MODULAR EXTENSIONS

SHIZUKA SATO

(Communicated by Louis J. Ratliff, Jr.)

ABSTRACT. M. E. Sweedler has proved that modular extensions of fields are characterized by a tensor product of primitive elements, and also by the equivalent condition that the ground field is the fixed field under higher derivations. In this paper we shall give an extension of his work about modular field extensions to modular integral domain extensions. Moreover, we shall prove that a modular extension is an extension that the derivation algebra is generated by components of higher derivations under some conditions. For example, in a finite extension of a field, a modular extension is characterized by the fact that the derivation algebra is generated by components of higher derivations.

0. INTRODUCTION AND TERMINOLOGIES

In [12] M. E. Sweedler has defined modular extensions of fields. Let K be a purely inseparable extension of a field k of characteristic $p > 0$. He has shown in [12] that if K is of finite exponent over k , then K is modular if and only if K can be written as the tensor product of simple extensions of k . In this paper, we shall give some characterizations of modular extensions for other cases. Let $K \subset R$ be integral domains of characteristic $p > 0$ and let φ be a mapping of $R \otimes_K R$ onto R such that $\varphi(a \otimes b) = ab$. We shall say that R is purely inseparable over K if and only if $\ker \varphi$ is a nil ideal [11]. In this case we say that R has exponent n over K if $(\ker \varphi)^{p^n} = 0$ but $(\ker \varphi)^{p^{n-1}} \neq 0$.

By a higher derivation of R , we mean a sequence $\{d_i\}$, $0 < i < \infty$, of linear mappings of R into R such that

$$d_0 = 1, \quad d_n(ab) = \sum_{i=0}^n d_i(a)d_{n-i}(b), \quad n = 0, 1, 2, \dots$$

1. MODULAR EXTENSIONS

Let $K \subset R$ be integral domains of characteristic $p > 0$. Suppose R is purely inseparable of finite exponent m over K . Then $Q(K)$ is purely inseparable

Received by the editors September 8, 1989 and, in revised form, October 16, 1989.

1980 *Mathematics Subject Classification* (1985 Revision). Primary 12F05, 12F10, 12F15; Secondary 13B02.

Key words and phrases. High order derivations, higher derivations, separable extensions, purely inseparable extensions, modular extensions.

of exponent m over $Q(K)$ where $Q(K)$, $Q(R)$ denote the quotient fields of K , R respectively.

Sweedler has defined a family of subsets $\{S_{i,j}\}$ of $Q(R)$ and a set N in [12]. But for the sake of convenience of readers we shall write down the definitions. We associate a p -basis of $Q(R)$ over $Q(K)^{p^{1-m}} \cap Q(R)$ with $S_{1,1}$. The set $S_{1,1}^p = \{x^p; x \in S_{1,1}\}$ lies in $Q(K)^{p^{1-m}} \cap Q(R)$. We choose $S_{2,1}$ to be a maximal p -independent subset of $S_{1,1}^p$ over $Q(K)^{p^{2-m}} \cap Q(R)$. $S_{2,2}$ consists of a completion of $S_{2,1}$ to a p -basis of $Q(K)^{p^{1-m}} \cap Q(R)$ over $Q(K)^{p^{2-m}} \cap Q(R)$. Assume we have subsets $S_{i,1}, S_{i,2}, \dots, S_{i,i}$ of $Q(K)^{p^{i-1-m}} \cap Q(R)$ by continuing in this manner. Let T be a maximal p -independent subset of $S_{i,1}^p \cup S_{i,2}^p \cup \dots \cup S_{i,i}^p$ over $Q(K)^{p^{i+1-m}} \cap Q(R)$. And let $S_{i+1,j} = S_{i,j}^p \cap T$ for $j = 1, 2, \dots, i$. $S_{i+1,i+1}$ consists of a completion of T to a p -basis of $Q(K)^{p^{i-m}} \cap Q(R)$ over $Q(K)^{p^{i+1-m}} \cap Q(R)$. Let $N = S_{1,1} \cup S_{2,2} \cup \dots \cup S_{m,m}$. For $x \in N$, let $C(x)$ be the integer i where $x \in S_{i,i}$. If $x \in N$ and $C(x) = i$, we define $\iota(x)$ to be the maximal integer j such that $x^{p^j} \in S_{i+j,i}$. Finally, for $x \in N$, we define $h(x) = m - C(x) + 1$. It is easy to see that the sets $\{S_{i,i}\}$, N can be chosen in R .

