ON SEPARABLE POLYNOMIALS OVER A COMMUTATIVE RING

TAKASI NAGAHARA

Throughout this paper B will mean a commutative ring with identity element and all rings will be assumed commutative with identity element, where all ring extensions of B will be assumed with identity element coinciding with the identity element of B. Moreover, X will be an indeterminate, and $B[X]$ will denote the ring of polynomials in X with coefficients in B where $bX=Xb$ $(b\in B)$. In [5], G. J. Janusz introduced the notion of separable polynomials over a commutative ring, and established several properties of separable polynomials.

The main purpose of this note is to prove that for a polynomial $f(X)\in B[X]$, if there is a ring extension of B which contains elements $a_1, \cdots, a_n$ such that $f(X)=(X-a_1)\cdots(X-a_n)$ and $\prod_{i\neq j}(a_i-a_j)$ is inversible in B then $f(X)$ is a separable polynomial over B, that is, $B[X]/(f(X))$ is a separable B-algebra (Theorem). As corollaries to this result, we include also some several results about separable polynomials over B.

In this paper, if $\mathfrak{G}$ is a set of ring automorphisms in a ring A, then $J(\mathfrak{G})$ denotes the fixring of $\mathfrak{G}$ in A, and moreover, for a subset T of A, $\mathfrak{G}|T$ denotes the restriction of $\mathfrak{G}$ to T. As to other notations and terminologies used in this paper, we follow [8]. We now begin with a lemma which plays an essential rôle in the proof of our theorem.

Lemma. *Let A be a ring extension of B and $J(\mathfrak{G})=B$ for a group $\mathfrak{G}$ of ring automorphisms in A. Let a be an element of A such that $\{\sigma(a)|\sigma\in\mathfrak{G}\}$ is a finite set and for $a\neq\sigma(a)$ $(\sigma\in\mathfrak{G})$, $a-\sigma(a)$ is inversible. Set $\{a_1, \cdots, a_n\}=\{\sigma(a)|\sigma\in\mathfrak{G}\}$ where $a_i\neq a_j$ for $i\neq j$, and $f(X)=(X-a_1)\cdots(X-a_n)$. Then*

(1) *$\prod_{i\neq j}(a_i-a_j)$ is inversible in B,*

(2) *$B[a_1, \cdots, a_n]$ is a Galois extension of B with a Galois group $\mathfrak{G}|B[a_1, \cdots, a_n]$,*

(3) *$B[X]/(f(X))\cong B[a_1]$ (as B-algebras),*

(4) *$f(X)$ is a separable polynomial over B.*

Proof. Set $u=\prod_{i\neq j}(a_i-a_j)$. Then $u\in B$ and is inversible in A. Hence we have $u^{-1}\in J(\mathfrak{G})=B$. We now set $T=B[a_1, \cdots, a_n]$ and $\mathfrak{H}=$

$\mathfrak{G}|T$. Since $u^{-1}\prod_{i\neq j}(a_i-\sigma(a_j))=\delta_{1,\sigma}$ $(\sigma\in\mathfrak{H})$, we can find elements $u_1, \cdots, u_m$; $v_1, \cdots, v_m$ of T such that $\sum_i u_i\sigma(v_i)=\delta_{1,\sigma}$ $(\sigma\in\mathfrak{H})$. Hence the assertion (2) follows immediately from [4, Th. 1. 3]. To see (3), we consider a B-algebra homomorphism $\varphi: B[X]\longrightarrow B[a_1]$ mapping $g(X)$ onto $g(a_1)$. Let $h(X)\in\mathrm{Ker}\,\varphi$. Then $h(a_1)=0$ $(i=1, \cdots, n)$. Hence we can find $q_1(X)\in A[X]$ with $h(X)=(X-a_1)q_1(X)$. Since a_2-a_1 is inversible, $q_1(a_2)=0$ so there is a $q_2(X)\in A[X]$ with $q_1(X)=(X-a_2)q_2(X)$. Continuing this way we reach $h(X)=f(X)q_n(X)$. Since $h(X)$, $f(X)\in B[X]$ and $f(X)$ is monic, we have $q_n(X)\in B[X]$. Thus we obtain $\mathrm{Ker}\,\varphi=f(X)B[X]=(f(X))$ which implies $B[X]/(f(X))\cong B[a_1]$. As to (4), we first consider a left T, right $B[a_1]$-module

