On Structure of a P-ring

이를 教育學碩士學位 論文으로 提出함

濟州大學校教育大學院數學教育專攻

提 出 者 高 希 姉

指導教授 宋 錫 準

1986 年 6 月 日

高希姊의 碩士學位 論文을 認准함

濟 州 大 學 校 教 育 大 學 院

主審 ㊞

副審 ㊞

副審 ㊞

1986 年 6 月 日

감 사 의 글

이 논문이 완성되기 까지 바쁘신 가운데도 자상하고 친절하게 지도를 하여 주신 송석준 교수님께 감사드리며, 아울러 그동안 많은 도움을 주신 수학과 여러 교수님들께 감사드립니다.

그리고 그동안 저에게 많은 사랑과 격려를 주신 가족, 친지 및 주위의 여러분들께 감사를 드립니다.

1986 년 6 월 일

고 희 자

CONTENTS

Ⅰ. Introduction

Stringall [5] and Haines [3] studied the properties of P-ring and they extended the properties of Boolean ring.

This paper will be primarily concerned with a P-ring.

This P-ring is a generalization of a Boolean ring.

In this paper, we have some structural theorems for a P-ring.

That is, a P-ring becomes a reduced ring and every right ideal of a P-ring is two-sided and so on.

And we show that imbeding theorem to a P-ring with identity.

Moreover, we prove the commutativity theorem for a P-ring.

Ⅱ. Preliminaries

Let P be a prime number.

The P-ring is a ring R which satisfies the identity $x^P = x$ for arbitrary x in R.

If $P = 2$ then R is called a Boolean ring.

Stringall established that the Categories of P-rings are equivalent.

And David C. Haines established that a P-ring is an injective object in the category of a P-rings if and only if it is quasi-orthogonally complete.

In this paper, we use the following properties on ring theory.

So we state them without proofs.

Theorem 2.1. Let R be a ring with identity 1R and characteristic $n>o$.

(i) If $g: Z \to R$ is the map given by $m \mapsto m1R$,

then g is a homomorphism of rings with kernel

$\langle n \rangle = \{kn \mid k \in Z\}$.

(ii) n is the least positive integer such that $n1R = 0$.

(iii) If R is an integral domain, then n is prime.

([1], Chapter Ⅲ−1)

lemma 2.2. Let R be a division ring of characteristic $q>o$, q is a prime. Suppose that the element a in R, $a \notin$ center of R, is such that $a^{q^m} = a$ for some $m>o$.

Then there exists an $x \in R$ for which

1) $xax^{-1} \neq a$.

2) $xax^{-1} = a^k \in Z_q(a)$,

the extension field obtained by adjoining a to Z_q, for some $k \geqq 2$.

([2], chapter 9)

Theorem 2.3. (Wedderburn's Theorem)

Every finite division ring is field.

([1], chapter Ⅸ−6)

Proposition 2.4. A ring R is completely reducible if and only if it is isomorphic to a finite direct product of completely reducible simple rings.

([6], chapter 3−4)

Proposition 2.5. If F is a finite field, then F has exactly q^m elements for some prime q and $m \in Z+$.

([4], Chapter Ⅱ−1)

Proposition 2.6. Let p be a prime and $n \geqq 1$ an integer.

Then F is a finite field with p^n elements if and only if F is a splitting field of $x^{p^n} - x$ over Zp.

([1], Chapter V−5)

Proposition 2.7. The Radical of R is the set of all $r \in R$ such that $1 - rs$ is right invertible for all $s \in R$.

([6], Chapter 3−2)

Proposition 2.8. In a nonzero ring R with identity maximal(left) ideals always exist.

In fact every(left) ideal in R (except R itself) is contained in a maximal (left) ideal.

([1], Chapter Ⅲ−2)

Ⅲ. Structural theorems and Commutativity theorem for a P-ring.

In this section, ring R is a P-ring

(not necessarily with identity)

Proposition 3.1. Let R be a P-ring then R is reduced ring.

Proof. Let $x \in R$ be an element such that

$x^m = 0$ for some m.

Then $x = x^p = x^{p^k} = x^{p^k - m} \times x^m$

for some K , $P^k \geqq m$

Since $x^m = 0$, $x = 0$.

Therefore, O is the only nilpotent element.

Proposition 3.2. Every idempotent element of R must be in the center of R.

