STRUCTURE OF FINITE RINGS AND CERTAIN INFINITE RINGS WITH PRIME-POWER CHARACTERISTIC

TAKAO SUMIYAMA

AICHI INSTITUTE OF TECHNOLOGY
TOYOTA JAPAN

MARCH 1996

DISSERTATION

SUBMITTED TO THE
OKAYAMA UNIVERSITY

STRUCTURE OF FINITE RINGS
AND CERTAIN INFINITE RINGS
WITH PRIME-POWER CHARACTERISTIC

TAKAO SUMIYAMA

AICHI INSTITUTE OF TECHNOLOGY
TOYOTA JAPAN

MARCH 1996

Contents

Introduction.

As a consequence of Cohen's structure theorem for commutative complete local rings (Theorem 1.3.2), we know that, if R is a commutative finite ring with identity 1 whose order is a power of a prime p, then R contains a unique subring S such that $J(S) = pS$ ($J(S)$ is the Jacobson radical of S), and S/pS is naturally isomorphic to $R/J(R)$. The existence and structure of such a subring S for commutative finite rings was known to Krull ([14, §4, p. 20]). For a commutative finite ring R, we see that the subring S is a direct sum of Galois rings (see Chapter I, §8 and Corollary 2.5.2).

In [20], R. Raghavendran proved that, if R is a finite local ring (not necessarily commutative), then R contains a unique (up to inner automorphism of R) subring S such that S is isomorphic to a Galois ring and S/pS is naturally isomorphic to $R/J(R)$.

On the other hand, if R is a finite ring whose characteristic is p, then by Wedderburn-Malcev theorem (Theorem 1.6.3), R contains a unique (up to inner automorphism of R) semisimple subring S such that S is naturally isomorphic to $R/J(R)$. Such a subring S is a direct sum of matrix rings over finite fields. Extending this result to the case of characteristic p^n, in [6], W. E. Clark proved that, if R is a finite ring with 1 whose characteristic is p^n, then R contains a subring S such that, S is isomorphic to a direct sum of matrix rings over Galois rings, and S/pS is naturally isomorphic to $R/J(R)$ (Corollary 2.5.2).

Such subrings S of R, as above, are called coefficient subrings of R.

In this paper, we shall show that the above results of Raghavendran and Clark can be naturally extended to certain infinite case, and establish structure theorems for such rings.

In Chapter I, we shall describe, as basic concepts, Witt vectors, valuation rings and Galois theory of finite commutative local rings. Then we shall construct Galois rings and further their inductive limits.

In Chapter II, we shall prove the existence of coefficient rings (which we call coefficient subrings, in this paper) for finite local rings, and consider about their numbers. Further it will be shown that the above results can be extended naturally to certain infinite case. There will be stated a counterexample which shows that the conjugacy statement, which is so prominent in the finite case, does not hold.

In Chapter III, by applying above results to Everett's theory of ring extension ([21, §52]), we shall show that local rings stated in Chapter II are given as algebraic structures called Everett sums.

In Chapter IV, we shall establish algorithms to determine, for a given positive integer $N > 1$, all finite rings of order N. Any finite ring is the direct sum of finite rings of prime-power order. If R is a finite ring (not necessarily with 1) of characteristic p^e, then we can regard R as an algebra over $\mathbf{Z}_{p^e} = \mathbf{Z}/(p^e)$. If the Abelian group of R is

$$\langle a_1 \rangle \bigoplus \langle a_2 \rangle \bigoplus \cdots \bigoplus \langle a_m \rangle,$$

where $\langle a_i \rangle$ is a cyclic group of order p^{e_i} generated by a_i $(1 \leq e_1 \leq e_2 \leq \cdots \leq e_m = e)$, then the product on R is determined by the set of integers $\{\alpha_{ijk}\}$ (structure constants) such that

$$a_i a_k = \textstyle\sum_{j=1}^{m} \alpha_{ijk} a_j \ (1 \leq i, k \leq m).$$

Making use of this idea by J. Wiesenbauer ([33]), we can determine, for a given prime power p^n, all finite rings of order p^n. We can determine existence of identity and decomposability for them. Also we can count orders of their Jacobson radicals.

Acknowledgement. The author would like to express his indebtedness and gratitude to Prof. Takasi Nagahara, Prof. Yasuyuki Hirano, Dr. Hiroaki Komatsu and the late Prof. Hisao Tominaga for their suggestions and valuable comments.

Chapter I

Basic Concepts and Preliminary Results

§1. Rings and Modules

In what follows, by a ring we mean an associative ring with identity 1, unless otherwise stated. A ring R is said to be commutative, if $ab = ba$ holds for any $a, b \in R$.

Let R be a ring. An element a of R is called a unit if there exists an element b of R such that $ab = ba = 1$. Such b is called the inverse of a, and is denoted by $b = a^{-1}$. An element of R which is not a unit is called a non-unit. The set of all units of R forms a group with respect to multiplication, which is called the unit group of R and is denoted by R^*. For any element a of R^*, the least positive integer n such that $a^n = 1$, if exists, is called the multiplicative order of a, and is denoted by $o(a)$.

The set $\{a \in R \mid ax = xa \text{ for any } x \in R\}$ is called the center of R. An element a of R is said to be nilpotent if there exists a positive integer m such that $a^m = 0$. A left (or right) ideal I of R is said to be nil, if any element of I is nilpotent. A left (or right) ideal I of R is said to be nilpotent if there exists a positive integer m such that $I^m = 0$ (that is, any product of m elements of I is 0). The positive integer m such that

$$I^{m-1} \neq 0 \ , \ I^m = 0$$

is called the nilpotency index of I.

A ring I (without identity) is said to be nilpotent if I itself is nilpotent.

An element a of R is said to be left (resp. right) quasi-regular if there exists an element b of R such that $a+b-ba=0$ (resp. $a+b-ab=0$).

A subset U of R is said to be left (resp. right) quasi-regular if any element of U is left (resp. right) quasi-regular. A subset U of R is said to be quasi-regular if any element of U is both left quasi-regular and right quasi-regular.

The set $J(R)=\{x \in R \mid xR \text{ is right quasi-regular }\}$ forms an ideal of R , which is called the Jacobson radical of R. As is well-known (see, for instance, [1, p. 166, Theorem 15.3]), $J(R)$ is the intersection of all maximal left (or right) ideals of R.

A ring R is said to be semisimple if $J(R)=0$. A ring R is said to be simple if R has no ideals except 0 and R itself.

A subring S of R must contain the identity 1 of R. The subring of R generated by 1 is called the prime ring of R. The opposite ring R^o of R is the ring with the same Abelian group of R and the multiplication $x*y=yx$.

When R is a ring, $(R)_{n\times n}$ denotes the ring of all $n\times n$ matrices having entries in R.

When R is a commutative ring, $R[X]$ denotes the ring of all polynomials in the indeterminate X with coefficients in R. Similarly, for a set $\{X_i\}_{i\in I}$ of indeterminates, $R[\{X_i\}_{i\in I}]$ denotes the ring of all polynomials in the indeterminates $\{X_i\}_{i\in I}$ with coefficients in R.

A local ring is a ring whose non-units form an ideal of R. If R is a local ring, the ideal of R consisting of all non-units of R coincides with the radical $J(R)$ of R. A finite ring is a ring consisting of only finitely many elements. A division ring is a ring in which any non-zero element is a unit. A field is a commutative division ring.

The following theorem is known as Wedderburn's theorem. For a simple proof, see, for instance, [32, Kapitel 14, §112, p. 109].

Theorem 1.1.1. A finite division ring is a finite field.

Let R be a ring, and M a left (resp. right) R-module. The module M is said to be finitely generated, if there exist finitely many elements $x_1, x_2, \cdots, x_m$ of M such that

$M = Rx_1 + Rx_2 + \cdots + Rx_m$

(resp. $M = x_1R + x_2R + \cdots + x_mR$).

For $x \in M$, the set $\{a \in R \mid ax = 0\}$ (resp. $\{a \in R \mid xa = 0\}$ is called the annihilator of x in R, and is denoted by $Ann(x)$. A non-zero left (or right) R-module M is said to be indecomposable, if there exists no non-trivial direct sum decomposition

$M = M_1 \oplus M_2$.

We say that M satisfies the ascending chain condition if, for any ascending chain

$M_1 \subset M_2 \subset \cdots \subset M_n \subset \cdots$

of R-submodules M, there exists a positive integer N such that

$M_i = M_{i+1}$ for any $i \geq N$.

Also, we say that M satisfies the descending chain condition if, for any descending chain

$M_1 \supset M_2 \supset \cdots \supset M_n \supset \cdots$

of R-submodules of M, there exists a positive integer N such that

$M_i = M_{i+1}$ for any $i \geq N$.

A non-zero left (or right) R-module M is said to be simple, if M has no nontrivial submodules.

A ring R itself can be regarded as a left (or right) R-module. A ring R is said to be left (resp. right) Noetherian, if the left (resp. right) R-module R satisfies the ascending chain condition. A ring R is said to be left (resp. right) Artinian, if the left (resp. right) R-module R satisfies the descending chain condition.

Let R and S be rings. An Abelian group M is called an (R, S)-bimodule if M has the structure of both left R-module and right S-module such that

$(ax)b = a(xb) \quad (a \in R, x \in M, b \in S)$.

Let $\mathbf{Z}$ denote the ring of all integers. For a positive integer n, $\mathbf{Z}_n$ denotes the residue ring $\mathbf{Z}/n\mathbf{Z}$.

The following is known as Wedderburn's structure theorem.

Theorem 1.1.2. ([8, p. 175, Theorem 26.4]) A ring R is a semisimple left Artinian ring if and only if R is isomorphic to a finite direct sum oj matrix rings over divison rings.

Let R be a ring. An element e of R is called an idempotent if $e^2 = e$. Let I be an ideal of R, and $\bar{R} = R/I$. Let $\pi : R \longrightarrow \bar{R}$ be the natural homomorphism. Let $\bar{e}$ be an idempotent of $\bar{R}$. We say that the idempotent $\bar{e}$ can be lifted to an idempotent e of R , if there exists an idempotent e of R such that $\pi(e) = \bar{e}$.

A ring R is said to be semiperfect, if $R/J(R)$ is left (and so necessarily right) Artinian, and if any idempotent of $R/J(R)$ can be lifted to an idempotent of R.

A left (or right) Artinian ring is a semiperfect ring ([2, p. 153, Theorem 6]).

If R is a semiperfect ring, an idempotent e of R is called primitive if eRe is a local ring (see [2, p. 156, Theorem 12]).

Theorem 1.1.3. ([2, p. 160, Theorem 21]) Let R be a semiperfect ring such that $R/J(R)$ is a simple ring. Then there exists a primitive idempotent e of R and a positive integer n such that R is isomorphic to the matrix ring $(eRe)_{n \times n}$.

A set $\{e_1, e_2, \cdots, e_n\}$ of idempotents of R is said to be mutually orthogonal if $e_i e_j = 0 \ \ (i \neq j)$.

Theorem 1.1.4. ([2, p. 152, Theorem 4]) Let R be a semiperfect ring. Let $\bar{R} = R/J(R)$ and $\pi : R \longrightarrow \bar{R}$ be the natural homomorphism. Let $\{\bar{e}_1, \bar{e}_2, \cdots, \bar{e}_n\}$ be a set of mutually orthogonal idempotents of $\bar{R}$. Then there exists a set $\{e_1, e_2, \cdots, e_n\}$ of mutually orthogonal idempotents oj R such that $\pi(e_i) = \bar{e}_i \ \ (1 \leq i \leq n)$.

Theorem 1.1.5. ([2, p. 158, Theorem 16]) Let R be a ring, and $\bar{R} = R/J(R)$. Let e, f be idempotents of R, $\bar{e} = e + J(R)$, and $\bar{f} = f + J(R) \in R/J(R)$. Then two left ideals Re and Rf of R are isomorphic as left R-modules if and only if $\bar{R}\bar{e}$ and $\bar{R}\bar{f}$ are isomorphic as left $\bar{R}$-modules.

Let R be a ring. Let M be a non-zero left R-module. A finite sequence of $n+1$ submodules of M

$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$

$(M_{i-1} \neq M_i \ , \ 1 \leq i \leq n)$

is called a composition series of finite length for M, if each M_{i-1}/M_i $(1 \leq i \leq n)$ is simple. We say that a left R-module M is of finite length, if there exists a composition series of finite length for M.

The following theorem is known as Krull-Schmidt theorem (see, for instance, [1, p. 147]).

Theorem 1.1.6. Let R be a ring, and let M be a non-zero left R-module of finite length. Then M has a finite indecomposable decomposition

$M = \bigoplus_{i=1}^{m} M_i$

such that, for any indecomposable decomposition

$M = \bigoplus_{j=1}^{n} N_i,$

it holds that $m = n$, *and there exists a permutation* σ *of* $\{1, 2, \cdots, n\}$ *such that*

$M_{\sigma(i)} \cong N_i \quad (1 \leq i \leq n)$

and, for each $1 \leq k \leq n$,

$M = (\bigoplus_{i=1}^{k} M_{\sigma(i)}) \bigoplus (\bigoplus_{j=k+1}^{n} N_j)$.

The following theorem is known as Nakayama's lemma (see [1, p. 169]).

Theorem 1.1.7. Let R *be a ring, and* I *a left ideal of* R *such that* $I \subset J(R)$. *If* M *is a finitely generated left* R*-module and* $IM = M$, *then* $M = 0$.

Let R be a commutative ring. An ideal I of R is said to be principal, if there exists an element a of R such that $I = Ra$. An integral domain is a commutative ring R in which $xy = 0$ $(x, y \in R)$ implies that either $x = 0$ or $y = 0$. A principal ideal domain is an integral domain in which any ideal is principal. The proof of the following theorem is essentially identical with the proof of the fundamental theorem of finitely generated Abelian groups ([32, §86]).

Theorem 1.1.8. Let R *be a principal ideal domain. Let* M *be a finitely generated* R*-module. Then*

$M = \bigoplus_{i=1}^{n} Ra_i$,

where $Ra_i \cong R/K_i$, K_i *is a principal ideal of* $R \quad (1 \leq i \leq n)$.

Moreover, if there is another decomposition

$M = \bigoplus_{j=1}^{m} Rb_j$,

where $Rb_j \cong R/L_j$, L_j *is a principal ideal of* $R \quad (1 \leq j \leq m)$,

then $n = m$ *and there exists a permutation* σ *of* $\{1, 2, \cdots, n\}$ *such that*

$K_i = L_{\sigma(i)} \quad (1 \leq i \leq n)$.

§2. Groups and Limits

When S is a set, $|S|$ denotes the cardinality of S.

Let G be a group, and e the identity of G. Let N be a normal subgroup of G. A subgroup H of G is called a complement of N if $G = NH$ and $N \cap H = \{e\}$. In this case, we say that G is a semidirect product of H with N, since any $a \in G$ is uniquely expressed as $a = bc \ (b \in N,\ c \in H)$.

The following theorem is well-known as Schur-Zassenhaus theorem (see, for instance, [15, p. 84]).

Theorem 1.2.1. Let G be a finite group, and let N be a normal subgroup of G. Assume that $|N|$ and the index $|G : N| = |G|/|N|$ are coprime. Then N has at least one complement H in G. Any two complements of N in G are conjugate in G.

Let G be a group. For subgroups H_1 and H_2 of G, let $C[H_1, H_2]$ denote the subgroup of G generated by $\{a^{-1}b^{-1}ab \mid a \in H_1,\ b \in H_2\}$. Let

$D_1(G) = C[G, G]$,

$D_{i+1}(G) = C[D_i(G), G] \ (i \geq 1)$.

Then we have a sequence of subgroups

$G \supset D_1(G) \supset D_2(G) \supset \cdots \supset D_n(G) \supset \cdots$.

The group G is said to be nilpotent if there exists a positive integer n such that $D_n(G) = \{e\}$.

Theorem 1.2.2. ([10, Chapter 10, Theorem 10.3.4]) If G is a finite group whose order is a prime-power, then G is a nilpotent group.

Let G be a finite group of order $|G| = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$, where p_i $(1 \leq$

$i \leq n$) are distinct primes, and e_i ($1 \leq i \leq n$) are positive integers. Then, for each p_i ($1 \leq i \leq n$), G has a subgroup G_i of order $p_i^{e_i}$. Such a subgroup G_i is called a Sylow subgroup of G corresponding to the prime divisor p_i of $|G|$. Any two Sylow subgroups of G corresponding to the same prime p are conjugate in G (see [10, Chapter 4, Theorem 4.2.2]).

Theorem 1.2.3. ([10, Chapter 10, Theorem 10.3.4]) Let G be a finite group of order $|G| = p_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}$, where p_i ($1 \leq i \leq n$) are distinct primes, and e_i ($1 \leq i \leq n$) are positive integers. Then the following (1) and (2) are equivalent.

(1) G is nilpotent.

(2) For each $1 \leq i \leq n$, G has exactly one Sylow subgroup G_i corresponding to the prime divisor p_i. And G is the direct product oj G_i ($1 \leq i \leq n$).

If I is a quasi-regular ring, then I has the structure of group by the operation

$x \circ y = x + y - xy \ (x,\ y \in I).$

This group is called the circle group of I.

Lemma 1.2.4. ([1, Chapter 4, §15], [18]) A nil ring is quasi-regular. If I is a nilpotent ring, then the circle group of I is a nilpotent group.

A group G is said to be locally finite if any finite subset of G generates a finite subgroup of G.

Theorem 1.2.5. ([22, Chapter 14, 14.3.1]) Let G be a group, and N a normal subgroup of G. If both N and G/N are locally finite, then G is locally finite.

A sequence of rings (or modules over a ring R) and homomorphisms

$$\cdots \longrightarrow \quad A_{i-1} \quad \longrightarrow^{\alpha_{i-1}} \quad A_i \quad \longrightarrow^{\alpha_i} \quad A_{i+1} \quad \longrightarrow \cdots$$

is said to be exact if the image $Im(\alpha_{i-1})$ of α_{i-1} coincides with the kernel $Ker(\alpha_i)$ of α_i .

An ordered set $(\Lambda, \leq)$ is called a directed set if, for any $\mu_1, \mu_2 \in \Lambda$, there exists some $\nu \in \Lambda$ with $\mu_1 \leq \nu,\ \mu_2 \leq \nu$.

Let $(\Lambda, \leq)$ be a directed set, and let $\{A_\alpha, \phi_{\beta\alpha}\}$ be an inductive system of rings relative to Λ. That is, each A_α $(\alpha \in \Lambda)$ is a ring, and for each $\alpha \leq \beta$, there exists a homomorphism $\phi_{\beta\alpha} : A_\alpha \longrightarrow A_\beta$ such that

$\phi_{\alpha\alpha} = id_{A_\alpha}$, $\phi_{\gamma\alpha} = \phi_{\gamma\beta} \circ \phi_{\beta\alpha}$ $(\alpha \leq \beta \leq \gamma)$.