$$M=Td_1\oplus\cdots\oplus Td_n$$

where $Td_i\cong T$ (as left T-modules) and $d_ig(a_1)=g(a_i)d_i$ $(i=1, \cdots, n,\ g(a_1)\in B[a_1])$. Set $e=d_1+\cdots+d_n$. Then $ea_1{}^i=a_1{}^id_1+\cdots+a_n{}^id_n$ $(i=0, 1, \cdots, n-1)$. Since the determinant of the matrix $\|a_j{}^i\|$ $(0\leqq i\leqq n-1,\ 1\leqq j\leqq n)$ is $\pm\prod_{i<j}(a_i-a_j)$ which is inversible in T, the matrix $\|a_j{}^i\|$ has an inverse in the matrix ring $(T)_n$. Hence the submodule $TeB[a_1]$ of M contains elements $d_1, \cdots, d_n$. This implies $M=TeB[a_1]$. Since $bd_i=d_ib$ for all $b\in B$ $(i=1, \cdots, n)$, we have a left T, right $B[a_1]$-homomorphism $\psi: T\otimes_B B[a_1]\longrightarrow M$ mapping $\sum_i t_i\otimes g_i(a_1)$ onto $\sum_i t_ieg_i(a_1)$. By (3), $B[a_1]$ is a free B-module with a free basis $1, a_1, \cdots, a_1^{n-1}$. This enables us to prove that ψ is an isomorphism. Hence we obtain $T\otimes_B B[a_1]\cong T\oplus\cdots\oplus T$ (as $(T\otimes_B B[a_1])$-modules). Thus $T\otimes_B B[a_1]$ is separable over T so by [1, Prop. 1. 7] (or by [3, Prop. 7. 1, p. 177]), $B[a_1]$ is separable over B. Since $B[X]/(f(X))\cong B[a_1]$, it follows that $f(X)$ is a separable polynomial over B. This completes the proof.

Now, let $R=B[X_1, \cdots, X_n]$ be the ring of polynomials in indeterminates $X_1, \cdots, X_n$ with coefficients in B, and S the ring of symmetric polynomials in R. Then $U=\prod_{i\neq j}(X_i-X_j)$ is an element of S which is not a zero-divisor in R. By $U^{-1}R$ (resp. $U^{-1}S$) we denote the ring of quotients of R (resp. of S), formed with respect to the multiplicatively closed set generated by U. Then $S\subset R\subset U^{-1}R$, $S\subset U^{-1}S\subset U^{-1}R$, and U is inversible in $U^{-1}S$ ([2]). Let $\mathfrak{S}_n$ be the symmetric group on letters $1, \cdots, n$. Then, for every element σ of $\mathfrak{S}_n$, we have a ring automorphism $\sigma^*: U^{-1}R\longrightarrow U^{-1}R$ mapping $g(X_1, \cdots, X_n)$ onto $g(X_{\sigma(1)}, \cdots, X_{\sigma(n)})$. By $\mathfrak{S}_n{}^*$ we denote the group of the automorphisms σ^* $(\sigma\in S_n)$. Then we obtain $J(\mathfrak{S}_n{}^*)=U^{-1}S$. Moreover, it is obvious that $\{\sigma^*(X_1)\,|\,\sigma^*\in\mathfrak{S}_n{}^*\}=$

$\{X_1, \cdots, X_n\}$ and for $i \neq j$, $X_i - X_j$ is inversible in $U^{-1}R$. Hence if we set $F(X)=(X-X_1)\cdots(X-X_n)$ where X, $X_1, \cdots, X_n$ are independent, then, by Lemma, we obtain the following

Corollary 1. *$U^{-1}R$ is a Galois extension of $U^{-1}S$ with a Galois group $\mathfrak{S}_n^*$, $U^{-1}S[X]/(F(X)) \cong U^{-1}S[X_1]$ (as $U^{-1}S$-algebras), and $F(X)$ is a separable polynomial over $U^{-1}S$.*

