Journal of Mathematical Research and Exposition
Vol.11 No.3 Aug.1991

Structure of Inner Isomorphic and Inner Non-isomorphic Rings*

Zhou Shifan

(Dept.Math., Suzhou University)

Abstract

An associative ring R is called an inner isomorphic, if any two proper subrings of it are isomorphic. An associative ring R is called an inner nonisomorphic, if the distinct subrings of it are always non-isomorphic. In this paper, we obtain several structure theorems of inner isomorphic and inner non-isomorphic ring, so that totally solve the open problem 81 provided by F.A.Szasz who asks "in which ring are the distinct subrings always non-isomorphic?" [1] additional, we point out that the main results and its proofs in paper [2] are mistaken.

Lemma 1 [3] If any two finitely generated proper subrings of associative ring R are always isomorphic, then R is isomorphic to one of the following types:

(1) $(p^2)/(p^4)$; (2) $(p)/(p^3)$; (3) Z_{p^2}; (4) $Z_p \oplus Z_p$; (5) $(R, +) \subseteq (Q, +)$ and $R^2 = 0$; (6) $(p)/(p^2)$; (7) $(p)/(p^2) \oplus (p)/(p^2)$; (8) $\left\{ \begin{bmatrix} 0 & a & b \\ 0 & 0 & a \\ 0 & 0 & 0 \end{bmatrix} \right\} a, b \in Z_p$; (9) An extension field of degree q over Z_p (q is either a prime number or 1).

Where p is a prime number, $(Q, +)$ is a rational number additive group.

Therefore we have the following:

Theorem 1 An associative ring R is an inner isomorphic iff R is isomorphic to one of the following types:

(1) $(p^2)/(p^4)$; (2) $(p)/(p^3)$; (3) Z_{p^2}; (4) $Z_p \oplus Z_p$; (5) $(R, +)$ is an infinite cyclic group, and $R^2 = 0$; (6) $(p)/(p^2)$; (7) $(p)/(p^2) \oplus (p)/(p^2)$; (8) $\left\{ \begin{bmatrix} 0 & a & b \\ 0 & 0 & a \\ 0 & 0 & 0 \end{bmatrix} \right| a, b \in Z_p \}$; (9) An extension field of degree q over Z_p (q is either a prime number or 1).

*Received Nov.20, 1989.

where p is a prime number.

The following are immediate consequences.

Corollary 1 The inner isomorphic ring is a commutative ring.

Corollary 2 Any two proper subgroups of a commutative group G are always isomorphic iff G is isomorpnic to one of the following type:

(1) $(Z_p, +)$; (2) $(Z_p, +)\oplus(Z_p, +)$; (3) $(Z_{p^2}, +)$;

(4) $(Z, +)$

where p is a prime number.

According to defintion of inner non-isomorphic ring and through calculation, we get the following:

Lemma 2 The subring of inner non-isomorphic ring an inner non-isomorphic.

Lemma 3 If a is an element of inner non-isomorphic ring R,

(1) When a is an infinite order element, then a is the algebraic element over integral number ring Z, i.e.,a is either a nilpotent element or one of roots of a polynomial $\sum_{i=1}^{n} a_i x^i$ (at least one of a_i $(i=1,\cdots, n)$ is not multiple of order of a^i).

(2) When a is a finite order element (let be m, $m\in N$), then a is an algebraic element over residue class ring Z_m, i.e.,a is either a nilpotent element or one of roots of a polynomial $\sum_{i=1}^{s} a_i x^i$ over Z_m, (at least one of a_i $(i=1, \cdots, s)$ is not multiple of order of a_i).

Lemma 4 If R is an inner non-isomorphic ring, and the additive group $(R, +)$ is torsion-free (R is simple called a torsion-free inner non-isomorphic ring). Then

(1) R doesn't contain non-zero nilpotent element;

(2) R contains at most one non-zero idempotent element.

Lemma 5 The torsion-free inner non-isomorphic ring R must be a subring of algebra R' over rational number field Q, and R' is also a torsion-free inn inner non-isomorphic ring.