Then the inductive limit $A = lim_{\rightarrow} A_\alpha$ is a ring. Let $\{E_\alpha, f_{\beta\alpha}\}$ be an inductive system of left A_α-modules relative to Λ. That is, each E_α $(\alpha \in \Lambda)$ is left A_α-module, and, for each $\alpha \leq \beta$ $(\alpha, \beta \in \Lambda)$, there exists an Abelian group homomorphism $f_{\beta\alpha} : E_\alpha \longrightarrow E_\beta$ such that

$f_{\alpha\alpha} = id_{E_\alpha}$, $f_{\gamma\alpha} = f_{\gamma\beta} \circ f_{\beta\alpha}$ $(\alpha \leq \beta \leq \gamma)$.

Moreover, let us assume that, for any $\alpha \leq \beta$,

$f_{\beta\alpha}(\lambda_\alpha x_\alpha) = \phi_{\beta\alpha}(\lambda_\alpha) f_{\beta\alpha}(x_\alpha)$ $(\lambda_\alpha \in A_\alpha$, $x_\alpha \in E_\alpha)$.

Then the inductive limit $E = lim_{\rightarrow} E_\alpha$ naturally has the structure of a module over A. In such a case, we shall say that $\{E_\alpha, f_{\beta\alpha}\}$ is an inductive system of left A_α-modules.

Theorem 1.2.6. ([3, Chapitre 2, §6, n^0 6, Proposition 8]) Let $\{A_\alpha\}$ be an inductive system of rings relative to a directed set Λ. Let $A = lim_{\rightarrow} A_\alpha$ be the inductive limit. Let $\{E_\alpha, f_{\beta\alpha}\}, \{E'_\alpha, f'_{\beta\alpha}\} and \{E''_\alpha, f''_{\beta\alpha}\}$ be inductive systems of left A_α-modules relative to Λ. Let us suppose that, for each $\alpha \in \Lambda$, there exists an exact sequence of A_α-modules

$$E'_\alpha \quad \longrightarrow^{u_\alpha} \quad E_\alpha \quad \longrightarrow^{v_\alpha} \quad E''_\alpha$$

such that, for any $\alpha \leq \beta$,

$u_\beta \circ f'_{\beta\alpha} = f_{\beta\alpha} \circ u_\alpha$, $v_\beta \circ f_{\beta\alpha} = f''_{\beta\alpha} \circ v_\alpha$.

Then the sequence of left A-modules

$$lim_{\rightarrow}E'_{\alpha} \quad \longrightarrow^{u} \quad lim_{\rightarrow}E_{\alpha} \quad \longrightarrow^{v} \quad lim_{\rightarrow}E''_{\alpha}$$

is exact, where $u = lim_{\rightarrow}u_{\alpha}$ and $v = lim_{\rightarrow}v_{\alpha}$.

Let $(\Lambda, \leq)$ be a directed set, and $\{G^{(\alpha)}, \rho_{\beta}^{(\alpha)}\}$ be an inverse system of groups relative to Λ. That is, each $G^{(\alpha)}$ $(\alpha \in \Lambda)$ is a group , and for each $\alpha \leq \beta$, there exists a group homomorphism $\rho_{\beta}^{(\alpha)} : G^{(\beta)} \longrightarrow G^{(\alpha)}$ such that

$$\rho_{\alpha}^{(\alpha)} = id_{G^{(\alpha)}} \ , \ \rho_{\beta}^{(\alpha)} \circ \rho_{\gamma}^{(\beta)} = \rho_{\gamma}^{(\alpha)} \quad (\alpha \leq \beta \leq \gamma).$$

Let $\Pi_{\alpha \in \Lambda} G^{(\alpha)}$ be the product set, and G be the set of all elements $\{x^{(\alpha)}\} \in \Pi_{\alpha \in \Lambda} G^{(\alpha)}$ such that

$$\rho_{\beta}^{(\alpha)}(x^{(\beta)}) = x^{(\alpha)} \quad (\alpha \leq \beta).$$

Then the set G naturally has the structure of a group, which is called the inverse limit of $\{G^{(\alpha)}, \rho_{\beta}^{(\alpha)}\}$, and is denoted by $G = lim_{\leftarrow} G^{(\alpha)}$. Let $\rho^{(\alpha)} : G \longrightarrow G^{(\alpha)}$ be the homomorphism given by $lim_{\leftarrow} G^{(\alpha)} \ni \{x^{(\alpha)}\} \longmapsto x^{(\alpha)}$.

Theorem 1.2.7. ([4, Chapitre 3, §7, n° 2, Proposition 1]) Let $\{G^{(\alpha)}, \rho_{\beta}^{(\alpha)}\}$ be an inverse system of groups relative to a directed set Λ. Let $G = lim_{\leftarrow} G^{(\alpha)}$ be the inverse limit of $\{G^{(\alpha)}, \rho_{\beta}^{(\alpha)}\}$. Let $\rho_{\alpha} : G \longrightarrow G^{(\alpha)}$ be as above. Let E be a group. Assume that, for each $\alpha \in \Lambda$, there exists a group homomorphism $f_{\alpha} : E \longrightarrow G^{(\alpha)}$ such that $f_{\alpha} = \rho_{\beta}^{(\alpha)} \circ f_{\beta}$ $(\alpha \leq \beta)$. Then there exists a group homomorphism $f : E \longrightarrow G$ such that $f_{\alpha} = \rho^{(\alpha)} \circ f$ $(\alpha \in \Lambda)$.

Theorem 1.2.8. ([4, Chapitre 3, §7, n° 2,Corollaire de Proposition 2]) Let $\{G^{(\alpha)}, \rho_{\beta}^{(\alpha)}\}$ and $\{\bar{G}^{(\alpha)}, \bar{\rho}_{\beta}^{(\alpha)}\}$ be inverse systems of groups relative to a directed set Λ. Let $G = lim_{\leftarrow} G^{(\alpha)}$ and $\bar{G} = lim_{\leftarrow} \bar{G}^{(\alpha)}$ be inverse limits. Let $\rho_{\alpha} : G \longrightarrow G^{(\alpha)}$ and $\bar{\rho}_{\alpha} : \bar{G} \longrightarrow \bar{G}^{(\alpha)}$ be the homomorphisms defined above. Assume that, for each $\alpha \in \Lambda$, there exists a group isomorphism f_{α} of $G^{(\alpha)}$ onto $\bar{G}^{(\alpha)}$ such that $f_{\alpha} \circ \rho_{\beta}^{(\alpha)} = \bar{\rho}_{\beta}^{(\alpha)} \circ f_{\beta}$ $(\alpha \leq \beta)$. Then there exists an isomorphism f of G onto $\bar{G}$ such that $f_{\alpha} \circ \rho_{\alpha} = \bar{\rho}_{\alpha} \circ f$

$(\alpha \in \Lambda)$.

§3. Witt Vectors

In this section, all rings must be commutative, and by a local ring we mean a commutative Noetherian local ring. When R is a local ring, the Jacobson radical $J(R)$ is the ideal of R consisting of all non-units of R, which will be simply called the radical of R. The residue ring $K = R/M$ is a field, which is called the residue field of R. Let R be a local ring with radical M. We can make R into a topological space by taking $\{M^i\}_{i=1}^{\infty}$ to be the base of neighborhoods of 0. The local ring R is said to be complete, if R is a complete space (that is, any Cauchy sequence of elements of R has a limit in R) with respect to this topology. Let R be a complete local ring with radical M and residue field $K = R/M$. Let p be the characteristic of K ($p = 0$ or p is a prime). The local ring R is said to be elementary if $M = pR$. An elementary complete local ring is uniquely determined by its residue field and its characteristic. That is:

Theorem 1.3.1. ([7, Corollary 2.3], [11, Satz B1], [23]) Let R_1 and R_2 be elementary complete local rings. If ch $R_1 =$ ch R_2 and $R_1/J(R_1) \cong R_2/J(R_2)$, then R_1 and R_2 are isomorphic.

A field K is said to be perfect if any algebraic extension of K is a separable extension. The following theorem is known as Cohen's structure theorem for complete local rings.

Theorem 1.3.2. ([19, p. 106, Theorem 31.1 and p. 111, Corollary

31.10]) A complete local ring R contains a subring S which satisfies the following:

(1) S is an elementary complete local ring.

(2) $J(S) = S \cap J(R)$.

(3) $R/J(R)$ is naturally isomorphic to $S/J(S)$, that is, $R = S + J(R)$.

Assume further that $R/J(R)$ is of characteristic $p \neq 0$. Then such a subring S of R is unique if and only if $R/J(R)$ is a perfect field.

Such a subring S, as above, is called a coefficient ring of R.

Let p denote a fixed prime. Let $\mathbf{Z}[p^{-1}]$ denote the subring of the field of rational numbers consisting of elements of the form a/p^i , where $a \in \mathbf{Z}$, and i is a non-negative integer. Let $X_0, X_1, \cdots, X_n, \cdots$ be a sequence of indeterminates. Let us consider the following polynomials:

$W_0 = X_0$,

$W_1 = X_0^p + pX_1$,

$\cdots$

$$\begin{aligned} W_n &= \textstyle\sum_{i=0}^n p^i X_i^{p^{n-i}} \\ &= X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n. \end{aligned}$$

These polynomials are called Witt polynomials ([36]). It is clear that each X_i can be expressed as polynomials of W_j with coefficients in $\mathbf{Z}[p^{-1}]$. That is:

$X_0 = W_0$,

$X_1 = p^{-1}W_1 - W_0^p, \cdots$etc.

Let $Y_0, Y_1, \cdots, Y_n, \cdots$ be another sequence of indeterminates. Then, by induction, we see that there exists uniquely a sequence

$S_0, S_1, \cdots, S_n, \cdots, P_0, P_1, \cdots, P_n, \cdots,$

of elements of $\mathbf{Z}[X_0, Y_0, X_1, Y_1, \cdots, X_n, Y_n, \cdots]$ such that

$W_n(S_0, S_1, \cdots, S_n, \cdots) = W_n(X_0, X_1, \cdots) + W_n(Y_0, Y_1, \cdots)$

and

$$W_n(P_0, P_1, \cdots, P_n, \cdots) = W_n(X_0, X_1, \cdots)W_n(Y_0, Y_1, \cdots)$$
$$(n = 0, 1, \cdots).$$

That is, if we write $X = (X_0, X_1, \cdots, X_n, \cdots)$ and $Y = (Y_0, Y_1, \cdots, Y_n, \cdots)$,

$S_0(X, Y) = X_0 + Y_0$,

$P_0(X, Y) = X_0Y_0$,

$S_1(X, Y) = X_1 + Y_1 + (1/p)\{X_0^p + Y_0^p - (X_0 + Y_0)^p\}$,

$P_1(X, Y) = Y_0^pX_1 + Y_1X_0^p + pX_1Y_1$,

$\cdots$ etc.

Let K be a commutative ring, and n a positive integer. For $a = (a_0, a_1, \cdots, a_{n-1})$, $b = (b_0, b_1, \cdots, b_{n-1}) \in K^n$, we set

$a + b = (S_0(a, b), S_1(a, b), \cdots, S_{n-1}(a, b))$ and

$ab = (P_0(a, b), P_1(a, b), \cdots, P_{n-1}(a, b))$.

Then we can see that the set K^n together with above sum and multiplication forms a commutative ring. This ring $W_n(K)$ is called the ring of Witt vectors of length n ([25, Chapter II, §6]). It is obvious that $0 = (0, 0, \cdots, 0)$ is the zero of $W_n(K)$, and $e = (1, 0, \cdots, 0)$ is the identity of $W_n(K)$, where 1 is the identity of K. Also we have $W_1(K) = K$.

Let $\rho : W_n(K) \longrightarrow W_{n-1}(K)$ be the ring homomorphism given by

$(a_0, a_1, \cdots, a_{n-1}) \longmapsto (a_0, a_1, \cdots, a_{n-2})$.

We have the following basic property of $W_n(K)$.

Theorem 1.3.3. ([12, p. 131, Theorem 11 and Chapter V, § 7]) Let K be a perfect field of characteristic $p(\neq 0)$. Then the ring $W_n(K)$ of Witt vectors of length n is an elementary complete local ring with radical

$N = \{(0, a_1, \cdots, a_{n-1})\}$

and residue field $K \cong W_n(K)/N$.

For $1 \leq i < j$, there exists a homomorphism $\rho^{j-i} : W_j(K) \longrightarrow$

$W_i(K)$. So there exists the projective limit $W(K) = lim_{\leftarrow} W_n(K)$. This ring $W(K)$, consisting of elements of the form $a = (a_0, a_1, \cdots, a_n, \cdots)$, is called the ring of Witt vectors of infinite length ([25, chapter II, §6]).

§4. Valuation Rings

Let K be a field. A real valuation v of K is a mapping of K into the field of real numbers such that

(1) $v(a) \geq 0$,

(2) $v(a) = 0$ if and only if $a = 0$,

(3) $v(ab) = v(a)v(b)$, and

(4) $v(a+b) \leq v(a) + v(b)$.

A real valuation v is said to be Archimedean if $v(n) > 1$ for some integer n $(= 1+1+\cdots+1$, n times), in the prime field of K. Otherwise the valuation v is said to be non-Archimedean.

Let us suppose that v is a non-Archimedean real valuation of the field K. Then the subset O_v of elements $a \in K$ such that $v(a) \leq 1$ is a subring of K. This ring O_v is called the valuation ring of v. The subset N of O_v consisting of the elements $b \in O_v$ such that $v(b) < 1$ is an ideal of O_v. We see that N is the set of all non-units of O_v. Hence O_v is a commutative local ring and N is the radical of O_v. The set $\Gamma = \{v(a) \mid a \in K \ , \ a \neq 0\}$ is a subgroup of the multiplicative group of all positive numbers. This Γ is called the value group of v. The valuation v is said to be discrete if Γ is a cyclic group.

Let us suppose that v is a discrete valuation of the filed K. Let d be an element of K such that $v(d)$ is the largest element among the set of all elements of Γ less than 1. Then $N = (d)$, and any non-zero element of K has the form rd^m, where $m \in \mathbf{Z}$ and r is a unit of O_v.

Proposition 1.4.1 ([12, Chapter V, §5]) A discrete valuation ring is a commutative local ring which is a unique factorization domain.

Now, let K be a perfect field of characteristic $p(\neq 0)$, and $W(K)$ be the ring of Witt vectors of infinite length.

Proposition 1.4.2. ([12, Chapter V, §7]) Let K be a perfect field oj characteristic $p \neq 0$. Then the ring $W(K)$ of Witt vectors of infinite length is a discrete valuation ring whose residue field is K. The ring $W_n(K)$ of Witt vectors of length n is a homomorphic image of $W(K)$.

§5. Polynomials over Commutative Artinian Rings

Throughout this section, R will denote a commutative Artinian local ring with radical M and residue field $K = R/M$. Let $\pi : R \longrightarrow K$ denote the natural homomorphism given by $a \longmapsto \bar{a} = a + M \in R/M$. Let $R[X]$ denote the ring of polynomials in the indeterminate X with coefficients in R . Let $\mu : R[X] \longrightarrow K[X]$ denote the natural homomorphism given by $\sum_{i=0}^{r} a_i X^i \longmapsto \sum_{i=0}^{r} \bar{a}_i X^i$ $(a_i \in R\ ,\ \bar{a}_i \in K)$. We can regard R as a subring of $R[X]$, and we see $\mu|_R = \pi$.

Let $f(X) = \sum_{i=0}^{r} a_i X^i$ $(a_r \neq 0)$ be an element of $R[X]$. The number r is called the degree of $f(X)$, and is denoted by *deg* $f(X)$. The polynomial $f(X)$ is said to be monic if $a_r = 1$. The polynomial $f(X)$ is said to be regular if $f(X)$ is not a zero-divisor in $R[X]$.

Let $f(X)$ be a monic polynomial of $R[X]$. We see that, if $\mu(f(X))$ is irreducible in $K[X]$, then $f(X)$ is irreducible in $R[X]$. When this is the case, we say that $f(X)$ is monic basic irreducible.

As a consequence of Hensel's lemma ([32, Kapitel VIII, §144]), we have the following.

Theorem 1.5.1. ([17, p. 292, Lemma XV.1]) Let R be a commutative Artinian local ring. Let K be the residue field of R , and $\pi : R \longrightarrow K$ be the natural homomorphism. Let $f(X)$ be a regular polynomial of $R[X]$. Assume that $\mu(f(X))$ has a simple zero $\bar{\alpha}$ in K. Then $f(X)$ has exactly one zero α in R such that $\pi(\alpha) = \bar{\alpha}$.

§6. Separability

Let R be a ring. An exact sequence of left R-modules

$0 \longrightarrow A \longrightarrow^{\alpha} B \longrightarrow^{\beta} C \longrightarrow 0$

is said to split if there exists an R-homomorphism

$\lambda : C \longrightarrow B$

such that $\beta \circ \lambda = id_C$. In this case, we have

$B = A \bigoplus \lambda(C)$.

Such λ is called a splitting homomorphism of β.

A left module M over a ring R is said to be projective if, for any exact sequence of left R-modules

$B \longrightarrow^{\varphi} A \longrightarrow 0$

and any R-homomorphism $\alpha : M \longrightarrow A$, there exists an

R-homomorphism $\beta : M \longrightarrow B$ such that $\varphi \circ \beta = \alpha$.

Theorem 1.6.1. ([1, p. 300, Corollary 26.7]) A left (or right) module M over a local ring R is projective if and only if M is a free R-module.

Let M be a left module over a ring R. The module M is said to be injective if, for any exact sequence

$$0 \longrightarrow A \longrightarrow^{\varphi} B$$

and for any R-homomorphism $\alpha : A \longrightarrow M$, there exists an R-homomorphism $\beta : B \longrightarrow M$ such that $\beta \circ \varphi = \alpha$.

Theorem 1.6.2. (Baer's criterion, [1, p. 205, 18.3.]) Let R be a ring. A left module M over a ring R is injective if and only if, for any left ideal I of R and any R-homomorphism $\psi : I \longrightarrow M$, there exists $x \in M$ such that $\psi(a) = ax$ for any $a \in I$.

Let R be a commutative ring. The ring R is said to be self-injective if R itself is injective as R-module (see [24, p. 453]). A ring T is called an algebra over R if there exists a ring homomorphism α from R into the center of T. The algebra T over R is regarded as a left R-module by the operation

$$ax = \alpha(a)x \ (a \in R, \ x \in T).$$

The algebra T over R is said to be finitely generated over R if it is finitely generated as R-module.

Let T be a finitely generated algebra over R.

Then, by tensor product, we get the enveloping algebra $T^e = T \otimes_R T^o$ (T^o is the opposite ring of T).

The algebra T is regarded as a left T^e-module by the operation

$$(a_1 \otimes a_2)x = a_1 x a_2 \ \ (a_1, a_2, x \in T).$$

There is a natural left T^e-module homomorphism

$\phi : T^e \longrightarrow T$

given by

$a_1 \otimes a_2 \longmapsto a_1 a_2.$

This mapping gives rise to an exact sequence of T^e-modules

$0 \longrightarrow Ker\ \phi \longrightarrow T^e \longrightarrow^{\phi} \ T \longrightarrow 0.$

The algebra T is said to be separable over R (or T is a separable extension of R) if T is projective as a left T^e-module.

Theorem 1.6.3. (Wedderburn-Malcev theorem, [8, p. 491]) Let A be a finitely generated algebra over a field K. Assume that $A/J(A)$ is separable over K. Then A contains a subalgebra B such that:

(1) B is semisimple.

