Journal of Mathematical Research and Exposition
Vol. 10, No.2, May, 1990

Classification of Rings of Order $P^k(k>3)$ With Additive Group of Type (P^{k-1}, P)*

Zhao Siyuan

(Shanghai Normal University)

Abstract

This paper gives a complete classification of associative rings of order $p^k(k>3)$ with additive group of type (p^{k-1}, p).

I Introduction

The classification of finite associative rings was reduced to that of rings of prime power order. Throughout this paper a ring always means an associative ring (not necessarily with an identity). Let $R(n)$ be a complete set of representatives of rings of order n. The number of elements of $R(n)$ is denoted by $N(n)$[5][6]. 1964, Bloom determined $R(2^2)$[1]; 1969, Raghavendran determined $R(p^2)$[2]; In 1947, Baliieu had given a correct result for $R(p^3)$ already[3]; 1973, Gilmer and Mott published a paper on the same problem[4] and made a correction by themselves on Review after three years, but there still remained a few errors; Liu Ke qin (刘克勤) corrected these errors[5] in 1982, and listed the representatives of order p^4 with identity[6] in 1983, which is a part of $R(p^4)$. We tried to determine $R(p^4)$ two years ago. Because the additive group of rings has 5 types, the work is divided into 5 parts. The first case, i.e., the case of cyclic type is trivial. The second case to consider is the type (p^3, p). Here we generalize the problem classification of rings of order $p^k(k>3)$ with additive group of type (p^{k-1}, p). We get the following two theorems:

Theorem 1 There are exactly $k+6$ if $p>2$, or $k+5$ if $p=2$, isomorphism classes of the non-nilpotent rings of order p^k $(k>3)$ with additive group of type (p^{k-1}, p).

Theorem 2 there are exactly $(p+1)(3k-7)+8$ if $p>2$, or $4(2k-3)$ if $p=2$, isomorphism classes of the nilpotent rings of order p^k $(k>3)$ with additive group

* Received Jul. 23, 1988

of type (p^{k-1}, p).

Ⅱ Preliminary

Assume that p is a positive prime, integer $k>3$, R is a ring of order p^k, it's additive group $(R, +) = (u) + (v)$ is the direct sum of cyclic subgroups (u) and (v) of order p^{k-1} and p respectively. Regarding it as a Z-module, we may write $R = \{au + \beta v | \beta \in P, a \in P_{k-1}\}$ where $P = \{0, 1, \cdots, p-1\} (\subset \cdots \subset P_i = \{0, 1, \cdots, p^i - 1\} \subset \cdots) \subset P_{k-1} = \{0, 1, \cdots, p^{k-1} - 1\} \subset Z$. Let $A = Z/Zp^{k-1}$, $B = Zp^{k-2}/Zp^{k-1}$ ($\cong N_p$------ null product ring of order p). When $p>2$, let

$$\varepsilon = \begin{cases} -1, & \text{if } p \equiv 3 \ (4). \\ \text{the smallest nonsquare residue mod } p \text{ in } \{1, 2, \cdots, \frac{p-1}{2}\} & \text{if } p \equiv 1 \ (4). \end{cases}$$

Let $E(p) = \{x \in R | o(x) = p\} = \{\gamma p^{k-2}u + \delta v | \gamma, \delta \in p, \ (\gamma, \delta) \neq (0, 0)\}$, where $o(x)$ is the order of $x \in (R, +)$, $E(p^{k-1}) = \{x \in R | o(x) = p^{k-1}\} = \{au + \beta v | a \in P_{k-1}, \ \beta \in P, \ (a, p) = 1\}$. We have $|E(p)| = p^2 - 1$, $|E(p^{k-1})| = \phi(p^{k-1}) p = (p-1) p^{k-1}$. There are just $p^k (p-1)^2$ generating sets of $(R, +)$.