Proof If R is an algebra over Q, then it's obvious. Otherwise, let $R' = \{r/n \mid r\in R, n\in N\}$ (Symbol r/n represents that $n(r/n)=r$). It is then easily verified that R' is an algebra over Q, and R' is torsion-free. If R' isn't an inner non-isomorphic, then R' contains subring $\langle r\rangle\cong\langle r'\rangle$, and $r\neq r'$ $\langle r\rangle\neq\langle r'\rangle$, therefore, at least one of r and r' doesn't belong to R. Thus there exists mr, $nr'\in R$ $(m, n\ N)$, such that $\langle kr\rangle\cong\langle kr'\rangle$ (k is the least common multiple of m and n),i.e., $kr=\sum_{i=1}^{s} a_i(kr')^{i-1}=k\sum_{i=1}^{s} a_i r'(kr')^{i-1}$, because

R is torsion-free, $r = \sum_{i=1}^{s} a_i r' (kr')^{i-1} \in \langle r' \rangle$. In the same way, $r' \in \langle r \rangle$, thus $\langle r' \rangle = \langle r \rangle$. this is a contradication.

Lemma 6 If the torsion-free inner non-isomorphic ring R contains the idempotent element $e \neq 0$, then R has only one non-zero idempotent element, and e is a unit element of R.

Proof Any idempotent element of torsion-free ring must belong to the centre of R[4], R contains only one non-zero idempotent element e by lemma 4. Therefore, by lemma 5, let torsion-free inner non-isomorphic ring $R' \supseteq R$, such that R' is an algebra over Q, then R' also has only one non-zero idempotent e which belongs to the centre of R'. Thus let R' be direct sum of ideals $eR'e$ and $R_1 = \{r - re \mid r \in R'\}$, because e is a unit element of R', e is also a unit element of R.

If $R_1 \neq 0$, then by lemma 3, a non-zero element a of R is an algebra element over Z, i.e., $\sum_{i=1}^{n} a_i a^i = 0$. according to lemma 4, a is not nilpotent, thus at least two elements of $a_1, \cdots, a_n$ are non-zero element, let $a_1 = \cdots = a_{k-1} = 0$, $a_k \neq 0$ such that $a_k a^k = -\sum_{i=k+1}^{n} a_i a^i$, i.e., $a^k = \sum_{i=k+1}^{n} a_i / a_k a^i = a^{k+1} g(a)$ $(g(a) = \sum_{i=k+1}^{n} a_i / a_k a^{i-k-1})$, thus $g^k(a) \cdot a^k$ is a non-zero idempotent element of R', i.e., $g^k(a) \cdot a^k = e$, and $a^k = a^k e$. By means of definition of direct sum, we have $a^k = a^k e = 0$. this is contrary to the assumption.

Similarly, we can get:

Lamma 7 Let R be a torsion-free inner non-isomorphic ring, then R is a subring of normal extension field E over Q, and E is an inner non-isomorphic, thus R is a commutative ring without zero divisor.

Theorem 2 If R is a torsion-free ring, then R is inner non-isomorphic iff R is a subring of normal extension field R' over Q, automorphism group G of R' over Q is either a commutative group of a Hamilton group ([5], [6]).

Proof If: By lemma 7, R is a subring of normal extension field R' over Q, and R' is an inner non-isomorphic. Because any subring F of R' $(F \supseteq Q)$ must be a subfield, F is a normal extension fiely over Q. Let H be an arbitrary subroup of G over Q and $|H| > 1$. therefore, let $\mathrm{Inv}H = \{a \mid a \in R', ha = a, h \in H\}$. Since Inv$H$ is a normal extension field over Q. $f(x)$ is a minimum polynomial of a over Q $(\forall a \in \mathrm{Inv}H)$ thus $f(x) = (x - a_i) \cdots (x - a_n)$ $(a_1 = a)$ over Inv$H$, $f(g(a)) = g(f(a)) = 0$. There exist that $g(a) = a_j \in \mathrm{Inv}H$, i.e. $g(\mathrm{Inv}H) \subseteq \mathrm{Inv}H$. So $H(g\mathrm{Inv}H) = gHg^{-1}g\mathrm{Inv}H$. i.e., the invarient subfield of conjugate

sub-group gHg^{-1} of H is $g\mathrm{Inv}H$. Therefore $gHg^{-1}\subseteq H$, i.e. $H\lhd G$.