(2) $A = B \oplus J(A)$ (as vector spaces over K).

(3) The homomorphism

$\lambda : B \longrightarrow A/J(A)$ defined by $b \longmapsto b + J(A)$ $(b \in B)$

is an isomorphism of B onto $A/J(A)$.

§7. Galois Theory of Finite Commutative Local Rings

In this section, we shall investigate Galois theory of finite commutative local rings. To begin with, we shall state a simple lemma.

Lemma 1.7.1. ([17, p. 111, Theorem VII.7]) A finite ring R (which need not be commutative) is a local ring if and only if R has no nontrivial idempotents.

In what follows, let T be a finite commutative local ring with radical

N and residue field $L = T/N$. Let R be a subring of T. Note that, under this assumption, R must be a commutative local ring, by Lemma 1.7.1.

An R-algebra automorphism of T is an automorphism of T which leaves the elements of R fixed. We say that T is an unramified extension of R if $J(T) = TJ(R)$.

Theorem 1.7.2. ([17, p. 287, Theorem XIV.8]) Let T be a commutative finite local ring, and R a subring of T. Then T is separable over R if and only if there exists a monic basic irreducible polynomial $f(X)$ of $R[X]$ such that T is isomorphic to $R[X]/(f(X))$ by an isomorphism which leaves the elements of R fixed.

By Theorem 1.7.2, we see that, if a commutative finite local ring T is separable over its subring R, then T is a free R-module of rank n, where $n = |T/J(T) : R/J(R)|$. So, in such a case, we shall say that T is an n-dimensional separable extension of R.

Let R be a commutative finite local ring. Let T and U be commutative finite local rings both contain R as a subring. Then the residue filed K of R is naturally regarded as a subfield of both $T/J(T)$ and $U/J(U)$. Under this assumption, we get the following.

Theorem 1.7.3. ([17, p. 293, Theorem XV.2]) Let R be a commutative finite local ring with radical M and residue field $K = R/M$. Let T be a commutative finite local ring which is a separable extension of R. Let U be a commutative finite local ring which is an extension of R such that $U/J(U)$ is isomorphic to $T/J(T)$. Then, for each K-algebra isomorphism $\bar{\sigma} : T/J(T) \longrightarrow U/J(U)$, there exists uniquely an R-algebra homomorphism $\sigma : T \longrightarrow U$ which induces $\bar{\sigma}$ modulo the radicals. Moreover, σ is an R-algebra isomorphism if and only if U is separable over

R.

Let T be a commutative finite local ring and R be a subring of T. Let $Aut_R(T)$ denote the group consisting of all R-algebra automorphisms of T. For a subgroup H of $Aut_R(T)$, let

$T^H = \{a \in T \mid \sigma(a) = a \text{ for all } \sigma \in H\}$

be the fixed subring of H.

Let $G = Aut_R(T)$. We say that T is a Galois extension of R with Galois group G, if

(1) $T^G = R$, and

(2) T is separable over R.

Then, by Theorem 1.7.3, we get the following.

Corollary 1.7.4. ([17, p. 294, Corollary XV.3]) Let T be a commutative finite local ring which is separable over its subring R. Then:

(1) T is a Galois extension of R with Galois group $Aut_R(T)$.

(2) $Aut_R(T) \cong Aut_{R/J(R)}(T/J(T))$.

(3) $Aut_R(T)$ is a cyclic group of order $|T/J(T) : R/J(R)|$.

Corollary 1.7.5. ([17, p. 295, Corollary XV.4]) Let T be a commutative finite local ring, and R a subring of T. Then the following are equivalent.

(1) T is a Galois extension of R with Galois group $Aut_R(T)$.

(2) T is separable over R.

(3) T is an unramified extension of R.

§8. Galois Rings

Let p be a prime, and $\mathbf{Z}_{p^k} = \mathbf{Z}/(p^k)$. By Theorem 1.7.2 and Theorem 1.7.3, we see that, for any positive integer r, there exists uniquely (up to $\mathbf{Z}_{p^k}$-algebra automorphism) an r-dimensional Galois extension of $\mathbf{Z}_{p^k}$. This ring is called the Galois ring of characteristic p^k and rank r, and is denoted by $GR(p^k, r)$. In particular, $GR(p, r)$ is the finite field $GF(p^r)$.

The Galois ring was first noticed by Krull [14], and was later rediscovered by Janusz [13] and Raghavendran [20].

By our previous discussion, Theorem 1.3.1 and Theorem 1.3.3, we already have the following property of Galois rings.

Proposition 1.8.1.

(1) If $f(X)$ is a monic, basic irreducible polynomial of $\mathbf{Z}_{p^k}[X]$ with degree r, then $\mathbf{Z}_{p^k}[X]/(f(X))$ is isomorphic to the Galois ring $GR(p^k, r)$.

(2) The Galois ring $R = GR(p^k, r)$ is a commutative, elementary complete local ring with characteristic p^k whose radical is $pR = (p)$ and whose residue field is $R/pR = GF(p^r)$.

(3) The Galois ring $GR(p^k, r)$ is isomorphic to the ring $W_k(GF(p^r))$ of Witt vectors of length k, having entries in $GF(p^r)$.

(4) Any ideal of the Galois ring $R = GR(p^k, r)$ is of the form $p^i R$ $(0 \leq i \leq k)$.

(5) The Galois ring $GR(p^k, r)$ is self-injective.

(6) For any divisor r' of r, the ring $GR(p^k, r)$ contains a unique subring which is isomorphic to $GR(p^k, r')$ ([20, Proposition 1]).

(7) Any subring of $GR(p^k, r)$ is of the form $GR(p^k, r')$ (r' is a divisor of r, [20, Proposition 1]).

(8) Let k_1, k_2, r_1 and r_2 be positive integers. Then

$$GR(p^{k_1}, r_1) \otimes_{\mathbf{Z}} GR(p^{k_2}, r_2) \cong \bigoplus^d GR(p^n, m) \quad \textit{(as rings)},$$

where n is the minimum of $\{k_1, k_2\}$, d is the greatest common divisor oj

$\{r_1, r_2\}$, and m is the least common multiple of $\{r_1, r_2\}$ ([34, Proposition 2.1]).

§9. Inductive Limits of Galois Rings

We shall call a ring R an inductive limit of Galois rings 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 $r_i | r_{i+1}$ $(i \geq 1)$. Being long, the term an "inductive limit of Galois rings" will hereinafter be abbreviated as an "IG-ring". 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 $1 = r_1 \leq r_2 \leq \cdots\cdot$ an infinite sequence of positive integers such that $r_i | r_{i+1}$. By Proposition 1.8.1 (6) and (7), there exists a natural embedding $\iota_i^{i+1} : GR(p^n, r_i) \longrightarrow GR(p^n, r_{i+1})$ for each $i \geq 1$. Let us put $\iota_i^i = id_{GR(p^n, r_i)}$ and $\iota_i^j = \iota_{j-1}^j \circ \iota_{j-2}^{j-1} \circ \cdots\cdot \circ \iota_i^{i+1}$ 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 $R = \bigcup_{i=1}^{\infty} GR(p^n, r_i)$ is a Galois ring if $|R|$ is finite. A subring S of a ring A is called an IG-subring of A if S is an IG-ring.

Proposition 1.9.1. Let $R = \bigcup_{i=1}^{\infty} GR(p^n, r_i)$ be an IG-ring. Then:

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

(2) If e is a positive integer such that $1 \leq e \leq n$, then R/p^eR is

naturally isomorphic to the IG-ring $\bigcup_{i=1}^{\infty} GR(p^e, r_i)$.

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

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

(5) R is self-injective.

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

Proof. (1) and (2). For each $i \geq 1$,

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

is an exact sequence of $GR(p^n, r_i)$-modules. So we get the result by Theorem 1.2.6.

(3) This is an immediate consequence of Theorem 1.3.1, Theorem 1.3.3 and Proposition 1.4.2.

(4) If R is a discrete valuation ring with radical pR, then by Proposition 1.4.1, any ideal of R is of the form $p^j R$ $(j \geq 0)$, so the result is clear from (3).

(5) By Baer's criterion (Theorem 1.6.2), we see that a proper homomorphic image of a principal ideal domain is self-injective. So (5) is immediate from (3).

(6) Suppose $i \leq j$. If τ is an automorphism of $GF(p^{r_j})$, the restriction $\tau' = \tau|_{GF(p^{r_i})}$ is an automorphism of $GF(p^{r_i})$. So $\bar{\pi}_j^{(i)} : \tau \longmapsto \tau|_{GF(p^{r_i})}$ is a group homomorphism of $Aut(GF(p^{r_j}))$ onto $Aut(GF(p^{r_i}))$. We see that $\{Aut(GF(p^{r_i})),\ \bar{\pi}_j^{(i)}\}$ forms an inverse system on the directed set $\mathbf{N} = \{1, 2, \cdots, n, \cdots\}$.

An automorphism σ of $GR(p^k, r_i)$ induces an automorphism $\bar{\sigma}$ of $GF(p^{r_i})$ modulo radicals. By Theorem 1.7.3, this correspondence $\lambda^{(i)} : \sigma \longmapsto \bar{\sigma}$ is an isomorphism of $Aut(GR(p^k, r_i))$ onto $Aut(GF(p^{r_i}))$. Let us put

$\pi_j^{(i)} = (\lambda^{(i)})^{-1} \circ \bar{\pi}_j^{(i)} \circ \lambda^{(j)}$ $(1 \leq i \leq j)$.

Then $\{Aut(GR(p^k, r_i))), \pi_j^{(i)}\}$ also forms an inverse system on $\mathbf{N}$, and we see that

$\lambda^{(i)} \circ \pi_j^{(i)} = \bar{\pi}_j^{(i)} \circ \lambda^{(j)}$ $(i \leq j)$.

So, by Theorem 1.2.8, there exists an group isomorphism λ of $lim_{\leftarrow} Aut(GR(p^k, r_i))$ onto $lim_{\leftarrow} Aut(GF(p^{r_i}))$.

Let τ be an isomorphism of $K = \bigcup_{i=1}^{\infty} GF(p^{r_i})$. Then the restriction $\tau|_{GF(p^{r_i})}$ is an automorphism of $GF(p^{r_i})$. So, the mapping $\varphi_i : \tau \longmapsto \tau|_{GF(p^{r_i})}$ is a group homomorphism of $Aut(K)$ onto $Aut(GF(p^{r_i}))$. Let $\rho_i : lim_{\leftarrow} Aut(GF(p^{r_i})) \longrightarrow Aut(GF(p^{r_i}))$ be the natural homomorphism given by $\{\sigma_i\} \longmapsto \sigma_i$. As

$\bar{\pi}_j^{(i)} \circ \varphi_j = \varphi_i$ $(i \leq j)$,

by Theorem 1.2.7, there exists a group homomorphism φ of $Aut(K)$ to $lim_{\leftarrow} Aut(GF(p^{r_i}))$ such that $\rho_i \circ \varphi = \varphi_i$ $(i \geq 1)$. It is easy to check that this φ is an isomorphism of $Aut(K)$ onto $lim_{\leftarrow} Aut(GF(p^{r_i}))$.

Similarly we see

$Aut(\bigcup_{i=1}^{\infty} GR(p^k, r_i)) \cong lim_{\leftarrow} Aut(GR(p^k, r_i))$.

Let $\{r_\ell\}_{\ell=1}^{\infty}$ be an infinite sequence of positive integers such that $r_1 = 1$ and $r_\ell | r_{\ell+1} (\ell \geq 1)$. Let $S = \bigcup_{\ell=1}^{\infty} GR(p^n, r_\ell)$ be an IG-ring of characteristic p^n. Let $n = n_1 \geq n_2 \geq \cdots \geq n_t$ be a decreasing sequence of positive integers. Let us put $S_j = \bigcup_{\ell=1}^{\infty} GR(p^{n_j}, r_\ell)$ for $1 \leq j \leq t$. Let $\varphi_j : S \longrightarrow S_j$ be the natural homomorphism followed by the isomorphism $S/p^{n_j}S \cong S_j$ of Proposition 1.9.1 (2). Let us put $U(S; n_1, n_2, \cdots, n_t) = \{(\alpha_{ij}) \in (S)_{t \times t} \mid \alpha_{ij} \in p^{n_j - n_i}S \text{ if } i > j\}$. It is easy to see that $U(S; n_1, n_2, \cdots, n_t)$ forms a subring of $(S)_{t \times t}$. Let $M(S; n_1, n_2, \cdots, n_t)$ 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 $U(S; n_1, n_2, \cdots, n_t)$ onto $M(S; n_1, n_2, \cdots, n_t)$ defined by $(\alpha_{ij}) \longmapsto (a_{ij})$, where $a_{ij} = \varphi_j(\alpha_{ij})$. It is easy to check that addition and multiplication in $M(S; n_1, n_2, \cdots, n_t)$ can be defined by stipulating that Φ preserves addition and multiplication. We shall call $M(S; n_1, n_2, \cdots, n_t)$ a ring of Szele matrices over S.

Lemma 1.9.2. (cf. [35, 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 decreasing sequence $n = n_1 \geq n_2 \geq \cdots \geq n_t$ of positive integers such that R is isomorphic to a subring of $M(S; n_1, n_2, \cdots, n_t)$.

Proof. By Proposition 1.9.1 (5), there exists a submodule N of R such that $R = S \bigoplus N$ as left S-module. By Proposition 1.9.1 (3), there exist a discrete valuation ring W and a homomorphism φ of W onto S. By defining

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

N is a finitely generated W-module. By Theorem 1.1.8, there exist $y_1, y_2, \cdots, y_s \in N$ such that $N = \bigoplus_{i=1}^{s} Wy_i$. Let $t = s + 1$, $x_1 = 1$ and $x_i = y_{i-1}$ $(2 \leq i \leq t)$. Then we get $R = \bigoplus_{i=1}^{t} Sx_i$. Let $Sx_i \cong S/p^{n_i}S$ as S-module $(n_1 = n)$. Without loss of generality, we may assume $n_1 \geq n_2 \geq \cdots \geq n_t$. 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 1.9.1 (4), $\alpha_{ij} \in p^{n_j - n_i}S$ if $i > j$. As α_{ij} is uniquely determined modulo $p^{n_j}S$ by a , we can define $\psi : R \longrightarrow M(S; n_1, n_2, \cdots, n_t)$ by $a \longmapsto (\psi_j(\alpha_{ij}))$. It is easy to see that ψ is an injective ring homomorphism.

Chapter II

Coefficient Subrings

§1. Coefficient Subrings of Finite Local Rings

Throughout this section, let R denote a finite local ring (not necessarily commutative) with radical M and residue field $K = R/M$. Though R needs not be commutative, by Wedderburn's theorem (Theorem 1.1.1), the residue field K is commutative.

A finite ring S is called a p-ring (p a prime) if the order $|S|$ of S is a power of p.

As a finite ring is the direct sum of finite p-rings, a finite local ring must be a p-ring for a prime p.

Theorem 2.1.1. ([20, Theorem 2]) Let R be a finite local ring with radical M and residue field K. Then:

(1) We can write $|R| = p^{nr}$, $|M| = p^{(n-1)r}$ and $|K| = p^r$, where p is a prime, and n, r are positive integers.

(2) $M^n = 0$.

(3) $ch\ R = p^k$, where k is a positive integer not greater than n.

Proof. (1) Since K is a finite field, $K = GF(p^r)$ for a prime p and a positive integer r. Let m be the nilpotency index of M. Each M^i/M^{i+1} $(1 \leq i \leq m-1)$ has the structure of left K-space by the operation

$(a + M)(x + M^{i+1}) = ax + M^{i+1}$ $(a + M \in K = R/M,\ x + M^{i+1} \in M^i/M^{i+1})$.

So $|M^i/M^{i+1}|$ is a power of p^r. Let us put $|M^i/M^{i+1}| = p^{rk_i}$ $(1 \leq$

$i \leq m-1$) and $n = k_1 + k_2 + \cdots k_{m-1} + 1$. Then $|M| = p^{(n-1)r}$. As $R/M = K$, so $|R| = |M| \cdot |K|$. Hence $|R| = p^{nr}$.

(2) is obvious from $n - 1 = k_1 + k_2 + \cdots + k_{m-1} \geq m - 1$.

(3) Let us suppose $ch\ R = p^k$ and $k > n$. As $pR \subset M$, we get

$0 = M^n \supset M^{k-1} \supset (pR)^{k-1} \neq 0$,

which is a contradiction.

Proposition 2.1.2. ([30, Lemma 1.1]) Let R be a finite local ring with characteristic p^k whose residue field is $K = GF(p^r)$. Then:

(1) R^* contains an element v such that $o(v) = p^r - 1$.

(2) If $v \in R^*$ satisfies $o(v) = p^r - 1$, then v generates a subring oj R which is isomorphic to $GR(p^k, r)$.

Proof. Let $\pi : R \longrightarrow K = R/M$ be the natural homomorphism. Let $\bar{u}_0$ be a generator of K^* , and let $f(X) \in \mathbf{Z}_{p^k}[X]$ be a monic polynomial of degree r such that the image $\bar{f}(X)$ in $\mathbf{Z}_p[X]$ gives the minimal polynomial of $\bar{u}_0$. By Theorem 1.5.1, there exists $u \in R$ such that $\pi(u) = \bar{u}_0$ and $f(u) = 0$. Let $S = \mathbf{Z}_{p^k}[u]$, and consider the natural homomorphism

$\psi : \mathbf{Z}_{p^k}[X]/(f(X)) \longrightarrow S$

given by $X \longmapsto u$.

We shall claim that in R,

$\mathbf{Z}_{p^k} + \mathbf{Z}_{p^k}u + \cdots + \mathbf{Z}_{p^k}u^{r-1}$

is a direct sum. Suppose that there exists a non-trivial expression

$a_0 + a_1 u + \cdots + a_{r-1}u^{r-1} = 0\ (a_i \in \mathbf{Z}_{p^k})$

with some $a_i \neq 0$. We can write

$a_i = p^{e_i}a_i'\ \ (0 \leq e_i \leq k,\ a_i'$ are units, $0 \leq i \leq r-1)$.

Let e_j be the smallest among $\{e_0, e_1, \cdots, e_{r-1}\}$. If $e_j = k$, then all $a_i = 0$, which contradicts our assumption. So we see $e_j < k$. We have

$p^{e_j}(p^{e_0 - e_j}a_0' + \cdots + a_j'u^j + \cdots + p^{e_{r-1}-e_j}a_{r-1}'u^{r-1}) = 0$

in R. Then $p^{e_0-e_j}a'_0+\cdots+a'_ju^j+\cdots+p^{e_{r-1}-e_j}a'_{r-1}u^{r-1}$ is in M, so we have

$$p^{e_0-e_j}\bar{a}'_0+\cdots+\bar{a}'_j\bar{u}^j+\cdots+p^{e_{r-1}-e_j}\bar{a}'_{r-1}\bar{u}^{r-1}=0$$

in K. As $\bar{a}'_j\neq 0$, this contradicts the fact that $\mathbf{Z}_{p^k}1+\mathbf{Z}_{p^k}u+\cdots+\mathbf{Z}_{p^k}u^{r-1}$ is a direct sum in K.

