Hokkaido Mathematical Journal Vol. 11 (1982) p. 111-115

On separable extensions over a local ring

By Kozo SUGANO

(Received July 22, 1980; Revised June 15, 1981)

1. Introduction

Throughout this paper Λ is a ring with 1 and Γ is a subring of Λ which contains 1 of Λ. Λ is a separable extension of Γ if and only if map π of $\Lambda\otimes_{\Gamma}\Lambda$ to Λ such that $\pi(x\otimes y)=xy$ for x, $y\in\Lambda$ splits as $\Lambda-\Lambda$-map, namely, if and only if there exists $\sum x_{i}\otimes y_{i}$ in $(\Lambda\otimes_{\Gamma}\Lambda)^{\Lambda}$ such that $\Sigma x_{i}y_{i}=1$, where $(\Lambda\otimes_{\Gamma}\Lambda)^{\Lambda}=\{\chi\in\Lambda\otimes_{\Gamma}\Lambda\,|\,x\chi=\chi x$ for all x in $\Lambda\}$. If σ is a ring automorphism of Λ, then by $\Lambda[X;\sigma]$, we denote as usual the ring of all polynomials $\Sigma_{i}X^{i}r_{i}$ $(r_{i}\in\Lambda)$ with an indeterminate X whose multiplication is defined by $rX=X\sigma(r)$ for each $r\in\Lambda$. In this paper we shall show that if Λ is a separable extension of a local ring Γ such that $\Lambda=\Gamma\oplus M$ as $\Gamma-\Gamma$-module with M a finitely generated left (or right) Γ-module and $M^{2}\subset\Gamma$, then $\Lambda\cong\Gamma[X;\sigma]/(X^{2}-a)$ for some $a\in\Gamma$ and σ. We will also show that any trivial extension can not be a separable extension (Theorem 1).

2. Structure of separable extension of a local ring

A modification of the proof of Lemma 1.2 [1] yields

PROPOSITION 1. *Let Λ be a separable extension of Γ, and suppose that there exists a ring homomorphism φ of Λ onto Γ such that $\varphi(r)=r$ for all $r\in\Gamma$. Then there exists a unique central idempotent e of Λ such that $\varphi(x)e=ex$ for all x in Λ and $\varphi(e)=1$. Furthermore, if φ_{1} and φ_{2} are mutually strongly distinct homomorphisms(*) which satisfy the same conditions as φ, then $\varphi_{i}(e_{j})=\delta_{ij}$ and $e_{i}e_{j}=e_{i}\delta_{ij}$, where each e_{i} is the unique central idempotent determined by φ_{i}.*

PROOF. Since Λ is a separable extension of Γ, there exists $\Sigma x_{i}\otimes y_{i}$ in $(\Lambda\otimes_{\Gamma}\Lambda)^{\Lambda}$ such that $\Sigma x_{i}y_{i}=1$. Set $e=\Sigma\varphi(x_{i})y_{i}$. Since $\Sigma xx_{i}\otimes y_{i}=\Sigma x_{i}\otimes y_{i}x$ for all x in Λ, and φ is a $\Gamma-\Gamma$-homomorphism, we have $\Sigma\varphi(x)\varphi(x_{i})y_{i}=\Sigma\varphi(xx_{i})y_{i}=\Sigma\varphi(x_{i})y_{i}x$ for all x in Λ, consequently, $\varphi(x)e=ex$. On the othere hand, $\varphi(e)=\varphi(\Sigma\varphi(x_{i})y_{i})=\Sigma\varphi(x_{i})\varphi(y_{i})=\varphi(\Sigma x_{i}y_{i})=\varphi(1)=1$. Then, $ee=\varphi(e)e=$

(*) When f and g are ring homomorphisms of Λ_{1} to Λ_{2}, f and g are said to be strongly distinct if for any central idempotent e of Λ_{2} there exists s in Λ_{1} such that $f(s)e\neq g(s)e$.

$1e=e$. Similarly if we put $f=\Sigma x_i\varphi(y_i)$, we have $f^2=f$, $\varphi(f)=1$ and $xf=f\varphi(x)$ for all x in Λ. Then $ef=f\varphi(e)=f1=f$ and $ef=\varphi(f)e=1e=e$. Therefore, we have $e=f$, and $xe=xfe=f\varphi(x)e=fex=ex$ for all x in Λ. Thus e is a central idempotent of Λ. The proof of the equality $e=f$ shows the uniqueness of such an idempotent. The latter half of this proposition can be proved by the same way as Lemma 1. 2 [1], since e_i's are central idempotents.

