

A NOTE ON SEPARABLE POLYNOMIALS IN SKEW POLYNOMIAL RINGS OF DERIVATION TYPE

SHÛICHI IKEHATA

Throughout the present note, K will represent a ring with 1, Z the center of K , and D a derivation of K . Let $R = K[X; D]$ be the skew polynomial ring, where the multiplication is given by $cX = Xc + D(c)$ ($c \in K$). Then the inner derivation $\tilde{D}$ of R effected by X is an extension of D and $\tilde{D}(\sum_i X^i a_i) = [\sum_i X^i a_i, X] = \sum_i X^i D(a_i)$. A monic polynomial f in R with $Rf = fR$ is called a *separable polynomial*, if R/Rf is a separable extension of K . The purpose of this note is to prove the following theorem which partially generalizes a theorem of T. Nagahara [2, Theorem 3.4].

Theorem. *Let p be a prime number, and assume that K is of characteristic p and $D(Z) = 0$. Then a monic polynomial $f = X^n - Xa - b$ in R with $Rf = fR$ is separable if and only if a is invertible in K .*

Proof. As is easily verified, the hypothesis $Rf = fR$ is equivalent to the following:

$$D(a) = D(b) = 0, \quad a \in Z \quad \text{and} \quad D^p(c) - D(c)a = [c, b] \quad (c \in K).$$

Assume that f is separable. Then, by [1, Theorem 3.2], there exists a polynomial $y = X^{p-1}d_{p-1} + \cdots + Xd_1 + d_0$ in R such that $\tilde{D}^{p-1}(y) - ya = 1$ and $[c, y] = 0$ for all $c \in K$. Obviously, $[c, y] = 0$ ($c \in K$) implies $d_{p-1} \in Z$, and therefore $D(d_{p-1}) = 0$. By induction, we shall prove that

$$(1) \quad [c, \tilde{D}^{i-1}(y)] = 0 \quad \text{for all} \quad c \in K$$

and

$$(2) \quad D^i(d_{p-i}) = 0 \quad (i = 1, \dots, p-1).$$

Assume that (1) and (2) have been proved for $i = 1, \dots, k$ ($k < p-1$). Since $0 = D([c, \tilde{D}^{k-1}(y)]) = [D(c), \tilde{D}^{k-1}(y)] + [c, \tilde{D}^k(y)] = [c, \tilde{D}^k(y)] = [c, X^{p-k-1}D^k(d_{p-k-1}) + \cdots + XD^k(d_1) + D^k(d_0)]$, it follows $D^k(d_{p-k-1}) \in Z$, and therefore $D^{k+1}(d_{p-k-1}) = 0$, completing the induction. In view of (1) and (2), we readily see that

$$0 = [c, \tilde{D}^{p-2}(y)] = [c, XD^{p-2}(d_1) + D^{p-2}(d_0)] \quad (c \in K),$$

$$1 = \tilde{D}^{p-1}(y) - ya = D^{p-1}(d_0) - X^{p-1}d_{p-1}a - \cdots - Xd_1a - d_0a.$$

Hence, comparing the coefficients in both sides, we obtain

$$(3) \quad D(c)D^{p-2}(d_1) + [c, D^{p-2}(d_0)] = 0 \quad (c \in K).$$

$$(4) \quad ad_1 (= d_1 a) = 0.$$

$$(5) \quad D^{p-1}(d_0) - d_0a = 1.$$

Specializing $c = D^{p-2}(d_0)$ in (3), we have

$$(3)' \quad D^{p-1}(d_0) D^{p-2}(d_1) = 0.$$

Now, by (3), (5), (3)' and (4), it follows that

$$\begin{aligned} [c, D^{p-2}(d_0)] &= -D(c)D^{p-2}(d_1) \\ &= -D(c)\{D^{p-1}(d_0) - d_0a\}D^{p-2}(d_1) \\ &= -D(c)\{D^{p-1}(d_0)D^{p-2}(d_1) - d_0D^{p-2}(ad_1)\} \\ &= 0. \end{aligned}$$

Hence, $D^{p-2}(d_0)$ is in Z , and therefore by (5), $1 = D^{p-1}(d_0) - d_0a = (-d_0)a$.

Conversely, assume that a is invertible in K . Since a is invertible in Z , there holds $D(a^{-1}) = 0$. Putting $y = -a^{-1}$, we have $\tilde{D}^{p-1}(y) - ya = 1$ and $[c, y] = 0$ for all $c \in K$. Thus, f is separable by [1, Theorem 3.2].

Remark. Under the hypothesis of our theorem, $f = X^p - X - b$ is seen to be Galois provided $fR = Rf$. In fact, $\bar{R} = R/fR$ has an automorphism $\bar{\sigma}$ of order p such that $\bar{\sigma}(\bar{X}) = \bar{X} + 1$ and $\bar{R}^{\langle \bar{\sigma} \rangle} = K$. Then the expansions of $\prod_{j=1}^{p-1} \{j^{-1}(\bar{X} + j) - j^{-1}(\bar{X})\} = 1$ and $\prod_{j=1}^{p-1} \{j^{-1}(\bar{X} + j) - j^{-1}(\bar{X} + k)\} = 0$ ($k = 1, \dots, p-1$) enable us to see the existence of a $\langle \bar{\sigma} \rangle$ -Galois coordinate system of $\bar{R}/K$.

REFERENCES

- [1] Y. MIYASHITA: On a skew polynomial ring, J. Math. Soc. Japan **31** (1979), 317–330.
- [2] T. NAGAHARA: On separable polynomials of degree 2 in skew polynomial rings, Math. J. Okayama Univ. **19** (1976), 65–95.

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY

(Received September 20, 1979)