COEFFICIENT SUBRINGS OF CERTAIN LOCAL RINGS
WITH PRIME-POWER CHARACTERISTIC

TAKAO SUMIYAMA

Department of Mathematics
Aichi Institute of Technology
Yakusa-chō, Toyota
470-03 Japan

(Received October 13, 1993 and in revised form September 15, 1994)

ABSTRACT. If \( R \) is a local ring whose radical \( J(R) \) is nilpotent and \( R/J(R) \) is a commutative field which is algebraic over \( GF(p) \), then \( R \) has at least one subring \( S \) such that \( S = \bigoplus_{i=1}^{n} S_i \), where each \( S_i \) is isomorphic to a Galois ring and \( S/J(S) \) is naturally isomorphic to \( R/J(R) \). Such subrings of \( R \) are mutually isomorphic, but not necessarily conjugate in \( R \).

KEY WORDS AND PHRASES: Coefficient ring, Galois ring, local ring, Szele matrix.

1991 AMS SUBJECT CLASSIFICATION CODES: 16L30, 16P10, 16D70

0. INTRODUCTION

Let \( p \) be a fixed prime. For any positive integers \( n \) and \( r \), there exists up to isomorphism a unique \( r \)-dimensional separable extension \( GR(p^n, r) \) of \( \mathbb{Z}/p^n\mathbb{Z} \), which is called the Galois ring of characteristic \( p^n \) and rank \( r \) (see [9, p. 293, Theorem XV.2]). This ring was first noticed by Krull [8], and was later rediscovered by Janusz [6] and Raghavendran [12].

By Wedderburn-Malcev theorem (see, for instance, [4, p. 491]), if \( R \) is a finite dimensional algebra over a field \( K \) such that \( R/R/J(R) \) is a separable algebra over \( K \), then \( R \) contains a semisimple subalgebra \( S \) such that \( R = S \oplus J(R) \) (direct sum as vector spaces). Such subalgebras of \( R \) are conjugate each other.

Concerning the case \( R \) is not an algebra over a field, Raghavendran [12, Theorem 8], Clark [3] and Wilson [17, Lemma 2.1] have proved the following: If \( R \) is a finite local ring with characteristic \( p^n \) whose residue field is \( GF(p^n) \), then \( R \) contains a subring \( S \) such that \( S \) is isomorphic to \( GR(p^n, r) \) (hence \( R = S + J(R) \)). Such a subring \( S \) of \( R \) is called a coefficient ring of \( R \). Coefficient rings of \( R \) are conjugate each other. We can embed \( R \) to a ring of Szele matrices over \( S \) (see §1).

If \( R \) is a finite ring of characteristic \( p^n \), then \( R \) contains a subring \( T \) (unique up to isomorphism) such that (1) \( R = T \oplus N \) (as abelian groups), where \( N \) is an additive subgroup of \( J(R) \), (2) \( T \) is a direct sum of matrix rings over Galois rings, (3) \( J(T) = T \cap J(R) = pT \), and (4) \( R = T + J(R) \).

The purpose of this paper is to extend these results to certain rings which are not necessarily finite.

1.

In what follows, when \( S \) is a set, \( |S| \) will denote the cardinal number of \( S \). When \( A \) is a ring, for any subset \( S \) of \( A \), \( (S) \) denotes the subring of \( A \) generated by \( S \). A ring \( A \) is called locally finite if any finite subset of \( A \) generates a finite subring. When \( A \) is a ring with \( 1 \), for \( B \) to be called a subring of \( A \), \( B \) must contain \( 1 \). Let \( J(A) \) denote the Jacobson radical of \( A \), \( Aut(A) \) the automorphism group of \( A \), and \( (A)_{n \times n} \) the ring of \( n \times n \) matrices having entries in \( A \). If \( A \ni 1, A^* \) denotes the group of units of \( A \). For \( a \in A^* \), \( o(a) \) denotes the multiplicative order of \( a \).

The Galois ring \( GR(p^n, r) \) is characterized as a ring isomorphic to \( (\mathbb{Z}/p^n\mathbb{Z})[X]/(f(X))(\mathbb{Z}/p^n\mathbb{Z})[X]) \), where \( f(X) \in (\mathbb{Z}/p^n\mathbb{Z})[X] \) is a monic polynomial of degree \( r \), and is irreducible modulo \( p\mathbb{Z}/p^n\mathbb{Z} \) (see [7, Chapter XVI]). By [12, Proposition 1], any subring of \( GR(p^n, r) \) is isomorphic to \( GR(p^n, s) \), where
s is a divisor of r. Conversely, if s is a divisor of r, then there is a unique subring of $GR(p^n, r)$ which is isomorphic to $GR(p^n, s)$.

The following lemma is easily deduced from [16, Theorem 3 (I)] and its proof.

**LEMMA 1.1.** Let R be a finite local ring of characteristic $p^n$ whose residue field is $GF(p^n)$. If $a \in R^*$ satisfies $o(a) = p^n - 1$, then the subring $(a)$ of R is isomorphic to $GR(p^n, r)$.

A ring $R$ will be called an IG-ring if there exists a sequence $\{R_i\}_{i=1}^\infty$ of subrings of $R$ such that $R_i \subset R_{i+1}$, $R_i \cong GR(p^n, r_i)$ ($i \geq 1$) and $R = \bigcup_{i=1}^\infty R_i$, where $\{r_i\}_{i=1}^\infty$ is a sequence of positive integers such that $r_i \mid r_{i+1}$ ($i \geq 1$). If $R$ is an IG-ring described above, then $R_i$ is the only subring of $R$ which is isomorphic to $GR(p^n, r_i)$. So we can write $R = \bigcup_{i=1}^\infty GR(p^n, r_i)$.

Let $p$ be a prime, $n$ a positive integer and $r_1 \leq r_2 \leq \ldots$ an infinite sequence of positive integers such that $r_i \mid r_{i+1}$. By the fact we observed above, there exists a natural embedding $GR(p^n, r_i) \to GR(p^n, r_{i+1})$ for each $i \geq 1$. Let us put $t'_i = id_{GR(p^n, r_i)}$ and $t'_i = t'_{i-1} \circ \ldots \circ t'_1$ for $1 \leq i \leq j$. Then we see that $\{GR(p^n, r_i), t'_i\}$ is an inductive system. The ring $R = \lim GR(p^n, r_i)$ is an IG-ring. Conversely, any IG-ring can be constructed in this way. An IG-ring $R = \bigcup_{i=1}^\infty GR(p^n, r_i)$ is a Galois ring if $|R|$ is finite. When $A$ is a ring with 1, a subring $S$ of $A$ is called an IG-subring of $A$ if $S$ is an IG-ring.

**PROPOSITION 1.2.** Let $R = \bigcup_{i=1}^\infty GR(p^n, r_i)$ be an IG-ring. Then:

(I) $R$ is a commutative local ring with radical $J(R) = pR$. The residue field $R/pR$ is $GF(p^n)$.

