Hokkaido Mathematical Journal Vol. 18 (1989), p. 211-215

Note on separable extensions of noncommutative rings

Kozo SUGANO
(Received March 29, 1988)

Introduction.

This paper is a continuation of the author's previous paper [3]. Let A be a ring and B a subring of A such that $A=B\oplus M$ as B-B-module, and assume that A is a separable extension of B. In [3] the author considered two cases of separable extensions of this type, that is, the case where $M^2\subset B$ and the case where $M^2\subset M$, and investigated the former case mainly. In this paper we will treat the latter case, and will show that, in the case where $A=B\oplus M$ such that M in an ideal of A and left B-faithful, A is a separable extension of B, if and only if M is generated by a central idempotent f of A and a separable extension of Bf (Theorem 1). In the process of the proof of this theorem we will consider the case where $A=R\oplus S$ with S a ring and R a subring of S, and the multiplication is defined by $(r, x)(s, y)=(rs, xs+ry+xy)$ for any $x, y\in S$ and $r, s\in R$. And we will show the equivalence of the following three conditions:

(a) A is a separable extension of R
(b) A is a separable extension of $R\oplus R$
(c) S is a separable extension of R (Theorem 2).

1. Throughout this paper every ring will have the identity, and all subrings of a ring will contain the identity of the ring. As for the definition and the fundamental properties of the separable extension of a noncommutative ring, see [2]. The author requires the readers to have already known them. In particular, we will use freely Propositions 2.4 and 2.5 [2]. Moreover we require the following fact: If A_i is a separable extension of B_i for $r=1, 2$, then $A=A_1\oplus A_2$ is a separable extension of $B=B_1\oplus B_2$. This is obvious by $A\otimes_B A=A_1\otimes_{B_1}A_1\oplus A_2\otimes_{B_2}A_2$.

The following lemma has been shown in [3] and [4].

LEMMA 1. *Let A be a ring and B a subring of A such that $A=B\oplus M$ as B-B-module with $M^2\subset M$. If A is a separable extension of B, then M is generated by a central idempotent of A. Consequently, M is a ring with the identity.*

PROOF. By the assumption M is an ideal of A, and there exists a ring homomorphism ψ of A to B such that $\psi(b)=b$ for each $b\in B$. Then by Proposition 1 [3] there exists a central idempotent e of A such that $\psi(e)=1$ and $xe=\psi(x)e$ for each $x\in A$. And we have $M=\mathrm{Ker}\,\psi=A(1-e)$.

Let A, B, M, ψ and e be as in Lemma 1, and put $f=1-e$. Then the map ρ of B to M defined by $\rho(b)=bf$ for each $b\in B$ is a ring homomorphism which gives M the same B-B-module structure as the one given originally. Let $\mathfrak{a}=\mathrm{Ker}\,\rho$. Then $\mathfrak{a}$ is an ideal of A, and $A/\mathfrak{a}=B/\mathfrak{a}\oplus M$ with $M^2\subset M$. Then $B/\mathfrak{a}$ is regarded as a subring of M. Later we will see that M is a separable extension of $B/\mathfrak{a}$. More generally we will have.

THEOREM 1. *Let A be a ring and B a subring of A such that $A=B\oplus M$ as B-B-module. Assume furthermore that M is an ideal of A and left (or right) B-faithful. Then A is a separable extension of B, if and only if M is generated by a central idempotent f of A, i. e., $M=Af$, and is a separable extension of Bf.*

The proof of the above theorem will be given later. The above observation naturally leads us to consider the case where R is a subring of a ring S, and $A=R\oplus S$ as R-R-module whose multiplication is defined by $(r, x)(s, y)=(rs, xs+ry+xy)$ for any $r, s\in R$ and $x, y\in S$. It is easily seen that A is an associative ring whose identity is $(1, 0)$. We will denote this ring by $R\#S$. Still more denote $(0, x)$ by $\bar{x}$ and $(r, 0)$ by r for each $x\in S$ and $r\in R$, respectively, and put $R=\{(r, 0)|r\in R\}$ and $\bar{S}=\{(0, x)|x\in S\}$. Then R is a subring of A, and $\bar{S}$ is an ideal of A. Let $e=(1, -1)$ and $f=(0, 1)$. Then we have $e^2=e$, $f^2=f$, $ef=0$, and for any $r\in R$ and $x\in S$,

$$(r, x)e=e(r, x)=(r, -r)=re$$
$$(r, x)f=f(r, x)=(0, r+x)=(0, r+x)f$$

Thus we have $Ae=Re$ and $Af=\bar{S}f=\bar{S}$, and see that e and f are orthogonal central idempotents of A with $e+f=1$. Note that f is the identity of $\bar{S}$. Now let ψ be the map of R to Re defined by $\psi(r)=(r, -r)=re$ for each $r\in R$. Since e is a central idempotent of A, ψ is a ring isomorphism, i. e., $R\cong Re=Ae$. Let furthermore $B=R\#R$. Of course B is a subring of A containing e and f. Hence we have $Ae=Be=Re$ and $Bf=Rf=\bar{R}$.