So we see

$$|S|\geq p^{kr}=|\mathbf{Z}_{p^k}[X]/(f(X))|,$$

which implies that ψ is an isomorphism of $\mathbf{Z}_{p^k}[X]/(f(X))$ onto S. This is the Galois ring $GR(p^k,r)$.

Since an element a of R is a unit if and only if $\pi(a)$ is a unit of K, so the restriction $\pi^*=\pi|_{R^*}$ induces an exact sequence of groups

$$1\longrightarrow 1+M\longrightarrow R^*\xrightarrow{\pi^*} K^*\longrightarrow 1.$$

Let u and $S=\mathbf{Z}_{p^k}[u]$ be as above. As

$$1\longrightarrow 1+pS\longrightarrow S^*\xrightarrow{\pi^*|_{S^*}} K^*\longrightarrow 1$$

is an exact sequence, we can write $o(u)=p^m(p^r-1)$ (m is a nonnegative integer). Let us put $v=u^{p^m}$. Then $o(v)=p^r-1$. As $\pi(v)$ is also a generator of K^*, we see that $\mathbf{Z}_{p^k}[u]=\mathbf{Z}_{p^k}[v]$.

Now let us suppose that an element v' of R^* satisfies $o(v')=p^r-1$. By Schur-Zassenhaus theorem (Theorem 1.2.1), two cyclic subgroups $\langle v\rangle$ and $\langle v'\rangle$ are conjugate in R^*. So there exists some $a\in R^*$ such that $S'=a^{-1}Sa$.

Let R be a finite local ring with characteristic p^k whose residue field is $GF(p^r)$. A subring of R which is isomorphic to $GR(p^k,r)$ is called a coefficient ring of R ([6]). However, in this paper, from our standpoint to consider the whole number of them, we shall call it a coefficient subring of R.

Theorem 2.1.3. ([20, Theorem 8]) Let R be a finite local ring with residue field $GF(p^r)$. Then:

(1) R contains at least one coefficient subring.

(2) If S and S' are coefficient subrings of R, then there exists a unit a of R such that $S' = a^{-1}Sa$.

(3) If S is a coefficient subring of R, then there exists an (S, S)-submodule N of M such that

$$R = S \bigoplus N$$

as (S, S)-bimodules.

Proof. (1) and (2) will be clear by Proposition 2.1.2 and its proof.

(3) By Proposition 1.8.1 (5) and (8), the inclusion $0 \longrightarrow S \longrightarrow R$ splits as modules over $S^e = S \bigotimes_R S$ (and hence as (S, S)-bimodules). So S is a direct summand of R as (S, S)-bimodules. Considering R as a left S-module, we have

$${}_SR = Sb_1 \bigoplus Sb_2 \bigoplus \cdots \bigoplus Sb_t.$$

As S is a direct summand of R, we can take $b_1 = 1$. And we can take other b_i such that $Ann_S(b_i) = 0$ $(1 \le i \le r)$ and $Ann_S(b_i) \neq 0$ $(r + 1 \le i \le t)$. So $b_i \in M$ for $r + 1 \le i \le t$. For $2 \le i \le t$, replace b_i by $b'_i = b_i - r_i$, where r_i is an element of S such that $\pi(r_i) = \pi(b_i)$. Then it is easy to see that again

$${}_SR = Sb_1 \bigoplus Sb'_2 \bigoplus \cdots \bigoplus Sb'_t,$$

where the annihilators are unchanged, and moreover, $b'_2, \cdots, b'_t$ belong to M. Thus

$$M = Sp \bigoplus (\bigoplus_{i=2}^t Sb'_i)$$

as left S-modules. Let

$$M = \bigoplus_{i=1}^d Sa_i$$

be a decomposition of M as (S, S)-bimodules. Since this decomposition is also a decomposition as left S-modules, by Krull-Schmidt theorem (Theorem 1.1.6), we have $d = t$, and, after renumbering, $Ann_S(a_1) = (p^{\lambda-1})$ and $Ann_S(a_i) = Ann_S(b'_i)$ $(2 \le i \le t)$. In particular, one can see that $\{1, a_2, \cdots, a_d\}$ are S-free. So,

$$S1 \bigoplus Sa_2 \bigoplus \cdots \bigoplus Sa_r$$

is an (S,S)-submodule of R. This submodule is injective and hence a direct summand of R as an (S,S)-bimodule. That is,

$$R = [S \bigoplus (\bigoplus_{i=2}^{r} Sa_i)] \bigoplus W$$

as (S,S)-bimodules, where W is an (S,S)-submodule of R. We can express $W = \bigoplus_{j=1}^{t-r} Sc_j$ as a direct sum of left S-modules. Then we have

$$R = [S \bigoplus (\bigoplus_{i=2}^{r} Sa_i)] \bigoplus [\bigoplus_{j=1}^{t-r} Sc_j].$$

Again, by Krull-Schmidt theorem, $Ann_S(c_j) \neq 0$ for $1 \leq j \leq t-r$. So $c_j \in M$ $(1 \leq j \leq t-r)$ and $W \subset M$. By taking $N = (\bigoplus_{i=2}^{r} Sa_i) \bigoplus W$, we complete the proof.

Note that, Theorem 2.1.1 and Theorem 2.1.3 forms a generalization of Wedderburn's theorem (Theorem 1.1.1). For, let F be a finite division ring. As $ch\ F = p$, by Theorem 2.1.1, $|F| = p^n$. By Theorem 2.1.3, F must contain $GR(p,r) = GF(p^r)$. So $F = GF(p^r)$, which is a commutative field.

In the above proof, we have already proved the following.

Theorem 2.1.4. ([26, Theorem]) Let R be a finite local ring, and S a coefficient subring of S . Let f be an inner automorphism of R. Ij $f(S) \subset S$, then the restriction $f|_S$ is the identity mapping of S.

Proof. Let M be the radical of R, and $K = R/M = GF(p^r)$. Let p^k be the characteristic of R, and let $S \cong GR(p^k, r)$ be a coefficient subring of R.

By Proposition 2.1.2 (1), there exists $u \in R^*$ such that $o(u) = p^r - 1$ and $S = \mathbf{Z}_{p^k}[u]$. Let I_a denote the inner automorphism of R given by $x \longmapsto a^{-1}xa \quad (x \in R)$. Suppose $I_a(S) \subset S$.

Since R^* is a semidirect product of $\langle u\rangle$ with $1+M$, we can write

$a = u^i(1+x) \ \ (i \geq 0, \ x \in M)$.

Then, we can easily see that

$I_a(u) - u = I_{1+x}(u) - u \in M$.

Combining this with $I_a(u) \in S$, we ready obtain

$I_{1+x}(u) - u = y_0 \in pS$.

By Theorem 2.1.3 (3), $R = S \bigoplus M'$ with some (S,S)-submodule M' of M. Let $x = x_0 + x'$ with $x_0 \in S$ and $x' \in M'$. Since S is commutative,

$(1+x)\{I_{1+x}(u) - u\} = (1+x)y_0$

simplifies to

$ux' - x'u - x'y_0 = (1+x_0)y_0$.

Obviously, the last belongs to $S \cap M' = 0$, and hence $(1+x_0)y_0 = 0$. Since x_0 is in pS , it follows $y_0 = 0$. We conclude therefore

$I_a(u) = I_{1+x}(u) = u$,

which proves that I_a induces the identity mapping on S.

Corollary 2.1.5. ([26]) Let R be a finite local ring with radical M and residue field $K = GF(p^r)$. Let u be an element of R such that $o(u) = p^r - 1$, and let

$N = \{x \in M \mid xu = ux\}$. Then:

(1) The number of all coefficient subrings of R is equal to $|M : N|$.

(2) R has exactly one coefficient subring if and only if R^* is nilpotent.

Proof. (1) Let $S = \mathbf{Z}_{p^k}[u]$. Two coefficient subrings $S_1 = a^{-1}Sa$ and $S_2 = b^{-1}Sb \ \ (a, \ b \in R^*)$ coincide if and only if $a^{-1}b \in \{x \in R^* \mid xS = Sx\}$. So, the number of all coefficient subrings of R is given by $|R^* : L|$, where $L = \{a \in R^* \mid I_a(S) = S\}$. By Theorem 2.1.4, we see that

$L = \{a \in R^* \mid I_a(u) = u\} = \{u^i(1+x) \mid xu = ux \ , \ x \in M \ , \ 1 \leq i \leq p^r - 1\}$.

Hence,

$|L| = (p^r - 1)|N|$,

so we obtain

$|R^* : L| = (p^r - 1)|M|/(p^r - 1)|N|$

$= |M : N|$.

(2) R contains exactly one coefficient subring if and only if $M = N$. Since R^* is a semidirect product of $\langle u \rangle$ with $1 + M$, this condition means that R^* is a direct product of $\langle u \rangle$ and $1 + M$. By Theorem 1.2.3 and Lemma 1.2.4, this implies that R^* is a nilpotent group.

Corollary 2.1.6. ([27, Corollary]) Let R be a finite local ring with residue field $GF(p)$. Then R has a unique coefficient subring.

Proof. Let M be the radical of R. Let u and N be as in Corollary 2.1.5. As K is the prime field, we see $N = M$. So by Corollary 2.1.5, R has a unique coefficient subring.

The following theorem also is a generalization of Wedderburn's theorem (Theorem 1.1.1).

Theorem 2.1.7. ([6, Lemma 2]) Let R be a finite local ring whose order is a power of a prime p. Then R is a Galois ring if and only ij $J(R) = pR$.

Proof. Let $R/J(R) = GF(p^r)$, and let p^k be the characteristic of R.

Suppose that $J(R) = pR$. Let S be a coefficient subring of R. Since $S + pR = R$, we have

$R = S + p(S + pR) = S + p^2R = \cdots = S + p^kR = S$.

So R must be commutative. The rest of the proof will be clear by Theorem 1.7.2 and Corollary 1.7.5.

§2. Coefficient Subrings of Certain Infinite Local Rings

Let G be a group, and N a normal subgroup of G. Let $\rho : G \longrightarrow H = G/N$ be the natural homomorphism. A monomorphism $\lambda : H \longrightarrow G$ 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 (Theorem 1.2.1).

Lemma 2.2.1. Let G be a group, and N a normal subgroup of G. Let $\rho : G \longrightarrow H = G/N$ be the natural homomorphism. Assume that N is locally finite, and there exists a sequence $\{H_i\}_{i=1}^{\infty}$ of finite subgroups oj H such that $H_i \subset H_{i+1}$ $(i \geq 1)$, $\bigcup_{i=1}^{\infty} H_i = H$ and, for any $a \in N$ and any $i \geq 1$, $o(a)$ and $|H_i|$ are coprime. Then:

(1) There exists a right inverse $\lambda : H \longrightarrow G$ of ρ.

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

(3) If $\mu' : H_m \longrightarrow G$ and $\mu'' : H_m \longrightarrow G$ 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.

(4) Assume further that both H and N are nilpotent. Then there exists a unique right inverse of ρ if and only if G is a nilpotent group.

Proof. (1) By Theorem 1.2.5, G is locally finite. For each $x \in H_1$, we can choose an element g_x of G such that $\rho(g_x) = x$. 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 (Theorem 1.2.1), there exists a right inverse

$\lambda_1 : H_1 \longrightarrow G_1$ 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. Again by Schur-Zassenhaus theorem, 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 $\lambda_2 : H_2 \longrightarrow G_2$ defined by $H_2 = G_2/N_2 \ni bN_2 \longmapsto b \ (b \in L)$ 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 $G_1 \subset G_2 \subset \cdots$ of finite subgroups of G and a sequence $\{\lambda_i\}_{i=1}^{\infty}$ of right inverses $\lambda_i : H_i \longrightarrow G_i$ of $\rho|_{G_i}$ such that $\lambda_j|_{H_i} = \lambda_i$ for any $1 \leq i \leq j$. Then $\lambda = \lim_{\rightarrow} \lambda_i : H = \bigcup_{i=1}^{\infty} H_i \longrightarrow G$ is a right inverse of ρ.

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

(3) 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.

(4) Assume that $\lambda : H \longrightarrow G$ 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 $\mu : H \longrightarrow G$ 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 $\lambda = \mu$.

Let G, N, H and $\rho : G \longrightarrow H$ be as in Lemma 2.2.1. 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 2.2.1 (3), G has the property (GC) with respect to N.

Let R be a ring. Let S be a subring of R , and $I = J(R) \cap S$. The homomorphism of S/I to $R/J(R)$ defined by $a + I \longmapsto a + J(R)$ $(a \in S)$ 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 the main theorems of this section, which generalize the result of R. Raghavendran [17, p. 373, Theorem XIX.4].

Theorem 2.2.2. ([30, 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 oj 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 $\bigcup_{i=1}^{\infty} K_i = K$. Let $K_i = GF(p^{r_i})$. The natural homomorphism $\pi : R \longrightarrow K$ 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. By the isomorphism

$1 + M \ni 1 + x \longmapsto -x$, we see that $1 + M$ is isomorphic to the circle group of M. So, by Lemma 1.2.4, $1 + M$ is a nilpotent group. Furthermore, $K^* = \bigcup_{i=1}^{\infty} K_i^*$, where $|K_i^*| = p^{r_i} - 1$ is coprime to p. So, by Lemma 2.2.1 (1), there exists a right inverse $\lambda\ : K^* \longrightarrow R^*$ of π^*. For each $i \geq 1$, let α_i be a generator of K_i^*. By Proposition 2.1.2 (2), 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, $S = \langle \lambda(K^*) \rangle = \bigcup_{i=1}^{\infty} S_i$ is an IG-subring of R, and S/pS is naturally isomorphic to K.

Such a subring S of R stated in Theorem 2.2.2 will be called a coefficient subring of R. When R is a commutative local ring satisfying the assumption of Theorem 2.2.2, S coincides with the subring described in Theorem 1.3.2.

Let R, M, S and $K = \bigcup_{i=1}^{\infty} GF(p^{r_i})$ be as in Theorem 2.2.2, where $\{r_i\}_{i=1}^{\infty}$ is a sequence of positive integers such that $r_i | r_{i+1}$ $(i \geq 1)$. Let p^n be the characteristic of R. Let S' be another coefficient subring of R. By Theorem 1.3.1 and Proposition 1.9.1 (1), $S' \cong \bigcup_{i=1}^{\infty} GR(p^n, r_i)$, which is isomorphic to S. By Proposition 1.9.1 (5), there exists a left S'-submodule N of R such that $R = S' \bigoplus N$ as left S'-modules.

If $\lambda : K^* \longrightarrow R^*$ is a right inverse of π^* , then by the proof of Theorem 2.2.2, $S = \langle \lambda(K^*) \rangle$ 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 $\bigcup_{i=1}^{\infty} K_i = K$. 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 Proposition 2.1.2 (2), both $T = \langle \lambda(K_j^*) \rangle$ and $T' = \langle \mu(K_j^*) \rangle$ are isomorphic to $GR(p^n, r_j)$. As $S = \bigcup_{i=1}^{\infty} \langle \lambda(K_i^*) \rangle$, there exists a number

$\ell \geq 1$ such that $T \cup T' \subset \langle \lambda(K_\ell^*) \rangle$. Since $\langle \lambda(K_\ell^*) \rangle$ 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 2.2.1 (1), we can easily see that, if S is a coefficient subring of R, there exists a right inverse $\lambda : K^* \longrightarrow S^*$ of π^* such that $S = \langle \lambda(K^*) \rangle$.

Summarizing the above, we obtain the following theorem.

Theorem 2.2.3. ([30, 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 $GF(p)$. Let $\pi^* : R^* \longrightarrow K^*$ be the group homomorphism induced by the natural ring homomorphism $\pi : R \longrightarrow K$. Then:

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

(2) All coefficient subrings of R are isomorphic.

(3) If $\lambda : K^* \longrightarrow R^*$ 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 $\lambda : K^* \longrightarrow R^*$ of π^* such that $S = \langle \lambda(K^*) \rangle$.

(4) 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 2.2.3, M/M^2 is regarded as a left K-space by the operation

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

Theorem 2.2.4. ([30, 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 $R = S \bigoplus N$ as left S-modules, and there exists a decreasing sequence $n_1 \geq n_2 \geq \cdots\cdot \geq n_t$ of positive integers (p^{n_1} is the characteristic of R) such that R is isomorphic to a subring of $M(S; n_1, n_2, \cdots\cdot, n_t)$.

Proof. Assume that R is finitely generated as a left S-module. Then R is a Noetherian left S-module, since S is a Noetherian ring by Proposition 1.9.1 (4). 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 $x_1, x_2, \cdots\cdot, x_d$ 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 y of M is written as

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

Let

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

be another element of M. Then

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

Each $x_i b_j$ is written as

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

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

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

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 2.2.3 (1), there exists a finitely generated left S-submodule N' of R such that $R = S \bigoplus N'$ as left S-modules. By Proposition 1.9.1 (3), 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 $x_1, x_2, \cdots, x_t \in N'$ such that $N' = \bigoplus_{i=1}^{t} V x_i = \bigoplus_{i=1}^{t} S x_i$. By putting $x_0 = 1$, we get $R = \bigoplus_{i=0}^{t} S x_i$. Let $c_1, c_2, \cdots, c_t$ be elements of S such that $\bar{c}_i = \bar{x}_i$ under the natural homomorphism $\pi : R \longrightarrow K$. 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 $R = \bigoplus_{i=0}^{t} S x_i = \bigoplus_{i=0}^{t} S y_i$. So $N = \bigoplus_{i=1}^{t} S y_i$ has the desired property. The last statement is immediate from Lemma 1.9.2.

As a corollary, we get the following.

Corollary 2.2.5. ([35, Lemma 2.1], [17, p. 371, Corollary XIX.3])

Let R be a finite local ring with characteristic p^k. Then R contains a coefficient subring S, and R is isomorphic to a subring of a ring of Szele matrices $M(S; n_1, n_2, \cdots, n_t)$, where $k = n_1 \geq n_2 \geq \cdots \geq n_t$.

§3. Number of Coefficient Subrings

Let R be a local ring described in Theorem 2.2.2. Then R may have more than one coefficient subrings. Concerning this subject, first we can state the following.

Theorem 2.3.1. ([30, 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 $T = \bigcup_{i=1}^{\infty} GR(p^n, r_i)$, where $\{r_i\}_{i=1}^{\infty}$ is a sequence of positive integers such that $r_i | r_{i+1}$ $(i \geq 1)$. Let $K = T/pT$ and $\pi' : T \longrightarrow K$ 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 1.9.1 (6)). Let A be a set of cardinality χ, and $V = \bigoplus_{\alpha \in A} T$ be a free T-module. The abelian group $T \bigoplus V$ together with the multiplication

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

forms a ring, which we denote by R. Let $\pi : R \longrightarrow K$ be the homomorphism defined by $(a, x) \longmapsto \pi'(a)$, 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 2.2.3 (3), 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 $\pi^* = \pi|_{R^*} : R^* \longrightarrow K^*$.