(II) If $e$ is a positive integer such that $1 \leq e \leq n$, then $R/p^eR$ is naturally isomorphic to the IG-ring $\bigcup_{i=1}^e GR(p^e, r_i)$.

(III) $R$ is a proper homomorphic image of a discrete valuation ring whose radical is generated by $p$.

(IV) Any ideal of $R$ is of the form $p^eR (0 \leq e \leq n)$.

(V) $R$ is self-injective.

(VI) $Aut(R) \cong \lim GR(GF(p^n, r_i)) \cong \lim_\leftarrow Aut(GF(p^n)) \cong \bigcup_{i=1}^\infty GF(p^n)$.

**PROOF.** (I) and (II). For each $i \geq 1$,

$$0 \to p^eGR(p^n, r_i) \to GR(p^n, r_i) \to GR(p^n, r_i) \to 0$$

is an exact sequence of $GR(p^n, r_i)$-modules. So we get the result by [2, Chapitre 2, §6, n° 6, Proposition 8].

(III) Let us put $K = \bigcup_{i=1}^\infty GF(p^n)$. Let $W_n(K)$ be the ring of Witt vectors over $K$ of length $n$ (see [15, Chapter II, §6] or [5, Kapitel II, §10.4]). By (I) and (5, Kapitel II, §10.4), both $R$ and $W_n(K)$ are elementary complete local rings (in [14], elementare vollständige lokale Ringe) of characteristic $p^n$ whose residue fields are $K$. Since an elementary complete local ring is uniquely determined by its characteristic and residue field (see [14, Anhang 2]), we see that $R$ is isomorphic to $W_n(K)$. Let $W(K)$ be the ring of Witt vectors over $K$ of infinite length. By [7, Chapter V, §7], $W(K)$ is a discrete
valuation ring whose radical is generated by \( p \). Since \( W(K) \) is the projective limit of \( \{ W_n(K) \}_{n=1}^{\infty} \) (see [15, Chapter II, §6]), \( W_n(K) \) is a homomorphic image of \( W(K) \).

(IV) If \( R \) is a discrete valuation ring with radical \( pR \), then any ideal of \( R \) is of the form \( p^jR \) \((j \geq 0)\), so the result is clear from (III).

(V) Clear from (III), since any proper homomorphic image of a principal ideal domain is self-injective.

(VI) Immediate by [9, p. 294, Corollary XV.3].

Let \( \{ r_i \}_{i=1}^{\infty} \) be an infinite sequence of positive integers such that \( r_i = 1 \) and \( r_i | r_{i+1} (i \geq 1) \), and \( S = \bigcup_{r_i} GR(p^r, r_i) \) be an IG-ring of characteristic \( p^* \). Let \( n = n_1 \geq n_2 \geq \ldots \geq n_t \) be a nonincreasing sequence of positive integers. Let us put \( S_j = \bigcup_{r_i} GR(p^{r_i}, r_i) \) for \( 1 \leq j \leq t \). Let \( \phi_j : S \to S_j \) be the natural homomorphism followed by the isomorphism \( S/p^nS \cong S_j \) of Proposition 1.2 (II). Let us put

\[
U(S; n_1, n_2, \ldots, n_t) = \{(x_j) \in (S)^t \mid \alpha_j \in p^{-r_j}S \text{ if } i > j\}.
\]

It is easy to see that \( U(S; n_1, n_2, \ldots, n_t) \) forms a subring of \( (S)^t \). Let \( M(S; n_1, n_2, \ldots, n_t) \) denote the set of all \( t \times t \) matrices \( (a_{ij}) \), where \( a_{ij} \in S_j \), and \( a_{ij} \in p^{-r_i}S_j \) for \( i > j \). Let \( \Phi \) be the mapping of \( U(S; n_1, n_2, \ldots, n_t) \) onto \( M(S; n_1, n_2, \ldots, n_t) \) defined by \( (\alpha_j) \mapsto (a_{ij}) \) where \( a_{ij} = \phi_j(\alpha_j) \). It is easy to check that addition and multiplication in \( M(S; n_1, n_2, \ldots, n_t) \) can be defined by stipulating that \( \Phi \) preserves addition and multiplication. Following [17], we call \( M(S; n_1, n_2, \ldots, n_t) \) a ring of Szele matrices over \( S \).

**Lemma 1.3.** (cf. [17, Lemma 2.1]) Let \( R \) be a ring with 1 which contains an IG-subring \( S \) of characteristic \( p^* \). If \( R \) is finitely generated as a left \( S \)-module, then there exists a nonincreasing sequence \( n = n_1 \geq n_2 \geq \ldots \geq n_t \) of positive integers such that \( R \) is isomorphic to a subring of \( M(S; n_1, n_2, \ldots, n_t) \).

**Proof.** By Proposition 1.2 (V), there exists a submodule \( N \) of \( R \) such that \( R = S \oplus N \) as left \( S \)-modules. By Proposition 1.2 (III), there is a discrete valuation ring \( W \) and a homomorphism \( \phi \) of \( W \) onto \( S \). By defining

\[
a y = \phi(a) y \quad (a \in W, y \in N),
\]

\( N \) is a finitely generated \( W \)-module. Since a finitely generated module over a principal ideal domain is a direct sum of cyclic modules, there exist \( y_1, y_2, \ldots, y_s \in N \) such that \( N = \oplus_{i=1}^{s} W y_i \). Let \( t = s + 1 \), \( x_1 = 1 \) and \( x_i = y_{i-1} (2 \leq i \leq t) \). Then we get \( R = \oplus_{i=1}^{t} S x_i \). Let \( S x_i \cong S/p^nS \) as \( S \)-modules \((n_1 = n)\). Without loss of generality, we may assume \( n_1 \geq n_2 \geq \ldots \geq n_t \). For each \( a \in R \), we can write

\[
x_i a = \sum_{j=1}^{t} \alpha_{ij} x_j \quad (\alpha_{ij} \in S).
\]

Since

\[
0 = p^n x_i a = \sum_{j=1}^{t} p^{n-r_i} \alpha_{ij} x_j,
\]

by Proposition 1.2 (IV), \( \alpha_{ij} \in p^{-r_i}S \) if \( i > j \). As \( \alpha_{ij} \) is uniquely determined modulo \( p^nS \) by \( a \), we can define \( \psi : R \to M(S; n_1, n_2, \ldots, n_t) \) by \( a \mapsto (\psi(a)) \). It is easy to see that \( \psi \) is an injective ring homomorphism.

2.

Let \( G \) be a group, and \( N \) a normal subgroup of \( G \). Let \( \rho : G \to H = G/N \) be the natural homomorphism. A monomorphism \( \lambda : H \to G \) will be called a right inverse of \( \rho \) if \( \rho \circ \lambda = id_H \). If \( \lambda \) is a right inverse of \( \rho \), then \( G \) is a semidirect product of \( N \) and \( \lambda(H) \).