Only if: If $H\lhd G$, $a\in \mathrm{Inv}H$. $f(x)$ is a minimum polynomial of a over Q, $f(x)=(x-a_1)\cdots(x-a_n)$. Because $g\mathrm{Inv}H$ is an invarient subfield of gHg^{-1}, $\mathrm{Inv}H = g\mathrm{Inv}H$.

The following can be verified.

Lamma 8 If additive group $(R, +)$ of associative ring R is a periodical group, then (1) R is direct sum of some ideals R_{p_i} $(p_i\in Z)$, where additive period of R_{p_i} is exponent of prime number p, $I=\{p \mid p$ is a prime number, $0\neq a\in R$, $pa=0\}$, (2) R_{p_i} $(p_i\in Z)$ are all inner non-isomorphic if and only if R is inner non-isomorphic.

Lemma 9 If additive period of every element of inner non-isomorphic ring R is a prime number, then (1) Nilpotent of any nilpotent element $a(a\neq 0)$ of R is either 2 or 3; (2) When nilpotent index of a is 3, then $R/\langle a\rangle$ doesn't contain nilpotent element; (3) When R only contains nilpotent element with index 2, then $R\backslash\langle a\rangle$ doesn't contain nilpotent element; (4) When R contains at most one idempotent element e $(e\neq 0)$, e is a unit element of Re, (5) When R doesn't contain non-zero nilpotent element, R is a normal algebra extension of Z_p.

Combining the lemmas above and verifying, we can obtain the following:

Theorem 3 If $(R, +)$ of associative ring R is a p-group and it contains complete subgroup, then R is an inner non-isomorphic if and only if R is isomorphic to one of the four following types:

(1) Zero-ring $Z[p^\infty]$; (2) $Z[p^\infty]\dot{+}[a]$ ($\dot{+}$ is direct sum of additive groups, a is a nilpotent element with index 3; $[a]$ is an additive group, $|a|=p$, $[a]+N_p$ is a ring with order p^2, $N_p=\langle a^2\rangle$ is a zero-subring with order p of $Z[p^\infty]$). (3) $\{Z[p^\infty]+[a]\}\oplus E$ ($\oplus$ is directsum of rings, a is described in (2). E is a normal extension over Z_p); (4) $Z[p^\infty]\oplus E$ (E is described in (3)).

Proof If: Since complete subring contained by $(R, +)$ is directsum of Priiferian group $Z[p^\infty]$ [1]. Then $(R, +)=\sum Z[p^\infty]+R'$, where R' is irreducible group [5]. and $Z[p^\infty]$ is zero-ideal of R[1]. Because R is an inner non-isomorphic ring, R contains only one $Z[p^\infty]$, i.e., $R=Z[p^\infty]\dot{+}R'$. When $R'=0$, this proves (1); when $R'\neq 0$, additive period of every non-zero element a of R is p. Otherwise, if additive period of a is p^n $(n>1)$, then $\langle p^{n-1}a\rangle\cong N_p\subseteq Z[p^\infty]$, as $\langle p^{n-1}a\rangle\neq N_p$ this would contradict the assumption. By lemma 9, R' at most contains a nilpotent subring $\langle a\rangle$ with nilpotent index 3. Let $\langle a\rangle=Z_pa+Z_pa^2$ $(a^3=0)$, Since R is an inner non-isomorphic ring, so $\langle a^2\rangle=Z_pa^2=N_p$. When $R=Z[p^\infty]\dot{+}[a]$, i.e., Result (2); When $R\supset Z[p^\infty]\dot{+}[a]$, $\forall\beta\in R/\{Z[p^\infty]\dot{+}[a]\}$, by

