Math. J. Okayama Univ. 33 (1991), 13−20

ON DOUBLE HOMOTHETISMS OF RINGS AND LOCAL RINGS WITH FINITE RESIDUE FIELDS

Dedicated to Professor Takasi Nagahara on his 60th birthday

TAKAO SUMIYAMA

In his paper [2], C. J. Everett gave a solution of Schreier's extension problem for rings. The detailed discussion on this subject will be found in [6, §§ 52, 53].

Let R be a ring extension of I by A. If there exists a multiplicative cross-section f: $A \to R$, then R is determined as the Everett sum $A \dotplus I$ .corresponding to a certain couple of mappings $[\ ,\ ]$: $A \times A \to I$ and d : $A \to DH(I)$ (Theorem 1). In §§ 2 and 3, our attention will be restricted to the case that R is a local ring with finite residue field. Theorem 1 enables us to give some structure theorems for such local rings (Theorems 2 and 3). Furthermore, we shall give a condition for such Everett sums or their unit groups to be equivalent (Theorems 4 and 5).

1. Throughout this section, I will represent an associative ring. Let $E_1(I)$ denote the right I-endomorphism ring of I, and $E_2(I)$ the left I-endomorphism ring of I. Any element of $E_1(I)$ and $E_2(I)$ will act on I from the left. Let $E'(I)$ be the abelian group $E_1(I) \oplus E_2(I) = \{f = (f^1, f^2) \mid f^1 \in E_1(I), f^2 \in E_2(I)\}$. Defining the multiplication on $E'(I)$ by $(f^1, f^2)(g^1, g^2) = (f^1g^1, g^2f^2)$, 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

(1) $(f^2x)y = x(f^1y)$

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

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

$$a^1x = ax \quad \text{and} \quad a^2x = xa.$$

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

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

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

This property is symmetric and reflexive, but not transitive in general. 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 what follows, A will represent a ring with 1. Elements of A will be denoted by $\alpha, \beta, \gamma, \ldots$, and elements of I by $x, y, z, \ldots$.

Now, let $[\ ,\ ]$ be a mapping of $A \times A$ to I such that

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

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

(7) $[0, \alpha] = [\alpha, 0] = 0\ (\alpha, \beta, \gamma \in A)$.

Further, let $d:\ \alpha \mapsto d_\alpha = (d^1_\alpha, d^2_\alpha)$ be a mapping of A to $DH(I)$ such that

(8) $d^1_{\alpha+\beta}x + [\alpha, \beta]x = d^1_\alpha x + d^1_\beta x$

(9) $d^2_{\alpha+\beta}x + x[\alpha, \beta] = d^2_\alpha x + d^2_\beta x$

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

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

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

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

(14) $d^1_0 x = d^2_0 x = 0$

(15) $d^1_1 x = d^2_1 x = x\ (\alpha, \beta \in A, x \in I)$.

Such a couple $([\ ,\ ], d)$ will be called an *Everett couple* (abbreviated *E-couple*) for A and I. By setting $\langle\ ,\ \rangle \equiv 0$ in [6, § 52, Satz 112], we can easily see that $A \times I$ forms a ring concerning the operations defined by

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

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

This ring will be called an *Everett sum* (abbreviated *E-sum*) of A and I, and denoted as $A \dotplus I$ (cf. [6, § 52]). Obviously, $e = (1, 0)$ is the identity element of $A \dotplus I$, I is regarded naturally as an ideal of $A \dotplus I$, and the quotient ring $(A \dotplus I)/I$ is naturally identified with A.

Conversely, let R be a ring with 1, I an ideal of R, and $A = R/I$. Assume that there exists a multiplicative cross-section $f:\ A \to R$, namely f satisfying (i) $f(\alpha\beta) = f(\alpha)f(\beta)$, (ii) $f(0) = 0$ and (iii) $\pi \circ f = \mathrm{id}_A$ (π: $R \to A$ is the natural homomorphism). Then we can define mappings $[\ ,\ ]$: $(\alpha, \beta) \mapsto [\alpha, \beta]$ of $A \times A$ to I and $d:\ \alpha \mapsto d_\alpha = (d^1_\alpha, d^2_\alpha)$ of A to $DH(I)$ by

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

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

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

It is easy to see that $([\ ,\ ], d)$ is an E-couple for A and I, so that we have an

E-sum $A\dotplus I$. Let σ: $R \rightarrow A\dotplus I$ be defined by $\sigma(a) = (\pi(a),\ a-f(\pi(a)))$. Then we see that σ is an isomorphism of R onto $A\dotplus I$ which leaves every element of I fixed and induces the identity mapping modulo I.

Summarizing the above, we state the following theorem.