By the embedding $T \ni a \longmapsto (a, 0) \in R$, T is regarded as a coefficient subring of R. So, by Theorem 2.2.3 (3), there exists a right inverse $\lambda : K^* \longrightarrow R^*$ of π^* such that $\langle \lambda(K^*) \rangle = T$. Since $K = \bigcup_{i=1}^{\infty} GF(p^{r_i})$, there exists a number $j \geq 1$ 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 $\mu'_z : GF(p^{r_j})^* \longrightarrow R^*$ by $\gamma^i \longmapsto (c, z)^i$. By Lemma 2.2.1 (2), 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 $|Y| \geq |V| = \chi$.

Let S be a coefficient subring of R. We shall show that S is conjugate to T. By Theorem 2.2.3 (3), there exists a right inverse $\lambda' : K^* \longrightarrow R^*$ 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

$(c, z) = \lambda'(\gamma) = \lambda'(\alpha^m) = (a, y)^m = (a^m, \{a^m - (\sigma(a))^m\}\{a - \sigma(a)\}^{-1} y)$,
we get $c = a^m$ 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 $GF(p^{r_j})^*$ (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 said to be of type $(\bullet)$ 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 $(\bullet)$, then T^* is not a nilpotent group. Let us suppose that T is a finite local ring of type $(\bullet)$. 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 2.3.2. ([30, 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.

(1) R has a unique coefficient subring.

(2) R^* is a nilpotent group.

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

(4) R^* has no finite local subring of type $(\bullet)$.

Proof. (1) $\Longleftrightarrow$ (2). Clear from Lemma 2.2.1 (4) and Theorem 2.2.3 (3).

(1) $\Longrightarrow$ (3). Let $\pi^* = \pi|_{R^*} : R^* \longrightarrow K^*$ be the group homomorphism induced by the natural homomorphism $\pi : R \longrightarrow K$. Since R has a unique coefficient subring, by Theorem 2.2.3 (3), 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 $\mu : K^* \longrightarrow R^*$ defined by $K^* \ni \alpha \longmapsto z^{-1}\lambda(\alpha)z$ 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 $\lambda(K^*)$.

(3) $\Longrightarrow$ (4). Let us suppose that R contains a finite local subring U of type ($\bullet$). By Theorem 1.2.4, $1 + M$, which is isomorphic to the circle group of 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.

(4) $\Longrightarrow$ (1). 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 $\bigcup_{i=1}^{\infty} K_i = K$. 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 ($\bullet$).

§4. Counterexample

Viewing Theorem 1.2.1, Theorem 2.1.3 and the proof of Theorem 2.3.1, one may expect that, in Theorem 2.2.3, any two coefficient subrings of R are always conjugate. However, from the following example, we see that this is incorrect.

Let $K = \bigcup_{i=1}^{\infty} GF(p^{r_i})$, 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 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 $V = \bigoplus_{i=1}^{\infty} Kx_i$ be a left K-vector space with basis $\{x_i\}_{i=1}^{\infty}$. We can regard V as a (K, K)-bimodule by defining

$$(\textstyle\sum_i c_i x_i)a = \sum_i c_i \sigma_i(a) x_i \quad (\sum_i c_i x_i \in V, a \in K).$$

The Abelian group $R = K \bigoplus V$ together with the multiplication

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

forms a local ring with radical $M = (0, V)$, which satisfies the assumption of Theorem 2.2.3. The homomorphism $\pi : R \longrightarrow K$ defined by $(a, x) \longmapsto a$ gives the isomorphism $R/M \cong K$. The subring $S = \{(a, 0) \mid a \in K\}$ of R is a coefficient subring of R.

By our definition, for any positive integer t and any

$$(\beta, \textstyle\sum_{j=1}^{n} b_j x_j) \in R \quad (\beta, b_j \in K)\ ,$$

it holds that

$$(\beta, \textstyle\sum_{j=1}^{n} b_j x_j)^t$$
$$= (\beta^t, \textstyle\sum_{j=1}^{n} \{\beta^{t-1} + \beta^{t-2}\sigma_j(\beta) + \cdots + \sigma_j(\beta)^{t-1}\} a_j x_j).$$

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 $u_n = (\gamma_n, \sum_{j=1}^{n} r_j x_j)$ $(r_j \in K)$, 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

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

Then

$$u_{i+1}^{p^{r_i}-1} = (\gamma_{i+1}^{p^{r_i}-1},\ \textstyle\sum_{j=1}^{i} \{\gamma_{i+1}^{p^{r_i}-2} + \cdots + \sigma_j(\gamma_{i+1})^{p^{r_i}-2}\} a_j x_j$$
$$+ \{\gamma_{i+1}^{p^{r_i}-2} + \cdots + \sigma_{i+1}(\gamma_{i+1})^{p^{r_i}-2}\} x_{i+1}),$$

where we see that

$$\gamma_i^{p^{r_i}-1} = 1 \text{ , and}$$

$$\gamma_{i+1}^{p^{r_i}-2} + \cdots + \sigma_j(\gamma_{i+1})^{p^{r_i}-2}$$

$$= \{\gamma_{i+1} - \sigma_j(\gamma_{i+1})\}^{-1} \cdot \{\gamma_{i+1}^{p^{r_i}-1} - \sigma_j(\gamma_{i+1})^{p^{r_i}-1}\}$$

$$= \{\gamma_{i+1} - \sigma_j(\gamma_{i+1})\}^{-1} \cdot \{1 - 1\}$$

$$= 0$$

for $1 \leq j \leq i+1$. So we see $o(u_i) = p^{r_i} - 1$. Also,

$$u_{i+1}^{m_i} = (\gamma_{i+1}, \textstyle\sum_{j=1}^{i} a_j x_j + x_{i+1})^{m_i}$$

$$= (\gamma_{i+1}^{m_i},\ \textstyle\sum_{j=1}^{i}\{\gamma_{i+1}^{m_i-1} + \cdots + \sigma_j(\gamma_{i+1})^{m_i-1}\}a_j x_j$$

$$+\{\gamma_{i+1}^{m_i-1} + \cdots + \sigma_{i+1}(\gamma_{i+1})^{m_i-1}\}x_{i+1}),$$

where

$$\gamma_{i+1}^{m_i} = \gamma_i,$$

$$\{\gamma_{i+1}^{m_i-1} + \cdots + \sigma_j(\gamma_{i+1})^{m_i-1}\}a_j$$

$$= \{\gamma_{i+1} - \sigma_j(\gamma_{i+1})\}^{-1} \cdot \{\gamma_{i+1}^{m_i} - \sigma_j(\gamma_{i+1})^{m_i}\}a_j$$

$$= \{\gamma_{i+1} - \sigma_j(\gamma_{i+1})\}^{-1} \cdot \{\gamma_i - \sigma_j(\gamma_i)\}a_j$$

$$= r_j \ (1 \leq j \leq i), \text{ and}$$

$$\gamma_{i+1}^{m_i-1} + \cdots + \sigma_{i+1}(\gamma_{i+1})^{m_i-1}$$

$$= \{\gamma_{i+1} - \sigma_{i+1}(\gamma_{i+1})\}^{-1} \cdot \{\gamma_i - \sigma_{i+1}(\gamma_i)\} = 0.$$

Hence we have

$$u_{i+1}^{m_i} = u_i$$

for each $i \geq 1$.

Now let $f_i : GF(p^{r_i})^* \longrightarrow R^*$ be defined by $\gamma_i^t \longmapsto u_i^t$ ($t \in \mathbf{Z}$). Since $f_i|_{GF(p^{r_j})^*} = f_j$ for $j \leq i$, there exists $f = \lim_{\rightarrow} f_i : K^* \longrightarrow R^*$. As f is a right inverse of $\pi^* = \pi|_{R^*} : R^* \longrightarrow K^*$, 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 $v = (s, \sum_i d_i x_i) \in R^*$ ($s \in K^*, d_i \in K$) 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,

$$\begin{aligned} u_i &= (\gamma_i, \textstyle\sum_{j=1}^{i-1} r'_j x_j + x_i) \ \ (r'_j \in K) \\ &= v^{-1}(b_i, 0)v \\ &= (s^{-1}, -s^{-1}(\textstyle\sum_i d_i x_i)s^{-1})(b_i, 0)(s, \textstyle\sum_i d_i x_i) \\ &= (b_i, \textstyle\sum_{j=1}^{i}(s^{-1}b_i d_j - s^{-1}d_j \sigma_j(b_i))x_j), \end{aligned}$$

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 $\sum_i d_i x_i$ is an element of the direct sum $V = \bigoplus_{i=1}^{\infty} K x_i$.

§5. A Generalization of W. E. Clark's Theorem

In this section, we shall state a theorem which is a generalization of [6, Theorem].

Theorem 2.5.1. ([30, Theorem 4.1]) Let R be a ring with 1. Assume that $J(R)$ is nilpotent. Let

$$R/J(R) = (K_1)_{n_1 \times n_1} \bigoplus (K_2)_{n_2 \times n_2} \bigoplus \cdots \cdot \bigoplus (K_d)_{n_d \times n_d},$$

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.

(1) $\quad R = T \oplus N \quad$ (as Abelian groups), where N is an additive subgroup of $J(R)$.

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

(3) $J(T) = T \cap J(R) = pT$.

(4) T/pT *is naturally isomorphic to* $R/J(R)$.

Moreover, if T' *is another subring of* R *satisfying (2) - (4), then* T' *is isomorphic to* T.

Proof. Let $\bar{R} = R/J(R) = \bar{R}\bar{e}_1 \bigoplus \bar{R}\bar{e}_2 \bigoplus \cdot \cdot \cdot \cdot \bigoplus \bar{R}\bar{e}_d$, where each $\bar{R}\bar{e}_i$ $(1 \leq i \leq d)$ is a simple component of $\bar{R}$, and $\bar{e}_i$ is a central idempotent of $\bar{R}$. Let $\bar{R}\bar{e}_i = (K_i)_{n_i \times n_i}$, where K_i is a commutative field which is algebraic over $GF(p)$. Let $\pi : R \longrightarrow \bar{R}$ be the natural homomorphism. There are mutually orthogonal idempotents $e_1, e_2, \cdots, e_d$ of R such that $e_1 + e_2 + \cdot \cdot \cdot \cdot + e_d = 1$ and $\pi(e_i) = \bar{e}_i$ $(1 \leq i \leq d)$. Then,

$$R = e_1Re_1 \bigoplus e_2Re_2 \bigoplus \cdot \cdot \cdot \cdot \bigoplus e_dRe_d \bigoplus (\textstyle\bigoplus_{i \neq j} e_iRe_j)$$

as abelian groups. Since each e_iRe_i is semiperfect and

$$e_iRe_i/J(e_iRe_i) \cong \bar{R}\bar{e}_i = (K_i)_{n_i \times n_i},$$

by Theorem 1.1.3, there exist a local ring S_i and an isomorphism φ_i of e_iRe_i onto $(S_i)_{n_i \times n_i}$. Let

$$\varphi = \varphi_1 + \varphi_2 + \cdot \cdot \cdot \cdot + \varphi_d : e_1Re_1 \bigoplus e_2Re_2 \bigoplus \cdot \cdot \cdot \cdot \bigoplus e_dRe_d \longrightarrow$$
$$A = (S_1)_{n_1 \times n_1} \bigoplus (S_2)_{n_2 \times n_2} \bigoplus \cdot \cdot \cdot \cdot \bigoplus (S_d)_{n_d \times n_d}$$

be the isomorphism. Since $S_i/J(S_i) \cong K_i$, by Theorem 2.2.2 and Theorem 2.2.3 (1), there exist an IG-subring T_i and a left T_i-submodule N_i of S_i such that $S_i = T_i \bigoplus N_i$ (as Abelian groups), and T_i/pT_i is naturally isomorphic to $S_i/J(S_i)$. Then

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

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

$$(e_1Re_1 \bigoplus e_2Re_2 \bigoplus \cdot \cdot \cdot \cdot \bigoplus e_dRe_d)/J(e_1Re_1 \bigoplus e_2Re_2 \bigoplus \cdot \cdot \cdot \cdot \bigoplus e_dRe_d)$$
$$= R/J(R).$$

Let us put

$$N = \varphi^{-1}\{(N_1)_{n_1 \times n_1} \bigoplus (N_2)_{n_2 \times n_2} \bigoplus \cdots \cdot \bigoplus (N_d)_{n_d \times n_d}\}$$
$$\bigoplus \{\bigoplus_{i \neq j} e_i R e_j\} \; .$$

Then we see $R = T \bigoplus N$.

Now, let us suppose that T' is a subring of R satisfying (2) - (4). 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 $\pi(e) = \bar{e}$ and $\pi(f) = \bar{f}$. Assume that $Re \cong Rf$. Then $\bar{R}\bar{e} \cong \bar{R}\bar{f}$ as left $\bar{R}$-modules. Both $\bar{R}\bar{e}$ and $\bar{R}\bar{f}$ are minimal left ideals of $\bar{R}$, so they are contained in the same simple component of $\bar{R}$, which implies that $J(R)$ does not include eRf. Conversely, if $J(R)$ does not include eRf, then $\bar{R}\bar{e} \cong \bar{R}\bar{f}$, which means $Re \cong Rf$ by Theorem 1.1.5. 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 $R/J(R)$, $J(R)$ includes 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

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

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

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

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

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 $f_{\ell j}$ are primitive idempotents of R. Then $R = \bigoplus Re_{ki} = \bigoplus Rf_{\ell j}$ are indecomposable decompositions.

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

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

and

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

where $e_{i1}Te_{i1}$ and $f_{j1}T'f_{j1}$ are IG-rings. Hence, to complete the proof it will be 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 $e_{i1}Re_{i1} \cong End(_R Re_{i1}) \cong End(_R Rf_{i1}) \cong f_{i1}Rf_{i1}$, we see $e_{i1}Te_{i1} \cong f_{i1}T'f_{i1}$ by Theorem 2.2.3 (2).

As a corollary of this theorem, we have the following.

Corollary 2.5.2. ([6, Theorem],[17, p. 376, Theorem XIX.5]) Let R be a finite ring with 1 *of characteristic p^n. Then R contains a subring T such that:*

(1) $R = T \bigoplus N$ as Abelian groups, where $J(T) = pT$ and N is an additive subgroup of $J(R)$.

(2) T/pT is naturally isomorphic to $R/J(R)$.

(3) T is isomorphic to $\bigoplus_{i=1}^{t}(R_i)_{n_i \times n_i}$, where R_i $(1 \leq i \leq t)$ are Galois rings.

Chapter III

Everett Ring Extensions

§1. Double Homothetisms

In this section, we shall give additional informations concerning the structure of rings considered in Theorem 2.2.2. The following description is based on [21, §52 and §53].

Let I be a ring not necessarily contain 1 . Let $E_1(I)$ denote the right I-endomorphism ring of I, and $E_2(I)$ denote the left I-endomorphism ring of I. Any element of $E_1(I)$ or $E_2(I)$ will act on I from the left. Let $E'(I)$ be the Abelian group

$$E_1(I) \bigoplus E_2(I) = \{f = (f^1, f^2) \mid f^1 \in E_1(I),\ f^2 \in E_2(I)\}.$$

Defining the multiplication on $E'(I)$ by

$$(f^1, f^2)(g^1, g^2) = (f^1 g^1, g^2 f^2),$$

we see that $E'(I)$ forms a ring. An element $f = (f^1, f^2) \in E'(I)$ is called a double homothetism of I if

(S1) $(f^2 x)y = x(f^1 y)$, and

(S2) $f^2(f^1 x) = f^1(f^2 x)$ $(x,\ y \in I)$.

We denote by $DH(I)$ the set of all double homothetisms of I. Although $DH(I)$ is closed under addition, it is not necessarily closed under multiplication.

Given $a \in I$, we define $[a] = (a^1, a^2)$ by

$$a^1 x = ax \ , \ a^2 x = xa \ (x \in I).$$

This $[a]$ is called the inner double homothetism induced by a.

Two double homothetisms $f = (f^1, f^2)$ and $g = (g^1, g^2)$ are said to be related if

(S3) $f^1(g^2x) = g^2(f^1x)$

(S4) $f^2(g^1x) = g^1(f^2x)$ $(x \in I)$.

This property is symmetric and reflexive, however, not transitive. Each inner double homothetism of I is related to any double homothetism of I. A set S of double homothetisms of I is said to be related if any two elements of S are related.

In [9], C. J. Everett gave a solution for Schreier's problem for extensions of rings.

Let A and I be rings (not necessarily contain 1). We shall say that R is an Everett extension of I by A, if I is an ideal of R and there exists an isomorphism φ of R/I onto A.

In what follows, we shall write elements of A by $\alpha, \beta, \cdots$, and elements of I by $x, y, \cdots$. We shall denote the zero of A by o, and the zero of I by 0.

A set $([\ ,\ ], \langle\ ,\ \rangle, d)$ of mappings

$[\ ,\ ] : A \times A \longrightarrow I$

$\langle\ ,\ \rangle : A \times A \longrightarrow I$

$d : A \longrightarrow DH(I)$

is called an Everett function triple for A and I if the following (S5) - (S16) are satisfied.

(S5) $[o, \alpha] = [\alpha, o] = 0$

(S6) $\langle o, \alpha\rangle = \langle \alpha, o\rangle = 0$

(S7) $d_o^1 x = d_o^2 x = 0$

(S8) $d_{\alpha+\beta}^1 x + [\alpha, \beta]x = d_\alpha^1 x + d_\beta^1 x$

(S9) $d_{\alpha+\beta}^2 x + x[\alpha, \beta] = d_\alpha^2 x + d_\beta^2 x$

(S10) $d_{\alpha\beta}^1 x + \langle \alpha, \beta\rangle x = d_\alpha^1(d_\beta^1 x)$

(S11) $d_{\alpha\beta}^2 x + x\langle \alpha, \beta\rangle = d_\beta^2(d_\alpha^2 x)$

(S12) $[\alpha, \beta] = [\beta, \alpha]$

(S13) $[\alpha,\beta]+[\alpha+\beta,\gamma]=[\alpha,\beta+\gamma]+[\beta,\gamma]$

(S14) $\langle\alpha\beta,\gamma\rangle+d^2_\gamma(\langle\alpha,\beta\rangle)=\langle\alpha,\beta\gamma\rangle+d^1_\alpha(\langle\beta,\gamma\rangle)$

(S15) $d^1_\gamma([\alpha,\beta])+\langle\gamma,\alpha+\beta\rangle=[\gamma\alpha,\gamma\beta]+\langle\gamma,\alpha\rangle+\langle\gamma,\beta\rangle$

(S16) $d^2_\gamma([\alpha,\beta])+\langle\alpha+\beta,\gamma\rangle=[\alpha\gamma,\beta\gamma]+\langle\alpha,\gamma\rangle+\langle\beta,\gamma\rangle$

$(\alpha,\beta,\gamma\in A,\ x\in I)$

Let $([\ ,\ ],\langle\ ,\ \rangle,d)$ be an Everett function triple for A and I. Then the set $A\times I$ together with the operations

$$(\alpha,x)+(\beta,y)=(\alpha+\beta,[\alpha,\beta]+x+y),$$

$$(\alpha,x)(\beta,y)=(\alpha\beta,\langle\alpha,\beta\rangle+d^1_\alpha y+d^2_\beta x+xy)$$

forms a ring. This ring is called the Everett sum of A and I corresponding to the Everett function triple $([\ ,\ ],\langle\ ,\ \rangle,d)$, and will be denoted by $A\Box I$. By the homomorphism

$$I\ni x\longmapsto(0,x),$$

I is regarded as an ideal of $A\Box I$. By the homomorphism

$$(\alpha,0)\longmapsto\alpha,$$

we have the isomorphism $A\Box I/I\cong A$.

