Internat. J. Math. & Math. Sci.
VOL. 18 NO. 3 (1995) 451-462

COEFFICIENT SUBRINGS OF CERTAIN LOCAL RINGS WITH PRIME-POWER CHARACTERISTIC

TAKAO SUMIYAMA

Department of Mathematics
Aichi Institute of Technology
Yakusa-chô, 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 $S = \cup_{i=1}^{\infty} S_i$, 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 $\mathbf{Z}/p^n\mathbf{Z}$, 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 $\overline{R} = R/J(R)$ 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 $GF(p^r)$, 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, $\langle S \rangle$ 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 $(\mathbf{Z}/p^n\mathbf{Z})[X]/(f(X)(\mathbf{Z}/p^n\mathbf{Z})[X])$, where $f(X) \in (\mathbf{Z}/p^n\mathbf{Z})[X]$ is a monic polynomial of degree r, and is irreducible modulo $p\mathbf{Z}/p^n\mathbf{Z}$ (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 $GF(p^r)$. If $a \in R^*$ satisfies $o(a) = p^r - 1$, then the subring $\langle a \rangle$ 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 $R = \cup_{i=1}^{\infty} R_i$, 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 $R = \cup_{i=1}^{\infty} GR(p^n, r_i)$.

Let p be a prime, n a positive integer and $1 = r_1 \leq r_2 \leq \ldots$ 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 $\iota_i^{i+1} : GR(p^n, r_i) \to GR(p^n, r_{i+1})$ for each $i \geq 1$. Let us put $\iota_i^i = id_{GR(p^n, r_i)}$ and $\iota_i^j = \iota_{j-1}^j \circ \iota_{j-2}^{j-1} \circ \ldots \circ \iota_i^{i+1}$ for $1 \leq i \leq j$. Then we see that $\{GR(p^n, r_i), \iota_i^j\}$ is an inductive system. The ring $R = \lim_{\rightarrow} GR(p^n, r_i)$ is an IG-ring. Conversely, any IG-ring can be constructed in this way. An IG-ring $R = \cup_{i=1}^{\infty} GR(p^n, r_i)$ 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 $R = \cup_{i=1}^{\infty} GR(p^n, r_i)$ be an IG-ring. Then:

(I) R is a commutative local ring with radical $J(R) = pR$. The residue field R/pR is $\cup_{i=1}^{\infty} GF(p^{r_i})$.

(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 $\cup_{i=1}^{\infty} GR(p^e, r_i)$.

(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) $Aut(R) \cong \lim_{\leftarrow} Aut(GR(p^n, r_i)) \cong \lim_{\leftarrow} Aut(GF(p^{r_i})) \cong Aut\left(\cup_{i=1}^{\infty} GF(p^{r_i})\right)$.

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

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

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 $K = \cup_{i=1}^{\infty} GF(p^{r_i})$. 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 $\{W_n(K)\}_{i=1}^{\infty}$ (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 $\{r_l\}_{l=1}^{\infty}$ be an infinite sequence of positive integers such that $r_1 = 1$ and $r_l \mid r_{l+1} (l \geq 1)$, and $S = \cup_{l=1}^{\infty} GR(p^n, r_l)$ be an IG-ring of characteristic p^n. Let $n = n_1 \geq n_2 \geq \ldots \geq n_t$ be a nonincreasing sequence of positive integers. Let us put $S_j = \cup_{l=1}^{\infty} GR\left(p^{n_j}, r_l\right)$ for $1 \leq j \leq t$. Let $\phi_j : S \to S_j$ be the natural homomorphism followed by the isomorphism $S/p^{n_j}S \cong S_j$ of Proposition 1.2 (II). Let us put $U(S;n_1,n_2,\ldots,n_t) = \{(\alpha_{ij}) \in (S)_{t\times t} \mid \alpha_{ij} \in p^{n_j - n_i}S \text{ if } i > j\}$. It is easy to see that $U(S;n_1,n_2,\ldots,n_t)$ forms a subring of $(S)_{t\times t}$. 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 $a_{ij} \in p^{n_j - n_i}S_j$ for $i > j$. Let Φ 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 $(\alpha_{ij}) \mapsto (a_{ij})$ where $a_{ij} = \phi_j(\alpha_{ij})$. 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 Φ 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^n. 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 are a discrete valuation ring W and a homomorphism ϕ of W onto S. By defining