The following lemma is a variation of Schur-Zassenhaus theorem [13, Chapter 9, 9.1.2].
LEMMA 2.1. Let G be a group, and N a normal subgroup of G. Let $\rho: G \to H = G/N$ be the natural homomorphism. Assume that N is locally finite, and there exists a sequence $\{H_i\}_{i=1}^{\infty}$ of finite subgroups of H such that $H_i \subseteq H_{i+1}$, and $\bigcup_{i=1}^{\infty} H_i = H$ and, for any $a \in N$ and any $i \geq 1$, $o(a)$ and $|H_i|$ are coprime. Then:

(I) There exists a right inverse $\lambda: H \to G$ of $\rho$.

(II) If, for some $m \geq 1$, there exists a monomorphism $\mu': H_m \to G$ such that $\rho \circ \mu' = id_{H_m}$, then there exists a right inverse $\mu: H \to G$ of $\rho$ such that $\mu|_{H_m} = \mu'$.

(III) There exists a unique right inverse of $\rho$ if and only if $G$ is a nilpotent group.

(IV) If $\mu': H_m \to G$ and $\mu'': H_m \to G$ are monomorphisms such that $\rho \circ \mu' = \rho \circ \mu'' = id_{H_m}$, then $\mu'(H_m)$ and $\mu''(H_m)$ are conjugate in G.

PROOF. (I) For each $x \in H$, we can choose an element $g_x$ of G such that $\rho(g_x) = x$. As G is locally finite (see [13, Chapter 14, 14.3.1]), the subgroup $G_1$ of G generated by $\{g_x\}_{x \in H_1}$ is finite, and $\rho|_{G_1}$ is a homomorphism of $G_1$ onto $H_1$. Let us put $N_1 = Ker(\rho|_{G_1})$. Since $|N_1|$ and $|H_1|$ are coprime, by Schur-Zassenhaus theorem [13, Chapter 9, 9.1.2], there exists a right inverse $\lambda_1: H_1 \to G_1$ of $\rho|_{G_1}$. Next, let $\{g'_1\}_{x \in H_1}$ be a set of elements of G such that $\rho(g'_1) = y$ for any $y \in H_2$, and $\{g'_1\}_{x \in H_1} \subseteq \{g'_1\}_{x \in H_1}$. Let $G_2$ be the finite subgroup of G generated by $\{g'_1\}_{x \in H_1}$. Then $\rho|_{G_2}$ is a homomorphism of $G_2$ onto $H_2$. By [13, Chapter 9, 9.1.3], there exists a complement subgroup $L$ of $N_2 = Ker(\rho|_{G_2})$ in $G_2$ such that $L \supseteq \lambda_2(H_1)$. The mapping $\lambda_2: H_2 \to G_2$ defined by $H_2 = G_2/N_2$ is a right inverse of $\rho|_{G_2}$. For any $a \in H_1$, $\lambda_2(a)$ is a right inverse of $\rho|_{G_2}$, hence we see $\lambda_2|_{H_1} = \lambda_1$. Continuing this process inductively, we get a sequence $\{G_i\}_{i=1}^{\infty}$ of finite subgroups of G and a sequence $\{\lambda_i\}_{i=1}^{\infty}$ of right inverses $\lambda_i: H_i \to G_i$ of $\rho|_{G_i}$ such that $\lambda_i|_{H_{i-1}} = \lambda_{i-1}$ for any $1 \leq i \leq j$. Then $\lambda = \lim_{i \to \infty} \lambda_i: H = \bigcup_{i=1}^{\infty} H_i \to G$ is a right inverse of $\rho$.

(II) can also be proved in the same way by starting from $\mu': H_m \to \mu'(H_m)$.

(III) Assume that $\lambda: H \to G$ is the unique right inverse of $\rho$. Then G is a semidirect product of N and $\lambda(H)$. We shall show that this is the direct product. Suppose that there exist $c \in N$ and $z \in H$ such that $c \lambda(z) \neq \lambda(z) c$. Let us define $\mu: H \to G$ by $\mu(b) = z^{\lambda(c)} \lambda(b) z$. Then $\mu$ is a right inverse of $\rho$ different from $\lambda$, which contradicts our hypothesis. So G is the direct product of N and $\lambda(H)$. Hence G is nilpotent.

Conversely, let us suppose that G is nilpotent, and $\lambda$ and $\mu$ are right inverses of $\rho$. For each $i \geq 1$, let $G_i$ be the subgroup of G generated by $\lambda(H_{i-1}) \cup \mu(H_i)$. Then $\rho|_{G_i}$ is a homomorphism of $G_i$ onto $H_i$. Both $\lambda(H_i)$ and $\mu(H_i)$ are complement subgroups for $N_i = Ker(\rho|_{G_i})$ in $G_i$. Since $G_i$ is a finite nilpotent group, for each prime divisor $q$ of $|G_i|$, $G_i$ contains a unique $q$-Sylow subgroup. Each $G_i$ is the direct product of such Sylow subgroups. As $|H_i|$ and $|N_i|$ are coprime, we have $\lambda(H_i) = \mu(H_i)$. So $\lambda|_{H_i} = \mu|_{H_i}$. Since this holds for each $i \geq 1$, we see $\lambda = \mu$.

(IV) Let L be the finite subgroup of G generated by $\mu'(H_m) \cup \mu''(H_m)$. Then $\rho|_{L}$ is a homomorphism of L onto $H_m$. Since $|Ker(\rho|_{L})| = |N \cap L|$ and $|H_m|$ are coprime, by Schur-Zassenhaus theorem, $\mu'(H_m)$ and $\mu''(H_m)$ are conjugate in L.

Let G, N, H and $\rho: G \to H$ be as in Lemma 2.1. We say that G has property (GC) with respect to N if, for any two right inverses $\mu$ and $\nu$ of $\rho$, $\mu(H)$ and $\nu(H)$ are conjugate in G. If H is finite, then by Lemma 2.1 (IV), G has the property (GC) with respect to N.
Let $R$ be a ring with 1. Let $S$ be a subring of $R$, and $I = J(R) \cap S$. The homomorphism of $S/I$ to $R/J(R)$ defined by $a + I \mapsto a + J(R) (a \in S)$ is injective. We shall say that $S/I$ is naturally isomorphic to $R/J(R)$ if this homomorphism is onto. If $S$ is a local subring of a local ring $R$ and if $J(S)$ is nilpotent, then $J(S) = J(R) \cap S$.

Now we shall state main theorems of this section, which generalize the result of R. Raghavendran [9, p. 373, Theorem XIX.4].

**THEOREM 2.2.** Let $R$ be a local ring with radical $M$. Assume that $M$ is nilpotent, and $K = R/M$ is a commutative field of characteristic $p$ ($p$ a prime) which is algebraic over $GF(p)$. Then there exists an IG-subring $S$ of $R$ such that $S/pS$ is naturally isomorphic to $K$.

