230. *Characterization of Separable Polynomials over a Commutative Ring*

By Takasi NAGAHARA
Department of Mathematics, Okayama University, Okayama

(Comm. by Kenjiro SHODA, M. J. A., Dec. 12, 1970)

Throughout this paper B will mean a commutative ring with an identity element, and all ring extensions of B will be assumed commutative with identity element coinciding with the identity element of B. Moreover, X will be an indeterminate, and by $B[X]$ denote the ring of polynomials in X with coefficients in B where $bX=Xb$ ($b \in B$). In [4], G. J. Janusz introduced the notion of separable polynomials over a commutative ring which is as follows: A polynomial $f(X) \in B[X]$ is called separable if it is a monic polynomial and if $B[X]/(f(X))$ is a separable B-algebra.[1] In [4, Theorem 2.2], it has been shown that under the assumption B has no proper idempotents, for a polynomial $f(X) \in B[X]$, $f(X)$ is separable if and only if there is a strongly separable B-algebra[2] A with no proper idempotents which contains elements $a_1, a_2, \cdots, a_n$ such that $f(X)=(X-a_1)(X-a_2)\cdots(X-a_n)$ and for $i \neq j$, $a_i - a_j$ is inversible in A. In [3], B. L. Elkins proved that if a polynomial $f(X) \in B[X]$ is separable then $f'(X+(f(X)))$ is an inversible element of $B[X]/(f(X))$, where $f'(X)$ is the derivative of $f(X)$. Recently, in [5], the present author proved 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 separable. The main purpose of this paper is to prove the following theorem.

Theorem 1. *Let $f(X) \in B[X]$. Then the following conditions are equivalent.*

(a) *$f(X)$ is separable.*

(b) *$f(X)$ is monic and $f'(X+(f(X)))$ is an inversible element of $B[X]/(f(X))$.*

(c) *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.*

---

1) A commutative B-algebra S is called separable if it is a projective ($S \otimes_B S$)-module (cf. [1, p. 369]).

2) A B-algebra S is called strongly separable if it is finitely generated. projective, and separable over B.

The theorem follows from the results of [3, Proposition 1.8], [5, Theorem], and the following theorem.

Theorem 2. *Let $f(X)\in B[X]$. If $f(X)$ is monic and $f'(X+(f(X)))$ is an inversible element of $B[X]/(f(X))$ then there is a Galois extension*[3] *A of B with a Galois group $\mathcal{G}$ which contains elements $x_1,\cdots,x_n$ such that*

(1) *$f(X)=(X-x_1)\cdots(X-x_n)$ and $\prod_{i\neq j}(x_i-x_j)$ is inversible in B;*

(2) *$A=B[x_1,\cdots,x_n]$ and is a free B-module of rank $n!$;*

(3) *for every permutation σ on letters $1,\cdots,n$, A has an automorphism σ^* mapping $g(x_1,\cdots,x_n)$ onto $g(x_{\sigma(1)},\cdots,x_{\sigma(n)})$;*

(4) *$\mathcal{G}$ is a group of order $n!$ which consists of the σ^*;*

(5) *if A' is a ring extension of B which contains elements $a_1,\cdots,a_n$ such that $A'=B[a_1,\cdots,a_n]$ and $f(X)=(X-a_1)\cdots(X-a_n)$ then A is B-algebra homomorphic to A' under the map $g(x_1,\cdots,x_n)\to g(a_1,\cdots,a_n)$.*