$$ay = \phi(a)y \quad (a \in W, y \in N),$$

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 $N = \oplus_{i=1}^{s} Wy_i$. Let $t = s + 1$, $x_1 = 1$ and $x_i = y_{i-1} (2 \leq i \leq t)$. Then we get $R = \oplus_{i=1}^{t} Sx_i$. Let $Sx_i \cong S/p^{n_i}S$ 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

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

Since

$$0 = p^{n_i} x_i a = \textstyle\sum_{j=1}^{n} p^{n_i} \alpha_{ij} x_j ,$$

by Proposition 1.2 (IV), $\alpha_{ij} \in p^{n_j - n_i}S$ if $i > j$. As α_{ij} is uniquely determined modulo $p^{n_j}S$ by a, we can define $\psi : R \to M(S;n_1,n_2,\ldots,n_t)$ by $a \mapsto (\psi_j(\alpha_{ij}))$. It is easy to see that ψ 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 ρ if $\rho \circ \lambda = id_H$. If λ is a right inverse of ρ, 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 $H_i \subset H_{i+1} (i \geq 1), \cup_{i=1}^{\infty} H_i = H$ 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 ρ.

(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 ρ such that $\mu |_{H_m} = \mu'$.

(III) There exists a unique right inverse of ρ 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 $x \in H_1$, 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 $\{g_y'\}_{y \in H_2}$ be a set of elements of G such that $\rho(g_y') = y$ for any $y \in H_2$, and $\{g_x\}_{x \in H_1} \subset \{g_y'\}_{y \in H_2}$. Let G_2 be the finite subgroup of G generated by $\{g_y'\}_{y \in H_2}$. 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 $L \supset \lambda_1(H_1)$. The mapping $\lambda_2 : H_2 \to G_2$ defined by $H_2 = G_2/N_2 \ni bN_2 \mapsto b (b \in L)$ is a right inverse of $\rho |_{G_2}$. For any $a \in H_1$, $\lambda_2(a)^{-1}\lambda_1(a) \in N_2 \cap L = \{1\}$, hence we see $\lambda_2 |_{H_1} = \lambda_1$. Continuing this process inductively, we get a sequence $G_1 \subset G_2 \subset \ldots$ 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 $\lambda_j |_{H_i} = \lambda_i$ for any $1 \leq i \leq j$. Then $\lambda = \lim_{\to} \lambda_i : H = \cup_{i=1}^{\infty} H_i \to G$ is a right inverse of ρ.

(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 ρ. 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 $\mu(b) = z^{-1}\lambda(b)z$. Then μ is a right inverse of ρ different from λ, 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 λ and μ are right inverses of ρ. For each $i \geq 1$, let G_i be the subgroup of G generated by $\lambda(H_i) \cup \mu(H_i)$. 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 μ and ν of ρ, $\mu(H)$ 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 $K_i \subset K_{i+1} (i \geq 1)$ and $\cup_{i=1}^{\infty} K_i = K$. Let $K_i = GR(p^{r_i})$. The natural homomorphism $\pi : R \to K$ induces a group homomorphism $\pi^* = \pi|_{R^*}$ of R^* onto K^*. Each $(1 + M^i)/(1 + M^{i+1})$ is isomorphic to the additive group M^i/M^{i+1}. As $pM^i \subset M^{i+1}$, the order of each element of $1 + M = Ker\pi^*$ is a power of p. Furthermore, $K^* = \cup_{i=1}^{\infty} K_i^*$, where $|K_i^*| = p^{r_i} - 1$ is coprime to p. So, by Lemma 2.1 (I), there exists a right inverse $\lambda : K^* \to R^*$ of π^*. For each $i \geq 1$, let α_i be a generator of K_i^*. By Lemma 1.1, the subring $S_i = \langle \lambda(\alpha_i) \rangle$ of R is isomorphic to $GR(p^n, r_i)$, where p^n is the characteristic of R. Consequently, $S = \langle \lambda(K^*) \rangle = \cup_{i=1}^{\infty} S_i$ 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 $K = \cup_{i=1}^{\infty} GF(p^{r_i})$ be as in Theorem 2.2, where $\{r_i\}_{i=1}^{\infty}$ is a sequence of positive integers such that $r_i \mid r_{i+1} (i \geq 1)$. Let p^n be the characteristic of R. Let S' be another coefficient subring of R. From what was stated in §1, $S' \cong \cup_{i=1}^{\infty} GR(p^n, r_i)$, 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 $\lambda : K^* \to R^*$ is a right inverse of π^*, then by the proof of Theorem 2.3, $S = \langle \lambda(K^*) \rangle$ is a coefficient subring of R.