The following is seen in [12] for the case of fields; we shall give a theorem for integral domains.

Theorem 1 [12]. *Under the above notations and conditions, the following are equivalent:*

- (a) *The sequence $0 \longrightarrow \otimes_{x \in N} K[x] \longrightarrow R$ is exact and $R / \otimes_{x \in N} K[x]$ is a torsion K -module.*
- (b) *R contains a sub K -module R_0 such that R_0 is isomorphic to a tensor product over K of extensions of K generated by 1 element and R/R_0 is a torsion K -module.*
- (c) *There are higher derivations $d^{(\lambda)} = \{d_i^{(\lambda)}\}$ of R into $Q(R)$, and there is a sub K -module R_1 of R such that (1) $d_i^{(\lambda)}(R_1) \subset R_1$ for all λ, i , (2) R/R_1 is a torsion K -module and $\bigcap_{\lambda, i > 0} \ker d_i^{(\lambda)} = Q(K) \cap R$.*
- (d) *$Q(R)^{p^i}$ and $Q(K)$ are linearly disjoint over their intersections for all $i > 0$.*
- (e) *R^{p^i} and K are linearly disjoint over their intersections for all $i > 0$.*
- (f) *$h(x) = \iota(x)$ for all $x \in N$.*
- (g) *$\{x^{p^{h(x)-1}}; x \in N\}$ forms a p -basis of $Q(K)^{p^{-1}} \cap Q(R)$ over $Q(K)$.*

Proof. That (a) implies (b) is clear. We shall prove that (b) implies (c). We can write $R_0 = \otimes_{y_\lambda \in M} K[y_\lambda]$ for some $M \subset R$. Then we have the exact sequence,

$$0 \longrightarrow \otimes_{y_\lambda \in M} K[y_\lambda] \longrightarrow R \longrightarrow R / \otimes_{y_\lambda \in M} K[y_\lambda] \longrightarrow 0.$$

Since $Q(K)$ is a flat K -module, we have the following exact sequence:

$$0 \longrightarrow Q(K) \otimes_K (\otimes_{y_\lambda \in M} K[y_\lambda]) \longrightarrow Q(R) \longrightarrow Q(K) \otimes_K (R / \otimes_{y_\lambda \in M} K[y_\lambda]) \longrightarrow 0.$$

Since $\otimes_{y_\lambda \in M} K[y_\lambda] = \varinjlim_{M^*} \otimes_{y_\lambda \in M^*} K[y_\lambda]$, where M^* are finite subsets of M , we have $Q(K) \otimes_K (\otimes_{y_\lambda \in M} K[y_\lambda]) = \otimes_{y_\lambda \in M} Q(K)[y_\lambda]$. Therefore we have an exact sequence:

$$0 \longrightarrow \otimes_{y_\lambda \in M} Q(K)[y_\lambda] \longrightarrow Q(R) \longrightarrow Q(K) \otimes_K (R / \otimes_{y_\lambda \in M} K[y_\lambda]) \longrightarrow 0.$$

By the assumption, it holds that $Q(K) \otimes_K (R / \otimes_{y_\lambda \in M} K[y_\lambda]) = 0$ and hence $\otimes_{y_\lambda \in M} Q(K)[y_\lambda] = Q(R)$. Since $Q(R)$, $Q(K)$ are fields, by Theorem 1(c) in [12], there are higher derivations $\{d_i^{(\lambda)}\}$ of $Q(R)$ over $Q(K)$ relative to which $Q(K)$ is the field of constants. From the method of construction of higher derivations $\{d_i^{(\lambda)}\}$ [4, p. 195], we have $d_i^{(\lambda)}(R_0) \subset R_0$ for all λ, i and $\bigcap_{i \geq 1} \ker d_i^{(\lambda)} = R \cap Q(K)$. (c) implies (d). Let $\bar{d}^{(\lambda)}$ be the unique extension of higher derivation $d^{(\lambda)}$ of R to $Q(R)$. Then we have $\bigcap_{i \geq 1} \ker \bar{d}_i^{(\lambda)} = Q(K)$. In fact,