Proof. If $e = e^2 \in R$,

then for arbitrary x in R,

$(xe - exe)^2 = (xe - exe)(xe - exe)$

$= xexe - exexe - xeexe + exeexe$

$= xexe - exexe - xexe + exexe$

$= 0.$

By Similary method,

$(ex - exe)^2 = 0.$

Then

$xe - exe = 0 = ex - exe$ by proposition 3.1..

Therefore,

$$xe = exe = ex$$

Hence,

x is in the center of R.

proposition 3.3. For every x in R, x^{p-1} is an idempotent element of R.

Proof. Let $e = x^{p-1}$ then

$$e^2 = (x^{p-1})^2$$
$$= x^{2p-2}$$
$$= x^p \cdot x^{p-2}$$
$$= x \cdot x^{p-2}$$
$$= x^{p-1}$$
$$= e.$$

Proposition 3.4. Every right ideal of R is a two-sided ideal of R.

Proof. Let I be a right ideal of R.

If $a \in I$ with $a^p = a$, then

a^{p-1} is an idempotent element by proposition 3.3.

Hence a^{p-1} is in the center of R

by proposition 3.2.

Therefore,

for any r in R

$$ra = r \cdot (a^{p-1} \cdot a)$$
$$= (a^{p-1} \cdot r) \cdot a$$
$$= a(a^{p-2} \cdot r \cdot a)$$

$= ar' \in I$ where $r' = a^{p-2} \cdot r \cdot a \in R$

Hence $ra \in I$ and this shows that

I is a two-sided ideal of R.

Proposition 3.5. The homomorphic image of P-ring is also a P-ring.

Proof. Let $f: R \to R'$ be an epimorphism,

Where R is a P-ring.

For any $y \in R'$,

there exist $x \in R$ such that $f(x) = y$, since $x^p = x$

We have

$$y = f(x) = f(x^p) = f(x)^p = y^p$$

Therefore,

R' is also a P-ring.

Corollary 3.6. (1) The quotient ring of a P-ring is also a P-ring.

(2) The subring of a P-ring is also a P-ring.

Proof. By Proposition 3.5 and definition, it is trivial.

Proposition 3.7. Any P-ring R of characteristic p can be imbedded in a P-ring with identity.

Proof. Consider the catesion product $R \times Zp$,

where $R \times Zp = \{ (r, n) \mid r \in R,\ n \in Zp \}$.

If addition and multiplication are defined by

$$(a, n) + (b, m) = (a+b,\ n+m \pmod p)$$

$$(a, n)(b, m) = (ab+ma+mb,\ nm \pmod p)$$

then $R \times Zp$ forms a P-ring.

Since,

$$(a,n)^p = (a^p + 2n\,pa,\ n^p \pmod p))$$
$$= (a,n)$$

by Fermat's theorem and characteristic of R.

And this system has a multiplicative identity (0,1);

$$(a,n)(0,1) = (a0 + 1a + n0,\ n1 \pmod p))$$
$$= (a,n)$$

and similarly,

$(0,1)(a,n) = (a,n)$.

Next, consider the subring $R\times\{0\}$ of $R\times Zp$.

consisting of all pairs of the form $(a,0)$.

This subring is isomorphic to the given ring R

under the mapping $f: R \to R\times\{0\}$ defined by $f(a) = (a,0)$.

This process imbeds R into $R\times Zp$, a P-ring with identity.

Theorem 3.8. Let R be a P-ring with identity.
If R forms a division ring, then R is commutative ring and hence a field.

Proof. First, let us show that R is of characteristic $q > 0$,
where q is a prime.

If characteristic of R is 2, we have done.

If characteristic of R is not 2, let us consider any element a in R.

Since $a^p = a$ and $(2a)^p = 2a$, we have

$$2^p a^p - 2a = (2^p - 2)a$$
$$= 2(2^{p-1} - 1)a$$
$$= 0.$$

But $2a \neq 0$, we have $(2^{p-1}-1)a=0$.

Therefore,

there exists a least positive integer q such that $qa=0$, which implies that the characteristic of R is q,

where q is a prime by Theorem 2.1.

Since the center of R is a subfield of R, R contains a prime subfield Z_q of characteristic q.

Since $a^p = a$, a is algebraic over Z_q

because a polynomial

$$f(x) = x^p - x = 0$$

with its coefficients in Z_q has a as its root by proposition 2.6.

Hence the extension $Z_q(a)$ constitutes a finite field.

Since $Z_q(a)$ is a finite extension of finite field Z_q.

Say, $Z_q(a)$ has q^m elements by proposition 2.5.

In particular, $a \in Z_q(a)$, so that $a^{q^m} = a$.