We shall show that, if λ and μ are different right inverses of π^*, 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 $K_i \cong GF(p^{r_i})$, $K_i \subset K_{i+1} (i \geq 1)$ and $\cup_{i=1}^{\infty} K_i = K$. As $\lambda \neq \mu$, there exist a number $j \geq 1$ and an element α 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 $GR(p^n, r_j)$. As $S = \cup_{i=1}^{\infty} \langle \lambda(K_i^*) \rangle$, there exists a number $l \geq 1$ such that $T \cup T' \subset \langle \lambda(K_l^*) \rangle$. Since $\langle \lambda(K_l^*) \rangle$ is a Galois ring, $T \cong T'$ 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 $\pi|_{T^*}$, so T^* is the direct product of $\lambda(K_j^*)$ and $Ker(\pi|_{T^*}) = 1 + pT$, 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 α.

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 $\lambda : K^* \to S^*$ of π^* 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 $\pi^* : R^* \to K^*$

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 π^*, then $S = \langle \lambda(K^*) \rangle$ 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 π^* such that $S = \langle \lambda(K^*) \rangle$.

(IV) All coefficient subrings of R are conjugate in R if and only if R^* has property (GC) with respect to $1 + M$.

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

$$\overline{a}\,\overline{x} = \overline{ax} \ (\overline{a} \in K = R/M, \overline{x} \in M/M^2) .$$

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 (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 $n_1 \geq n_2 \geq \ldots \geq n_t$ of positive integers (p^{n_1} is the characteristic of R) such that R is isomorphic to a subring of M $(S; n_1, n_2, \ldots, n_t)$.

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 ω be the nilpotency index of M. Let $x_1, x_2, \ldots, x_d$ 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 of y of M is written as

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

Let

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

be another element of M. Then

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

Each $x_i b_j$ is written as

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

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

$$v' = \textstyle\sum_{i,j=1}^{d} a_{ij} x_i x_j + v'' \quad (a_{ij} \in S, v'' \in M^3) .$$

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 ξ 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 $x_1, x_2, \ldots, x_t \in N'$

such that $N' = \oplus_{i=1}^{t} V x_i = \oplus_{i=1}^{t} S x_i$. By putting $x_0 = 1$, we get $R = \oplus_{i=0}^{t} S x_i$. Let $c_1, c_2, \ldots, c_t$ be elements of S such that $\bar{c}_i = \bar{x}_i$ under the natural homomorphism $\pi : R \to K$. Let us put $y_0 = 1$ and $y_i = x_i - c_i$ for $1 \le i \le t$. Then $y_i \in M (1 \le i \le t)$ and $R = \oplus_{i=0}^{t} S x_i = \oplus_{i=0}^{t} S y_i$. So $N = \oplus_{i=1}^{t} S y_i$ 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 χ, 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) χ is the number of all coefficient subrings of R.