REMARK. Let Λ, Γ, φ and e be as in Prop. 1. Then we have Ker $\varphi=\{x-\varphi(x)\mid x\in\Lambda\}=\Lambda(1-e)$, since $xe=\varphi(x)e$ for all $x\in\Lambda$ and $\varphi(e)=1$.

We say that Λ is a trivial extension of Γ, in case $\Lambda=\Gamma\oplus M$ as $\Gamma-\Gamma$-module and $M^2=0$. As a corollary to Prop. 1, we have

THEOREM 1. *No trivial extension is a separable extension.*

PROOF. Let Λ be a trivial extension of Γ by a $\Gamma-\Gamma$-module M. Then M is an ideal of Λ, and we have a natural ring homomorphism of Λ to $\Lambda/M=\Gamma$ such that $\varphi(r)=r$ for all $r\in\Gamma$. If Λ is separable over Γ, M must be generated by a central idempotent of Λ, and $M^2=M$. This contradicts to $M^2=0$. Hence Λ is not a separable extension of Γ.

Now let us consider the case where Λ is a separable extension of Γ and Γ is a $\Gamma-\Gamma$-direct summand of Λ. Set $\Lambda=\Gamma\oplus M$, where M is a $\Gamma-\Gamma$-submodule of Λ. If $M^2\subset M$, M becomes an ideal of Γ, and we can apply Prop. 1. Therefore there exists a central idempotent e of Λ, such that $M=\Lambda(1-e)$ and $\Lambda e\cong\Gamma$ as ring. Next consider the case where $M^2\subseteq\Gamma$. which means that Λ is a graded ring of degree 2.

PROPOSITION 2. *Let Λ be a separable extension of Γ, and suppose that $\Lambda=\Gamma\oplus M$ as $\Gamma-\Gamma$-module and $M^2\subseteq\Gamma$. Then $M^3=M$, and M^2 is an idempotent ideal of Γ.*

PROOF. Set $M^2=\mathfrak{a}$. It is obvious that $\mathfrak{a}$ is an ideal of Λ. Since $\Lambda=\Gamma\oplus M$ as $\Gamma-\Gamma$-module, $\mathfrak{a}\Lambda=\Lambda\mathfrak{a}=M^2\oplus M^3$ is an ideal of Λ. Then, $\Lambda/\mathfrak{a}\Lambda=\Gamma/\mathfrak{a}\oplus M/M^3$ is a separable extension of $\Gamma/\mathfrak{a}$ by Prop. 2. 4 [2]. Since $M^2=\mathfrak{a}$, $(M/M^3)^2=0$ in $\Lambda/\mathfrak{a}\Lambda$. Hence $\Lambda/\mathfrak{a}\Lambda$ is a trvial extension of $\Gamma/\mathfrak{a}$, which can not be a separable extension. Therefore $M/M^3=0$. Thus $M=M^3$ and $M^2=M^4$.

THEOREM 2. *Let Γ be a local ring with the unique maximal ideal $J(\Gamma)$ and Λ a separable extension of Γ. Suppose that Λ is a left (or right) Γ-finitely generated module, and $\Lambda=\Gamma\oplus M$ as $\Gamma-\Gamma$-module with $M^2\subseteq\Gamma$. Then M is a left as well as right Γ-free module of rank* 1, *and there* *exists a unit x in M and an automorphism σ of Γ such that $\Lambda=\Gamma\oplus\Gamma x$ and $rx=x\sigma(r)$ for all $r\in\Gamma$.*