$$\begin{aligned} \bar{d}_i^{(\lambda)}(x/s) &= s^{-i-1} \sum_{j=0}^i (-1)^j \binom{i+1}{j+1} s^{i-j} d_i^{(\lambda)}(xs^j) \\ &= (1/s) \left\{ \sum_{j=0}^i (-1)^j \binom{i+1}{j+1} \right\} d_i^{(\lambda)}(x) = (1/s) d_i^{(\lambda)}(x) \end{aligned}$$

for $s \in K - (0)$, $x \in R$, where $\binom{i}{j}$ represents a binomial coefficient. Thus the next implication is satisfied:

$$(x/s) \in \bigcap_{i \geq 1} \ker \bar{d}_i^{(\lambda)} \iff x \in \bigcap_{i \geq 1} \ker d_i^{(\lambda)}.$$

Therefore, by Theorem 1(d) in [12], $Q(R)^{p^i}$ and $Q(K)$ are linearly disjoint over their intersection for all $i \geq 1$. That (d) is equivalent to (e) is proved by a simple calculation. It is shown in [12, Theorem 1] that (d) implies (f), that (f) implies (a) and that (f) is equivalent to (g). $\square$

Definition. Let $K \subset R$ be integral domains. R is called a modular extension of K if R satisfies condition (e) of Theorem 1.

Let $B \subset A$ be rings. A B -linear mapping D is called an n th order B -derivation [1, 3, 6, 10] if

$$D(x_0 x_1 x_2 \cdots x_n) = \sum_{s=1}^n (-1)^{s-1} \sum_{i_1 < i_2 < \cdots < i_s} x_{i_1} x_{i_2} \cdots x_{i_s} D(x_0 \cdots \hat{x}_{i_1} \cdots \hat{x}_{i_s} \cdots x_n)$$

for $x_i \in A$.

Let $D_B^{(n)}(A, M)$ be the set of all n th order B -derivations of A into an A -module M , and let us set $D_B(A, M) = M + \sum_{n \geq 1} D_B^{(n)}(A, M)$. Then $D_B(A, A)$ is an algebra with usual operations [6, 10].

A is called a P.H.D. ring over B with respect to an A -module M if $D_B(A, M) = \text{Hom}_B(A, M)$. A is called a P.H.D. ring over B if A is a P.H.D. ring over B with respect to all A -modules M [9, 11]. In [7], we already know that a purely inseparable extension field L of finite degree over a field K is a P.H.D. ring over K .

Theorem 2. *Let R be a finite purely inseparable extension field of a field K of characteristic $p > 0$. Then R is modular over K if and only if $D_K(R, R)$ is generated by components of higher derivations of R as R -algebras.*

Proof. At first we shall prove the only if part. By [12, Theorem 1] there exist elements x_i ($1 \leq i \leq t$) in R of exponent e_i such that $R = \otimes_{i=1}^t K[x_i]$. Now we can define higher derivations $\{d_i^{(\lambda)}\}_{1 \leq \lambda \leq t, 0 \leq i \leq p}$ of R s.t. $d_i^{(\lambda)}(x_\lambda^n) = \binom{n}{\lambda} x_\lambda^{n-i}$ and the constant field of $d^{(\lambda)}$ is $K[x_1, x_2, \dots, x_{\lambda-1}, x_{\lambda+1}, \dots, x_n]$. Then $\{d_{i_1}^{(\lambda_1)} d_{i_2}^{(\lambda_2)} \dots d_{i_t}^{(\lambda_t)}\}$ are linearly independent over R . Now let $\mathcal{S}$ be the R -algebra generated by components of $\{d^{(\lambda)}\}_{1 \leq \lambda \leq t}$. Then $\dim_R \mathcal{S} = \pi p^{e_i} = p^{\sum e_i}$. On the other hand, $\dim_K R = \pi p^{e_i}$ and hence $\dim_R(\text{Hom}_K(R, R)) = p^{\sum e_i}$. Therefore $\mathcal{S} = \text{Hom}_K(R, R)$ and hence $\mathcal{S} = D_K(R, R)$.