PROOF. Let $T = \cup_{i=1}^{\infty} GR(p^n, r_i)$, where $\{r_i\}_{i=1}^{\infty}$ is a sequence of positive integers such that $r_i \mid r_{i+1} (i \ge 1)$. Let $K = T/pT$ and $\pi' : T \to K$ be the natural homomorphism. As K is a proper extension of $GF(p)$, there exists an automorphism $\bar{\sigma}$ of K different from id_K. Let σ be the automorphism of T which induces $\bar{\sigma}$ modulo pT (see Proposition 1.2 (VI)). Let A be a set of cardinality χ, and $V = \oplus_{\alpha \in A} T$ be a free T-module. The abelian group $T \oplus V$ together with the multiplication

$$(a, x)(a', x') = (aa', ax' + \sigma(a')x)$$

forms a ring, which we denote by R. Let $\pi : R \to K$ 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 $\pi^* = \pi|_{R^*} : R^* \to K^*$.

By the embedding $T \ni a \to (a, 0) \in R$, T is regarded as a coefficient subring of R. So, by Theorem 2.3 (III), there exists a right inverse $\lambda : K^* \to R^*$ of π^* such that $\langle \lambda(K^*) \rangle = T$. Since $K = \cup_{i=1}^{\infty} GF(p^{r_i})$, there exists a number $j \ge 1$ such that $\bar{\sigma}$ is not the identity on $GF(p^{r_j})$. Let γ be a generator of $GF(p^{r_j})^*$, and $c = \lambda(\gamma)$. It is easy to see that, for any $z \in V$, $R^* \ni h = (c, z)$ is of multiplicative order $p^{r_j} - 1$. So, for each $z \in V$, we can define a group homomorphism

$\mu_z' : GF(p^{r_j})^* \to R^*$ by $\gamma^i \mapsto (c, z)^i$. By Lemma 2.1 (II), we can extend μ_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 $|Y| \ge |V| = \chi$.

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 $\lambda' : K^* \to R^*$ of π^* such that $S = \langle \lambda'(K^*) \rangle$. 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 $GF(p^{r_j})^*$, by Schur-Zassenhaus theorem, there exists $(b, w) \in R^* (b \in T, w \in V)$ and an integer i such that $\lambda'(\gamma) = (b, w)^{-1} \lambda(\gamma^i)(b, w)$. Then, $(c', z) = (b, w)^{-1}(c^i, 0)(b, w)$, which implies $c' = c^i$. As $\pi'(c') = \pi(\lambda'(c')) = \gamma = \pi(\lambda(\gamma)) = \pi'(c)$, so $c' = c$ and $\lambda'(\gamma) = (c, z)$. Let $x = \{c - \sigma(c)\}^{-1} z$. Suppose that $\alpha \in K$ satisfies $\alpha^m = \gamma$ 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

$$(c,z) = \lambda'(\gamma) = \lambda'(\alpha''') = (a, y)''' = (a''', \{a''' - (\sigma(a))'''\}\{a - \sigma(a)\}^{-1}y),$$

we get $c = a'''$ 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 α which contain $GF(p^{r'})^*$ (generated by γ), this proves $S = \langle\lambda'(K^*)\rangle = (1,x)^{-1}T(1,x)$. So $|Y|$, the number of all coefficient subrings of R, does not exceed χ. 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 (I) if T is generated by two units a and b such that

(1) $ab \neq ba$,

(2) $a - b \in J(T)$, and

(3) $o(a) = o(b) = |T/J(T)| - 1$.

If T is a finite local ring of type (I), then T^* is not a nilpotent group. For, let us suppose that T is a finite local ring of type (I). Let a and b be generators of T satisfying (1)-(3). Let A and B be cycic subgroups of T^* generated by a and b respectively. Let $K = T/J(T) = GF(p^r)$. Then $|A| = |B| = p^r - 1$ 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 (I).

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

(i) $\Rightarrow$ (iii). Let $\pi^* = \pi|_{R^*} : R^* \to K^*$ be the group homomorphism induced by the natural homomorphism $\pi : R \to K$. Since R has a unique coefficient subring, by Theorem 2.3 (III), there exists a unique right inverse λ of π^*. Then R^* is a semidirect product of $1 + M$ and K^*. Let z be any fixed element of $1 + M$. The mapping $\mu : K^* \to R^*$ defined by $K^* \ni \alpha \mapsto z^{-1}\lambda(\alpha)z$ is a right inverse of π^*, 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 (I). 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 λ and μ of π^*. Let $\{K_i\}_{i=1}^{\infty}$ be a sequence of finite subfields of K such that $K_i \subset K_{i+1}$ and $\cup_{i=1}^{\infty} K_i = K$. There exists a number j such that $\lambda|_{K_j^*} \neq \mu|_{K_j^*}$. Let γ be a generator of K_j^*. Then the subring $\langle\lambda(\gamma), \mu(\gamma)\rangle$ of R is a finite local ring of type (I).