We now have enough information to prove the following

Theorem. *Let $f(X) \in B[X]$. If there is a ring extension of B which contains elements $a_1, \cdots, a_n$ such that $f(X)=(X-a_1)\cdots(X-a_n)$ and $\prod_{i \neq j}(a_i - a_j)$ is inversible in B then $f(X)$ is a separable polynomial over B.*

Proof. We consider the polynomial ring $U^{-1}R[X]$ where X, $X_1, \cdots, X_n$ are independent. Then we have a ring homomorphism $\varphi: U^{-1}R[X] \longrightarrow B[a_1, \cdots, a_n][X]$ mapping $\sum_i g_i(X_1, \cdots, X_n)X^i$ onto $\sum_i g_i(a_1, \cdots, a_n)X^i$. By the fundamental theorem on symmetric polynomials ([9, p. 90]), it follows that $\varphi(U^{-1}S)=B$. This implies $\varphi(U^{-1}S[X])=B[X]$, and $\varphi(F(X)U^{-1}S[X])=f(X)B[X]$ where $F(X)=(X-X_1)\cdots(X-X_n)$. Hence φ induces a ring homomorphism $\bar{\varphi}: U^{-1}S[X]/(F(X)) \longrightarrow B[X]/(f(X))$. By Coro. 1, $U^{-1}S[X]/(F(X))$ is separable over $U^{-1}S$. It is obvious that $\bar{\varphi}(U^{-1}S)=B$. Then, by the following remark, $B[X]/(f(X))$ is a separable extension of B which implies that $f(X)$ is a separable polynomial over B.

Remark 1. Let a ring A be a separable extension of a ring C and $\varphi: A \longrightarrow A'$ a ring epimorphism. Set $C'=\varphi(C)$. Then A' is a separable extension of C'. The proof is as follows: The C'-algebra A' is turned into a C-algebra by the homomorphism $\varphi \mid C: C \longrightarrow C'$. Then φ induces a C-algebra homomorphism $A \longrightarrow A'$. Hence by [1, Prop. 1.4], the C-algebra A' is a separable algebra, that is, A' is a projective $(A' \otimes_C A')$-module, the operation being given by $(x \otimes y)z=xzy$ $(x, y, z \in A')$. Since $A' \otimes_C A' \cong A' \otimes_{C'} A'$ (as rings), A' is a projective $(A' \otimes_{C'} A')$-module. Therefore A' is a separable C'-algebra.

Now, as a direct consequence of Theorem, we obtain the following

Corollary 2. *Let $f(X) \in B[X]$. If there is a ring extension A of B which contains elements $a_1, \cdots, a_n$ such that $f(X)=(X-a_1)\cdots(X-a_n)$ and $u=\prod_{i \neq j}(a_i - a_j)$ is not a zero-divisor in A then $f(X)$ is a separable polynomial over $u^{-1}B$ (the ring of quotients of B, formed with respect*

to the multiplicatively closed set generated by u).

In Theorem, $B[a_1, \cdots, a_n]$ is a homomorphic image of a strongly separable B-algebra $B[X_1]/(f(X_1))\otimes_B \cdots \otimes B[X_n]/(f(X_n))$ where the X_i are indeterminates ([1, Prop. 1.5]). By a similar way, we have the following

Corollary 3. *Let A be a ring extension of B. Let $f(X)\in B[X]$, and suppose A contains elements $a_1, \cdots, a_n$ such that $f(X)=(X-a_1)\cdots(X-a_n)$ and $\prod_{i\neq j}(a_i-a_j)$ is inversible in B. If $a_1^*, \cdots, a_m^*$ $(m<\infty)$ are roots of $f(X)$ in A then $B[a_1^*, \cdots, a_m^*]$ is a homomorphic image of a strongly separable B-algebra.*

As an application of Theorem, we shall prove the following

Corollary 4. *Let B be an algebra over a prime field $GF(p)$ $(p\neq 0)$. Then, for every element b of B, X^p-X+b is a separable polynomial over B.*