PROOF. Set $M^2=\mathfrak{a}$. Then by Prop. 2, $\mathfrak{a}M=M^3=M$. Hence $\mathfrak{a}\Lambda=\mathfrak{a}\oplus\mathfrak{a}M=\mathfrak{a}\oplus M$, and $\Gamma+\mathfrak{a}\Lambda=\Gamma+M=\Lambda$. Then if $\mathfrak{a}\subset J(\Gamma)$, $\Gamma=\Lambda$ by Nakayama's Lemma. Hence $\mathfrak{a}\not\subset J(\Gamma)$. This means that $MM=\Gamma$, since Γ is local. Therefore there exist m_i and n_i (finite) in M such that $\Sigma m_i n_i=1$. It is well known that in this case M is said to be invertible, and ${}_\Gamma M$ and M_Γ are progenerators, ${}_\Gamma M_\Gamma\cong{}_\Gamma\mathrm{Hom}({}_\Gamma M, {}_\Gamma\Gamma)_\Gamma$, ${}_\Gamma M_\Gamma\cong{}_\Gamma\mathrm{Hom}(M_\Gamma, \Gamma_\Gamma)_\Gamma$, $\Gamma^0=\mathrm{Hom}({}_\Gamma M, {}_\Gamma M)$ and $\Gamma\cong\mathrm{Hom}(M_\Gamma, M_\Gamma)$, where Γ^0 means the opposite ring of Γ. In fact it is easy to prove these matters by using m_i and n_i's. But since Γ is local, M is free of finite rank. Hence ${}_\Gamma M\cong{}_\Gamma\Gamma$ and $M_\Gamma\cong\Gamma_\Gamma$, and there exist $x, y\in M$ such that $M=\Gamma x=y\Gamma$. Then $\Gamma x\Gamma x=M^2=\Gamma$, and $1=\Sigma r_i x s_i x=mx$ for some r_i, s_i in Γ and $m=\Sigma r_i x s_i\in M$. Then $0\neq xm=xmxm$, and $xm\in M^2=\Gamma$. Hence $xm=mx=1$, since Γ has no nontrivial idempotents. Similarly y is a unit. Set $y=tx$ with $t\in\Gamma$. Then t is a unit of Γ, since $y^{-1}\in M$ and $t^{-1}=xy^{-1}\in M^2=\Gamma$. Hence $\Gamma y=\Gamma tx=\Gamma x=y\Gamma$, and similarly $\Gamma x=x\Gamma$. Then since x is a unit, there exists a unique element $\sigma(a)$ in Γ such that $ax=x\sigma(a)$, for each a in Γ. It is easy to see that σ is an automorphism of Γ.

REMARK. Let Λ, Γ, σ and x be as in Theorem 2, and set $x^2=a$ $(\in\Gamma)$. Then since $ax=x^3=xa$, we have $\sigma(a)=a$ and $ra=rxx=a\sigma^2(r)$ for each r in Γ. Therefore we have $\Gamma[X,\sigma](X^2-a)=(X^2-a)\Gamma[X,\sigma]$, and $\Lambda\cong\Gamma[X,\sigma]/(X^2-a)$.

The next proposition which we need to prove our main theorem has been proved by Y. Miyashita in [4] in more general form. Here we will give the proof by direct computations for the sake of reader's convenience.

PROPOSITION 3. (Theorem 3.1 [3]) *Let R be a ring with 1 and σ an automorphism of R. For a unit element a of R such that $\sigma(a)=a$ and $ra=a\sigma^n(r)$ for all $r\in R$, $R[X;\sigma]/(X^n-a)$ is a separable extension of R if and only if there exists c in the center of R such that $\Sigma_{i=0}^{n-1}\sigma^i(c)=1$.*

PROOF. Denote the center of R by C, and set $\Lambda=R[X;\sigma]/(X^n-a)$. First note that $(\Sigma X^i a_i)(X^n-a)=(X^n-a)(\Sigma X^i\sigma^n(a_i))$, and $R[X;\sigma]/(X^n-a)=(X^n-a)R[X;\sigma]$. Set $x=X+(X^n-a)$. Then we have that $\Lambda=R\oplus Rx\oplus\cdots\oplus Rx^{n-1}$, and $x^n=a$ and $rx=x\sigma(r)$ for all $r\in R$. x is a unit since a is so. Hence $\{x^i\otimes x^j\mid i, j=0, 1, \cdots, n-1\}$ forms a free basis of $\Lambda\otimes_R\Lambda$ over Λ. If Λ is a separable extension of R, there exists $\Sigma\alpha_i\otimes\beta_i$ in $(\Lambda\otimes_R\Lambda)^\Lambda$ such that $\Sigma\alpha_i\beta_i=1$. We can set $\Sigma\alpha_i\otimes\beta_i=\Sigma x^i\otimes x^j r_{ij}$ with $r_{ij}\in R$. Then from $\Sigma\alpha_i\beta_j=$