**PROOF.** Since $K$ is algebraic over $GF(p)$, $|K|$ is either finite or countably infinite. So there exists a sequence $\{K_i\}_{i=1}^{\infty}$ of finite subfields of $K$ such that $K_i \subseteq K_{i+1}, (i \geq 1)$ and $\bigcup_{i=1}^{\infty} K_i = K$. Let $K_i = GR(p^{r_i})$.

The natural homomorphism $\pi: R \rightarrow K$ induces a group homomorphism $\pi^* = \pi|_{R^*}$ onto $K^*$. Each $(1 + M')/(1 + M'^{n+1})$ is isomorphic to the additive group $M'/M'^{n+1}$. As $p^{r_i} \subseteq M'^{n+1}$, the order of each element of $1 + M = Ker(\pi^*)$ is a power of $p$. Furthermore, $K^* = \bigcup_{i=1}^{\infty} K_i^*$, where $|K_i^*| = p^{r_i} - 1$ is coprime to $p$. So, by Lemma 2.1 (I), there exists a right inverse $\lambda: K^* \rightarrow R^*$ of $\pi^*$. For each $i \geq 1$, let $\alpha_i$ be a generator of $K_i^*$. By Lemma 1.1, the subring $S_i = \langle \alpha_i \rangle$ of $R$ is isomorphic to $GR(p^{r_i}, r_i)$. Consequently, $S = \langle \lambda(K^*) \rangle = \bigcup_{i=1}^{\infty} S_i$ is an IG-subring of $R$, and $S/pS$ is naturally isomorphic to $K$.

Such a subring $S$ of $R$ stated in Theorem 2.2 will be called a coefficient subring of $R$. When $R$ is a commutative local ring satisfying the assumption of Theorem 2.2, $S$ coincides with the subring described in [11, p. 106, Theorem 31.1].

Let $R, M, S$ and $K = \bigcup_{i=1}^{\infty} GF(p^{r_i})$ be as in Theorem 2.2, where $\{r_i\}_{i=1}^{\infty}$ is a sequence of positive integers such that $r_i | r_{i+1}, (i \geq 1)$. Let $p^*$ be the characteristic of $R$. Let $S'$ be another coefficient subring of $R$. From what was stated in §1, $S' = \bigcup_{i=1}^{\infty} GR(p^{r_i}, r_i)$, which is isomorphic to $S$. By Proposition 1.2 (V), there exists a left $S'$-submodule $N$ of $R$ such that $R = S' \oplus N$ as left $S'$-modules.

If $\lambda: K^* \rightarrow R^*$ is a right inverse of $\pi^*$, then by the proof of Theorem 2.3, $S = \langle \lambda(K^*) \rangle$ is a coefficient subring of $R$.

We shall show that, if $\lambda$ and $\mu$ are different right inverses of $\pi^*$, then $\langle \lambda(K^*) \rangle \neq \langle \mu(K^*) \rangle$. Let us suppose $\langle \lambda(K^*) \rangle = \langle \mu(K^*) \rangle$ and denote it by $S$. Let $\{K_i\}_{i=1}^{\infty}$ be a sequence of finite subfields of $K$ such that $K_i \equiv GF(p^{r_i}), K_i \subset K_{i+1}, (i \geq 1)$ and $\bigcup_{i=1}^{\infty} K_i = K$. As $\lambda \neq \mu$, there exist a number $j \geq 1$ and an element $\alpha$ of $K_j$ such that $\lambda(\alpha) \neq \mu(\alpha)$. By Lemma 1.1, both $T = \langle \lambda(K_j^*) \rangle$ and $T' = \langle \mu(K_j^*) \rangle$ are isomorphic to $GR(p^{r_j}, r_j)$. As $S = \bigcup_{i=1}^{\infty} \langle \lambda(K_i^*) \rangle$, there exists a number $l \geq 1$ such that $T \cup T' \subset \langle \lambda(K_j^*) \rangle$. Since $\langle \lambda(K_j^*) \rangle$ is a Galois ring, $T \cap T'$ implies $T = T'$. The restriction $\pi_{T'}$, is a homomorphism of $T^*$ onto $K_j^*$. Both $\lambda|_{K_j^*}$ and $\mu|_{K_j^*}$ are right inverses of $\pi|_{K_j^*}$, so $T^*$ is the direct product of $\lambda(K_j^*)$ and $Ker(\pi|_{K_j^*}) = 1 + pT$, and is also the direct product of $\mu(K_j^*)$ and $1 + pT$. As $|K_j^*|$ and $|1 + pT|$ are coprime, we have $\lambda(K_j^*) = \mu(K_j^*)$. So there exists some $\beta \in K_j^*$ such that $\lambda(\alpha) = \mu(\beta)$. Then $\alpha = \pi^* \circ \lambda(\alpha) = \pi^* \circ \mu(\beta) = \beta$, which means $\lambda(\alpha) = \mu(\alpha)$. This contradicts our choice of $\alpha$.

By making use of Lemma 2.1 (I), we can easily see that, if $S$ is a coefficient subring of $R$, there exists a right inverse $\lambda: K^* \rightarrow S^*$ of $\pi^*$ such that $S = \langle \lambda(K^*) \rangle$.

Summarizing the above, we obtain the following theorem.

**THEOREM 2.3.** Let $R$ be a local ring with radical $M$. Assume that $M$ is nilpotent, and $K = R/M$ is a commutative field of characteristic $p$ ($p$ a prime) which is algebraic over $GR(p)$. Let $\pi^*: R^* \rightarrow K^*$
be the group homomorphism induced by the natural ring homomorphism $\pi : R \to K$. Then:

(I) If $S'$ is a coefficient subring of $R$, then there exists a $S'$-submodule $N$ of $R$ such that $R = S' \oplus N$ as left $S'$-modules.

(II) All coefficient subrings of $R$ are isomorphic.

(III) If $\lambda : K^* \to R^*$ is a right inverse of $\pi^*$, then $S = (\lambda(K))^+$ is a coefficient subring of $R$. Conversely, if $S$ is a coefficient subring of $R$, then there exists uniquely a right inverse $\lambda : K^* \to R^*$ of $\pi^*$ such that $S = (\lambda(K))^+$.

(IV) All coefficient subrings of $R$ are conjugate in $R$ if and only if $R^*$ has property (GC) with respect to $I + M$.

With the same notation as in Theorem 2.2, $M/M^2$ is regarded as a left $K$-space by the operation

$$\bar{a} \bar{x} = \bar{a} \bar{x}$$

THEOREM 2.4. Let $R$ be a local ring with radical $M$. Assume that $M$ is nilpotent, and $K = R/M$ is a commutative field of characteristic $p$ (a prime) which is algebraic over $GF(p)$. Let $S$ be a coefficient subring of $R$. Then $R$ is finitely generated as a left $S$-module if and only if $M/M^2$ is a finite dimensional left $K$-space. In this case, there exists a finitely generated left $S$-submodule $N$ of $M$ such that $R = S \oplus N$ as left $S$-modules, and there exists a nonincreasing sequence $n_1 \geq n_2 \geq \cdots \geq n_i$ of positive integers ($p^n$ is the characteristic of $R$) such that $R$ is isomorphic to a subring of $M (S,n_1,n_2,\ldots,n_i)$.