Proof. Let $f(X)=X^p-X+b\in B[X]$ $(b\in B)$, and Y an indeterminate where X, Y are independent. We now consider the B-algebra $B[Y]/(f(Y))=B[\overline{Y}]$ where $\overline{Y}$ is the residue class of Y modulo $(f(X))$. Then $B[\overline{Y}]$ is a ring extension of B, and elements $\overline{Y}$, $\overline{Y}+1, \cdots, \overline{Y}+p-1$ are roots of $f(X)$. Since $(\overline{Y}+i)-(\overline{Y}+j)$ $(i\neq j)$ is inversible in B, it follows that $f(X)=(X-\overline{Y})(X-(\overline{Y}+1))\cdots(X-(\overline{Y}+p-1))$. Hence by Theorem, $f(X)$ is a separable polynomial over B.

As to separable polynomials over a ring B without proper idempotents, we shall present some corollaries to Theorem. If $f(X)$ is a separable polynomial over a ring B without proper idempotents then, by [5, Th. 2.2] there is a strongly separable B-algebra without proper idempotents which contains elements $a_1, \cdots, a_n$ such that $f(X)=(X-a_1)\cdots(X-a_n)$ and $\prod_{i\neq j}(a_i-a_j)$ is inversible in B. Combining this fact with Theorem, we obtain the following

Corollary 5. *Let B be a ring without proper idempotents, and $f(X)\in B[X]$. Then, $f(X)$ is a separable polynomial over B if and only if there is a ring extension of B which contains elements $a_1, \cdots, a_n$ such that $f(X)=(X-a_1)\cdots(X-a_n)$ and $\prod_{i\neq j}(a_i-a_j)$ is inversible in B.*

Remark 2. It is a result of G. J. Janusz that if A is a separable B-algebra without proper idempotents and $f(X)$ is a separable polynomial

of degree n over B then $f(X)$ cannot have more than n roots in A; and moreover, for distinct roots a, b of $f(X)$ in A, $a-b$ is inversible in A ([5, Lemma 2. 1]). However, in the result, the assumption of separability of A over B may be omitted. For, if $a_1, \cdots, a_m$ $(m<\infty)$ are distinct roots of $f(X)$ in A then $B[a_1, \cdots, a_m]$ is a separable B-algebra without proper idempotents. Applying Janusz' result to $B[a_1, \cdots, a_m]$, we have $m \leqq n$ and for $i \neq j$, $a_i - a_j$ is inversible in A.

Now, we shall prove the following

Corollary 6. *Let A be a ring without proper idempotents which is a ring extension of B. Let $f(X) \in B[X]$, and suppose A contains elements $a_1, \cdots, a_n$ such that $f(X)=(X-a_1)\cdots(X-a_n)$ and $\prod_{i \neq j}(a_i-a_j)$ is inversible in B. Then, every root of $f(X)$ in A coincides with one of the a_i. Moreover, for $T=B[a_1, \cdots, a_n]$, the following conditions are equivalent.*

(a) *$J(\mathfrak{H})=B$ for a group $\mathfrak{H}$ of ring automorpisms in T.*

(b) *T is Galois over B.*

(c) *T is projective over B.*

Proof. The first assertion follows immediately from Theorem and Remark 2. Since T is finitely generated, and separable over B, it follows from [7, Th. 1] and [4, Th. 1. 3] that (a) implies (b) and (b) implies (c). We now assume (c). Then by [5, Th. 1. 1], T is imbedded in a Galois extension of B without proper idempotents. The Galois group will be denoted by $\mathfrak{G}$. Then for every a_i, we have $f(\sigma(a_i))=0$ $(\sigma \in \mathfrak{G})$; hence $\sigma(a_i)$ coincides with one of the a_j. Thus we obtain $\sigma(T)=T$ $(\sigma \in \mathfrak{G})$. This implies (a).