Now we will get our main theorem, by which Theorem 1 can be obtained immediately.

THEOREM 2. *Let R, S, A and B be as above. Then the following three conditions are equivalent :*

(a) *A is a separable extension of R*

(b) *A is a separable extension of B*
(c) *S is a separable extension of R*

PROOF Suppose A is separable over B. Since $A=Ae\oplus Af$ and $B=Be\oplus Bf$ with $Ae=Be(=Re)$, $Af(=A/Re)$ is a separable extension of $Bf(=B/Re)$. But $Af=\bar{S}\cong S$ and $Bf=\bar{R}\cong R$. Hence S is a separable extension of R. Conversely suppose that S is a separable extension of R. Then Af is a separable extension of Bf, since $Af=\bar{S}$ and $Bf=\bar{R}$. But we have $Ae=Be$. Then $A=Ae\oplus Af$ is a separable extension of $B=Be\oplus Bf$. Thus (b) and (c) are equivalent. (a)$\Longrightarrow$(b) is due to Proposition 2.5 [2], while (b)$\Longrightarrow$(a) is an immediate consequence of Proposition 2.5 [2]· and the next proposition

PROPOSITION 1. *$R\#R$ is a separable extension of R*

PROOF. Put $B=R\#R$. We will find an element $\Sigma\alpha_i\otimes\beta_i$ of $B\otimes_R B$ such that $\Sigma\alpha_i\beta_i=(1,0)$ and $\Sigma a\alpha_i\otimes\beta_i=\Sigma\alpha_i\otimes\beta_i a$ for all $a\in B$. Put $\Sigma\alpha_i\otimes\beta_i=1\otimes 1-1\otimes f-f\otimes 1+2f\otimes f$, where $1=(1,0)$ and $f=(0,1)$. It is obvious that $\Sigma\alpha_i\beta_i=1$. Moreover for each $r, y\in R$, we have

$$\begin{aligned}\Sigma(r,y)\alpha_i\otimes\beta_i&=(r,y)\otimes(1,0)-(r,y)\otimes(0,1)-(0,r+y)\otimes(1,0)\\&\quad+2(0,r+y)\otimes(0,1)\\&=(r,-r)\otimes(1,0)+(-r,2r+y)\otimes(0,1),\ \text{and}\\ \Sigma\alpha_i\otimes\beta_i(r,y)&=(1,0)\otimes(r,y)-(1,0)\otimes(0,r+y)\\&\quad-(0,1)\otimes(r,y)+(0,2)\otimes(0,r+y)\\&=(1,-1)\otimes(r,y)-(1,-2)\otimes(0,r+y)\\&=(1,-1)\otimes(r,0)(1,0)+(1,-1)\otimes(y,0)(0,1)\\&\quad-(1,-2)\otimes(r+y,0)(0,1)\\&=(1,-1)(r,0)\otimes(1,0)+(1,-1)(y,0)\otimes(0,1)\\&\quad-(1,-2)(r+y,0)\otimes(0,1)\\&=(r,-r)\otimes(1,0)+(-r,2r+y)\otimes(0,1)=(r,y)\Sigma\alpha_i\otimes\beta_i\end{aligned}$$

Thus B is a separable extension of R.

2. Now let A be a ring and B a subring of A. Throughout this section assume that there exist a ring homomorphism ψ of A to B and a central idempotent e of A such that $\psi(e)=1$, $\psi(b)=b$ and $\psi(x)e=xe$ hold for any $b\in B$ and $x\in A$, respectively. Such ψ and e exist, if A and B satisfy the condition of Lemma 1, but Theorem 2 shows that there exist such ψ and e even if A is not a separable extension of B. Denote $M=\mathrm{Ker}\,\psi$. Then $M=A(1-e)=\{x-\psi(x)|x\in A\}$, $A=B\oplus M$ as B-B-module, and $B\cong Be=Ae$, where the former isomorphism is given by $b\longrightarrow be$, for each $b\in B$. Moreover the converse of the above statements are true, that is, the following

conditions are equivalent

(a) There exist ψ and e which satisfy the above conditions

(b) There exists a central idempotent e such that $Ae=Be$ and $B\cong Be$, via $b\longrightarrow be$, for each $b\in B$

(c) $A=B\oplus M$, where M is an ideal of A generated by a central idempotent of A.