Next we shall prove the if part. Since R is a finite purely inseparable extension of K , R is a P.H.D. ring by [7, Theorem 4]. Therefore, for any $x \in R - K$, there exists an element $D_i \in D_K^{(i)}(R, R)$ such that $D_i(x) \neq 0$. Hence from the assumption there are higher derivations $\{d^{(\lambda)}\}$ such that D_i is written by components of $\{d^{(\lambda)}\}$. Thus $D_i(x) \neq 0$ implies $d_i^{(\lambda)}(x) \neq 0$ for some λ, i . Therefore K is the constant field of higher derivations of R and R is modular over K . $\square$

Theorem 3. *Let $K \subset R$ be integral domains of characteristic $p > 0$ and R be free over K of finite rank. Suppose R is purely inseparable over K . Then R is modular over K if and only if $D_K(R, R)$ is generated by components of higher derivations of R as R -algebras.*

Proof. If K is a field, then R is a field. Therefore it follows from Theorem 2 in this case. Suppose K is not a field. Let $S = K - (0)$. Then $S^{-1}K = Q(K)$ and $S^{-1}R = Q(R)$. At first we shall prove the necessity. Since R is modular over K , $Q(R)$ is modular over $Q(K)$. By Theorem 1, there are elements $x_i \in R$ such that $Q(R) \simeq \otimes_{i=1}^n Q(K)[x_i]$. From $D_{Q(K)}(Q(R), Q(R)) = Q(R) \otimes_R D_K(R, R)$, we have $D_{Q(K)}(Q(R), Q(R)) = Q(R)[d^{(1)}, d^{(2)}, \dots, d^{(n)}]$, where $D^{(\lambda)}$ are higher derivations of R over K such that $d_i^{(\lambda)}(x_j^{n_j}) = \binom{n_j}{\lambda} \delta_{ij} x_j^{n_j-i}$. For any $f \in D_K(R, R)$, there are elements $a_{j_1 j_2 \dots j_n} \in Q(R)$ such that

$$f = \sum a_{j_1 j_2 \dots j_n} (d_{j_1}^{(1)})(d_{j_2}^{(2)}) \dots (d_{j_n}^{(n)}).$$

Now we can write $f = \sum f_m$, where

$$f_m = \sum_{j_1 + j_2 + \dots + j_n = m} a_{j_1 j_2 \dots j_n} (d_{j_1}^{(1)})(d_{j_2}^{(2)}) \dots (d_{j_n}^{(n)}).$$

Suppose that there are integers m such that $a_{j_1 j_2 \dots j_n} \notin R$, $m = j_1 + j_2 + \dots + j_n$. Let m_0 be the minimum integer among such integers. Then, for $j_1 + j_2 + \dots + j_n = m_0$,

$$f(x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}) = \sum_{m < m_0} f_m(x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}) + a_{j_1 j_2 \dots j_n}.$$

By the assumption on m we have $f_m(x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}) \in R$ for $m < m_0$, and hence we have $a_{j_1 j_2 \dots j_n} \in R$ for $j_1 + j_2 + \dots + j_n = m_0$. This is a contradiction to the assumption on m_0 . Therefore it follows that $a_{j_1 j_2 \dots j_n} \in R$ for all j_k . Hence we have $f \in R[d^{(1)}, d^{(2)}, \dots, d^{(n)}]$.

Next, we shall prove the if part. From $\text{rank}_K R < \infty$, the module $\Omega_K(R)$ of differentials of R over K [6, 10] is a finite R -module. Therefore we have isomorphisms

$$\begin{aligned} D_{Q(K)}(Q(R), Q(R)) &\simeq \text{Hom}_{Q(K)}(\Omega_{Q(K)}(Q(R)), Q(R)) \\ &\simeq Q(R) \otimes_R \text{Hom}_K(\Omega_K(R), R) \\ &\simeq Q(R) \otimes_R D_K(R, R). \end{aligned}$$

With these isomorphisms, higher K -derivations of R correspond to higher $Q(K)$ -derivations of $Q(R)$. Therefore $D_{Q(K)}(Q(R), Q(R))$ is generated by components of higher $Q(K)$ -derivations of $Q(R)$, and hence, by Theorem 2, $Q(R)$ is modular over $Q(K)$. By Theorem 1, R is modular over K . $\square$

Theorem 4. *Let R be a finite extension field of a field K . Then R is modular over K if and only if $D_K(R, R)$ is generated by components of higher derivations of R as R -algebras.*