PROOF. Assume that $R$ is finitely generated as left $S$-module. Then $R$ is a Noetherian left $S$-module, since $S$ is a Noetherian ring by Proposition 1.2 (IV). As $M$ is a left $S$-submodule of $R$, $M$ is a finitely generated left $S$-module. This implies that $M/M^2$ is a finite dimensional left $K$-space.

Conversely, let us assume that $M/M^2$ is a finite dimensional left $K$-space. Let $\omega$ be the nilpotency index of $M$. Let $x_1, x_2, \ldots, x_\omega$ be elements of $M$ whose images modulo $M^2$ form a $K$-basis of $M/M^2$. As $S/pS$ is naturally isomorphic to $K$, any element $y$ of $M$ is written as

$$y = \sum_{i=1}^{\omega} a_i x_i + y' \quad (a_i \in S, y' \in M^2).$$

Let

$$z = \sum_{j=1}^{\omega} b_j x_j + z' \quad (b_j \in S, z' \in M^2)$$

be another element of $M$. Then

$$yz = \sum_{i,j=1}^{\omega} a_i b_j x_i x_j + w' \quad (w' \in M^3).$$

Each $x_i b_j$ is written as

$$x_i b_j = \sum_{k=1}^{\omega} c_{ij} x_k + w_{ij} \quad (c_{ij} \in S, w_{ij} \in M^2).$$

So we see that any element $v'$ of $M^2$ can be written as

$$v' = \sum_{i,j=1}^{\omega} a_i b_j x_i x_j + v'' \quad (a_i \in S, v'' \in M^3).$$

Continuing in this way, we see that any element of $M$ is written as an $S$-coefficient linear combination of distinct products of $\omega - 1$ or fewer $x_i$'s. So $M$ is a finitely generated left $S$-module. Also $K = R/M$ is a finitely generated left $S$-module, hence $R$ is a finitely generated left $S$-module.

Now suppose that $R$ is finitely generated as left $S$-module. By Theorem 2.3 (I), there exists a finitely generated left $S$-submodule $N'$ of $R$ such that $R = S \oplus N'$ as left $S$-modules. By Proposition 1.2 (III), there exist a discrete valuation ring $V$ and a homomorphism $\xi$ of $V$ onto $S$. Defining $ay = \xi(a)y$ ($a \in V, y \in N'$), we can regard $N'$ as a left $V$-module. Then there exist $x_1, x_2, \ldots, x_\omega \in N'$
such that \( N' = \bigoplus_{i=1}^{t} Vx_{i} = \bigoplus_{i=1}^{t} Sx_{i} \). By putting \( x_{0} = 1 \), we get \( R = \bigoplus_{i=1}^{t} Sx_{i} \). Let \( c_{1}, c_{2}, \ldots, c_{t} \) be elements of \( S \) such that \( \overline{c}_{i} = x_{i} \) under the natural homomorphism \( \pi : R \rightarrow K \). Let us put \( y_{0} = 1 \) and \( y_{i} = x_{i} - c_{i} \), for \( 1 \leq i \leq t \). Then \( y_{i} \in M(1 \leq i \leq t) \) and \( R = \bigoplus_{i=1}^{t} Sx_{i} = \bigoplus_{i=0}^{t} Sy_{i} \). So \( N = \bigoplus_{i=1}^{t} Sy_{i} \) has the desired property. The last statement is immediate from Lemma 1.3.

3.

Let \( R \) be a local ring described in Theorem 2.2. Then \( R \) may have more than one coefficient subring. Concerning this subject, first we can state the following.

**Theorem 3.1.** Let \( T \) be an IG-ring of characteristic \( p^{n} \) different from \( GR(p^{n}, 1) \). Then, for any infinite cardinal number \( \chi \), there exists a local ring \( R \) such that

1. \( M = J(R) \) is nilpotent,
2. \( K = R/M \) is a commutative field of characteristic \( p \) (\( p \) a prime) which is algebraic over \( GF(p) \),
3. coefficient subrings of \( R \) are isomorphic to \( T \),
4. all coefficient subrings of \( R \) are conjugate in \( R \), and
5. \( \chi \) is the number of all coefficient subrings of \( R \).

**Proof.** Let \( T = \bigcup_{i=1}^{\infty} GR(p^{n}, r_{i}) \), where \( \{r_{i}\}_{i=1}^{\infty} \) is a sequence of positive integers such that \( r_{i} \mid r_{i+1} \), \( (i \geq 1) \). Let \( K = T/pT \) and \( \pi' : T \rightarrow K \) be the natural homomorphism. As \( K \) is an extension of \( GF(p) \), there exists an automorphism \( \sigma \) of \( K \) different from \( id_{K} \). Let \( \sigma \) be the automorphism of \( T \) which induces \( \overline{\sigma} \) modulo \( pT \) (see Proposition 1.2 (VI)). Let \( A \) be a set of cardinality \( \chi \), and \( V = \bigoplus_{a \in A} T \) be a free \( T \)-module. The abelian group \( T \otimes V \) together with the multiplication

\[
(a, x)(a', x') = (aa', ax + (a')x)
\]

forms a ring, which we denote by \( R \). Let \( \pi : R \rightarrow K \) be the homomorphism defined by \( (a, x) \mapsto \pi'(a) \), and \( M = Ker \pi \). As \( R/M \cong K \) and \( M^{n+1} = 0 \), \( R \) is a local ring with radical \( M \) whose residue field is \( K \).

By Theorem 2.3 (III), there exists a one-to-one correspondence between the set of all coefficient subrings of \( R \) and the set \( Y \) of all right inverses of \( \pi \). By the embedding \( T \ni a \mapsto (a, 0) \in R \), \( T \) is regarded as a coefficient subring of \( R \). So, by Theorem 2.3 (III), there exists a right inverse \( \lambda : K \rightarrow R^{*} \) of \( \pi \) such that \( (\lambda(K)) = T \). Since \( K = \bigcup_{i=1}^{\infty} GF(p^{i}) \), there exists a number \( j \geq 1 \) such that \( \overline{\sigma} \) is not the identity on \( GF(p^{i}) \). Let \( \gamma \) be a generator of \( GF(p^{i})^{*} \), and \( c = \lambda(\gamma) \). It is easy to see that, for any \( z \in V \), \( R^{*} \ni h = (c, z) \) is of multiplicative order \( p^{i} - 1 \). So, for each \( z \in V \), we can define a group homomorphism

\[
\mu_{z} : GF(p^{i})^{*} \rightarrow R^{*} \text{ by } \gamma \mapsto (c, z).
\]

By Lemma 2.1 (II), we can extend \( \mu_{z} \) to \( \mu_{z} \in Y \). If \( V \ni z_{1}, z_{2} \) and \( z_{1} \neq z_{2} \), then \( \mu_{z_{1}} \neq \mu_{z_{2}} \). So \( |Y| \geq |V| = \chi \).