1, we obtain $r_{00}+\Sigma_{i=1}^{n-1} ar_{n-i,i}=1$. While from $\Sigma xx^i\otimes x^j r_{ij}=\Sigma x^k\otimes x^l r_{kl}x=\Sigma x^k\otimes x^{l+1}\sigma(r_{kl})$, we obtain $r_{ij}=\sigma(r_{i+1,j-1})$, $\sigma(r_{0,i-1})=ar_{n-1,i}$, $r_{i-1,0}=a\sigma(r_{i,n-1})$, in particular, $\sigma(r_{00})=ar_{n-1,1}$ and $\sigma(r_{n-i,i})=r_{n-i-1,i+1}$, for $i=0,1,\cdots,n-1$. Hence $ar_{n-i,i}=\sigma^i(r_{00})$ for all i. It is also obvious that $r_{00}\in C$, since $\Sigma r\alpha_i\otimes\beta_i=\Sigma\alpha_i\otimes\beta_i r$ for all $r\in R$. Thus we have $\Sigma_{i=0}^{n-1}\sigma^i(r_{00})=1$ with $r_{00}\in C$. Conversely suppose that there exists c in C such that $\Sigma\sigma^i(c)=1$. Then we have $\sigma^n(c)=c$. While by assumption we have $\sigma(a)=a$ and $\sigma^n(r)a^{-1}=a^{-1}r$ for all $r\in R$, too. Then by these three conditions we easily see that $\Sigma x^{n-i}\otimes x^i a^{-1}\sigma^i(c)\in(\Lambda\otimes_R\Lambda)^\Lambda$ and $\Sigma x^{n-i}x^i a^{-1}\sigma^i(c)=\Sigma\sigma^i(c)=1$. Therefore Λ is a separable extension of R.

THEOREM 3. *If Γ is a local ring, the following two conditions are equivalent*;

(i) *Λ is a separable extension of Γ with $\Lambda=\Gamma\oplus M$ as $\Gamma-\Gamma$-module where M is finitely generated as left (or right) Γ-module and $M^2\subseteq\Gamma$.*

(ii) *$\Lambda\cong\Gamma(X;\sigma]/(X^2-a)$ with some automorphism σ and a unit a of Γ such that $\sigma(a)=a$ and $ra=a\sigma^2(r)$ for all $r\in R$, and there exists c in the center of Γ such that $c+\sigma(c)=1$.*

PROOF. This is obvious by Theorem 2, Prop. 3 and the remark after Theorem 2.

REMARK. In the case where Γ is a left (or right) Noetherian local ring, we can omit the condition that M is Γ-finitely generated case Γ-module in the proofs of Theorem 2 and Theorem 3. Because in this case $\mathfrak{a}$ $(=M^2)$ is left Γ-finitely generated, and $\mathfrak{a}^2=\mathfrak{a}\subseteq J(\Gamma)$ implies that $\mathfrak{a}=\mathfrak{a}\mathfrak{a}\subset J(\Gamma)\mathfrak{a}\subseteq\mathfrak{a}$. This means $\mathfrak{a}=J(\Gamma)\mathfrak{a}$. Hence $\mathfrak{a}=0$ by Nakayama's lemma, which contradicts to Theorem 1. Hence $\Gamma=M^2$. Now we can follow the same lines as the proof of Theorem. 2.

3. Commutative Noetherian semi-local ring

In this section we will consider the case where Γ is a commutative Noetherian semi-local ring. To begin with we will introduce

LEMMA 1 (Lemma 2 [3]). *Let R be a commutative ring with* 1 *and S a commutative R-algebra. Then if $\mathfrak{a}$ is an idempotent ideal of S which is R-finitely generated, $\mathfrak{a}=Se$ for some $e=e^2\in S$.*

PROOF. See Lemma 2 [3].

THEOREM 4. *Let Γ be a commutative Noetherian semi-local ring and Λ a separable extension of Γ, and suppose that $\Lambda=\Gamma\oplus M$ with a $\Gamma-\Gamma$-*

submodule M such that M_Γ is faithful and $M^2 \subseteq \Gamma$. Then $\Lambda \cong \Gamma[X; \sigma]/(X^2-u)$ for some automorphism σ of Γ and a unit u of Γ such that $\sigma(u)=u$ and $xu=u\sigma^2(x)$ for all $x \in \Gamma$.