Proof. The only if part. There is an intermediate field M such that R is separable over M and M is purely inseparable modular over K [5, Theorem 1]. From [11, Theorem 12] and Theorem 2, it follows that

$$\begin{aligned} D_K(M, R) &= \text{Hom}_K(M, R) \\ &= \sum R(d_{j_1}^{(1)})(d_{j_2}^{(2)}) \dots (d_{j_n}^{(n)}), \end{aligned}$$

where $M = \otimes_{\lambda=1}^n K[x_\lambda]$ and every $\{d_j^{(\lambda)}\}$ is a higher derivation of M such that $d_j^{(\lambda)}(x_\lambda^m) = \binom{m}{j} x_\lambda^{m-j}$ and $d_j^{(\lambda)}(K[x_1, x_2, \dots, x_{\lambda-1}, x_{\lambda+1}, \dots, x_n]) = 0$. Since R is finite separable algebraic over M , every $\{d_j^{(\lambda)}\}$ is uniquely extended to a higher derivation $\{\bar{d}_j^{(\lambda)}\}$ of R by [2]. Let D be an element of $D_K(R, R)$. Then the restriction $D|_M$ of D on M is an element of $D_K(M, R)$. By Theorem 2, we can write

$$D|_M = \sum \alpha_{j_1 j_2 \dots j_n} (d_{j_1}^{(1)})(d_{j_2}^{(2)}) \dots (d_{j_n}^{(n)}), \text{ for } \alpha_{j_1 \dots j_n} \in R.$$

Since the extension of $D|_M$ to R is unique, we have

$$D = \sum \alpha_{j_1 j_2 \dots j_n} (\bar{d}_{j_1}^{(1)})(\bar{d}_{j_2}^{(2)}) \dots (\bar{d}_{j_n}^{(n)})$$

and hence $D_K(R, R)$ is generated by components of higher derivations of R as R -algebras. Next, we shall prove the if part. Since $\dim_K R < \infty$, there is a subfield K_0 of R containing K such that R is finite purely inseparable over K_0 and K_0 is separable algebraic over K . Hence we have $D_{K_0}(R, R) = \text{Hom}_{K_0}(R, R)$ and $D_K(R, R) = D_{K_0}(R, R)$ by Theorem 4 and [7, Proposition 6]. Thus $D_K(R, R)$ is generated by components of higher derivations of R as R -algebras. Therefore K_0 is the constant field of higher derivations of R . By [12, Theorem 1], R is modular over K_0 . Therefore, from [12, Lemma 5(2)], R is modular over K .

REFERENCES

1. A. Grothendieck, *Éléments de Géométrie Algébrique* IV, Étude Locale des Schémas et des Morphismes de Schémas, **16.8** (1967).
2. N. Heerema, *Higher derivations and automorphisms of complete local rings*, Bull. Amer. Math. Soc. **76** (1970), 1212–1225.
3. R. G. Heyneman and M. E. Sweedler, *Affine Hopf algebra*, J. Algebra **13** (1969), 192–241.
4. N. Jacobson, *Lectures in abstract algebra* III, Van Nostrand Company, New York.
5. H. F. Kreimer and N. Heerema, *Modularity vs. separability for field extensions*, Canad. J. Math. **27** (1975), 1176–1182.
6. Y. Nakai, *High order derivations* I, Osaka J. Math. **7** (1970), 1–27.
7. Y. Nakai, K. Kosaki, and Y. Ishibashi, *High order derivations* II, J. Sci. Hiroshima Univ. Ser. A-I **34** (1970), 17–27.
8. Y. Nakai, *Commutative rings and derivations* (in Japanese), Kyoritsu shuppan.
9. —, *On a ring with a plenty of high order derivations*, J. Math. Kyoto Univ. **13** (1972), 159–164.
10. S. Sato, *Notes on derivations of high order*, J. Sci. Hiroshima Univ. Ser. A-I **33** (1969), 41–46.
11. —, *On purely inseparable algebras and P.H.D. rings*, Trans. Amer. Math. Soc. **226** (1981), 483–498.
12. M. E. Sweedler, *Structure of inseparable extensions*, Ann. Math. **87** (1968), 401–410.

DEPARTMENT OF MATHEMATICS, FACULTY OF ENGINEERING, OITA UNIVERSITY, JAPAN