lemma 9, β isn't a nilpotent and is an algebra element over Z_p, thus $R \setminus \{Z[p^\infty]+[a]\}$ has non-zero idempotent element e and every element has inverse. Because $(R, +)$ is a primary group and is a bounded group, by Prüfer first theorem[5] $(R', +) = [a] \dot{+} E$, when E is directsum of some cyclic groups with order p, every non-zero element β of E is not nilpotent, and E has non-zero idempotent element, β has inverse $\beta^{-1} \in E$, so E is a division algebra over Z_p, and E is a normal extension field over Z_p. As $ea \cdot a = ea = 0$, $ea(ae)$ is not inversible. Let $ea = a + ka$ $(a \in N_p,\ 0 \leq k\ (p)$, $ea = e \cdot ea = e(a + ka) = 0 + kea$, so ea is either a or 0, when $ea = a$, $a^2 = ea \cdot a = ea^2 = 0$, this would contradict $a^2 \neq 0$. Thus $ea = 0 (ae = 0)$, $\beta a = a\beta = 0$ and $\beta\gamma = \gamma\beta = 0 (\beta \in E,\ \gamma \in Z[p$ $Z[p^\infty])$. This proves (3); If R' doesn't contain nilpotent element with inde 3, then R' doesn't contain non-zero nilpotent element. As above we can prove (4).

Iff: It can be verified easily.

Lemma 10 If R is an inner non-isomorphic ring, $(R, +)$ is not a p-group and it doesn't contain complete subgroup, then R hasn't infinite height element[5].

Theorem 4 If $(R, +)$ is a p-group without complete subgroup, and R has no non-zero idempotent element. Then R is inner non-isomorphic iff R is isomorphic to one of the following types:

(1) $(p^k)/(p^{n+k})$ $(k, n \in N,\ n \leq 2k)$; (2) $Z_p a \dot{+} Z_p a^2$ $(a^3 = 0)$;

(3) $(p^n)/(p^{2n}) \dot{+} [a]$ $(n \in N$, $[a]$ is a cyclic group with order p, $\langle a \rangle = Z_p a + Z_p a^2$, $\langle a^2 \rangle = (p^{2n-1})/(p^{2n})$, $a \cdot p^n = p^n \cdot a = 0)$.

Proof If: It can be verified easily;

Only if: By assumption and lemma 10, $(R, +)$ doesn't contain infinite height element, by Prufer second theorem[5], $(R, +)$ can be decomposed into directsum of cyclic group G with order p^{n_i}.

(1) If $\forall\, n_i = 1$, then the character of R is p, by assumption and lemma 8, R only contains nilpotent element with index 2 or 3. By lemma 9, result (1), (2) can be get;

(2) Contrary to (1), let $n_1 > 1$, we can proof that $n_i = 1$ $(i > 1)$.

1° If $R = G_1 = \{ka_1 \mid 0 \leq k < p^{n_1}\}$, let $a_1^2 = ma_1$, we can get $p \mid m$. Therefore. let $a_1^2 = p^k q a_1$, $(p, q) = 1$, where $(qa_1) = \langle a_1 \rangle$. Let $a_1^2 = p^k a_1$, we have $R = \langle a_1 \rangle \cong (p^k)/(p^{n_1+k})$, because nilpotent index of a is less than or equal to 3. $n \leq 2k$. This proves (1).

2° If $R \supset G_1$, where additive periodes of every non-zero element of $\sum_i' G_i$ are all p. By lemma 9, nilpotent index of them are of all 2 or 3. It can be

verified that they doesn't contain nilpotent element with index 2, thus $R=G_1+G_2=\{ka_1 \mid 0\leq k<p^{n_1}\}\dot{+}[a_2]$, and $\langle a_2\rangle=Z_p a_2\dot{+}Z_p a_2^2$, $a_2^2=p^{n_1-1}a_1$. By lemma 9, nilpotent inder of a_1 is either 2 or 3.

(i) If nilpotent index of a_1 is 2, then G_1 is a zero-ring with order p^{n_1}, let $G_1=(p^{n_1})/(p^{2n_1})$. Result (3) is get;

(ii) If nilpotent index of a_1 is 3, then $\langle a_1\rangle=Z_{p^{n_1}}a_1\dot{+}Z_{p^m}a_1^2\subseteq R$ $(m\in N)$. Since $|R|=p^{n_1+1}$, then $m=1$ and $R=Z_{p^{n_1}}a_1+Z_p a_1^2$, where $\langle p^{n_1-1}a_1\rangle\cong\langle a_1^2\rangle$, but $\langle p^{n_1-1}a_1\rangle\neq\langle a_1^2\rangle$, controdicts the assumtion.