PROOF. Set $\mathfrak{a}=M^2$. Then $0 \neq \mathfrak{a}=\mathfrak{a}^2$ by Theorem 1 and Prop. 2, and $\mathfrak{a}$ is finitely generated. Hence $\mathfrak{a}=\Gamma e$ for some $0 \neq e^2=e \in \Gamma$ by Lemma 1. We have also $M=M\mathfrak{a}=Me$ by Prop. 2. Hence $M(1-e)=Me(1-e)=0$. But M is faithful as right Γ-module. Hence $e=1$, and we have that $M^2=\Gamma$. Then M is invertible and $\Gamma \cong \mathrm{Hom}\,({}_\Gamma M, {}_\Gamma M)$. Now let $\mathfrak{m}$ be a maximal ideal of Γ and let $r=\dim_{\Gamma/\mathfrak{m}} M/\mathfrak{m}M$. Since M is left Γ-projective, there exists a ring homomorphisms of $\mathrm{Hom}\,({}_\Gamma M, {}_\Gamma M)$ onto $\mathrm{Hom}\,({}_\Gamma M/\mathfrak{m}M, {}_\Gamma M/\mathfrak{m}M) \cong (\Gamma/\mathfrak{m})_r$, the $r \times r$-full matrix ring over $\Gamma/\mathfrak{m}$. But the former is commutative. Hence $(\Gamma/\mathfrak{m})_r$ is also commutative, which means that $r=1$. Now let $\mathfrak{m}_1, \mathfrak{m}_2, \cdots, \mathfrak{m}_s$ be the set of maximal ideals of Γ. Since $MM=\Gamma$, we see that $\mathfrak{m}_1 \cdots \mathfrak{m}_{i-1}\mathfrak{m}_{i+1} \cdots \mathfrak{m}_s M \not\subset \mathfrak{m}_i M$ for each i. Hence there exists $m_i \in \mathfrak{m}_1 \cdots \mathfrak{m}_{i-1}\mathfrak{m}_{i+1} \cdots \mathfrak{m}_s M$ such that $m_i \notin \mathfrak{m}_i M$. Set $m=\Sigma m_i$. Then $m \notin \mathfrak{m}_j M$ for each j. Therefore, $\Gamma/\mathfrak{m}_i(m+\mathfrak{m}_i M)=M/\mathfrak{m}_i M$, and $M=\Gamma m+\mathfrak{m}_i M$ for each maximal ideal $\mathfrak{m}_i$ of Γ. Then by Nakayama's lemma we have $M=\Gamma m$. Similarly we have $M=n\Gamma$ for some $n \in M$. Then $M^2=n\Gamma m=\Gamma$, and there is an s in Γ such that $nsm=1$. But $n(smn-1)=0$, and $smn \in M^2=\Gamma$. Hence $M(smn-1)=n\Gamma(smn-1)=n(smn-1)\Gamma=0$. Then, since M is right Γ-faithful, $smn=1$. Thus m, n and s are units, and we see that $M=\Gamma m=m\Gamma$. Then the same proof as Theorem 2 shows that $\Lambda \cong \Gamma[X; \sigma]/(X^2-u)$ with $u=m^2$.

REMARK. In the case where Γ is indecomposable commutative Noetherian and semi-local, we can ommit the assumption that M is Γ-faithful.

References

[1] D. K. HARRISON and S. U. CHASE and Alex ROSENBERG: Galois theory and Galois cohomology of commutative rings, Memoirs Amer. Math. Soc., 52 (1965).

[2] K. HIRATA and K. SUGANO: On semisimple extensions and separable extensions over non commutative rings, J. Math. Soc. Japan, 18 (1966), 360–373.

[3] T. KANZAKI: On Galois algebra over a commutative ring, Osaka J. Math., 2 (1965), 309–317.

[4] Y. MIYASHITA: On a skew polynomial ring, J. Math. Soc. Japan 31 (1979), 317–330.

[5] T. NAGAHARA and K. KISHIMOTO: On a free cyclic extensions of rings, Proc. 10th symposium on ring theory, 1978, Okayama Japan.

Department of Mathematics
Hokkaido University