $x^{2^{m+1}}=x$ for all x in R. Hence $x^{2^r}=(x^{2^{m+1}})^{2^r}=x^{2^{m+1+r}}$. Therefore we obtain

$$x^{2^r+2^m}=x^{2^{m+1+r}+2^m}$$
$$=x^{2^{q(m+1)+r}+2^m} \text{ (by the proof of Proposition 3.)}$$
$$=x, \text{ for all } x \text{ in } R. \text{ By Proposition 1, we have}$$

$x^{2^{r+1}}=x$ for all x in R. Obviously, we have the following two corollaries.

Corollary 1. *Let n be a fixed positive even integer and R be a ring such that $x^{2^n+2}=x$ for all x in R. Then R is a Boolean ring.*

Corollary 2. *Let n be a fixed positive odd integer and R be a ring such that $x^{2^n+2}=x$ for all x in R. Then $x^4=x$ for all x in R and hence R is commutative.*

The commutativity of R in Corollary 2 is a consequence of Jacobson's theorem ([2]), but we can give a simple proof as follow (also refer to *R. Ayoub* and *C. Ayoub*): Since by Lemma 4, $x+x^2=(x+x^2)^2$, $x+x^2$ is a central idempotent. If x and y are two elements of R, both $x+y+(x+y)^2$ and $x+y+x^2+y^2$ are in the center of R, hence $xy+yx$ is in the center of R. In particlular, $x(xy+yx)=(xy+yx)x$ implies $x^2y=yx^2$, i.e. x^2 is in the center of R for x in R. therefore, x is in the center of R for all x in R, R is commutative. The following example proves that there is a ring satisfying $x^4=x$ for all x but it is not a Boolean ring:

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

In general, for each positive integer n, there is a ring R such that $x^{2^{n+1}}=x$ for all x in R and there is an a in R such that $a^k \neq a$ for all $1<k<2^{n+1}$.

Let Z_2 be the field of integers modulo 2, $Z_2[t]$ be the ring of all polynomials of t over Z_2. For each positive integer n there is a polynomial $f(t)$ which is irreducible over Z_2 and its degree is n. Let R be the quotient ring of $Z_2[t]$ over the ideal $(f(t))$, then R contains exactly 2^{n+1} elements, since $f(t)$ is irreducible over Z_2, R is in fact a field. Hence $x^k=x$ contains at most k distinct solutions for each $1<k<2^{n+1}$. Furthermore, for each nonzero element x in R, we have $x^{2^{n+1}-1}=1$, and there is an a in R such that $a^k \neq 1$ for all $1 \leq k<2^{n+1}-1$ (the multiplicative group of a field is cyclic). Hence $a^{2^{n+1}}=a$ and $a^k \neq a$ for all $1 \leq k<2^{n+1}$.

Proposition 5. *For each positive integer n there is a ring R such that* $x^{2^{m+1}}=x$ *for all x in R and there is an a in R such that* $a^k \neq a$ *for all* $1 \leq k<2^{n+1}$.

REFERENCES

[1] R. Ayoub and C. Ayoub, *On the commutativity of rings.* The American Mathematical Monthly, 71 (1964) 267-271.

[2] N. Jacobson, *Structure theory for algebraic algebras of bounded degree.* Annals of Math., 46(1945) 695-707.

Department of Mathematical Sciences
National Chengchi University
Taipei, Taiwan
Rep. of China

Department of Mathematics
University of Chicago
Chicago, Illinois
U.S.A.