Remark 3. Let B, $a_1, \cdots, a_n$ be as in the preceding corollary. If B is a separably closed domain then $B[a_1, \cdots, a_n]$ is projective over B; hence Galois over B ([8]). However, in general, $B[a_1, \cdots, a_n]$ is not always Galois over B. To see this, we shall present an example. We consider a ring $B=Z^*+Z^*\sqrt{5}$ where Z^* is the ring of rational numbers $m/5^n$ (the m, n are rational integers). We set $f(X)=X^2-X-1$. Then $f(X)=(X-a_1)(X-a_2)$ where $a_1=(1+\sqrt{5})/2$, $a_2=(1-\sqrt{5})/2$. Clearly $(a_1-a_2)(a_2-a_1)=-(a_1-a_2)^2=-5$ and is inversible in B. Hence $f(X)$ is a separable polynomial over B. Moreover, from $a_1 \notin B$, $f(X)$ is irreducible in $B[X]$, and so, $B[a_1]$ is a homomorphic image of a strongly separable B-algebra without proper idempotents. However, since $\sqrt{5} \in$

$B \subset B[a_1] = B[a_1, a_2]$ and the quotient field of $B[a_1]$ is a field generated by $\sqrt{5}$ over the field of rational numbers, it follows that $B[a_1]$ is not Galois over B and hence not projective over B.

The following corollary contains the result of [5, Lemma 2. 7].

Corollary 7. *Let A be a ring without proper idempotents which is a ring extension of B, and $J(\mathfrak{G})=B$ for a group $\mathfrak{G}$ of ring automorphisms in A. For an element a of A, the following conditions are equivalent.*

(a) *$\{\sigma(a)|\sigma\in\mathfrak{G}\}$ is a finite set, and for $a\neq\sigma(a)$ $(\sigma\in\mathfrak{G})$, $a-\sigma(a)$ is inversible.*

(b) *a is a root of a separable polynomial over B.*

(c) *$B[a]$ is finitely generated, and separable over B.*

Proof. Assume (a). If we set $\{a_1, \cdots, a_n\}=\{\sigma(a)|\sigma\in\mathfrak{G}\}$ ($a_i\neq a_j$ for $i\neq j$) and $f(X)=(X-a_1)\cdots(X-a_n)$ then $f(a)=0$ and by Lemma $f(X)$ is a separable polynomial over B. Thus we obtain (b). It is obvious that (b) implies (c). Assume (c). Then by [7, Th. 1], $\{\sigma(a)|\sigma\in\mathfrak{G}\}$ is a finite set and the B-subalgebra of A generated by $\{\sigma(a)|\sigma\in\mathfrak{G}\}$ is Galois over B; hence as in the proof of [5, Lemma 2. 7], it follows that for $a\neq\sigma(a)$ $(\sigma\in\mathfrak{G})$, $a-\sigma(a)$ is inversible.

Remark 4. In the proof of the preceding corollary, $f(X)$ is an irreducible polynomial in $B[X]$, $B[a]\cong B[X]/(f(X))$ and is a free B-module (Lemma).

Recently, K. Kishimoto presented a theory of cyclic extensions of rings ([6]). Lately, one will have a chance to see that Coro. 4 plays an important rôle in studying cyclic extensions of commutative rings.

REFERENCES

[1] M. AUSLANDER and O. GOLDMAN: The Brauer group of a commutative rings, Trans. Amer. Math. Soc. 97 (1960), 367—409.

[2] N. BOURBAKI: Algèbre commutative, Chapitres I-II, Actualités Sci. Ind. No. 1290, Herman, Paris, 1962.

[3] H. CARTAN and S. EILENBERG: Homological algebra, Princeton, 1956.

[4] S. U. CHASE, D. K. HARRISON and A. ROSENBERG: Galois theory and cohomology of commutative rings, Mem. Amer. Math. Soc. No. 52 (1965).

[5] G. J. JANUSZ: Separable algebras over commutative rings, Trans. Amer. Math. Soc. 122 (1966), 461—479.

[6] K. KISHIMOTO: On abelian extensions of rings I, Math. J. of Okayama Univ., 14 (1970), 159—174.
[7] T. NAGAHARA: A note on Galois theory of commutative rings, Prcc. Amer. Math. Soc. 18 (1967), 334—340.
[8] T. NAGAHARA: On separable extensions of domains, Math. J. of Okayama Univ., 14 (1970), 59—65.
[9] B. L. VAN DER WAERDEN: Mcderne Algebra I, Springer, 1950.

DEPARTMENT OF METHEMATICS
OKAYAMA UNIVERSITY

(Received July 1, 1970)