Proof. In case $\deg f(X)\leqq 1$, the theorem is trivial. Hence let $\deg f(X)>1$. Let X_1 be an indeterminate, and set $x_1=X_1+(f(X_1))\in B[X_1]/(f(X_1))$. Then $f(X)=(X-x_1)f_2(X)$ where $f_2(X)\in B[x_1][X]$. Clearly $f_2(X)$ is a monic polynomial. If $\deg f_2(X)>1$ then there is a ring extension $B[x_1][x_2]$ of $B[x_1]$ such that $B[x_1][x_2]\cong B[x_1][X]/(f_2(X))$ $(x_2\leftrightarrow X+(f_2(X)))$ and $f_2(X)=(X-x_2)f_3(X)$ where $f_3(X)\in B[x_1,x_2][X]$. Continuing this way, there is a ring extension A of B which contains elements $x_1,\cdots,x_{n-1},x_n$ such that $A=B[x_1,\cdots,x_{n-1}]=B[x_1,\cdots,x_{n-1},x_n]$, $f(X)=(X-x_1)f_2(X)=\cdots=(X-x_1)\cdots(X-x_m)f_{m+1}(X)=(X-x_1)\cdots(X-x_n)$, and $B[x_1,\cdots,x_m][x_{m+1}]\cong B[x_1,\cdots,x_m][X]/(f_{m+1}(X))$ $(x_{m+1}\leftrightarrow X+(f_{m+1}(X)))$ where $0\leqq m<n$, and $f_1(X)=f(X)$. Clearly A is a free B-module of rank $n!$. Now, let A' be a ring extension of B which contains elements $a_1,\cdots,a_n$ such that $A'=B[a_1,\cdots,a_n]$ and $f(X)=(X-a_1)\cdots(X-a_n)$. Set $A_m=B[x_1,\cdots,x_m]$, $A'_m=B[a_1,\cdots,a_m]$, and $A_0=A'_0=B$. For a number $m<n$, assume that A_m is homomorphic to A'_m under the map $\varphi: g(x_1,\cdots,x_m)\to g(a_1,\cdots,a_m)$. Then $A_m[X]$ is homomorphic to $A'_m[X]$ under the map $g(X)=\sum_i g_i(x_1,\cdots,x_m)X^i\to g^\varphi(X)=\sum_i g_i(a_1,\cdots,a_m)X^i$. Since $f(X)=(X-x_1)\cdots(X-x_m)f_{m+1}(X)$, it follows that $(X-a_1)\cdots(X-a_m)f^\varphi_{m+1}(X)=f^\varphi(X)=f(X)=(X-a_1)\cdots(X-a_m)\{(X-a_{m+1})\cdots(X-a_n)\}$ $(\in A'[X])$, so that $f^\varphi_{m+1}(X)=(X-a_{m+1})\cdots(X-a_n)$. Then $f^\varphi_{m+1}(a_{m+1})=0$. Hence we have homomorphisms $A_{m+1}\to A_m[X]/(f_{m+1}(X))\to A'_m[X]/(f^\varphi_{m+1}(X))\to A'_m[a_{m+1}]=A'_{m+1}$ which are defined by maps $g(x_1,\cdots,x_m,x_{m+1})=h(x_{m+1})\to h(X)+(f_{m+1}(X))\to h^\varphi(X)+(f^\varphi_{m+1}(X))\to h^\varphi(a_{m+1})=g(a_1,\cdots,a_m,a_{m+1})$. From this argument, it follows that $A=A_{n-1}$ is B-algebra homomorphic to $A'=A'_{n-1}$ under the map $g(x_1,\cdots,x_n)\to g(a_1,\cdots,a_n)$. Furthermore, this implies that for every permutation σ on letters $1,\cdots,n$, A has an automorphism σ^*

3) See [2, Definition 1.4 (p. 20)].

mapping $g(x_1, \cdots, x_n)$ onto $g(x_{\sigma(1)}, \cdots, x_{\sigma(n)})$. Let $\mathcal{G}$ be the group consisting of the σ^*. Since $f(X)=(X-x_1)f_2(X)$, we have $f'(X)=f_2(X)+(X-x_1)f'(X)$, and $f'(x_1)=f_2(x_1)=(x_1-x_2)\cdots(x_1-x_n)$ which is inversible in A by our assumption. Hence for every $j\neq 1$, x_1-x_j is inversible in A. If $n>2$ then for every $i\neq j$ there exists an element σ^* in $\mathcal{G}$ such that $\sigma^*(x_1)=x_i$ and $\sigma^*(x_j)=x_j$; hence $\sigma^*(x_1-x_j)=x_i-x_j$ and is inversible in A. Now, let B' be the fixring of $\mathcal{G}$ in A. For a non-zero $n-m<n$, assume that $B'\subset A_{n-m}$ $(\subset A=A_{n-1})$. Then for $b'\in B'$, we may write $b'=\sum_{s=0}^{m} c_s(x_{n-m})^s$ where $c_0, \cdots, c_m \in A_{n-m-1}$. If $n-m\leqq t\leqq n$ then there exists an element σ^* in $\mathcal{G}$ such that $\sigma^*(x_{n-m})=x_t$ and $\sigma^*(x_i)=x_i$ for all $i<n-m$. Hence we have $\sum_{s=1}^{m} c_s(x_t)^s+c_0-b'=0$ $(n-m\leqq t\leqq n)$. The determinant of the matrix $\|(x_t)^s\|$ $(0\leqq s\leqq m,$ $n-m\leqq t\leqq n)$ is $\pm\prod_{n-m\leqq t<u\leqq n}(x_t-x_u)$ which is an inversible element of A; hence the matrix $\|(x_t)^s\|$ is inversible in the ring of $(m+1)$-square matrices with elements in A. Then we see that $c_0-b'=0$, that is, $c_0=b'$. Thus we obtain $B'\subset A_{n-m-1}$. From this argument, it follows that $B'=A_0=B$. Therefore, by [5, Lemma], A is a Galois extension of B with a Galois group $\mathcal{G}$, and $\prod_{i\neq j}(x_i-x_j)$ is an inversible element of B. This completes the proof.