If we now assume that a is not in the center of R, then all the hypothesis of Lemma 2.2 will be satisfied.

Thus there exists an element $b \in R$ and integer $k>1$ satisfying $bab^{-1} = a^k \neq a$ −(*).

Similar reasoning applied to the extension field $Zq(b)$ indicates that $b^{q^m} = b$ for some integer $m>1$.

At this point we turn our attension to the set of finite sums

$$W = \sum_{i=0}^{q^n-1} \sum_{j=0}^{q^m-1} r_{ij}\, a^i b^j \mid r_{ij} \in Z_q$$

It should be apparent that w is a finite set which is closed under addition.

Since the relation $a^k b = ba$ allows us to bring the a's and b's together in a product.

W is also closed under multiplication.

Hence W is a subring and a finite division ring by corollary 3.6.

Therefore, by Wedderburn's Theorem 2.3

we know that W is necessarily commutative.

In particular, $a, b \in W$ so that $ab = ba$

which contradict to(*) ; $bab^{-1} = a^k \neq a$.

Therefore, a must be in the center of R.

Hence R is commutative.

Proposition 3.9. Let R be a P-ring with identity.

For any a and b in R, we have $ab - ba \in \mathrm{Rad}\ R$,

where Rad R is the intersection of all maximal ideals of R.

Proof. Since R has a maximal right ideals by proposition 2.8.

We have that they are two-sided ideals by proposition 3.4.

Hence R/M is a division ring and

R/M is a P-ring by corollary 3.6(1).

Theorem 3.8 shows that

R/M is commutative and hence it is a field.

In other words, for all a,b in R,

$(a+M)(b+M) = (b+M)(a+M)$

or equivalently $ab - ba \in M$.

As this last relation holds for every maximal ideal of R, it follows that ab−ba is in Rad R.

Theorem 3.10. Let R be a P−ring with identity.

Then R is semisimple.

Proof. Suppose that the element x is in the Rad R.

Then x^{p-1} is an idempotent.

Since Rad R is an ideal, we have $x^{p-1} \in \text{Rad } R$.

In the proposition 2.7, if we have S=1, then we see that $1-x^{p-1}$ is right invertible, say $(1-x^{p-1})y=1$ where $y \in R$.

This leads to,

$$x^{p-1} = x^{p-1}(1-x^{p-1})y$$

$$= (x^{p-1} - x^{2p-2})y$$

$$= 0.$$

Then $x=0$ by proposition 3.1.

Therefore,

$$\text{Rad } R = 0.$$

Hence R is semisimple.

Theorem 3.11. Every P−ring with identity is a commutative ring.

Proof. Let $a, b \in R$ then $ab-ba \in \text{Rad } R$ by proposition 3.9.

Since Rad $R=\{0\}$ by Theorem 3.10, $ab-ba \in \{0\}$.

Therefore, $ab=ba$.

Hence R is commutative.

REFERENCES

[1] T.W. Hungerford, Algebra, Holt Rinehart and Winston, 1974.

[2] D.W. Burton, A first course in rings and ideals, Addison – Wesley Publishing Company, 1970.

[3] D.C. Haines, Injective objects in the category of P–rings, Proc. Amer. Math. Soc. 42 (1), 1974, p.57 ~ 60.

[4] E. Artin, Galois Theory, Notre Dame Math Lectures Number 2, 1971.

[5] R.W. Stringall, The categories of P–rings are equivalent, Proc. Amer. Math. Soc. 29(1971) 229–236.

[6] J. Lambek. Lectures on Rings and Modules, Chelsea Publishing Company. N.Y, 1976.

[7] H. Tominoga, and H. Komatsu, A characterization of Boolean Ring (II), Chinese J. of Math. vol 11 (4) 1983, 327–329.

(國文抄錄)

P-環의 構造에 관하여

高 希 姉

濟州大學校 敎育大學院 數學敎育轉攻

(指導敎授 宋 錫 準)

本 論文은 Boolean 環을 확장시킨 P-環에 대하여 調査하였다.

이 P-環은 Stringall 과 Haines 등에 의하여 研究되었었다.

本 論文에서는 이들의 研究를 바탕으로, Boolean 環의 性質들을 P-環으로 一般化시켰다.

특히, P-環은 semisimple이 되고 可換環이 됨을 증명하였다.

이 증명을 위한 몇가지 보조정리를 통하여 P-環의 性質들을 찾았고, 恒等元이 없는 P-環을 恒等元이 있는 P-環으로서의 확장성을 보였다.