Let \( S \) be a coefficient subring of \( R \). We shall show that \( S \) is conjugate to \( T \). By Theorem 2.3 (III), there exists a right inverse \( \lambda : K \rightarrow R^{*} \) of \( \pi \) such that \( S = (\lambda(K)) \). Let \( \lambda(\gamma) = (c', z) \), where \( c' \in T \) and \( z \in V \). Let \( U \) be the finite subgroup of \( R^{*} \) generated by \( \lambda(\gamma) \) and \( \lambda'(\gamma) \). As the restriction \( \pi_{|U} \) is a homomorphism of \( U \) onto \( GF(p^{i})^{*} \), by Schur-Zassenhaus theorem, there exists \( (b, w) \in R^{*} \) \( (b \in T, w \in V) \) and an integer \( i \) such that \( \lambda'(\gamma) = (b, w)^{-1}\lambda(\gamma)(b, w) \). Then, \( (c', z) = (b, w)^{-1}(c', 0)(b, w) \), which implies \( c' = c' \). As \( \pi(c') = \pi(\lambda'(\gamma)) = \gamma = \pi(\lambda(\gamma)) = \pi(c) \), so \( c' = c \) and \( \lambda'(\gamma) = (c, z) \). Let \( x = (c - \sigma(c))^{-1}z \). Suppose that \( \alpha \in K \) satisfies \( \alpha^{\gamma} = \gamma \) for some integer \( m \). Let \( \lambda(\alpha) = a \). Then, by the same reason as above, we can write \( \lambda(\alpha) = (a, y) \) for some \( y \in V \).
As
\[(c, z) = \lambda'(\gamma) = \lambda'(\alpha^n) = (a, y)^n = (a^n, (a^n - (\sigma(a))^n) \{a - \sigma(a)\}^{-1} y),\]
we get \(c = a^n\) and \(z = (c - \sigma(c)) \{a - \sigma(a)\}^{-1} y\). So \((1, x) \lambda'(\alpha) = (a, y + \sigma(a)x) = (a, ax) = \lambda(\alpha)(1, x)\).

As \(K^*\) is the union of cyclic subgroups generated by such \(\alpha\) which contain \(GF(p')^*\) (generated by \(\gamma\), this proves \(S = \langle \lambda'(K^*) \rangle = (1, x)^{\lambda(\gamma)}(1, x)\). So \(|Y|\), the number of all coefficient subrings of \(R\), does not exceed \(\chi\). As we have seen \(|Y| \geq \chi\), we get \(|Y| = \chi\).

Next we shall consider the uniqueness of coefficient subrings.

A finite local ring \(T\) is called of type \((1)\) if \(T\) is generated by two units \(a\) and \(b\) such that
\[(1) \ ab \neq ba,\]
\[(2) \ a - b \in J(T), \text{ and} \]
\[(3) \ \sigma(a) = \sigma(b) = |T/J(T)| - 1.\]

If \(T\) is a finite local ring of type \((1)\), then \(T^*\) is not a nilpotent group. For, let us suppose that \(T\) is a finite local ring of type \((1)\). Let \(a\) and \(b\) be generators of \(T\) satisfying \((1)-(3).\) Let \(A\) and \(B\) be cyclic subgroups of \(T^*\) generated by \(a\) and \(b\) respectively. Let \(K = T/J(T) = GF(p').\) Then \(|A| = |B| = p' - 1\) is coprime to \(|J(T)|.\) If \(T^*\) is nilpotent, then \(A = B\), as both \(A\) and \(B\) are complement subgroups of \(1 + J(T)\) in \(T^*.\) This contradicts \((1)\), so we see that \(T^*\) is not nilpotent.

**THEOREM 3.2.** Let \(R\) be a local ring with radical \(M.\) Assume that \(M\) is nilpotent, and \(K = R/M\) is a commutative field of characteristic \(p\) \((p\ a\ prime)\) which is algebraic over \(GF(p).\) Then the following are equivalent.

(i) \(R\) has a unique coefficient subring.

(ii) \(R^*\) is a nilpotent group.

(iii) \(R^*\) is isomorphic to the direct product of \(K^*\) and \(1 + M.\)

(iv) \(R^*\) has no finite local subring of type \((1)\).

**PROOF.** (i) \(\Leftrightarrow\) (ii). Clear from Lemma 2.1 (III) and Theorem 2.3 (III).

(i) \(\Rightarrow\) (iii). Let \(\pi^* = \pi^*_{1*} : R^* \rightarrow K^*\) be the group homomorphism induced by the natural homomorphism \(\pi : R \rightarrow K.\) Since \(R\) has a unique coefficient subring, by Theorem 2.3 (III), there exists a unique right inverse \(\lambda\) of \(\pi^*.\) Then \(R^*\) is a semidirect product of \(1 + M\) and \(K^*.\) Let \(z\) be any fixed element of \(1 + M.\) The mapping \(\mu : K^* \rightarrow R^*\) defined by \(K^* \ni \alpha \mapsto z^{-1}\lambda(\alpha)z\) is a right inverse of \(\pi^*,\) so \(\mu = \lambda\) by our hypothesis. This implies that each element of \(\lambda(K^*)\) commutes with each element of \(1 + M.\) Hence \(R^*\) is the direct product of \(1 + M\) and \(\lambda(K^*).\)

(iii) \(\Rightarrow\) (iv). Let us suppose that \(R\) contains a finite local subring \(U\) of type \((1)\). By the proof of [10, Lemma 1], \(1 + M\) is a nilpotent group. If \(R^*\) is isomorphic to the direct product of \(K^*\) and \(1 + M,\) then \(R^*\) is nilpotent. So \(U^*\) is nilpotent, which is a contradiction.

(iv) \(\Rightarrow\) (i). Assume that \(R\) has at least two different coefficient subrings. Then there exist at least two different right inverses \(\lambda\ and \(\mu\ of \(\pi^*.\) Let \(\{K_j\}_{j=1}^{\infty}\) be a sequence of finite subfields of \(K\) such that \(K_j \subset K_{j+1}\) and \(\cup_{j=1}^{\infty} K_j = K.\) There exists a number \(j\) such that \(\lambda |_{K_j} \neq \mu |_{K_j}.\) Let \(\gamma\) be a generator of \(K^*_j.\) Then the subring \((\lambda(\gamma), \mu(\gamma))\) of \(R\) is a finite local ring of type \((1).\)

4.