The proof of the above equivalence is very easy, so we will omit it.

LEMMA 2. *Let A, B, ψ, e and M be as above. Assume furthermore that there exist another ring homomorphism ϕ of A to B and a central idempotent f of A which satisfy the same conditions as ψ and e. Denote $N=\mathrm{Ker}\,\phi$. Then we have*

(1) $\psi(f)=\phi(e)$

(2) *If $\psi(f)=1$ (or $\phi(e)=1$), then we have $\psi=\phi$ and $e=f$*

PROOF. (1). Since $\psi(f)e=fe$ and $\psi(e)=\phi(f)=1$, we have $\psi(f)=\psi(e)\psi(f)=\psi(ef)=\psi(\phi(e)f)=\phi(e)\psi(f)=\phi(e\psi(f))=\phi(ef)=\phi(e)\phi(f)=\phi(e)$. (2). If $\psi(f)=1$, we have also $\phi(e)=1$ by (1), and $f=\phi(e)f=ef=e\psi(f)=e$. Then for each $x\in A$, we have $(\psi(x)-\phi(x))e=\psi(x)e-\phi(x)f=ex-xf=0$. This implies that $\psi(x)=\phi(x)$, since $B\cong Be$.

PROPOSITION 2. *With the same notation as Lemma 2, the following conditions are equivalent :*

(a) *$e\in N$ (or equivalently, $f\in M$)*

(b) *$ef=0$*

(c) *$A=M+N$*

(d) *For any non zero central idempotent c of B, there exists an $x\in A$ such that $\psi(x)c\neq\phi(x)c$, that is, ψ and ϕ are strongly distinct in the sense of* [1]. (*See Lemma* 1.2 [1])

PROOF. By (1) Lemma 2, we have $e\in N$ if and only if $f\in M$. Suppose $e\in N$. Then $ef=\phi(e)f=0$. Conversely if $ef=0$, then $0=\psi(ef)=\psi(e\psi(f))=\psi(e)\psi(f)=\psi(f)$, and we have $f\in M$. Thus (a) and (b) are equivalent. Suppose (a) and (b) are satisfied. Then $M=A(1-e)=Af\oplus A(1-e-f)$ and $N=Ae\oplus A(1-e-f)$. Hence we have $M+N=Ae\oplus Af\oplus A(1-e-f)=A$. Next suppose that $A=M+N$. Then we have $1=m+n$ with $m\in M$ and $n\in N$, and $e=em+en$. But $Me=A(1-e)e=0$. Hence we have $e=en\in N$. Finally we will prove the equivalence of (a) and (d). Assume (a), and let c be any non zero central idempotent of B. Then we have $\psi(ce)c=\psi(c)\psi(e)c=c^2=c$ and $\phi(ce)c=\phi(c)\phi(e)c=0$. Thus $\psi(ce)c\neq\phi(ce)c$, and we have (d). Assume (d), and suppose $\phi(e)\neq 0$.

Since $\phi(e)$ is a central idempotent of B, there exists an $x \in A$ such that $\phi(x)\phi(e)=\psi(x)\phi(e)$. But $\phi(x)\phi(e)=\phi(xe)=\phi(\psi(x)e)=\psi(x)\phi(e)$, which is a contradiction. Hence we have $\phi(e)=0$, which means (a).

EXAMPLE. Let $A=R\#(R\#S)$ and $e=(1,(-1,0))$, $f=(0,(1,-1))$. Then we have $e^2=e$, $f^2=f$ and $ef=0$. Moreover, we see that

$$(r,(s,x))e=e(r,(s,x))=(r,(-r,0))=re$$
$$(r,(s,x))f=f(r,(s,x))=(0,(r+s,\quad -r-s))=(r+s)f$$

hold for each $r, s \in R$ and $x \in S$. Thus e and f are central idempotents of A such that $Ae=Re$ and $Af=Rf$. It is obvious that R is isomorphic to both Re and Rf, via $r \rightarrow re$ and $r \rightarrow rf$, respectively, for each $r \in R$. Therefore, we have two decompositions $A=R \oplus M=R \oplus N$ with $M=A(1-e)$ and $N=A(1-f)$, which satisfy the conditions of Proposition 2.

References

[1] S. CHASE, D. HARRISON and A. ROSENBERG, Galois theory and Galois cohomology of commutative rings, Memoirs A. M. S., No. 52 (1965), 1-18.

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

[3] K. SUGANO, On separable extensions over a local ring, Hokkaido Math. J., 11 (1982), 111-115.

[4] K. SUGANO, On automorphisms in separable extensions of rings, Proc. 13th Sympo. Ring Theory, Okayama Lecture Notes (1981), 44-55.

Department of Mathematics
Hokkaido University