$$\{(u', v') | u' = au + \beta v, \ v' = \gamma p^{k-2} u + \delta v, a \in P_{k-1} \beta, \gamma, \delta \in P, \ (a, p) = 1 = (\delta, p)\}. \qquad (1)$$

Since px is nilpotent for all $x \in R$, $pR \subseteq \mathrm{rad}(R)$---the radical of ring R. We have $pR \stackrel{\angle}{=} (pu)$ for any $u \in E(p^{k-1})$ which is a nilpotent ideal of ring R with cyclic additive group of order p^{k-2}. And $p^{k-2}R = (p^{k-2}u) \cong N_p$ for any $u \in E(p^{k-1})$.

Let (u, v) be an arbitrary generating set of $(R, +)$. Since $pv = 0$, We have $pv^2 = puv = pvu = 0$, and so $\{uv, vu, v^2\} \subset E(p) \cup (0)$. The multiplication table of (u, v) is as follows

$$\begin{cases} u^2 = au + \tau_{11} v, & uv = \sigma_{12} p^{k-2} u + \tau_{12} v, \\ vu = \sigma_{21} p^{k-2} u + \tau_{21} v, & v^2 = \sigma_{22} p^{k-2} u + \tau_{22} v, \end{cases} \qquad (2)$$

where $a \in P_{k-1}$, $\sigma_{ij}, \tau_{ij} \in P$ are the structural constants, which obey the associative law of multiplication, that is

$$\begin{cases} \tau_{11}(\sigma_{12} - \sigma_{21}) \equiv \tau_{11}(\tau_{12} - \tau_{21}) \equiv \sigma_{22}(\tau_{12} - \tau_{21}) \equiv \tau_{22}(\tau_{12} - \tau_{21}) \equiv 0 (p) \\ \tau_{12}(\tau_{12} - a) \equiv \tau_{11}\tau_{22} \equiv \tau_{21}(\tau_{21} - a)(p), \sigma_{21}(\tau_{12} - a) \equiv \sigma_{12}(\tau_{21} - a)(p), \\ \tau_{22}\sigma_{12} \equiv \sigma_{22}(\tau_{12} - a)(p), \ \tau_{22}\sigma_{21} \equiv \sigma_{22}(\tau_{21} - a)(p), \\ \sigma_{12}\tau_{12} \equiv \tau_{11}\sigma_{22} \equiv \sigma_{21}\tau_{21} (p). \end{cases} \qquad (3)$$

Ⅲ Non-nilpotent Case

Let $N = \mathrm{rad}(R)$, $\bar{R} = R/N$. Since $R \supseteq N = \mathrm{rad}(R) \supseteq pR$, we have $p^{k-2} = |pR| \leqslant |N| \leqslant p^k$. Hence $|N| \in \{p^{k-2}, p^{k-1}, p^k\}$. If $|N| = p^k$, then $R = N$ is nilpotent. We first consider the other two cases in which R is non-nilpotent.

Ⅰ. $|N| = p^{k-2}$ case. $N = pR$ and semi-simple $\bar{R} \cong F_{p^2}$ or $F_p \oplus F_p$, where F_q denote a field with q elements. It is easy to prove that $\bar{R} \not\cong F_{p^2}$, thus, $F_p \oplus F_p \cong \bar{R} = (\bar{u}) \oplus (\bar{v})$, where $\bar{u}\bar{v} = \bar{v}\bar{u} = 0$, $\bar{u}^2 = \bar{u} = u + N$, $\bar{v}^2 = \bar{v} = v + N$, $v \in E(p)$, $u \in E(p^{k-1})$, $(pu) = pR = N$,

$R=(u)+(v)$. Now (2) is

$$\begin{cases} u^2=(1+\beta p)u, & uv=\sigma_{12}p^{k-2}u, \\ vu=\sigma_{21}p^{k-2}u, & v^2=\sigma_{22}p^{k-2}u+v \end{cases} \quad (\beta\in P_{k-2},\ \sigma_{ij}\in P) \qquad (2')$$