Theorem 3.1.1. (fundamental theorem of Everett for ring extensions, [21, §52, Satz 112, Satz 113]) Let A and I be rings. Let $([\ ,\ ],\langle\ ,\ \rangle,d)$ *be an Everett function triple for A and I. Then the Everett sum corresponding to* $([\ ,\ ],\langle\ ,\ \rangle,d)$ *is an Everett extension of I by A.*

Conversely, let R be an Everett extension of I by A. Then there exists an Everett function triple $([\ ,\ ],\langle\ ,\ \rangle,d)$ *for A and I, and an isomorphism of the Everett sum* $A\Box I$ *corresponding to* $([\ ,\ ],\langle\ ,\ \rangle,d)$ *onto R which leaves the elements of I fixed and induces the identity mapping of A modulo I.*

Proof. The first half will be clear. Let us suppose that R is an Everett extension of I by A. We can take a choice function

$$f:\alpha\longmapsto f(\alpha)\in\alpha$$

of $A = R/I$ to R such that $f(o) = 0$. Let us put

$[\alpha, \beta] = f(\alpha) + f(\beta) - f(\alpha + \beta)$,

$\langle \alpha, \beta \rangle = f(\alpha)f(\beta) - f(\alpha\beta)$,

$d^1_\alpha x = f(\alpha)x$, and

$d^2_\alpha x = xf(\alpha)$.

Then it is easy to check that this $([\ ,\ ], \langle\ ,\ \rangle, d)$ is an Everett function triple for A and I, and the homomorphism

$(\alpha, x) \longmapsto f(\alpha) + x$

is an isomorphism of $A\square I$ to R with the desired property.

§2. Everett Function Couple

By the proof of Theorem 3.1.1, we see that, if there exists a choice function

$\alpha \longmapsto f(\alpha) \in A$

of $A = R/I$ to R such that $f(o) = 0$ and $f(\alpha\beta) = f(\alpha)f(\beta)$ $(\alpha,\ \beta \in A)$, then we can take $\langle \alpha, \beta \rangle \equiv 0$.

Let A be a ring with 1. Let $([\ ,\ ], d)$ be a set of mappings

$[\ ,\ ] : A \times A \longrightarrow I$ and

$d : A \longrightarrow DH(I)$

which satisfies (S5), (S7), (S8), (S9), (S12), (S13) and the following (S17) - (S21).

(S17) $d_{\alpha\beta} = d_\alpha d_\beta$

(S18) $d^1_\gamma([\alpha, \beta]) = [\gamma\alpha, \gamma\beta]$

(S19) $d^2_\gamma([\alpha, \beta]) = [\alpha\gamma, \beta\gamma]$

(S20) $d^1_\alpha(d^2_\beta x) = d^2_\beta(d^1_\alpha x)$

(S21) $d_1^1 x = d_1^2 x = x \quad (\alpha, \beta, \gamma \in A,\ x \in I)$

Such a couple of mappings $([\ ,\ ], d)$ will be called an Everett function couple for A and I. It is easy to check that the set $A \times I$ forms a ring concerning the operations defined by

(S22) $(\alpha, x) + (\beta, y) = (\alpha + \beta, [\alpha, \beta] + x + y)$

(S23) $(\alpha, x)(\beta, y) = (\alpha\beta, d_\alpha^1 y + d_\beta^2 x + xy)$.

This ring will be called an Everett sum of A and I corresponding to the Everett function couple $([\ ,\ ], d)$, and denoted by $A\Box I$ (cf. [21, §52]). Obviously, $e = (1, 0)$ is the identity of $A\Box I$. By the mapping $x \longmapsto (0, x)$, I is regarded as an ideal of $A\Box I$, and the residue ring $(A\Box I)/I$ is naturally identified with A.

Conversely, let R be a ring with 1, I an ideal of R, and $A = R/I$. Let $\pi : R \longrightarrow A$ be the natural homomorphism. A mapping $f : A \longrightarrow R$ is called a multiplicative cross-section if (i) $f(\alpha\beta) = f(\alpha)f(\beta)$ $(\alpha, \beta \in A)$, (ii) $f(o) = 0$, and (iii) $\pi \circ f = id_A$.

Theorem 3.2.1. ([29, Theorem 1]) Let R be a ring with 1, I an ideal oj R, and $A = R/I$. Suppose that there exists a multiplicative cross-section $f : A \longmapsto R$. Then there exists an Everett function couple $([\ ,\ ], d)$ for A and I such that R is isomorphic to the Everett sum $A\Box I$ corresponding to $([\ ,\ ], d)$.

Proof. Let $f : A \longrightarrow R$ be a multiplicative cross-section. We can define the mapping $[\ ,\ ] : A \times A \longrightarrow I$ and the mapping $d : A \longrightarrow DH(I)$ by

(S24) $[\alpha, \beta] = f(\alpha) + f(\beta) - f(\alpha + \beta)$,

(S25) $d_\alpha^1 x = f(\alpha)x$, and

(S26) $d_\alpha^2 x = xf(\alpha)$.

It is easy to check that $([\ ,\ ], d)$ is an Everett function couple for A and I. So we can construct the Everett sum $A\Box I$ corresponding to $([\ ,\ ], d)$.

Let us define $\sigma : R \longrightarrow A\Box I$ by $a \longmapsto (\pi(a), a - f(\pi(a)))$. We see that σ is an isomorphism of R onto $A\Box I$.

§3. Structure Theorem for Certain Local Rings

In this section, we shall study the structure of local rings stated in Theorem 2.2.3.

Theorem 3.3.1. (cf. [29, Theorem 2]) Let M be a nilpotent ring, and K be a commutative field of characteristic p (p a prime) which is algebraic over $GF(p)$.

If $([\ ,\ ], d)$ is an Everett function couple for K and M, then the Everett sum $K\Box M$ corresponding to $([\ ,\ ], d)$ is a local ring with radical M whose residue field is K. In particular, if $[\alpha, \beta] \equiv 0$, then $K\Box M$ is of characterictic p.

Conversely, if R is a local ring with radical M whose residue field is K, then there exists an Everett function couple $([\ ,\ ], d)$ for K and M such that R is isomorphic to the Everett sum $K\Box M$ corresponding to $([\ ,\ ], d)$. If furthermore R is of characteristic p, then there exists such an Everett couple with $[\alpha, \beta] \equiv 0$.

Proof. Assume that $([\ ,\ ], d)$ is an Everett function couple for K and M, and $R = K\Box M$ is the Everett sum corresponding to it. As $R/M \cong K$ is simple as a left K-module, M is a maximal left ideal of R. So we see $M \supset J(R)$. On the other hand, as M is a nil ideal of R, $M \subset J(R)$. Hence we have $M = J(R)$, which implies that R is a local ring with radical M.

If $[\alpha, \beta] \equiv 0$, then $p(1,0) = (p,0) = 0$, so $K \Box M$ is of characteristic p.

Conversely, let R be a local ring with radical M whose residue field is K. By the proof of Theorem 2.2.2, we see that there exists a multiplicative cross-section $f : K \longrightarrow R$. Then by Theorem 3.2.1, there exists an Everett function couple $([\ ,\ ], d)$ for K and M, and the Everett sum $K \Box M$ corresponding to $([\ ,\ ], d)$ is isomorphic to R. Suppose further that $ch\ R = p$. Then by Theorem 2.2.2, R contains a coefficient subring K', which is a copy of K. By Theorem 2.2.3 (1), $R = K' \bigoplus M'$ as Abelian groups, where M' is a submodule of M. So we can define a multiplicative cross-section $f : K \longrightarrow R$ such that $f(\alpha + \beta) = f(\alpha) + f(\beta)$. So (S24) becomes $[\alpha, \beta] \equiv 0$.

In what follows, let M be a nilpotent ring, and K be a commutative field of characteristic p (p a prime) which is algebraic over $GF(p)$. Let $([\ ,\ ], d)$ be an Everett function couple for K and M, and $K \Box M$ be the Everett sum corresponding to $([\ ,\ ], d)$. Then the unit group $(K \Box M)^*$ is an extension of $1 + M$ by K^*, and is a semidirect product of K^* and $1 + M$. Note that the group structure of $1 + M$ is completely determined by the ring structure of M, and does not depend on the whole structure of $K \Box M$.

We shall say that an Everett function couple $([\ ,\ ], d)$ is symmetric if $d^1_\alpha x = d^2_\alpha x$ ($\alpha \in K,\ x \in M$).

Theorem 3.3.2. (cf. [29, Theorem 3]) Let M be a nilpotent ring, and K be a commutative field of characteristic p (p a prime) which is algebraic over $GF(p)$. Let $K \Box M$ be the Everett sum corresponding to an Everett function couple $([\ ,\ ], d)$ for K and M. Let N be the subring of M generated by $\{[\alpha, \beta] \mid \alpha, \beta \in K\}$. Then:

(1) $S = \{(\alpha, x) \in K \Box M \mid \alpha \in K,\ x \in N\}$ is a coefficient subring oj $K \Box M$.

(2) S is the only coefficient subring of $K \square M$ if and only if $([\ ,\ ], d)$ is symmetric.

Proof. (1) Let $R = K \square M$, and $ch\ R = p^k$. Let $W = \{(u, 0) \in K \square M \mid u \in K\}$. Then by Theorem 2.2.3 (3), the subring U of R generated by W is a coefficient subring of R. It is clear that S is a ring containing W. On the other hand,

$$(0, [\alpha, \beta]) = (\alpha, 0) + (\beta, 0) - (\alpha + \beta, 0) \in U.$$

This implies $S \subset U$, and so $S = U$.

(2) Let us assume that S is the only coefficient subring of R. Suppose that $d^1_\gamma x_0 \neq d^2_\gamma x_0$ for some $\gamma \in K$ and $x_0 \in M$. Let K' be a finite subfield of K which contains γ. Let N_1 be the subring of M generated by $\{d^1_\alpha(d^2_\beta x_0),\ [\alpha, \beta] \mid \alpha, \beta \in K'\}$. Then $R_1 = \{(\alpha, x) \mid \alpha \in K',\ x \in N_1\}$ is a finite local ring with residue field K. By Theorem 2.2.3 (3) and Lemma 2.2.1 (3), R_1 contains a coefficient subring, which is unique by our assumption. Then, by Corollary 2.1.5 (2), R_1^* is nilpotent. So, by Theorem 1.2.3, R_1^* is the direct product of $B = \{(\alpha, 0) \mid \alpha \in (K')^*\}$ and $1 + N_1$. Then

$$(\gamma, d^1_\gamma x_0) = (\gamma, 0)(1, x_0) = (1, x_0)(\gamma, 0) = (\gamma, d^2_\gamma x_0),$$

which contradicts $d^1_\gamma x_0 \neq d^2_\gamma x_0$.

Conversely, let us assume that $([\ ,\ ], d)$ is symmetric. Then $(K \square M)^*$ is the direct product of K^* and $1 + M$. By Lemma 1.2.4, $1 + M$ is nilpotent. So $(K \square M)^*$ is nilpotent. Hence, by Theorem 2.3.2, $K \square M$ has a unique coefficient subring.

§4. Equivalence of Extensions

Let I and A be rings. Assume that there exist two Everett extensions R and R' of I by A. Two extensions R and R' are said to be equivalent if there exists an isomorphism of R onto R' which leaves the elements of I fixed and induces the identity mapping of A modulo I ([21, §52]).

Theorem 3.4.1. ([29, Theorem 4]) Let M be a nilpotent ring and K be a commutative field of characteristic p (p a prime) which is algebraic over $GF(p)$. Let $K\square M$ and $K\tilde{\square}M$ be two Everett sums of K and M corresponding to two Everett function couples $([\ ,\ ], d)$ and $([\ ,\tilde{}\ ], \tilde{d})$, respectively. Then $K\square M$ and $K\tilde{\square}M$ are equivalent (as extensions of M by K) if and only if there exists a mapping $\lambda : K \longrightarrow M$ such that

(S27) $\lambda(\alpha+\beta) - \lambda(\alpha) - \lambda(\beta) = [\alpha,\tilde{\beta}] - [\alpha,\beta]$,

(S28) $\lambda(\alpha\beta) - \lambda(\alpha)\lambda(\beta) = \tilde{d}^1_\alpha(\lambda(\beta)) + \tilde{d}^2_\beta(\lambda(\alpha))$,

(S29) $\lambda(\alpha)x = d^1_\alpha x - \tilde{d}^1_\alpha x$, *and*

(S30) $x\lambda(\alpha) = d^2_\alpha x - \tilde{d}^2_\alpha x \ (\alpha, \beta \in K,\ x \in M)$.

When this is the case, $\{d_\alpha\}_{\alpha\in K} \cup \{\tilde{d}_\alpha\}_{\alpha\in K}$ is a related set of double homothetisms of M.

Proof. If $\sigma : K\square M \longrightarrow K\tilde{\square}M$ is an isomorphism which leaves the elements of M fixed and induces the identity mapping of K modulo M, then we can write

$\sigma(\alpha, 0) = (\alpha, \lambda(\alpha))$

for some mapping $\lambda : K \longrightarrow M$. We can deduce (S27) - (S30) from the fact that σ is a ring homomorphism having the above described property.

Conversely, suppose that $\lambda : K \longrightarrow M$ satisfies (S27) - (S30). Then $\sigma : K\square M \longrightarrow K\tilde{\square}M$ defined by $(\alpha, x) \longmapsto (\alpha, x + \lambda(\alpha))$ is the desired isomorphism.

If $K\square M$ and $K\tilde{\square}M$ are equivalent, then by (S20), (S30) and the definition of double homothetisms,

$d^1_\alpha(\tilde{d}^2_\beta x) = d^1_\alpha(d^2_\beta x - x\lambda(\beta)) = d^2_\beta(d^1_\alpha x) - (d^1_\alpha x)\lambda(\beta)$

$= \tilde{d}^2_\beta(d^1_\alpha x).$

This proves the final assertion.

Let N and H be groups. A group G is called an extension of N by H if N is a normal subgroup of G and there exists an isomorphism $G/N \cong H$. Two extensions G and G' of N by H are said to be equivalent if there exists an isomorphism of G onto G' which leaves the elements of N fixed and induces the identity mapping of H modulo N. If $K \square M$ is an Everett sum of a ring K with 1 and a nil ring M, then $(K \square M)^*$ is an extension of $1 + M$ by K^*.

Theorem 3.4.2. ([29, Theorem 5]) Let M be a nilpotent ring and K be a commutative field of characteristic p (p a prime) which is algebraic over $GF(p)$. Let $K \square M$ and $K \tilde{\square} M$ be two Everett sums of K and M corresponding to two Everett function couples $([\ ,\ ], d)$ and $([\ ,\tilde{\ }], \tilde{d})$, respectively. Then $(K \square M)^*$ and $(K \tilde{\square} M)^*$ are equivalent (as group extensions of $1+M$ by K^*) if and only if there exists a mapping $\mu : K^* \longrightarrow M$ such that

(S31) $\mu(\alpha\beta) - \mu(\alpha)\mu(\beta) = \tilde{d}^1_\alpha(\mu(\beta)) + \tilde{d}^2_\beta(\mu(\alpha))$ *and*

(S32) $\mu(\alpha)(d^1_{\alpha^{-1}}x) - (d^2_{\alpha^{-1}}x)\mu(\alpha) = \tilde{d}^2_\alpha(d^2_{\alpha^{-1}}x) - \tilde{d}^1_\alpha(d^1_{\alpha^{-1}}x)$

$$(\alpha, \beta \in K^*,\ x \in M).$$

Proof. If $\tau : (K \square M)^* \longrightarrow (K \tilde{\square} M)^*$ is an isomorphism which leaves the elements of $1+M$ fixed and maps every class modulo $1+M$ onto itself, then we can write $\tau(\alpha, 0) = (\alpha, \mu(\alpha))$ for some mapping $\mu : K^* \longrightarrow M$. It is easy to check that this μ satisfies (S31) and (S32). Conversely, suppose that $\mu : K^* \longrightarrow M$ satisfies (S31) and (S32). Then we can define $\tau : (K \square M)^* \longrightarrow (K \tilde{\square} M)^*$ by

$$\tau(\alpha, x) = (\alpha, \tilde{d}^1_\alpha(d^1_{\alpha^{-1}}x) + \mu(\alpha) + \mu(\alpha)(d^1_{\alpha^{-1}}x)).$$

It is obvious that τ leaves the elements of $1 + M$ fixed and maps every class modulo $1 + M$ onto itself. By

$$\tau(\alpha, 0)\tau(1, x) = \tau((\alpha, 0)(1, x)),$$
$$\tau(\alpha, x)\tau(\beta, 0) = \tau((\alpha, x)(\beta, 0)), \text{ and}$$
$$\tau(\alpha, x)\tau(1, y) = \tau((\alpha, x)(1, y)),$$

it is a routine to verify that τ is a group isomorphism.

It is obvious that, if $K \square M$ and $K \tilde{\square} M$ are equivalent as ring extensions of M by K, then $(K \square M)^*$ and $(K \tilde{\square} M)^*$ are equivalent as group extensions of $1 + M$ by K^*. However, the following example shows that the converse is not true.

Let $M = \{0, a, 2a\}$ be a zero ring ($M^2 = 0$) of order 3. We shall define two Everett function couples $([\ ,\ ], d)$ and $([\ \tilde{,}\ ], \tilde{d})$ for $K = GF(3)$ and M as follows:

$$[\alpha, 0] = [0, \alpha] = 0$$
$$[1, 1] = a,\ [1, 2] = [2, 1] = 0,\ [2, 2] = 2a$$
$$[\alpha \tilde{,} \beta] \equiv 0$$
$$d_0^1 x = d_0^2 x = \tilde{d}_0^1 x = \tilde{d}_0^2 x = 0$$
$$d_1^1 x = d_1^2 x = \tilde{d}_1^1 x = \tilde{d}_1^2 x = x$$
$$d_2^1 x = d_2^2 x = \tilde{d}_2^1 x = \tilde{d}_2^2 x = 2x\ (x \in M).$$

It is easy to check that $([\ ,\ ], d)$ and $([\ \tilde{,}\ ], \tilde{d})$ are Everett function couples for K and M. Let $K \square M$ and $K \tilde{\square} M$ be Everett sums corresponding to $([\ ,\ ], d)$ and $([\ \tilde{,}\ ], \tilde{d})$, respectively. Since $ch\ (K \square M) = 9$ and $ch\ (K \tilde{\square} M) = 3$, we see that $K \square M$ and $K \tilde{\square} M$ are not equivalent. Whereas, by putting $\mu(\alpha) \equiv 0$ in Theorem 3.4.2, we see that $(K \square M)^*$ and $(K \tilde{\square} M)^*$ are equivalent.

§5. Finite Local Rings with Many Coefficient Subrings

Let R be a finite local ring with $|R| = p^{nr}$ and $|J(R)| = p^{(n-1)r}$ (see Theorem 2.1.1 (1)). Then, by Corollary 2.1.5, the number ν of all coefficient subrings of R satisfies the inequality $1 \leq \nu \leq p^{(n-1)r}$.