Theorem 1. *Let R be a ring with* 1, *I an ideal of R, and $A = R/I$. Suppose that there exists a multiplicative cross-section f: $A \rightarrow R$. Then there exists an E-couple* $([\ ,\ ], d)$ *for A and I such that R is isomorphic to the E-sum $A\dotplus I$ corresponding to* $([\ ,\ ], d)$.

2. In what follows, by making use of Theorem 1, we shall study on the structure of local rings with finite residue fields. The first main theorem of this section is stated as follows.

Theorem 2. *Let M be a nil ring, and $K = GF(p^r)$ (p a prime). If* $([\ ,\ ], d)$ *is an E-couple for K and M,* then the *E-sum $K\dotplus M$ corresponding to* $([\ ,\ ], d)$ *is a local ring with radical M whose residue field is K. In particular, if $[\alpha, \beta] \equiv 0$, then $K\dotplus M$ is of characteristic p. Conversely, if R is a local ring with radical M whose residue field is K, then there exists an E-couple* $([\ ,\ ], d)$ *for K and M such that R is isomorphic to the E-sum $K\dotplus M$ corresponding to* $([\ ,\ ], d)$. *If furthermore R is of characteristic p, then there exists an E-couple with $[\alpha, \beta] \equiv 0$.*

Proof. By definition, it is easy to see that $K\dotplus M$ is a local ring with radical M whose residue field is K. If $[\alpha, \beta] \equiv 0$, then $p(1, 0) = (p, 0) = 0$, so $K\dotplus M$ is of characteristic p.

Conversely, let R be a local ring with radical M whose residue field is K. Then, as is well-known, R is of characteristic p^m. Let $\bar{v} = v+M$ be a generator of the unit group K^* of K. Then $v^{p^r-1} = 1+x$ for some $x \in M$. As is easily seen, $(1+x)^{p^t} = 1$ for some positive integer t. We put $u = v^{p^t}$ whose multiplicative order is p^r-1. Now, we can define a multiplicative cross-section f : $K \rightarrow R$ by $f(\bar{u}^i) = u^i$ $(1 \leqq i \leqq p^r-1)$ and $f(0) = 0$. Then R is isomorphic to an E-sum $K\dotplus M$ by Theorem 1. Henceforth, suppose further that R is of characteristic p. Let $R_1 = \langle u \rangle$ be the subring of R generated by u. Since the natural homomorphism π: $R \rightarrow K$ induces a homomorphism of R_1 onto K, so R_1 is a finite commutative local ring with radical $M_1 = M \cap R_1$ whose residue field is K. Since K is separable over $GF(p)$, by Wedderburn—Malcev theorem [1, Theorem 72. 19], $R_1 = K' \oplus M_1$ as abelian group, where K' is a subfield of R_1. Then we can define a multiplicative cross-section $f: K \to R$ such that $f(\alpha+\beta) = f(\alpha)+f(\beta)$. So (18) becomes $[\alpha, \beta] \equiv 0$.

In what follows, M will represent a nilpotent ring, and $K = GF(p^r)$ (p a prime). Let $K\dot{+}M$ be the E-sum of K and M corresponding to the E-couple $([\ ,\ ], d)$. Then $(K\dot{+}M)^*$ is an extension of $1+M$ by K^*, and is a semidirect product of K^* and $1+M$.

We shall say that an E-couple $([\ ,\ ], d)$ is *symmetric* when $d^1_\alpha x = d^2_\alpha x$ for any $\alpha \in K$ and $x \in M$. When this is the case, $(K\dot{+}M)^*$ is the direct product of K^* and $1+M$.

Given a prime p and positive integers k, r, there exists (uniquely) an r-dimensional Galois extension $GR(p^{kr}, p^k)$ of $\mathbb{Z}_{p^k} = \mathbb{Z}/(p^k)$, which is called a *Galois ring* of characteristic p^k and rank r (see [3, Chapter XVI]). This ring is a commutative local ring with radical (p) whose residue field is $GF(p^r)$. Now, we are in a position to state the second main theorem of this section.

Theorem 3. *Let $K\dot{+}M$ be the E-sum of K and the nilpotent ring M corresponding to the E-couple $([\ ,\ ], d)$. Let p^k be the characteristic of $K\dot{+}M$. Let N be the subring of M generated by $\{[\alpha, \beta] \mid \alpha, \beta \in K\}$, and $S = \{(\alpha, x) \in K\dot{+}M \mid \alpha \in K, x \in N\}$.*

(I) *S is a subring isomorphic to $GR(p^{kr}, p^k)$,* and *$S = \langle(u, 0)\rangle$ for any generator u of K^*.*

(II) *If S' is a subring of $K\dot{+}M$ isomorphic to $GR(p^{kr}, p^k)$, then there exists a unit $b \in (K\dot{+}M)^*$ such that $S' = b^{-1}Sb$* (cf. [5, Theorem 8 (ii)]).