It follows from (3) that $\sigma_{12}=\sigma_{21}=-\sigma_{22}$. Let

$$a=1-\beta p+(\beta p)^2-\cdots+(-1)^{k-2}(\beta p)^{k-2}, \qquad (4)$$

then $a(1+\beta p)=1+(\beta p)^{k-1}\equiv 1\ (p^{k-1})$. Under the transformation: $u'=au$, $v'=-\sigma_{12}p^{k-2}u+v$, $(2')$ becomes: $(u')^2=u'$, $u'v'=v'u'=0$, $(v')^2=v'$, and so $R=(u')\oplus(v')\cong A\oplus F_p$.

II. $|N|=p^{k-1}$ case. $R\supsetneq N\supsetneq pR$, $\overline{R}\cong F_p$. There are two possibilities:

1°. $N\cap E(p^{k-1})\neq\phi$. Thus $N=(u)$, $u\in E(p^{k-1})$, $R=(u)+(v)$, $v\in E(p)-(u)$, $\overline{R}=R/(u)=(\overline{v})\cong F_p, \overline{v}^2=\overline{v}=v+N=v+(u)$. Now (2) becomes

$$\begin{cases} u^2=p^lu,\ l\in\{1,2,\cdots,k-1\}, & uv=\sigma_{12}p^{k-2}u, \\ vu=\sigma_{21}p^{k-2}u, & v^2=\sigma_{22}p^{k-2}u+v\ . \end{cases} \quad (\sigma_{ij}\in p) \qquad (2'')$$

It follows from (3) that $\sigma_{12}=\sigma_{21}=0$, We may assume $\sigma_{22}=0$, by replacing v with $v+\sigma_{22}p^{k-2}u$ if necessary. Now $(2'')$ is

$u^2=p^lu$, $l\in\{1,2,\cdots,k-1\}$, $uv=vu=0$, $v^2=v$, we get $k-1$ new representatives: $R=(u)\oplus(v)\cong(Zp^l/Zp^{k-l+1})\oplus F_p$, $l=1,2,\cdots,k-1$.

2°. $N\cap E(p^{k-1})=\phi$. Now $N\supsetneq pR=(pu)$, $u\in E(p^{k-1})$. Hence there exists $v\in E(p)$ such that $N=(pu)+(v)$, $R=(u)+(v)$, $\overline{R}=(\overline{u})\cong F_p$, $\overline{u}^2=\overline{u}=u+N$.Since v is nilpothet, we have $\tau_{22}=0$ in (2), and $u^2=\tau_{11}v+(1+\beta p)u$. Now (3) is

$$\begin{cases} \tau_{11}(\sigma_{12}-\sigma_{21})\equiv 0\equiv\tau_{11}(\tau_{12}-\tau_{21})\ (p), & \sigma_{22}(\tau_{12}-1)\equiv 0\equiv\sigma_{22}(\tau_{21}-1)\ (p), \\ \tau_{12}(\tau_{12}-1)\equiv 0\equiv\tau_{21}(\tau_{21}-1)\ (p), & \sigma_{12}(\tau_{21}-1)\equiv\sigma_{21}(\tau_{12}-1)\ (p), \\ \sigma_{12}\tau_{12}\equiv\tau_{11}\sigma_{22}\equiv\sigma_{21}\tau_{21}\ (p)\ . \end{cases} \qquad (5)$$

1) If $\tau_{11}=0$, then (5) becomes

$$\begin{cases} \sigma_{12}\tau_{12}\equiv 0\equiv\sigma_{21}\tau_{21}\ (p), & \tau_{12}(\tau_{12}-1)\equiv 0\equiv\tau_{21}(\tau_{21}-1)\ (p), \\ \sigma_{12}(\tau_{21}-1)\equiv\sigma_{21}(\tau_{12}-1)\ (p), & \sigma_{22}(\tau_{12}-1)\equiv 0\equiv\sigma_{22}(\tau_{21}-1)\ (p)\ . \end{cases} \qquad (5')$$