The following corollary is a direct consequence of Theorem 1, Theorem 2 and its proof.

Corollary 1. *Let $f(X)$ be a monic polynomial in $B[X]$. Then there is a ring extension of B which contains elements $a_1, \cdots, a_n$ such that $f(X)=(X-a_1)\cdots(X-a_n)$. In this case, $f(X)$ is separable if and only if $\prod_{i\neq j}(a_i-a_j)$ is inversible in B.*

The following corollary contains the result of [3, Corollary 2.4].

Corollary 2. *Let $X^n-b\in B[X]$ and $n>1$. Then, X^n-b is separable if and only if $n\cdot 1$ and b are inversible elements of B.*

Proof. We set $B[x]=B[X]/(X^n-b)$ where $x=X+(X^n-b)$. By Theorem 1, X^n-b is separable if and only if nx^{n-1} is inversible in $B[x]$. Noting $x^n=b$, nx^{n-1} is inversible in $B[x]$ if and only if $n\cdot 1$ and b are inversible in $B[x]$. Since $B[x]$ is a free B-module of finite rank, $n\cdot 1$ and b are inversible in $B[x]$ if and only if these are inversible in B.

The following corollary contains the result of [5, Corollary 4].

Corollary 3. *Let B be an algebra over a prime field $GF(p)$ $(p\neq 0)$. Let $f(X)=X^{pm}+b_{m-1}X^{p(m-1)}+\cdots+b_1X^p+bX^n+c\in B[X]$ where $m\geqq 1$ and $p>n$. Then*

(1) *if $n=0$ then $f(X)$ is not separable.*

(2) *In case $n=1$, $f(X)$ is separable if and only if b is inversible in B.*

(3) *In case $n>1$, $f(X)$ is separable if and only if b and c are inversible in B.*

Proof. (1) and (2) are direct consequences of Theorem 1. Let $n>1$ and set $B[x]=B[X]/(f(X))$ where $x=X+(f(X))$. By Theorem 1, $f(X)$ is separable if and only if $f'(x)=nbx^{n-1}$ is inversible in $B[x]$, which is equivalent to that b and x are inversible in $B[x]$. Let x be inversible in $B[x]$. Then we may write $x^{-1}=c_{pm-1}x^{pm-1}+\cdots+c_1x+c_0$. From $f(x)=0$, we have $0=c_{pm-1}f(x)-(xx^{-1}-1)=(-c_{pm-2})\cdot x^{pm-1}+\cdots+(-c_0)x+c_{pm-1}c+1$. Since $\{x^{pm-1}, \cdots, x, 1\}$ is a free B-basis of $B[x]$, it follows that $c_{pm-1}c+1=0$, and so, c is inversible in $B[x]$. Conversely, if c is inversible in $B[x]$ then, from $f(x)=0$, x is inversible in $B[x]$. Hence $f(X)$ is separable if and only if b and c are inversible in $B[x]$ which is equivalent to that b and c are inversible in B.

Remark. As another characterization of the separable polynomials over B, we have the following information which contains the result of [4, Theorem 2.2].

For a monic polynomial $f(X)$ in $B[X]$, the following conditions are equivalent.

(a) $f(X)$ is separable.

(b) There is a Galois 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.

(c) For each maximal ideal M of B, $f(X)$ is separable when viewed as a polynomial over the local ring B_M.

(d) For each maximal ideal M of B, the polynomial obtained from $f(X)$ by reducing the coefficients modulo M has no repeated roots in an algebraic closure of B/M.

(e) Let t denote the trace map of the free B-module $B[X]/(f(X))$ and let x denote the coset of X modulo $(f(X))$. Then the determinant of the matrix $\|t(x^ix^j)\|$ $(0\leqq i, j<\deg f(X))$ is an inversible element of B.

The equivalence of (a) and (b) is a direct consequence of Theorem 1 and Theorem 2. The others will be proved later in a paper: On separable polynomials over a commutative ring II, Math. J. of Okayama Univ., **15** (to appear).

References

[1] M. Auslander and O. Goldman: The Brauer group of a commutative ring. Trans. Amer. Math. Soc., **97**, 367–409 (1960).

[2] S. U. Chase, D. K. Harrison, and A. Rosenberg: Galois theory and Galois cohomology of commutative rings. Mem. Amer. Math. Soc., No. 52, 15–33 (1965).

[3] B. L. Elkins: Characterization of separable ideals. Pacific J. Math., **34**,

45–49 (1970).
[4] G. J. Janusz: Separable algebras over commutative rings. Trans. Amer. Math. Soc., **122**, 461–479 (1966).
[5] T. Nagahara: On separable polynomials over a commutative ring. Math. J. Okayama Univ., **14** (to appear).