(III) *The following are equivalent.*

(i) *S is the only subring of $K\dot{+}M$ isomorphic to $GR(p^{kr}, p^k)$.*

(ii) *$([\ ,\ ], d)$ is symmetric.*

(iii) *$(K\dot{+}M)^*$ is a nilpotent group* (cf. [8, Theorem 2 (2)]).

Proof. (I) Noting that M is a nilpotent ring whose characteristic is a power of p, we can easily see that every finite subset of $K\dot{+}M$ generates a finite subring. Let u be a generator of K^* and $u' = (u, 0)$. Then $\langle u'\rangle$ is a finite local ring with radical $N' = M \cap \langle u'\rangle$ whose residue field is K. By the proof of [7, Theorem], $\langle u'\rangle$ contains a unit u_1 of multiplicative order p^r-1 such that $\langle u_1\rangle$ is isomorphic to $GR(p^{kr}, p^k)$. Let $|N'| = p^h$ ($h \geqq 0$). Then $(\langle u'\rangle)^*$ is an abelian group of order $p^h(p^r-1)$. Since both cyclic subgroups (u') and (u_1) of $(\langle u'\rangle)^*$ have the same order p^r-1, we have $(u') =$

(u_1). Hence $\langle u' \rangle = \langle u_1 \rangle \simeq GR(p^{kr}, p^k)$. By (16), (17), (11) and (12), it is easy to see that S is a ring containing $\langle u' \rangle$. On the other hand, $(0, [\alpha, \beta]) = (\alpha, 0)+(\beta, 0)-(\alpha+\beta, 0) \in \langle u' \rangle$. This implies $S \subset \langle u' \rangle$, and so $S = \langle u' \rangle$.

(II) The ring S_1 generated by $S' \cup S$ is a finite local ring with residue field K. As S' and S are isomorphic to $GR(p^{kr}, p^k)$, there exists a unit $b \in S_1$ such that $S' = \mathrm{b}^{-1}Sb$ by [5, Theorem 8 (ii)].

(III) (i) $\Rightarrow$ (ii). Suppose that $d^1_\gamma x_0 \neq d^2_\gamma x_0$ for some $\gamma \in K$ and $x_0 \in M$. 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 [5, Theorem 8 (i)], R_1 contains a subring isomorphic to $GR(p^{kr}, p^k)$, which is unique by our assumption. Then, by [8, Theorem 2 (2)], R_1^* is nilpotent. Let $|N_1| = p^s$. Then the order of R_1^* is $p^s(p^r-1)$. Since any finite nilpotent group is the direct product of its Sylow subgroups and $B = \{(\alpha, 0) \mid \alpha \in K^*\}$ is a subgroup of order p^r-1, R_1^* is the direct product of B 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 $d^1_\gamma x_0 \neq d^2_\gamma x_0$.

(ii) $\Rightarrow$ (iii). By the proof of [4, Lemma 1], we see that $1+M$ is a nilpotent group. Hence $(K\dot{+}M)^*$ is nilpotent as the direct product of K^* and $1+M$.

(iii) $\Rightarrow$ (i). Suppose there exists a subring S' of $K\dot{+}M$ isomorphic to $GR(p^{kr}, p^k)$. Then $S' \cup S$ generates a finite local ring S_2 with residue field K. Since S_2^* is nilpotent as a subgroup of $(K\dot{+}M)^*$, $S' = S$ by [8, Theorem 2 (2)].

3. Throughout this section, $K\dot{+}M$ and $K\widetilde{\dot{+}}M$ will represent E-sums corresponding to E-couples $([\ ,\ ], d)$ and $(\widetilde{[\ ,\ ]}, \tilde{d})$, respectively. According to [6, § 52], $K\dot{+}M$ and $K\widetilde{\dot{+}}M$ are said to be *equivalent* (as ring extensions of M by K) if there exists an isomorphism of $K\dot{+}M$ onto $K\widetilde{\dot{+}}M$ which leaves every element of M fixed and maps every class $(\alpha, 0)+M$ of $(K\dot{+}M)/M$ to $(\alpha, 0)+M$ of $(K\widetilde{\dot{+}}M)/M$ $(\alpha \in K)$.

Two groups $(K\dot{+}M)^*$ and $(K\widetilde{\dot{+}}M)^*$ are said to be *equivalent* (as group extensions of $1+M$ by K^*) if there exists a group isomorphism of $(K\dot{+}M)^*$ onto $(K\widetilde{\dot{+}}M)^*$ which leaves every element of $1+M$ fixed and maps every class $(\alpha, 0)(1+M)$ of $(K\dot{+}M)^*/(1+M)$ to $(\alpha, 0)(1+M)$ of $(K\widetilde{\dot{+}}M)^*/(1+M)$ $(\alpha \in K^*)$.