①. When $\sigma_{22}=0$, i.e., $v^2=0$, our discussion is divided into 4 cases:

(i) $\tau_{12}\neq 0\neq\tau_{21}$ case, we have $\sigma_{12}=\sigma_{21}=0$, $\tau_{12}=\tau_{21}=1$, we may assume $\beta=0$ by taking a as (4), and replacing u by au. Thus (2) becomes $u^2=u$, $v^2=0$, $uv=v=vu$, and $R\cong A[\theta]$, $\theta^2=0$.

(ii) $\tau_{12}\neq 0=\tau_{21}$ case, we have $\sigma_{12}=0$, $\tau_{12}=1$, and $\sigma_{22}=0$, i.e.,$v^2=0$. Taking a as (4), and using the transformation: $u'=au$, $v'=v-\sigma_{21}p^{k-2}u$, we reduce relation (2) to $(u')^2=u'$, $u'v'=v'$, $v'u'=0=(v')^2$. Then the right regular representation gives

$R\cong\left\{\begin{pmatrix} a & \beta \\ 0 & 0 \end{pmatrix}\middle| a\in A,\ \beta\in B\right\}$.

(iii) $\tau_{12}=0\neq\tau_{21}$ case is similar as (ii), we may reduce (2) to be $(u')^2=u'$, $v'u'=v'$, $u'v'=(v')^2=0$, and the left regular representation gives: $R\cong\left\{\begin{pmatrix} a & 0 \\ \beta & 0 \end{pmatrix}\middle| a\in A,\right.$

$\beta\in B\}$, which is anti-isomorphic to (ii).

(iv) $\tau_{12}=0=\tau_{21}$ case, we have $\sigma_{22}=0, \sigma_{12}=\sigma_{21}$. Taking a as(4), and using the transformation: $u'=au$, $v'=v-\sigma_{12}p^{k-2}u$, we reduce relation (2) to $(u')^2=u'$, $u'v'=v'u'=(v')^2=0$, and $R=(u')\oplus(v')\cong A\oplus N_p$.

②. When $\sigma_{22}\neq 0$, i.e., $v^2\neq 0$, we get $\tau_{12}=\tau_{21}=1, \sigma_{12}=\sigma_{21}=0$ from (5').We take a as (4). When $p=2$ we have $\sigma_{22}=1$. When $p>2$, we may take $\delta\in p$ such that $\delta^2\sigma_{22}=a$ or εa (p), and so $\delta^2\sigma_{22}=1$ or ε (p) according to σ_{22} is a square residue mod p or not. Under the transformation: $u'=au$, $v'=\delta v$, relation (2) becomes: $(u')^2=u'$, $u'v'=v'u'=v'$, $(v')^2=p^{k-2}u$ or $\varepsilon p^{k-2}u$, then $R\cong A[\theta]$, $\theta^2=p^{k-2}1$, or $\theta^2=\varepsilon p^{k-2}1$ (if $p>2$).

2) If $\tau_{11}\neq 0$, then we get $\sigma_{12}=\sigma_{21}, \tau_{12}=\tau_{21}$ from (5). If we take a as (4), and use the transformation: $u'=au+\tau_{11}v$, $v'=v$ when $\sigma_{22}=0$, or $u'=au-\tau_{11}v$, $v'=v$ when $\sigma_{22}\neq 0$, then both cases are reduced to 1).