By lemma 8, we get the following:

Lemma 11 If character of inner non-isomorphic ring R is a prime number p, and R has a unit element and contains nilpotent element with index 2, then $R=Z_p e\dot{+}\langle a\rangle$, $ea=ae=a$, $a^2=0$.

Lemma 12 The character of inner non-isomorphic ring R with unit element e is a prime number p, and $\exists a\in R$, nilpotent index of a is 3, then $R=Z_p e+\langle a\rangle$, $ea=ae=a$.

Theorem 5 If $(R, +)$ of associative ring is a p-group (p is a prime number), and it contains non-zero idempotent element, but doesn't contain complete subgroup, then R is an inner non-isomorphic ring iff R is isomorphic to one of types:

(1) Z_{p^n} $(n\in N,\ n>1)$;

(2) A normal extension E over Z_p;

(3) $Z_p e\dot{+}\langle a\rangle$ $(e^2=e,\ a^2=0,\ ea=ae=a)$;

(4) $Z_p e\dot{+}\langle a\rangle$ $(e^2=e,\ a^3=0,\ a^2\neq 0,\ ea=ae=a)$;

(5) $E\oplus(p^k)/(p^{n-k})$ (E is a normal extension E over Z_p, $n,\ k\in N,\ n\leq 2k$);

(6) $Z_p e\dot{+}\langle a\rangle$ $(e^2=e,\ a^2=0,\ ae=0,\ ea=a)$;

(7) $E\oplus\langle a\rangle$ (E is a normal extension over Z_p, $\langle a\rangle=Z_p a+Z_p a^2$, $a^3=0$);

(8) $E\oplus((p^n)/(p^{2n})\dot{+}[a])$ (E is a normal extension over Z_p, $\langle a\rangle=Z_p a+Z_p a^2$, $\langle a^2\rangle=(p^{2n-1})/(p^{2n})$, $p^n a=a\ p^n=0$).

Proof If: We can verify directly.

Only if: (I) If the additive period of non-zero idempotent element e in R is p^n $(n>1)$, then define a directsum of left ideal $R=Re\dot{+}R_1$ $(R_1=\{r-re\mid r\in R\})$, we can prove $R_1=0$ by lemma 9, hence $R=Re$. We can also prove that R contains only one right unit element, thus e is the unit element of R. By Prüfer first theorem[5] we can get that $R\cong Z_{p^n}$, this proves result (1);

(II) If the additive period of non-zero idempotent element e in R is p, then let $R=Re\dot{+}R_1$ $(R_1=\{r-re\mid r\in R\})$, as above, we have that R has only one non-zero idempotent element e, and e is a unit element of Re. Therefore Re is

an algebric extension over $Z_p e$.

(1°) If $R_1 = 0$, then $R = eRe$.

①When R doesn't contain non-zero nilpotent element, by Lemma 9, R is a normal extension over Z_p. This proves result (2);

②When R contains non-zero nilpotent element by lemma 9, its nilpotent index is either 2 or 3:

(i) When R contains only nilpotent with index 2, by Lemma 9 and Lemma 11, we can get result (3);

(ii) When R contains nilpotent element with index 3, by Lemma 9 and Lemma 12, we can get result (4) directly.

(2°) If $R_1 \neq 0$, then $R = eRe \dot{+} R_1$, then the inner non-isomorphic ring eRe must be isomorphic to that in result (2), (3) or (4).

If eRe is isomorphic to result (3) or (4). Then additive period of every non-zero element of R_1 is p by assumption, therefore R_1 contains non-zero idempotent element, it's impossible, thus eRe can only be a normal extension E over Z_p.