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 $K = \cup_{i=1}^{\infty} GF(p^{r_i})$, where $\{r_i\}_{i=1}^{\infty}$ is a strictly increasing sequence of positive integers such that $r_i \mid r_{i+1} (i \geq 1)$. Let $\{\sigma_i\}_{i=1}^{\infty}$ be automorphisms of K such that σ_i is not the identity on $GF(p^{r_i}) (i \geq 1)$ and, for $j < i$, σ_i is the identity on $GF(p^{r_j})$. Let $V = \oplus_{i=1}^{\infty} Kx_i$ be a left K-vector space with basis $\{x_i\}_{i=1}^{\infty}$. We can regard V as a (K,K)-bimodule by defining

$$(\Sigma_i c_i x_i)a = \Sigma_i c_i \sigma_i(a) x_i \; (\Sigma_i c_i x_i \in V, a \in K) .$$

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 γ_i be a generator of $GF(p^{r_i})^*$. Then we can write $\gamma_i = \gamma_{i+1}^{m_i}$ 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 $u_n = (\gamma_n, \Sigma_{j=1}^{n} r_j x_j)$ $(r_j \in K)$, 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

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

Then it is easy to check that $o(u_i) = p^{r_i} - 1$ and $u_i = u_{i+1}^{m_i}$. Let $f_i : GF(p^{r_i})^* \to R^*$ be defined by $\gamma_i^t \mapsto u_i^t (t \in \mathbf{Z})$. Since $f_i \mid_{GF(p^{r_j})^*} = f_j$ for $j \leq i$, there exists $f = \lim_{\to} f_i : K^* \to R^*$. As f is a right inverse of $\pi^* = \pi \mid_{R^*} : R^* \to K^*$, so $S_1 = \langle f(K^*) \rangle$ 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 $v = (s, \Sigma_i d_i x_i) \in R^*$ $(s \in K^*, d_i \in K)$ 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,

$$\begin{aligned} u_i &= (\gamma_i, \Sigma_{j=1}^{i-1} r_j' x_j + x_i) \; (r_j' \in K) \\ &= v^{-1}(b_i, 0)v \\ &= (s^{-1}, -s^{-1}(\Sigma_i d_i x_i)s^{-1})(b_i, 0)(s, \Sigma_i d_i x_i) \\ &= (b_i, \Sigma_{j=1}^{i}(s^{-1} b_i d_j - s^{-1} d_j \sigma_j(b_i)) x_j) , \end{aligned}$$

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 $\Sigma_i d_i x_i$ is an element of the direct sum $V = \oplus_{i=1}^{\infty} Kx_i$.

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 $\overline{R} = R/J(R) = \overline{R}\overline{e}_1 \oplus \overline{R}\overline{e}_2 \oplus \ldots \oplus \overline{R}\overline{e}_d$, where each $\overline{R}\overline{e}_i (1 \le i \le d)$ is a simple component of $\overline{R}$ and $\overline{e}_i$ is a central idempotent of $\overline{R}$. Let $\overline{R}\overline{e}_i = (K_i)_{n_i \times n_i}$, 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 $\pi(e_i) = \overline{e}_i (1 \le i \le d)$. Then,

$$R = e_1Re_1 \oplus e_2Re_2 \oplus \ldots \oplus e_dRe_d \oplus (\oplus_{i \neq j} e_iRe_j)$$

as abelian groups. Since each e_iRe_i is semiperfect and $e_iRe_i/J(e_iRe_i) \cong \overline{R}\overline{e}_i = (K_i)_{n_i \times n_i}$, there exist a local ring S_i and an isomorphism ϕ_i of e_iRe_i onto $(S_i)_{n_i \times n_i}$ (see, for instance, [1, p. 160, Theorem 21]). Let