Concerning the case $\nu = 1$, we have already considered in Corollary 2.1.5. (2) and Theorem 3.3.2 (2). In this section, we shall consider the case $\nu = p^{(n-1)r}$.

Let r and n be positive integers with $r \geq 2, n \geq 2$. Let $K = GF(p^r)$. Let V be a finite nilpotent ring, and moreover two-sided vector space over K with dimension $n-1$ which satisfies the following (V1) - (V5).

(V1) $\alpha(xy) = (\alpha x)y$

(V2) $(xy)\alpha = x(y\alpha)$

(V3) $(\alpha x)\beta = \alpha(x\beta)$

(V4) $(x\alpha)y = x(\alpha y)$ $(\alpha, \beta \in K,\ x, y \in V)$

(V5) If x is a non-zero element of V, then there exists some $\alpha \in K$ such that $\alpha x \neq x\alpha$.

Let us define $d : K \longrightarrow DH(V)$ and $[\ ,\ ] : K \times K \longrightarrow V$ by

$d^1_\alpha x = \alpha x,\ d^2_\alpha x = x\alpha$ $(\alpha \in K,\ x \in V)$ and

$[\alpha, \beta] \equiv 0$.

We see that this $([\ ,\ ], d)$ is an Everett function couple for K and I, so we can construct a finite local ring $K \square V$ by (S22) and (S23). Let u be a generator of K^*, and $u' = (u, 0) \in K \square V$. As $x = 0$ is the only element of V such that $u'x = xu'$, by Corollary 2.1.5 (1), the number of all coefficient subrings of $K \square V$ is $p^{(n-1)r}$.

Theorem 3.5.1. ([28, Theorem 3]) Let R be a finite local ring with radical M whose residue field is $K = GF(p^r)$. Assume that $|R| = p^{nr}$ and $|M| = p^{(n-1)r}$, where $n \geq 2$ and $r \geq 2$. If the number of all coefficient subrings of R is $p^{(n-1)r}$, then R is isomorphic to $K \square V$, constructed *above.*

Proof. Let us assume that $ch\ R = p^k$ and $k \geq 2$. By Proposition 2.1.2 and its proof, R contains a unit u such that $o(u) = p^r - 1$, and $\sum_{i=1}^r \mathbf{Z}_{p^k}u^i$ is a direct sum in R. Let $N = \{x \in M \mid ux = xu\}$. As $\sum_{i=1}^r p\mathbf{Z}_{p^k}u^i$ is a subset of N consisting of $p^{(k-1)r}$ elements, by Corollary 2.1.5 (1), the number of all coefficient subrings of R is

$|M : N| \leq p^{(n-1)r}/p^{(k-1)r} \leq p^{(n-2)r}$,

which contradicts our assumption. So we see $ch\ R = p$. By Theorem 2.1.3 (3), there exists a subfield K', which is a copy of K, and $R = K' \bigoplus M$ as (K', K')-spaces. Let u' be an element of $(K')^*$ with $o(u') = p^r - 1$. By Corollary 2.1.5 (1), $N' = \{x \in M \mid u'x = xu'\}$ consists of only one element, so $x = 0$ is the only element of M with $u'x = xu'$. By Theorem 3.3.1 and its proof, there exists an isomorphism of R onto $K' \square M$.

One may doubt that really there exists such a nilpotent ring V satisfying (V1) - (V5).

Let V be a left vector space over $K = GF(p^r)$ of dimension $n-1$. Let $\{x_1, x_2, \cdots, x_{n-1}\}$ be a basis of V as left K-space. Let $\sigma_1, \sigma_2, \cdots, \sigma_{n-1}$ be automorphisms of K with $\sigma_i \neq id_K$ $(1 \leq i \leq n-1)$. Let us define the right K-space structure on V by

$(\sum_{i=1}^{n-1} c_i x_i)\alpha = \sum_{i=1}^{n-1} \sigma_i(\alpha) c_i x_i$ $(c_i, \alpha \in K)$.

(distinguished basis, see [20, §1]). We can define the product on V to satisfy (V1) - (V4), for instance, $xy \equiv 0$ $(x, y \in V)$.

Note that, by [29, Theorem 2] and the proof of Theorem 2.2.2, our theorems 3.3.1, 3.3.2, 3.4.1 and 3.4.2 are valid even under the assumption that M is a nil ring, and K is a finite field.

Chapter IV

Algorithms to Determine Finite Rings

In chapters II and III, we have seen some theorems on the structure of finite rings. In this chapter, we shall consider an algorithm to find, for a given positive integer $N > 1$, all finite rings of order N .

As is easily seen, a finite ring is the direct sum of finite rings of prime-power order. So, without loss of generality, we can consider only finite rings of prime-power order.

In this chapter, a finite ring does not necessarily contain 1. First, we shall introduce structure constants of finite rings.

§1. Structure Constants

When p is a prime, $C(p^e)$ denotes the finite cyclic group of order p^e. Let $\langle a \rangle$ denote the cyclic group generated by a. An Abelian group A is said to be of type $(p^{f_1}, n_1)(p^{f_2}, n_2) \cdots (p^{f_t}, n_t)$, where $n_1, n_2, \cdots, n_t$ and $f_1 < f_2 < \cdots < f_t$ are positive integers, if A is isomorphic to the direct sum of n_1 copies of $C(p^{f_1})$, n_2 copies of $C(p^{f_2}), \cdots$, and n_t copies of $C(p^{f_t})$.

When R is a ring, R^+ denotes the additive group of R.

Let $e_1 \leq e_2 \leq \cdots \leq e_n$ be an increasing sequence of positive integers. Let $S_n = \{(a_{ij}) \in \mathbf{Z}_{n \times n} \mid a_{ij} \equiv 0 \mod p^{e_j - e_i} \text{ for } i < j\}$. It is easy to check that S_n is a subring of $(\mathbf{Z})_{n\times n}$. For (a_{ij}) and (b_{ij}) of S_n , we shall write $(a_{ij}) \equiv (b_{ij})$ if $a_{ij} \equiv b_{ij} \mod p^{e_j}$ $(1 \leq i,j \leq n)$. Let $\mathbf{0}$ denote the zero matrix of S_n , and let $I = \{(a_{ij}) \in S_n \mid (a_{ij}) \equiv \mathbf{0}\}$. We see that I is an ideal of S_n. Let $\bar{S}_n = S_n/I$, and $\varphi : S_n \longrightarrow \bar{S}_n$ be the natural projection. An element $(a_{ij}) \in S_n$ is said to be non-singular if $\varphi((a_{ij}))$ is an invertible element of $\bar{S}_n$.

Let $\pi : S_n \longrightarrow (\mathbf{Z}/p\mathbf{Z})_{n\times n}$ be the natural homomorphism given by $(a_{ij}) \longmapsto (\bar{a}_{ij})$.

Theorem 4.1.1. ([33, Satz 2]) Let R be a finite p-ring whose additive group is

$R^+ = \langle a_1\rangle \oplus \langle a_2\rangle \oplus \cdots \oplus \langle a_n\rangle,$

where $\langle a_i\rangle \cong C(p^{e_i})$ $(1 \leq i \leq n)$ and $1 \leq e_1 \leq e_2 \leq \cdots \leq e_n$. Let us write

(1) $\quad a_i a_k = \sum_{j=1}^n \alpha_{ijk} a_j \quad (1 \leq i,k \leq n),$

where α_{ijk} are integers such that

(2) $\quad 0 \leq \alpha_{ijk} \leq p^{e_j} - 1 \quad (1 \leq i,j,k \leq n).$

Then it holds that

(3) $\quad \alpha_{ijk} \equiv 0 \mod p^{e_j - e_k}$ *for* $1 \leq k < j \leq n,$

(4) $\quad \alpha_{ijk} \equiv 0 \mod p^{e_j - e_i}$ *for* $1 \leq i < j \leq n,$

and

(5) $\quad \sum_{k=1}^n \alpha_{rki}\alpha_{kjs} \equiv \sum_{k=1}^n \alpha_{iks}\alpha_{rjk} \mod p^{e_j} \quad (1 \leq i,j,r,s \leq n).$

Conversely, let

(6) $\quad A = \langle a_1\rangle \oplus \langle a_2\rangle \oplus \cdots \oplus \langle a_n\rangle$

$(\langle a_i\rangle \cong C(p^{e_i}), 1 \leq e_1 \leq e_2 \leq \cdots \leq e_n)$

be a finite Abelian p-group. If α_{ijk} $(1 \leq i,j,k \leq n)$ are integers which satisfy (2), (3), (4) and (5), then we can make A into a ring by defining the multiplication on A by (1). By this manner we can construct all rings which have the Abelian group A as their additive group.

Proof. Assume that R forms a ring under the multiplication given by

$a_i a_k = \sum_{j=1}^{n} \alpha_{ijk} a_j$.

Since $p^{e_i} a_i = 0$,

$0 = p^{e_i} a_i a_k$

$= p^{e_i}(\sum_{j=1}^{n} \alpha_{ijk} a_j)$

$= \sum_{j=1}^{n} p^{e_i} \alpha_{ijk} a_j$.

Then $p^{e_i}\alpha_{ijk} \in (p^{e_j})$, so we see that

$\alpha_{ijk} \in p^{e_j - e_i}$ for $i < j$.

Similarly we have

$\alpha_{ijk} \in p^{e_j - e_k}$ for $k < j$.

For each $1 \leq r, i, s \leq n$,

$(a_r a_i) a_s = (\sum_{k=1}^{n} \alpha_{rki} a_k) a_s$

$= \sum_{k=1}^{n} \alpha_{rki}(a_k a_s)$

$= \sum_{k=1}^{n} \alpha_{rki}(\sum_{j=1}^{n} \alpha_{kjs} a_j)$

$= \sum_{j=1}^{n}(\sum_{k=1}^{n} \alpha_{rki}\alpha_{kjs}) a_j$.

On the other hand, by the associativity of R , this is equal to

$a_r(a_i a_s) = \sum_{j=1}^{n}(\sum_{k=1}^{n} \alpha_{iks}\alpha_{rjk}) a_j$,

so we have

$\sum_{k=1}^{n} \alpha_{rki}\alpha_{kjs} \equiv \sum_{k=1}^{n} \alpha_{iks}\alpha_{rjk} \mod p^{e_j}$ $(1 \leq i, j, r, s \leq n)$.

Now the converse will be clear.

By Theorem 4.1.1, for a given prime power p^e , we can construct all rings of order p^e, since the additive group of any ring of order p^e has the additive group of type $(p^{f_1}, n_1)(p^{f_2}, n_2) \cdots (p^{f_t}, n_t)$, where $f_1 n_1 + f_2 n_2 + \cdots + f_t n_t = e$.

When α_{ijk} $(1 \leq i, j, k \leq n)$ are integers which satisfy (2), (3), (4) and (5), we call $\{\alpha_{ijk}\}_{i,j,k=1}^{n}$ a set of structure constants for the Abelian group (6).

Let $\{\alpha_{ijk}\}_{i,j,k=1}^{n}$ and $\{\beta_{ijk}\}_{i,j,k=1}^{n}$ be two sets of structure constants for the Abelian group (6). We shall say that $\{\alpha_{ijk}\}_{i,j,k=1}^{n}$ and $\{\beta_{ijk}\}_{i,j,k=1}^{n}$ are equivalent if there exists a non-singular element $(t_{ij}) \in S_n$ such that

$\sum_{j=1}^{n} \beta_{ijk} t_{js} \equiv \sum_{j=1}^{n} \sum_{r=1}^{n} t_{ij} t_{kr} \alpha_{jsr} \mod p^{e_s}$

$(1 \leq i, k, s \leq n)$.

Theorem 4.1.2. ([33, Satz 5]) Let $\{\alpha_{ijk}\}_{i,j,k=1}^{n}$ and $\{\beta_{ijk}\}_{i,j,k=1}^{n}$ be two sets of structure constants for the Abelian group (6). Let R be the ring whose additive group is (6) and whose multiplication is defined by

$a_i a_k = \sum_{j=1}^{n} \alpha_{ijk} a_j \ \ (1 \leq i, k \leq n)$.

Let R' be the ring whose additive group is (6) and whose multiplication $\circ$ is defined by

$a_i \circ a_k = \sum_{j=1}^{n} \beta_{ijk} a_j \ \ (1 \leq i, k \leq n)$.

Then R and R' are isomorphic if and only if $\{\alpha_{ijk}\}_{i,j,k=1}^{n}$ and $\{\beta_{ijk}\}_{i,j,k=1}^{n}$ are equivalent.

Proof. Let us assume that there exists a ring isomorphism $\varphi : R' \longrightarrow R$. Then we can write

$\varphi(a_i) = \sum_{j=1}^{n} t_{ij} a_j \ (1 \leq i \leq n)$

and

$\varphi^{-1}(a_i) = \sum_{j=1}^{n} t'_{ij} a_j \ (1 \leq i \leq n)$,

with (t_{ij}), $(t'_{ij}) \in S_n$. From $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = id$, we have

$(t_{ij})(t'_{ij}) \equiv (t'_{ij})(t_{ij}) \equiv E_n$.

So we see that both (t_{ij}) and (t'_{ij}) are non-singular. For each $1 \leq i,\ k \leq n$,

$\varphi(a_i)\varphi(a_k) = (\sum_{j=1}^{n} t_{ij} a_j)(\sum_{r=1}^{n} t_{kr} a_r)$

$= \sum_{j=1}^{n} \sum_{r=1}^{n} t_{ij} t_{kr} (a_j a_r)$

$= \sum_{j=1}^{n} \sum_{r=1}^{n} t_{ij} t_{kr} (\sum_{s=1}^{n} \alpha_{jsr} a_s)$

$= \sum_{s=1}^{n} (\sum_{j=1}^{n} \sum_{r=1}^{n} t_{ij} t_{kr} \alpha_{jsr}) a_s$.

On the other hand, this is equal to

$\varphi(a_i \circ a_k) = \varphi(\sum_{j=1}^{n} \beta_{ijk} a_j)$

$= \sum_{j=1}^{n} \beta_{ijk}\varphi(a_j)$
$= \sum_{j=1}^{n} \beta_{ijk}(\sum_{s=1}^{n} t_{js}a_s)$
$= \sum_{s=1}^{n}(\sum_{j=1}^{n} \beta_{ijk}t_{js})a_s.$

So we have

$\sum_{j=1}^{n} \beta_{ijk}t_{js} \equiv \sum_{j=1}^{n}\sum_{r=1}^{n} t_{ij}t_{kr}\alpha_{jsr} \mod p^{e_s}$

$(1 \leq i, k, s \leq n).$

The converse will be certified similarly.

§2. Indecomposability of Rings

Now we shall consider an algorism to determine decomposability of a given finite ring. Let $\{\alpha_{ijk}\}_{i,j,k=1}^{n}$ be a set of structure constants for the Abelian group (6). We shall say that $\{\alpha_{ijk}\}_{i,j,k=1}^{n}$ is decomposable if there exists a partition $\{1, 2, \cdots, n\} = J_1 \cup J_2$ such that (i) $J_1 \cap J_2 = \phi$, (ii) $J_1 \neq \phi, J_2 \neq \phi$, (iii) if $i \in J_1, j \in J_2$ and $e_i = e_j$, then $i < j$, and (iv) if, $i \in J_1$ and $j \in J_2$, or, $i \in J_2$ and $j \in J_1$, or, $j \in J_1$ and $k \in J_2$, or, $j \in J_2$ and $k \in J_1$, then $\alpha_{ijk} = 0$. By the following theorem, we can see whether a ring with given structure constants is indecomposable or not.

Theorem 4.2.1. ([31, Theorem 3]) Let $\{\alpha_{ijk}\}_{i,j,k=1}^{n}$ be a set of structure constants for the Abelian group (6). Let R be the ring whose additive group is (6) and whose multiplication is defined by

$a_i a_k = \sum_{j=1}^{n} \alpha_{ijk}a_j \quad (1 \leq i, k \leq n).$

Then R is indecomposable if and only if there exists no set of structure constants for the Abelian group (6) which is decomposable and equivalent to $\{\alpha_{ijk}\}_{i,j,k=1}^{n}$.

Proof. Let us suppose that the Abelian group (6) is of type (p^{f_1}, n_1) $(p^{f_2}, n_2) \cdots (p^{f_t}, n_t)$, where $n_1 + n_2 + \cdots + n_t = n$ and $f_1 n_1 + f_2 n_2 + \cdots + f_t n_t = e_1 + e_2 + \cdots + e_n$. Let us assume that there exist non-trivial ideals I_1 and I_2 of R such that $R = I_1 \oplus I_2$. Let $\{b_i\}_{i=1}^{s}$ be a basis of I_1^+ and $\{b_i\}_{i=s+1}^{n}$ a basis of I_2^+ , that is,

$$I_1 = \langle b_1 \rangle \oplus \langle b_2 \rangle \oplus \cdots \oplus \langle b_s \rangle$$

and

$$I_2 = \langle b_{s+1} \rangle \oplus \langle b_{s+2} \rangle \oplus \cdots \oplus \langle b_n \rangle.$$

Then $\{b_i\}_{i=1}^{n}$ is a basis of R^+. After renumbering, we can set $\{b_i\}$ as follows:

$$R^+ = \langle b_1 \rangle \oplus \langle b_2 \rangle \oplus \cdots \oplus \langle b_{m_1} \rangle$$
$$\oplus \langle b_{m_1+1} \rangle \oplus \langle b_{m_1+2} \rangle \oplus \cdots \oplus \langle b_{n_1} \rangle$$
$$\oplus \langle b_{n_1+1} \rangle \oplus \langle b_{n_1+2} \rangle \oplus \cdots \oplus \langle b_{n_1+m_2} \rangle$$
$$\oplus \langle b_{n_1+m_2+1} \rangle \oplus \langle b_{n_1+m_2+2} \rangle \oplus \cdots \oplus \langle b_{n_1+n_2} \rangle$$
$$\oplus \cdots \oplus \langle b_{n_1+n_2+\cdots+n_{t-1}+1} \rangle \oplus \cdots \oplus \langle b_{n_1+n_2+\cdots+n_{t-1}+m_t} \rangle$$
$$\oplus \langle b_{n_1+n_2+\cdots+n_{t-1}+m_t+1} \rangle \oplus \cdots \oplus \langle b_{n_1+n_2+\cdots+n_{t-1}+n_t} \rangle \ ,$$

where $ch\ b_i = p^{f_1} \quad (1 \leq i \leq n_1), ch\ b_i = p^{f_2} \quad (n_1 + 1 \leq i \leq n_1 + n_2), \cdots, ch\ b_i = p^{f_t} \ (n_1 + n_2 + \cdots + n_{t-1} + 1 \leq i \leq n_1 + n_2 + \cdots + n_{t-1} + n_t)$,

$$I_1 = \langle b_1 \rangle \oplus \langle b_2 \rangle \oplus \cdots \oplus \langle b_{m_1} \rangle$$
$$\oplus \langle b_{n_1+1} \rangle \oplus \langle b_{n_1+2} \rangle \oplus \cdots \oplus \langle b_{n_1+m_2} \rangle$$
$$\oplus \cdots \oplus \langle b_{n_1+n_2+\cdots+n_{t-1}+1} \rangle \oplus \langle b_{n_1+n_2+\cdots+n_{t-1}+2} \rangle \oplus \cdots$$
$$\oplus \langle b_{n_1+n_2+\cdots+n_{t-1}+m_t} \rangle,$$

and

$$I_2 = \langle b_{m_1+1} \rangle \oplus \langle b_{m_1+2} \rangle \oplus \cdots \oplus \langle b_{n_1} \rangle$$
$$\oplus \langle b_{n_1+m_2+1} \rangle \oplus \langle b_{n_1+m_2+2} \rangle \oplus \cdots \oplus \langle b_{n_1+n_2} \rangle$$
$$\oplus \cdots \oplus \langle b_{n_1+n_2+\cdots n_{t-1}+m_t+1} \rangle \oplus \langle b_{n_1+n_2+\cdots n_{t-1}+m_t+2} \rangle \oplus \cdots$$
$$\oplus \langle b_{n_1+n_2+\cdots+n_{t-1}+n_t} \rangle.$$

Let $J_1 = \{1, 2, \cdots, m_1, n_1 + 1, n_1 + 2, \cdots, n_1 + m_2,$
$\cdots, n_1 + n_2 + \cdots + n_{t-1} + 1, n_1 + n_2 + \cdots + n_{t-1} + 2,$

$\cdots, n_1 + n_2 + \cdots + n_{t-1} + m_t\}$

and

$J_2 = \{m_1 + 1, m_1 + 2, \cdots, n_1,$

$n_1 + m_2 + 1, n_1 + m_2 + 2, \cdots, n_1 + n_2,$

$\cdots, n_1 + n_2 + \cdots + n_{t-1} + m_t + 1, n_1 + n_2 + \cdots + n_{t-1} + m_t + 2,$

$\cdots, n_1 + n_2 + \cdots + n_{t-1} + n_t\}.$

It is clear that $\{1, 2, \cdots, n\} = J_1 \cup J_2$ and $J_1 \cap J_2 = \phi$. As $I_i \neq 0$, so $J_i \neq \phi$ $(i = 1, 2)$. Let

(7) $\quad b_i b_k = \sum_{j=1}^{n} \beta_{ijk} b_j \ \ (0 \leq \beta_{ijk} \leq p^{e_j} - 1)$

in R. It is easy to see that $\{\beta_{ijk}\}_{i,j,k=1}^{n}$ satisfy (2), (3), (4) and (5). If $i \in J_1, j \in J_2$ and $e_i = e_j$, then $ch\ b_i = ch\ b_j$,so by our renumbering, $i < j$. If $i \in J_1$, then $b_i \in I_1$. So, for each $1 \leq k \leq n$,

$b_i b_k = \sum_{j=1}^{n} \beta_{ijk} b_j \in I_1$.