From [9, p. 373, Theorem XIX.4 (b)] and the proof of Theorem 3.1, one may expect that, in Theorem 2.3, any two coefficient subrings of \(R\) are always conjugate. However, from the following example, we see that this is incorrect.
Let $K = \bigcup_{i=1}^{\infty} GF(p^i)$, where $\{r_i\}_{i=1}^{\infty}$ is a strictly increasing sequence of positive integers such that $r_i | r_{i+1}$ ($i \geq 1$). Let $\{\sigma_i\}_{i=1}^{\infty}$ be automorphisms of $K$ such that $\sigma_i$ is not the identity on $GF(p^i)$ ($i \geq 1$) and, for $j < i$, $\sigma_j$ is the identity on $GF(p^i)$. Let $V = \bigoplus_{i=1}^{\infty} Kx_i$ be a left $K$-vector space with basis $\{x_i\}_{i=1}^{\infty}$. We can regard $V$ as a $(K,K)$-bimodule by defining

$$(a,x)(c,y) = \sum c, \sigma_i(a)x_i \in V, a \in K.$$

The abelian group $R = K \oplus V$ together with the multiplication

$$(a,y)(b,z) = (ab, az + yb) \ (a,b \in K, y,z \in V)$$

forms a local ring with radical $M = (0,V)$, which satisfies the assumption of Theorem 2.3. The homomorphism $\pi: R \to K$ defined by $(a,x) \mapsto a$ gives the isomorphism $R/M \cong K$. The subring $S = \{(a,0) \mid a \in K\}$ of $R$ is a coefficient subring of $R$.

For each $i \geq 1$, let $\gamma_i$ be a generator of $GF(p^i)^*$. Then we can write $\gamma_i^{m_i}$ for a suitable integer $m_i$. We shall define elements $\{u_i\}_{i=1}^{\infty}$ of $R^*$ inductively as follows: Let $u_1 = (\gamma_1, x_1)$. For $u_n = (\gamma_n, \sum_{j=1}^{n-1} r_j x_j)$ ($r_j \in K$), let

$$a_j = (\gamma_n - \sigma_j(\gamma_n))^{-1} (\gamma_{n+1} - \sigma_j(\gamma_{n+1}))r_j \quad (1 \leq j \leq n)$$

and

$$u_{n+1} = (\gamma_{n+1}, \sum_{j=1}^{n} a_j x_j + x_{n+1}).$$

Then it is easy to check that $\sigma(u_n) = p^n - 1$ and $u_n = u_{n+1}^{-1}$. Let $f: GF(p^i)^* \to R^*$ be defined by $\gamma_i^{m_i} \mapsto u_i$ ($t \in Z$). Since $f_{|GF(p^i)^*} = f_j$ for $j \leq i$, there exists $f = \lim_{i \to \infty} f_i : K^* \to R^*$. As $f$ is a right inverse of $\pi^*: \pi^*: R^* \to K^*$, so $S = \{f(K^*)\}$ is a coefficient subring of $R$.

We shall show that $S_1$ and $S$ are not conjugate in $R$. Let us suppose that there exists an element $v = (s, \sum d_j x_j) \in R^*$ ($s \in K^*, d_j \in K$) such that $S_1 = v^{-1} S v$. Then, for each $i \geq 1$, there exists some $b_i \in K^*$ such that $f(\gamma_i) = v^{-1}(b_i,0)v$. Then,

$$u_i = (\gamma_i, \sum_{j=1}^{i-1} r_j' x_j + x_i) \ (r_j' \in K)$$

$$= v^{-1}(b_i,0)v$$

$$= (s^{-1}, s^{-1}(\sum d_j x_j) s^{-1}) (b_i,0) (s, \sum d_j x_j)$$

$$= (b_i, \sum_{j=1}^{i-1} (s^{-1} b_j d_j - s^{-1} d_j \sigma_j(b_j)) x_j),$$

which yields

$$1 = s^{-1} (b_i - \sigma_i(b_i)) d_i.$$

So, for any $i \geq 1$, we see $d_i \neq 0$. This contradicts that $\sum d_j x_j$ is an element of the direct sum $V = \bigoplus_{i=1}^{\infty} Kx_i$.

In conclusion, we shall state a theorem which is a generalization of [3, Theorem].

**THEOREM 4.1.** (cf [9, p. 376, Theorem XIX.5] and [4, p. 491, Theorem 72.19]) Let $R$ be a ring with 1. Assume that $J(R)$ is nilpotent. Let

$$R/J(R) = (K_1)_{n_1 \times n_1} \oplus (K_2)_{n_2 \times n_2} \oplus \ldots \oplus (K_d)_{n_d \times n_d},$$

where each $K_i (1 \leq i \leq d)$ is a commutative field of characteristic $p$ ($p$ a prime) which is algebraic over $GF(p)$. Then there exists a subring $T$ of $R$ which satisfies the following.
(i) \( R = T \oplus N \) (as abelian groups), where \( N \) is an additive subgroup of \( R \).

(ii) \( T \) is isomorphic to a finite direct sum of matrix rings over IG-rings.

(iii) \( J(T) = T \cap J(R) = pT \).

(iv) \( T/pT \) is naturally isomorphic to \( R/J(R) \).

Moreover, if \( T' \) is another subring of \( R \) satisfying (ii)-(iv), then \( T' \) is isomorphic to \( T \).

**Proof.** Let \( \overline{R} = R/J(R) = \overline{Re_1} \oplus \overline{Re_2} \oplus \ldots \oplus \overline{Re_d} \), where each \( \overline{Re_i} \) (\( 1 \leq i \leq d \)) is a simple component of \( \overline{R} \) and \( \overline{e} \) is a central idempotent of \( \overline{R} \). Let \( \overline{Re_i} = (K_{i})_{n \times n} \), where \( K_{i} \) is a commutative field which is algebraic over \( GF(p) \). Let \( \pi: R \to \overline{R} \) be the natural homomorphism. There are mutually orthogonal idempotents \( e_1, e_2, \ldots, e_d \) of \( R \) such that \( e_1 + e_2 + \ldots + e_d = 1 \) and \( \pi(e_i) = \overline{e_i} \) (\( 1 \leq i \leq d \)). Then,

\[
R = e_1 Re_1 \oplus e_2 Re_2 \oplus \ldots \oplus e_d Re_d \oplus (\oplus_{1 \leq i \leq d} e_i Re_i)
\]
as abelian groups. Since each \( e_i Re_i \) is semiperfect and \( e_i Re_i/J(e_i Re_i) \equiv \overline{Re_i} = (K_{i})_{n \times n} \), there exist a local ring \( S \), and an isomorphism \( \phi \) of \( e_i Re_i \) onto \( (S_{i})_{n \times n} \) (see, for instance, [1, p. 160, Theorem 21]). Let