Summarizing, we obtain Theorem 1 mentioned in (Ⅰ).The list of representatives is as follows:

$N=\text{rad}(R)$		$\bar{R}=R/N$	Num	representatives	Multiplication table
$\lvert N\rvert$	N				
p^{k-2}	(pu)	$F_p\oplus F_p$	1	$A\oplus F_p$	$u^2=u$, $uv=0=vu$, $v^2=v$
p^{k-1}	(u)	F_p	$k-1$	$(Zp^l/Zp^{k-1+l})\oplus F_p$ $l=1,2,\cdots,k-1$	$u^2=p^lu$, $uz=0=vu$, $v^2=v$
	$(pu)+(v)$	F_p	1	$A[\theta]$, $\theta^2=0$	$u^2=u$, $uv=v=vu$, $v^2=0$
			1	$A\oplus N_p$	$u^2=u$, $uv=vu=v^2=0$
			1	$\{\begin{pmatrix} a & \beta \\ 0 & 0\end{pmatrix} \mid a\in A,\ \beta\in B\}$	$u^2=u$, $uv=v$, $vu=v^2=0$
			1	$\{\begin{pmatrix} a & 0 \\ \beta & 0\end{pmatrix} \mid a\in A, \beta\in B\}$	$u^2=u$, $vu=v$, $uv=v^2=0$
			1	$A[\theta]$, $\theta^2=p^{k-2}1$	$u^2=u$, $uv=v=vu$, $v^2=p^{k-2}u$
			1	$A[\theta]$, $\theta^2=\varepsilon p^{k-2}1$	$u^2=u$, $uv=v=vu$, $v^2=\varepsilon p^{k-2}u$ $(p>2)$
Total			$k+6$ $k+5$	when $p>2$ when $p=2$	

Ⅳ Nilpotent Case

In an analogous manner to (Ⅲ) we get theorem 2 mentioned in (Ⅰ), The following is a list of the representatives