This is a linear combination of $\{b_j\}_{j \in J_1}$, so $\beta_{ijk} = 0$ for $j \in J_2$. Similarly we see that, if, $i \in J_2$ and $j \in J_1$, or, $k \in J_2$ and $j \in J_1$, or, $k \in J_1$ and $j \in J_2$, then $\beta_{ijk} = 0$. So the set of structure constants $\{\beta_{ijk}\}_{i,j,k=1}^{n}$ is decomposable. We shall show that $\{\alpha_{ijk}\}_{i,j,k=1}^{n}$ and $\{\beta_{ijk}\}_{i,j,k=1}^{n}$ are equivalent. There are integers t_{ij} and t'_{ij} $(1 \leq i, j \leq n)$ such that

(8) $\quad b_i = \sum_{j=1}^{n} t_{ij} a_j \ , \ a_i = \sum_{j=1}^{n} t'_{ij} b_j \ \ (0 \leq t_{ij}, t'_{ij} \leq p^{e_j} - 1).$

It is easy to see that $\varphi((t_{ij}))\varphi((t'_{ij})) = E_n$ in $\bar{S}_n$, so (t_{ij}) is a non-singular element of S_n. We have

$b_i b_k = (\sum_{j=1}^{n} t_{ij} a_j)(\sum_{\ell=1}^{n} t_{k\ell} a_\ell)$

$= \sum_{j=1}^{n} \sum_{\ell=1}^{n} t_{ij} t_{k\ell} a_j a_\ell$

$= \sum_{j=1}^{n} \sum_{\ell=1}^{n} t_{ij} t_{k\ell} (\sum_{r=1}^{n} \alpha_{jr\ell} a_r)$

$= \sum_{r=1}^{n} (\sum_{j=1}^{n} \sum_{\ell=1}^{n} t_{ij} t_{k\ell} \alpha_{jr\ell}) a_r.$

On the other hand, by (7) and (8),

$b_i b_k = \sum_{j=1}^{n} \beta_{ijk} (\sum_{r=1}^{n} t_{jr} a_r)$

$= \sum_{r=1}^{n} (\sum_{j=1}^{n} \beta_{ijk} t_{jr}) a_r.$

So we get

(9) $\sum_{j=1}^{n} \sum_{\ell=1}^{n} t_{ij} t_{k\ell} \alpha_{jr\ell} \equiv \sum_{j=1}^{n} \beta_{ijk} t_{jr} \mod p^{e_r}$
$(1 \leq r \leq n)$.

Now, let S be the ring whose additive group is (6) and whose multiplication $\circ$ is defined by

$a_i \circ a_k = \sum_{j=1}^{n} \beta_{ijk} a_j \quad (1 \leq i, k \leq n).$

We can define a group homomorphism $\tau : S^+ \longrightarrow R^+$ by

$\tau a_i = \sum_{j=1}^{n} t_{ij} a_j \quad (1 \leq i \leq n).$

Since

$$\begin{aligned}
&\tau(a_i \circ a_k) = \tau(\textstyle\sum_{j=1}^{n} \beta_{ijk} a_j) \\
&= \textstyle\sum_{j=1}^{n} \beta_{ijk} \tau a_j \\
&= \textstyle\sum_{j=1}^{n} \beta_{ijk} (\sum_{r=1}^{n} t_{jr} a_r) \\
&= \textstyle\sum_{r=1}^{n} (\sum_{j=1}^{n} \beta_{ijk} t_{jr}) a_r
\end{aligned}$$

and

$$\begin{aligned}
&(\tau a_i)(\tau a_k) = (\textstyle\sum_{j=1}^{n} t_{ij} a_j)(\sum_{\ell=1}^{n} t_{k\ell} a_\ell) \\
&= \textstyle\sum_{j=1}^{n} \sum_{\ell=1}^{n} t_{ij} t_{k\ell} a_j a_\ell \\
&= \textstyle\sum_{j=1}^{n} \sum_{\ell=1}^{n} t_{ij} t_{k\ell} (\sum_{r=1}^{n} \alpha_{jr\ell} a_r) \\
&= \textstyle\sum_{r=1}^{n} (\sum_{j=1}^{n} \sum_{\ell=1}^{n} t_{ij} t_{k\ell} \alpha_{jr\ell}) a_r,
\end{aligned}$$

from (9), we see that

$\tau(a_i \circ a_k) = (\tau a_i)(\tau a_k).$

This means that τ is a ring isomorphism of S onto R. So, by Theorem 4.1.2, $\{\alpha_{ijk}\}_{i,j,k=1}^{n}$ and $\{\beta_{ijk}\}_{i,j,k=1}^{n}$ are equivalent.

Conversely, let us assume that there exists a set of decomposable structure constants $\{\beta_{ijk}\}_{i,j,k=1}^{n}$ for the Abelian group (6) which is equivalent to $\{\alpha_{ijk}\}_{i,j,k=1}^{n}$. Let $\{1, 2, \cdots, n\} = J_1 \cup J_2$ be the partition satisfying the condition (i) - (iv). Let S be the ring whose additive group is (6) and whose multiplication is defined by

$a_i a_k = \sum_{j=1}^{n} \beta_{ijk} a_j \quad (1 \leq i, k \leq n).$

Let $I_j = \oplus_{i \in J_j} \langle a_i \rangle \quad (j = 1, 2)$. Then, by what was stated above, there exists a non-trivial ideal decomposition $S = I_1 \oplus I_2 \quad (I_1 \neq \phi, I_2 \neq \phi)$.

Then R is not indecomposable, since R is isomorphic to S by Theorem 4.1.2.

§3. Identity and Jacobson Radical

In [33, Satz 6], there was shown an algorism to determine whether or not a given finite ring has identity elements.

However, the following theorem will give a more practical algorism to determine existence of identity elements. In what follows, δ_{ij} denotes the Kronecker's delta.

Theorem 4.3.1. ([31, Theorem 4]) Let $\{\alpha_{ijk}\}_{i,j,k=1}^{n}$ *be a set of structure constants for the Abelian group (6). Let R be the ring whose additive group is (6) and whose multiplication is defined by*

$a_i a_k = \sum_{j=1}^{n} \alpha_{ijk} a_j \quad (1 \leq i, k \leq n).$

Then:

(I) R has a left (resp. right) identity if and only if there exist integers $c_1, c_2, \cdots, c_n$ *such that* $0 \leq c_i \leq p^{e_i} - 1 \quad (1 \leq i \leq n)$ *and*

$\sum_{i=1}^{n} c_i \alpha_{ijk} \equiv \delta_{jk} \quad (\textit{resp. } \sum_{i=1}^{n} c_i \alpha_{kji} \equiv \delta_{jk}\ ) \quad \textit{mod } p^{e_j}$

$(1 \leq j, k \leq n).$

(II) R has an identity if and only if there exist integers $c_1, c_2, \cdots, c_n$ *such that* $0 \leq c_i \leq p^{e_i - 1} \quad (1 \leq i \leq n)$ *and*

$\sum_{i=1}^{n} c_i \alpha_{ijk} \equiv \sum_{i=1}^{n} c_i \alpha_{kji} \equiv \delta_{jk} \quad \textit{mod } p^{e_j}$

$(1 \leq j, k \leq n).$

Proof. Let $u = \sum_{i=1}^{n} c_i a_i \quad (0 \leq c_i \leq p^{e_i} - 1)$ be a left identity of R. For each $1 \leq k \leq n$, it holds that

$a_k = u a_k = (\sum_{i=1}^{n} c_i a_i) a_k$

$= \sum_{i=1}^{n} c_i a_i a_k$

$= \sum_{i=1}^{n} c_i (\sum_{j=1}^{n} \alpha_{ijk} a_j)$

$= \sum_{j=1}^{n} (\sum_{i=1}^{n} c_i \alpha_{ijk}) a_j.$

So we get

$\sum_{i=1}^{n} c_i \alpha_{ijk} \equiv \delta_{jk} \mod p^{e_j} \quad (1 \leq j, k \leq n).$

Now the rest of the proof would be clear.

Finally, we shall give an algorism to count the order of $J(R)$.

Theorem 4.3.2. ([31, Theorem 5]) Let $\{\alpha_{ijk}\}_{i,j,k=1}^{n}$ be a set of structure constants for the Abelian group (6). Let R be the ring whose additive group is (6) and whose multiplication is defined by

$a_i a_k = \sum_{j=1}^{n} \alpha_{ijk} a_j \quad (1 \leq i, k \leq n).$

Then, $b = \sum_{i=1}^{n} u_i a_i \quad (0 \leq u_i \leq p^{e_i} - 1, 1 \leq i \leq n)$ belongs to $J(R)$ if and only if, for any n integers $x_1, x_2, \cdots, x_n$ satisfying $0 \leq x_i \leq p^{e_i} - 1 \quad (1 \leq i \leq n)$, there exist n integers $y_1, y_2, \cdots, y_n$ such that $0 \leq y_i \leq p^{e_i} - 1 \quad (1 \leq i \leq n)$ and

$\sum_{i,j=1}^{n} u_i x_j \alpha_{irj} + y_r - \sum_{i,j,k,t=1}^{n} u_i x_j \alpha_{ikj} y_t \alpha_{krt} \equiv 0 \ mod \quad p^{e_r}$

$(1 \leq r \leq n).$

Proof. An element b of R belongs to $J(R)$ if and only if bx is right quasi-regular for any $x \in R$ (see Chapter I). Let us put $x = \sum_{i=1}^{n} x_i a_i$ and $y = \sum_{i=1}^{n} y_i a_i \quad (0 \leq x_i, y_i \leq p^{e_i} - 1, 1 \leq i \leq n)$. Then

$bx + y - bxy =$

$(\sum_{i=1}^{n} u_i a_i)(\sum_{j=1}^{n} x_j a_j) \ + \ \sum_{r=1}^{n} y_r a_r$

$- \ (\sum_{i=1}^{n} u_i a_i)(\sum_{j=1}^{n} x_j a_j)(\sum_{k=1}^{n} y_k a_k)$

$= \sum_{r=1}^{n} \{\sum_{i,j=1}^{n} u_i x_j \alpha_{irj} + y_r - \sum_{i,j,k,t=1}^{n} u_i x_j \alpha_{ikj} y_t \alpha_{krt}\} a_r,$

which proves our assertion.

References

[1] Anderson, F. W. and Fuller, K. R., Rings and Categories of Modules, Graduate Texts in Mathematics 13, Springer (1974).

[2] Behrens, E. A., Ring Theory, Academic Press (1972).

[3] Bourbaki, N., Éléments de Mathématique, Algèbre, Hermann (1962).

[4] Bourbaki, N., Éléments de Mathématique, Théorie des Ensembles, Hermann (1963).

[5] Brawley, J. V. and Schnibben, G. E., Infinite Algebraic Extensions of Finite Fields, Contemporary Mathematics 95, American Mathematical Society (1989).

[6] Clark, W. E., A coefficient ring for finite non-commutative rings, Proc. Amer. Math. Soc. 33 (1972), 25 - 28.

[7] Cohen, I. S., On the structure and ideal theory of complete local rings, Trans. Amer. Math. Soc. 59 (1946), 54 - 106.

[8] Curtis, C. W. and Reiner, I., Representation Theory of Finite Groups and Associative Algebras, Pure and Applied Mathematics Series 11, Interscience (1962).

[9] Everett, C. J., An extension theory for rings, Amer. J. Math. 64 (1942), 363 - 370.

[10] Hall, M., The Theory of Groups, Macmillan (1959).

[11] Hasse-Schmidt, F. K., Die Struktur diskret bewerteter Körper, J. Reine Angew. Math. 170 (1934), 4 - 63.

[12] Jacobson, N., Lectures in Abstract Algebra, vol. III, Springer (1964).

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

[14] Krull, W., Algebraische Theorie der Ringe, II, Math. Ann. 91 (1924), 1 - 46.

[15] Kurzweil, H., Endliche Gruppen, Springer (1977).

[16] Lambek, J., Lectures in Rings and Modules, Blaisdell Publishing Company (1966).

[17] McDonald, B. R., Finite Rings with Identity, Pure and Applied Mathematics Series 28, Marcel Dekker (1974).

[18] Motose, K. and Tominaga, H., Group rings with nilpotent unit groups, Math. J. Okayama Univ. 14 (1969), 43 - 46.

[19] Nagata, M., Local Rings, Interscience Tracts in Pure and Applied Mathematics 13, Interscience (1962).

[20] Raghavendran, R., Finite associative rings, Compositio Math. 21 (1969), 195 - 229.

[21] Rédei, L., Algebra I , Akademische Verlagsgesellschaft, Leipzig (1959).

[22] Robinson, D. J. S., A Course in the Theory of Groups, Springer (1982).

[23] Roquette, P., Abspaltung des Radikals in vollständigen lokalen Ringen, Hamb. Abh. 23 (1959), 75 - 113.

[24] Rowen, L. H., Ring Theory, Pure and Applied Mathematics 127, Academic Press (1988).

[25] Serre, J. P., Local Fields, Springer (1979).

[26] Sumiyama, T., Note on maximal Galois subrings of finite local rings, Math. J. Okayama Univ. 21 (1979), No. 1, 31 -32.

[27] Sumiyama, T., On unit groups of finite local rings, Math. J. Okayama Univ. 23 (1981), No. 2, 195 - 198.

[28] Sumiyama, T., On cohomology of groups in finite local rings, Math. J. Okayama Univ. 29 (1987), 77 - 81.

[29] Sumiyama, T., On double homothetisms of rings and local rings

with finite residue fields, Math. J. Okayama Univ. 33 (1991), 13 - 20.

[30] Sumiyama, T., Coefficient subrings of certain local rings with prime-power characteristic, Internat. J. Math. and Math. Sci. 18 (1995), No. 3, 451 - 462.

[31] Sumiyama, T., On algorisms for finite rings, (to appear in Mathematica Japonica, vol. 44, No. 2).

[32] Waerden, van der, Algebra, Zweiter Teil, Heidelberger Taschenbücher, Springer (1967).

[33] Wiesenbauer, J., Über die endlichen Ringe mit gegebener additiver Gruppe, Monatsh. Math. 78 (1974), 164 - 173.

[34] Wilson, R. S., On the structure of finite rings, Compositio Math. 26 (1973), 79 - 93.

[35] Wilson, R. S., Representation of finite rings, Pacific J. Math. 53 (1974), 643 - 649.

[36] Witt, E., Zyklische Körper und Algebren der Charakteristik p vom Grade p^m , J. Reine Angew. Math. 176 (1936), 126 - 140.

List of Papers by Takao SUMIYAMA

[1] T. Sumiyama: Note on ℓ-rings, Mathematica Japonica 23 (1978), 369 - 370.

[2] T. Sumiyama: Note on maximal Galois subrings of finite local rings, Mathematical Journal of Okayama University, vol. 21 (1979), No. 1, 31 - 32.

[3] T. Sumiyama: On unit groups of finite local rings, Mathematical Journal of Okayama University, vol. 23 (1981), No. 2, 195 - 198.

[4] T. Sumiyama: Nonexistence of certain finite rings, Mathematical Journal of Okayama University, vol. 26 (1984), 169 - 173.

[5] T. Sumiyama: On cohomology of groups in finite local rings, Mathematical Journal of Okayama University, vol. 29 (1987), 77 - 81.

[6] T. Sumiyama: On double homothetisms of rings and local rings with finite residue fields, Mathematical Journal of Okayama University, vol. 33 (1991), 13 - 20.

[7] Y. Hirano and T. Sumiyama: On orders of directly indecomposable finite rings, Bulletin of the Australian Mathematical Society, vol. 46 (1992), No. 3, 353 - 359.

[8] T. Sumiyama: Coefficient subrings of certain local rings with prime-power characteristic, International Journal of Mathematics and Mathematical Sciences, vol. 18 (1995), No. 3, 451- 462.

[9] T. Sumiyama: On algorisms for finite rings (to appear in Mathematica Japonica, vol. 44, No. 2).

[10] T. Sumiyama: Finite rings with central prime radical (to appear in

Yokohama Mathematical Journal, vol. 43, No. 2).

[11] Y. Hirano and T. Sumiyama: Finite rings with commuting nilpotent elements (to appear in Communications in Algebra).

The contents of the following (I) are based on those of (II) respectively.

(I)	(II)
Chapter I	[2], [8]
Chapter II	[3], [5], [8]
Chapter III	[6]
Chapter IV	[9]