\[
\phi = \phi_1 + \phi_2 + \ldots + \phi_d : e_1 Re_1 \oplus e_2 Re_2 \oplus \ldots \oplus e_d Re_d \to \bigoplus_{1 \leq i \leq d} (S_{i})_{n \times n}
\]
be the isomorphism. Since \( S_i/J(S_i) \equiv K_i \), by Theorem 2.2 and Theorem 2.3 (i), there exist an IG-subring \( T_i \) and a left \( T_i \)-submodule \( N_i \) of \( S_i \) such that \( S_i = T_i \oplus N_i \) (as abelian groups), and \( T_i/pT_i \) is naturally isomorphic to \( S_i/J(S_i) \). Then

\[
B = (T_1)_{n \times n_1} \oplus (T_2)_{n \times n_2} \oplus \ldots \oplus (T_d)_{n \times n_d}
\]
is a subring of \( A \). Let \( T = \phi^{-1}(B) \). As \( J(e_i Re_i) \cap \phi^{-1}((T_i)_{n \times n_i}) = J\phi^{-1}((T_i)_{n \times n_i}) \), we see \( J(t) = T \cap J(R) = pT \) and that \( T/pT \) is naturally isomorphic to

\[
(e_1 Re_1 \oplus e_2 Re_2 \oplus \ldots \oplus e_d Re_d)/J(e_1 Re_1 \oplus e_2 Re_2 \oplus \ldots \oplus e_d Re_d) = R/J(R).
\]

Let us put

\[
N = \phi^{-1}\left( (N_1)_{n \times n_1} \oplus (N_2)_{n \times n_2} \oplus \ldots \oplus (N_d)_{n \times n_d} \right) \oplus \{ \oplus_{1 \leq i \leq d} e_i Re_i \}.
\]
Then we see \( R = T \oplus N \).

Now, let us suppose that \( T' \) is a subring of \( R \) satisfying (ii)-(iv). Let \( e \) and \( f \) be primitive idempotents of \( T' \). We claim that \( Re \equiv Rf \) (as left \( R \)-modules) if and only if \( T'e \equiv T'f \) (as left \( T' \)-modules). Let \( \pi(e) = \overline{e} \) and \( \pi(f) = \overline{f} \). Assume that \( Re \equiv Rf \). Then \( \overline{Re} = \overline{Rf} \) as left \( \overline{R} \)-modules. Both \( \overline{Re} \) and \( \overline{Rf} \) are minimal left ideals of \( \overline{R} \), so they are contained in the same simple component of \( \overline{R} \), which implies that \( J(R) \) does not include \( eRef \). Conversely, if \( J(R) \) does not include \( eRef \), then \( \overline{Re} = \overline{Rf} \), which means \( Re \equiv Rf \) (see, for instance, [1, p. 158, Theorem 16]). Thus we see that \( Re \equiv Rf \) (as left \( R \)-modules) if and only if \( J(R) \) does not include \( eRef \). Similarly, \( T'e \equiv T'f \) (as left \( T' \)-modules) if and only if \( J(T') \equiv pT' \) does not include \( eT'f \). Since \( T'/pT' \) is naturally isomorphic to \( R/J(R) \), \( J(R) \) include \( eRf \) if and only if \( pT' \) includes \( eT'f \). So we see that \( Re \equiv Rf \) (as left \( R \)-modules) if and only if \( T'e \equiv T'f \) (as left \( T' \)-modules).

By making use of matrix units, 1 of \( R \) is written in \( T \) as

\[
1 = (e_{11} + e_{12} + \ldots + e_{1n}) + (e_{21} + e_{22} + \ldots + e_{2n}) + \ldots + (e_{d1} + e_{d2} + \ldots + e_{dn}),
\]
where \( e_{ii} \) are mutually orthogonal primitive idempotents of \( T \), and \( Te_{ii} \equiv Te_{ij} \) (as left \( T \)-modules) if and
only if \( k = l \). Similarly,
\[
1 = (f_{11} + f_{12} + \ldots + f_{1m_1}) + (f_{21} + f_{22} + \ldots + f_{2m_2}) + \ldots + (f_{l1} + f_{l2} + \ldots + f_{lm_l}),
\]
where \( f_{ij} \) are mutually orthogonal primitive idempotents of \( T' \), and \( T'f_{ij} \equiv Tf_{ij} \) (as left \( T' \)-modules) if and only if \( k = l \).

As \( e_i T e_i/p e_i T e_i \equiv e_i R e_i/e_i J(R)e_i \), we see that \( e_i \) and \( f_i \) are primitive idempotents of \( R \). Then \( R \equiv \bigoplus R e_i = \bigoplus R f_i \) are indecomposable decompositions.

By what was stated above, Krull-Schmidt theorem tells us that there exists a permutation \( \sigma \) of \( \{1, 2, \ldots, d\} \) such that \( n_i = m_{\sigma(i)} \) and \( R e_{i\sigma(i)} \equiv R f_{i\sigma(i)} \) as left \( R \)-modules \( (1 \leq i \leq d, 1 \leq k, l \leq n_i) \). By renumbering, we may assume \( n_i = m_i \) and \( R e_{i\sigma(i)} \equiv R f_{i\sigma(i)} \) \((1 \leq i \leq d, 1 \leq k, l \leq n_i) \). Now,
\[
T \equiv (e_{i_1} T e_{i_1})_{n_1 \times n_1} \oplus (e_{i_2} T e_{i_2})_{n_2 \times n_2} \oplus \ldots \oplus (e_{i_d} T e_{i_d})_{n_d \times n_d},
\]
and
\[
T' \equiv (f_{i_1} T' f_{i_1})_{n_1 \times n_1} \oplus (f_{i_2} T' f_{i_2})_{n_2 \times n_2} \oplus \ldots \oplus (f_{i_d} T' f_{i_d})_{n_d \times n_d},
\]
where \( e_{i_1} T e_{i_1} \) and \( f_{i_1} T' f_{i_1} \) are IG-rings. Hence, to complete the proof it will suffice to show \( e_{i_1} T e_{i_1} \equiv f_{i_1} T' f_{i_1} \).

As \( e_{i_1} T e_{i_1} \) is an IG-ring which is naturally isomorphic to \( e_{i_1} R e_{i_1}/e_{i_1} J(R)e_{i_1} \), so \( e_{i_1} T e_{i_1} \) is a coefficient subring of \( e_{i_1} R e_{i_1} \). Similarly, \( f_{i_1} T' f_{i_1} \) is a coefficient subring of \( f_{i_1} R f_{i_1} \). As \( e_{i_1} R e_{i_1} \equiv \text{End}(q R e_{i_1}) \equiv \text{End}(q R f_{i_1}) \equiv f_{i_1} R f_{i_1} \), we see \( e_{i_1} T e_{i_1} \equiv f_{i_1} T' f_{i_1} \) by Theorem 2.3 (II).

Note. It is unknown when the subring \( T \) of Theorem 4.1 is unique up to inner automorphism of \( R \) (see [3, Problem].

**ACKNOWLEDGEMENT.** The author would like to express his indebtedness and gratitude to Prof. Y. Hirano and Dr. H. Komatsu for their helpful suggestions and valuable comments.

**REFERENCES**