$$\phi = \phi_1 + \phi_2 + \ldots + \phi_d : e_1Re_1 \oplus e_2Re_2 \oplus \ldots \oplus e_dRe_d \to$$
$$A = (S_1)_{n_1 \times n_1} \oplus (S_2)_{n_2 \times n_2} \oplus \ldots \oplus (S_d)_{n_d \times n_d}$$

be the isomorphism. Since $S_i/J(S_i) \cong K_i$, 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

$$B = (T_1)_{n_1 \times n_1} \oplus (T_2)_{n_2 \times n_2} \oplus \ldots \oplus (T_d)_{n_d \times n_d}$$

is a subring of A. Let $T = \phi^{-1}(B)$. As $J(e_iRe_i) \cap \phi^{-1}\big((T_i)_{n_i \times n_i}\big) = J\Big(\phi^{-1}\big((T_i)_{n_i \times n_i}\big)\Big)$, we see $J(t) = T \cap J(R) = pT$ and that T/pT is naturally isomorphic to

$$(e_1Re_1 \oplus e_2Re_2 \oplus \ldots \oplus e_dRe_d)/J(e_1Re_1 \oplus e_2Re_2 \oplus \ldots \oplus e_dRe_d) = R/J(R).$$

Let us put

$$N = \phi^{-1}\Big\{ (N_1)_{n_1 \times n_1} \oplus (N_2)_{n_2 \times n_2} \oplus \ldots \oplus (N_d)_{n_d \times n_d} \Big\} \oplus \{\oplus_{i \neq j} e_iRe_j\}.$$

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 $Re \cong Rf$ (as left R-modules) if and only if $T'e \cong T'f$ (as left T'-modules). Let $\pi(e) = \overline{e}$ and $\pi(f) = \overline{f}$. Assume that $Re \cong R'f$. Then $\overline{R}\,\overline{e} \cong \overline{R}\,\overline{f}$ as left $\overline{R}$-modules. Both $\overline{R}\,\overline{e}$ and $\overline{R}\,\overline{f}$ 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 eRf. Conversely, if $J(R)$ does not include eRf, then $\overline{R}\overline{e} \cong \overline{R}\overline{f}$, which means $Re \cong Rf$ (see, for instance, [1, p. 158, Theorem 16]). Thus we see that $Re \cong Rf$ (as left R-modules) if and only if $J(R)$ does not include eRf. Similarly, $T'e \cong T'f$ (as left T'-modules) if and only if $J(T') = pT'$ 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 $Re \cong Rf$ (as left R-modules) if and only if $T'e \cong T'f$ (as left T'-modules).

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

$$1 = (e_{11} + e_{12} + \ldots + e_{1n_1}) + (e_{21} + e_{22} + \ldots + e_{2n_2}) + \ldots + (e_{d1} + e_{d2} + \ldots + e_{dn_d}),$$

where e_{ki} are mutually orthogonal primitive idempotents of T, and $Te_{ki} \cong Te_{lj}$ (as left T-modules) if and only if $k = l$. Similarly,

$$1 = (f_{11} + f_{12} + \dots + f_{1m_1}) + (f_{21} + f_{22} + \dots + f_{2m_2}) + \dots + (f_{d1} + f_{d2} + \dots + f_{dm_d}),$$

where f_{ki} are mutually orthogonal primitive idempotents of T', and $T'f_{ki} \cong T'f_{lj}$ (as left T'-modules) if and only if $k = l$.

As $e_{ki}Te_{ki}/pe_{ki}Te_{ki} \cong e_{ki}Re_{ki}/e_{ki}J(R)e_{ki}$, we see that e_{ki} and f_{lj} are primitive idempotents of R. Then $R = \oplus Re_{ki} = \oplus Rf_{lj}$ are indecomposable decompositions.