multiplication table	representatives	number
$u^2 = p^l u + v,\ uv = vu = v^2 = 0$ $l = 1, 2, \cdots, k-2$	$N_l \cong \left\{ \begin{pmatrix} 0 & 0 & 0 \\ a & p^l a & 0 \\ \beta & a & 0 \end{pmatrix} \middle\vert\, a \in A,\ \beta \in B \right\}$	$k-2$
$u^2 = p^l u + \tau v, v^2 = 0,\ uv = vu = p^{k-2} u$ $l = 1, 2, \cdots, k-3, \tau = 1, 2, \cdots, p-1;$	$N_l(\tau) \cong \left\{ \begin{pmatrix} p^l a + p^{k-2}\beta & p^{k-2} a \\ \tau a & 0 \end{pmatrix} \middle\vert\, \begin{matrix} a \in A \\ \beta \in B \end{matrix} \right\}$	$(p-1)(k-3)$
$u^2 = v,\ v^2 = 0, uv = vu = p^{k+2} u$	$N_{k-1}(1) \cong \left\{ \begin{pmatrix} p^{k-2}\beta & p^{k-2} a \\ a & 0 \end{pmatrix} \middle\vert\, \begin{matrix} a \in A \\ \beta \in B \end{matrix} \right\}$	1
$u^2 = \varepsilon v,\ v^2 = 0,\ uv = vu = p^{k+2} u$ $(p > 2)$	$N_{k-1}(\varepsilon) \cong \left\{ \begin{pmatrix} p^{k-2}\beta & p^{k-2} a \\ \varepsilon a & 0 \end{pmatrix} \middle\vert\, \begin{matrix} a \in A \\ \beta \in B \end{matrix} \right\}$	1
$u^2 = p^l u,\ uv = vu = v^2 = 0,$ $l = 1, 2, \cdots, k-1$	$(Zp^l / Zp^{k-1+l}) \oplus N_p$	$k-1$
$u^2 = p^l u,\ v^2 = 0,$ $-vu = uv = p^{k-2} u,$ $l = 1, 2, \cdots, k-1$	$N_l' \cong \left\{ \begin{pmatrix} 0 & 0 & 0 \\ a & p^l a - p^{k-2}\beta & p^{k-2} a \\ \beta & 0 & 0 \end{pmatrix} \middle\vert\, \begin{matrix} a \in A \\ \beta \in B \end{matrix} \right\}$	$k-1$
$u^2 = p^l u,\ vu = v^2 = 0,$ $uv = p^{k-2} u$ $l = 1, 2, \cdots, k-2$	$N_l'' = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ a & p^l a & p^{k-2} a \\ \beta & 0 & 0 \end{pmatrix} \middle\vert\, a \in A,\ \beta \in B \right\}$	$k-2$
$u^2 = p^l u,\ v^2 = 0, uv = \sigma vu =$ $\sigma p^{k-2} u,\quad l = 1, 2, \cdots, k-2;$ $\sigma = 0, 1, \cdots, p-2$	$N_l'(\sigma) = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ a & p^l a + p^{k-2}\beta & p^{k-2} a \\ \beta & 0 & 0 \end{pmatrix} \middle\vert\, \begin{matrix} a \in A \\ \beta \in B \end{matrix} \right\}$	$(p-1)(k-2)$
$u^2 = vu = 0,\ \sigma v^2 = uv = \sigma p^{k-2} u,$ $\sigma = 0, 1.$	$\overline{N}_{k-1}(\sigma) = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ a & 0 & p^{k-2}(\sigma a + \beta) \\ \beta & 0 & 0 \end{pmatrix} \middle\vert\, \begin{matrix} a \in A \\ \beta \in B \end{matrix} \right\}$	2
$u^2 = p^l u,\ vu = 0, \sigma v^2 = uv =$ $\sigma p^{k-2} u,\quad l = 1, 2, \cdots, k-2;$ $\sigma = 0, 1, \cdots, (p-1)/2.$	$\overline{N}_l(\sigma) = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ a & p^l a & p^{k-2}(\sigma a + \beta) \\ \beta & 0 & 0 \end{pmatrix} \middle\vert\, \begin{matrix} a \in A \\ \beta \in B \end{matrix} \right\}$	$(p+1)(k-2)$ if $p > 2$, $2(k-2)$ if $p = 2$
$u^2 = p^l u,\ vu = 0, uv = \sigma p^{k-2} u,$ $v^2 = \varepsilon p^{k-2} u,\quad l = 1, 2, \cdots, k-2;$ $\sigma = 0, 1, \cdots, (p-1)/2.$	$N_l^{\varepsilon}(\sigma) = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ a & p^l a & p^{k-2}(\sigma a + \varepsilon\beta) \\ \beta & 0 & 0 \end{pmatrix} \middle\vert\, \begin{matrix} a \in A \\ \beta \in B \end{matrix} \right\}$	
Total	$p > 2$ $\qquad (p+1)(3k-7) + 8$	
	$p = 2$ $\qquad 4(2k-3)$	

References

[1] Bloom, D. M. Amer. Math. Monthly, 71(1964), 918—920.

[2] Raghevendran, R. Compositio Math. 21(1969), 195—229.

[3] Ballieu, R. Ann. Soc. Sei. Bruxelles, Ser. I, 61(1947), 222—227.

[4] Gilmer, R. and Mott, J. Proc. Japan Acad. 49(1973), 795—799.

[5] Liu Ke Qin Mathematic Magazine 1(1982), 57—74.

[6] Liu Ke Qin Science Bulletin 13(1983), 769—771.

加群(P^{k-1}, P)型的 p^k ($k>3$)阶结合环的同构分类

赵 嗣 元

(上海师范大学数学系)

摘 要

本文给出加群(p^{k-1}, p)型的 p^k ($k>3$)阶结合环的同构分类，类数如下表：

	非幂零环	幂零环	合计
$p>2$	$k+6$ (个)	$(p+1)(3k-7)+8$ (个)	$(3k-7)p+(4k+7)$(个)
$p=2$	$k+5$ (个)	$4(2k-3)$(个)	$9k-7$ (个)

并按幂零和非幂零分别列表举出一个全体代表团．