Theorem 4. *$K\dot{+}M$ and $K\widetilde{\dot{+}}M$ are equivalent if and only if there exists a mapping $\lambda\colon K \to M$ such that*

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

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

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

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

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 $\sigma\colon K\dot{+}M \to K\widetilde{\dot{+}}M$ is an isomorphism which leaves every element of M fixed and maps every class modulo M onto itself, we can write $\sigma(\alpha,0) = (\alpha, \lambda(\alpha))$ for some mapping $\lambda\colon K \to M$. We can deduce (21)–(24) from the fact that σ is a ring homomorphism having the above described property.

Conversely, suppose that $\lambda\colon K \to M$ satisfies (21)–(24). Then $\sigma\colon K\dot{+}M \to K\widetilde{\dot{+}}M$ defined by $\sigma(\alpha,x) = (\alpha, x+\lambda(\alpha))$ is the desired isomorphism.

If $K\dot{+}M$ and $K\widetilde{\dot{+}}M$ are equivalent, then by (13), (24) 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.

Theorem 5. *$(K\dot{+}M)^*$ and $(K\widetilde{\dot{+}}M)^*$ are equivalent if and only if there exists a mapping $\mu\colon K^* \to M$ such that*

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

(26) $\mu(\alpha)(d^1_{\alpha^{-1}}x)-(d^2_{\alpha^{-1}}x)\mu(\alpha) = \tilde{d}^2_\alpha(d^2_{\alpha^{-1}}x)-\tilde{d}^1_\alpha(d^1_{\alpha^{-1}}x)$
$(\alpha,\beta \in K^*, x \in M)$.

Proof. If $\tau\colon (K\dot{+}M)^* \to (K\widetilde{\dot{+}}M)^*$ is an isomorphism which leaves every element 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 $\mu\colon K^* \to M$. It is easy to see this μ satisfies (25) and (26).

Conversely, suppose that $\mu\colon K^* \to M$ satisfies (25) and (26). Then we can define $\tau\colon (K\dot{+}M)^* \to (K\widetilde{\dot{+}}M)^*$ 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 every element of $1+M$ fixed and maps every class modulo $1+M$ onto itself. By

$$\tau(\alpha,0)\tau(1,x) = \tau((\alpha,0)(1,x))$$

$$\begin{aligned} \tau(\alpha, x)\tau(\beta, 0) &= \tau((\alpha, x)(\beta, 0)) \\ \tau(\alpha, x)\tau(1, y) &= \tau((\alpha, x)(1, y)), \end{aligned}$$

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

If $K\dot{+}M$ and $K\tilde{+}M$ are equivalent, then so are $(K\dot{+}M)^*$ and $(K\tilde{+}M)^*$. But, the following example shows that the converse need not be true.

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

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

It is easy to see that $([\ ,\ ], d)$ and $([\tilde{,}], \tilde{d})$ are E-couples for K and M. Let $K\dot{+}M$ and $K\tilde{+}M$ be E-sums corresponding to $([\ ,\ ], d)$ and $([\tilde{,}], \tilde{d})$, respectively. Since $\mathrm{ch}(K\dot{+}M) = 9$ and $\mathrm{ch}(K\tilde{+}M) = 3$, $K\dot{+}M$ and $K\tilde{+}M$ are not equivalent. Whereas, by putting $\mu(\alpha) \equiv 0$ in Theorem 5, we see that $(K\dot{+}M)^*$ and $(K\tilde{+}M)^*$ are equivalent.

In conclusion, the author would like to express his indebtedness and gratitude to Prof. Y. Hirano and Prof. H. Komatsu for their helpful suggestion and valuable comments.

REFERENCES

[1] C. W. CURTIS and I. REINER : Representation Theory of Finite Groups and Associative Algebras, Interscience Publishers, New York—London—Sydney, 1962.

[2] C. J. EVERETT : An extension theory for rings, Amer. J. Math. **64** (1942), 363—370.

[3] B. R. MCDONALD : Finite Rings with Identity, Pure & Appl. Math. Ser. 28, Marcel Dekker, New York, 1974.

[4] K. MOTOSE and H. TOMINAGA : Group rings with nilpotent unit groups, Math. J. Okayama Univ. **14** (1969), 43—46.

[5] R. RAGHAVENDRAN : Finite associative rings, Compositio Math. 21 (1969), 195—229.

[6] L. RÉDEI : Algebra I, Akademische Verlagsgesellschaft, Leipzig, 1959.

[7] T. SUMIYAMA : Note on maximal Galois subrings of finite local rings, Math. J. Okayama Univ. **21** (1979), 31—32.

[8] T. SUMIYAMA : On unit groups of finite local rings, Math. J. Okayama Univ. **23** (1981), 195—198.

Aichi Institute of Technology
Toyota 470-03, Japan

(*Received December 25, 1989*)