By assumotion and Theorem 4, we have one of following:

1) R_1 is isomorphic to $(p^k)/(p^{n+k})$ $(k, n \in N,\ n \leq 2k)$;

2) R_1 is isomorphic to $Z_p a \dot{+} Z_p a^2$ $(a^3 = 0)$;

3) R_1 is isomorphic to $(p^n)/(p^{2n}) \dot{+} [a]$ $(n \in N,\ [a]$ is a cyclic group with order p, $\langle a \rangle = Z_p a + Z_p a^2$, $\langle a^2 \rangle = (p^{2n-1})/(p^{2n})$, $a p^n = p^n a = 0)$.

When 1), if $e p^k = p^k e = 0$ and $n > 1$, this proves result (5); if $n = 1$, by Lemma 11 we can prove result (6);

When 2), we have $R \cong E \dot{+} Z_p a \dot{+} Z_p a^2$ $(a^3 = 0)$, since $ae = 0$, so $(ea)^2 = 0$, thus $ea = 0$. This proves result (7);

When 3), if $R = E \oplus ((p^n)/(p^{2n}) \dot{+} [a])$, we can prove result (8).

As above we have

Theorem 6 If the additive group $(R, +)$ of non-zero associative ring R is a cyclic group, i.e., R is a directsum of some ideals R_p $(p \in 1)$, $(R_p = \{a \mid a \in R, \exists n \in N,\ p^n a = 0\}$, $I = \{p \mid p$ is a prime number, $\exists 0 \neq a \in R,\ pa = 0\})$, then R is an inner non-isomorphic ring iff every ideal R_p $(p \in I)$ of R is isomorphic to one of the following 15 types:

(Ⅰ) Type (1) to (4) in Theorem 3;

(Ⅱ) Tppe (1) to (3) in Theorem 4;

(Ⅲ) Type (1) to (8) in Theorem 5.

We can calculate directly, and get

Lemma 13 If R is an inner non-isomorphic ring, then

(1) $R_0=\{a \mid a\in R,\ \exists n\in N,\ na=0\}\lhd R$, and when $R_0\neq 0$, R_0 has the structure in Theorem 6;

(2). When $R\neq R_0$, $\forall a\in R\backslash R_0$, $\langle a\rangle$ is a torsion-free subring, then R/R_0 has at most one non-zero idempotent element.

Similary, we can prove

Theorem 7 If R is an inner non-isomorphic ring, $(R,\ +)$ has a torsion-free complete subgroup. Then $R\cong R_0\oplus E$, where E is a normal extension over Q, and every subring of E containing Q is a normal extension over Q, $R_0=\{r \mid r\in R,\ \exists n\in N,\ nr=0\}$ is an inner non-isomorphic ring without non-zero idempotent element, therefore $R_0\cong \sum_{p\in I}^{\oplus} R_p$ ($R_p=\{a \mid a\in R,\ \exists n\in N,\ pa=0\}$, $I=\{p \mid p$ is a prime number, $\exists 0\neq a\in R,\ pa=0\}$, and R_p must be isomorphic to one of 15 types in theorem 6.

Additionally, we point out that the main results and its proofs in paper [2] are mistaken.

References

[1] Szasz F.A., Radicals of Rings, Chichester.New York. Brisbane. Toroto, (1981), 210, 43.

[2] Zhang Changqian, J.Math.Res.and Exposition, 8(2) (1988). 163~169 (in chinese).

[3] Zhou Shifan, Wu Zhixiang, J.Suzhou University, 4(1988).477~482.

[4] Herstain I.N., Rings with Involution, University of chicago Press, (1976).4.

[5] Kurosh A.G., The Theory of Groups, NewYork: Chelsea Publishing Company, (1960).

[6] Jacobson N., Structure of Rings, AMS.Call.Publ., Vol 37(1956): 217

[7] Hall M., The Theory of Groups, NewYork, Macmillan Company, (1959).

内同构环与内异环的结构

周 士 藩

(苏州大学数学系)

摘 要:

所有真子环都同构的结合环，称为内同构环，任两不同的子环都不同构的结合环，称为内异环．本文目的是给出内同构环与内异环的一些结构定理，从而基本上解决了Szasz F.A.提出的问题81：怎样的结合环，它的不同子环总不同构？