By what was stated above, Krull-Schmidt theorem tells us that there exists a permutation σ of $\{1, 2, \dots, d\}$ such that $n_i = m_{\sigma(i)}$ and $Re_{ik} \cong Rf_{\sigma(i)l}$ as left R-modules $(1 \le i \le d, 1 \le k, l \le n_i)$. By renumbering, we may assume $n_i = m_i$ and $Re_{ik} \cong Rf_{il}$ $(1 \le i \le d, 1 \le k, l \le n_i)$. Now,

$$T \cong (e_{11}Te_{11})_{n_1 \times n_1} \oplus (e_{21}Te_{21})_{n_2 \times n_2} \oplus \dots \oplus (e_{d1}Te_{d1})_{n_d \times n_d}$$

and

$$T' \cong (f_{11}T'f_{11})_{n_1 \times n_1} \oplus (f_{21}T'f_{21})_{n_2 \times n_2} \oplus \dots \oplus (f_{d1}T'f_{d1})_{n_d \times n_d},$$

where $e_{i1}Te_{i1}$ and $f_{j1}T'f_{j1}$ are IG-rings. Hence, to complete the proof it will suffice to show $e_{i1}Te_{i1} \cong f_{i1}T'f_{i1}$.

As $e_{i1}Te_{i1}$ is an IG-ring which is naturally isomorphic to $e_{i1}Re_{i1}/e_{i1}J(R)e_{i1}$, so $e_{i1}Te_{i1}$ is a coefficient subring of $e_{i1}Re_{i1}$. Similarly, $f_{i1}T'f_{i1}$ is a coefficient subring of $f_{i1}Rf_{i1}$. As $e_{i1}Re_{i1} \cong \mathrm{End}(_RRe_{i1}) \cong \mathrm{End}(_RRf_{i1}) \cong f_{i1}Rf_{i1}$, we see $e_{i1}Te_{i1} \cong f_{i1}T'f_{i1}$ 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

[1] BEHRENS, E. A., *Ring Theory*, Academic Press (1972).

[2] BOURBAKI, N., *Éléments de Mathématique*, Algèbre, Hermann (1962).

[3] CLARK, W. E., A coefficient ring for finite noncommutative rings, *Proc. Amer. Math. Soc.* **33** (1972), 25-28.

[4] CURTIS, C. W. & REINDER, I., *Representation Theory of Finite Groups and Associative Algebras*, Pure & Appl. Math. Ser. 11, Wiley-Interscience (1962).

[5] HASSE, H., *Zahlentheorie*, 2, Auflage, Akademie-Verlag (Berlin, 1963).

[6] JANUSZ, G. T., Separable algebras over commutative rings, *Trans. A. M. S.* **122** (1966), 461-479.

[7] JACOBSON, N., *Lectures in Abstract Algebra*, vol. III, Van Nostrand (1964).

[8] KRULL, W., Algebraische Theorie der Ringe, I, II and III, *Math. Annalen* **88** (1923), 80-122, **91** (1924), 1-46 and **92** (1924), 183-213.

[9] MCDONALD, B. R., *Finite Rings with Identity*, Pure & Appl. Math. Ser. 28, Marcel Dekker (1974).

[10] MOTOSE, K. & TOMINAGA, H., Group rings with nilpotent unit groups, *Math. J. Okayama Univ.* **14** (1969), 43-46.

[11] NAGATA, M., *Local Rings*, Wiley-Interscience (1962).

[12] RAGHAVENDRAN, R., Finite associative rings, *Compositio Math.* **21** (1969), 195-229.

[13] ROBINSON, D. J. S., *A Course in the Theory of Groups*, Springer-Verlag (1982).

[14] ROQUETTE, P., Abspaltung des Radikals in vollständigen lokalen Ringen, *Abh. Math. Sem. Univ. Hamburg* **23** (1959), 75-113.

[15] SERRE, J. P., *Local Fields*, Springer-Verlag (1979).

[16] SUMIYAMA, T., On double homothetisms of rings and local rings with finite residue fields, *Math. J. Okayama Univ.* **33** (1991), 13-20.

[17] WILSON, R. S., Representations of finite rings, *Pacific J. Math.* **53** (1974), 643-649.