149. *On a Theorem of F. DeMeyer*

By Takasi NAGAHARA
Department of Mathematics, Okayama University

(Comm. by Kenjiro SHODA, M. J. A., Nov. 12, 1973)

Throughout this paper, all rings will be assumed commutative with identity element, and given any ring $S, B(S)$ will mean the Boolean algebra consisting of all idempotents of S. Moreover, R will mean a ring, and all ring extensions of R will be assumed with identity element 1, the identity element of R. Further, $R[X]$ will mean the ring of polynomials in an indeterminate X with coefficients in R, and all monic polynomials will be assumed to be of degree $\geqq 1$. Given a monic polynomial f in $R[X]$, a ring extension S of R is called a splitting ring of f (over R) if $S=R[\alpha_1, \cdots, \alpha_n]$ and $f=(X-\alpha_1)\cdots(X-\alpha_n)$ (cf. [4, Definition]). A polynomial $f \in R[X]$ is called separable if f is monic and $R[X]/(f)$ is a separable R-algebra. In [3], F. DeMeyer introduced the notion of uniform separable polynomials. By [5, Theorem 3.3], it is seen that a separable polynomial $f \in B[X]$ is uniform if and only if f has a splitting ring S which is projective over R and with $B(S)=B(R)$.

In [3], F. DeMeyer stated the following theorem:

Let R be a regular ring (in the sense of Von Neumann) and let S be a finite projective separable extension of R with $B(S)=B(R)$. Then there is an element $\alpha \in S$ and a separable polynomial $p(X) \in R[X]$ so that $S=R[\alpha]$ and α is a root of $p(X)$. Moreover, if S is a weakly Galois extension of R then the polynomial $p(X)$ can be chosen to be uniform ([3, Theorem 2.7]).

However, the proof contains an error which is the statement "Applying the usual compactness argument and decomposing R by a finite number of orthogonal idempotents e as above gives the first assertion of the theorem". Indeed, applying the usual compactness argument, we obtain a polynomial $p(X)$ of $R[X]$ so that $R[X]/(p(X))$ (R-separable)$\sim S$; but if S has not $\mathrm{rank}_R S$ (in the sense of [1, Definition 2.5.2]) then $p(X)$ is not monic, and so, is not separable over R.

The purpose of this note is to improve on the result of the above theorem. First, we shall prove the following lemma which is useful in our study.

Lemma. *Let K be a field, L a field extension of K which is finite dimensional separable, and $L=K[\alpha]$. Let $n \geqq \mathrm{rank}_K L$ be an integer. Then, there exists a monic polynomial $g(X)$ in $K[X]$ of degree n so that $g(\alpha)=0$ and $g(X)$ has no multiple roots (whence $g(X)$ is separable over*

K by [4, Theorem 2.3]). *If L is Galois over K and if $n=\operatorname{rank}_K L$ or K is an infinite field then $g(X)$ can be chosen to be $L=$the splitting field of $g(X)$.*

Proof. Let $m=\operatorname{rank}_K L$. Then there exists an irreducible monic polynomial $f(X)$ in $K[X]$ of degree m so that α is a root of $f(X)$. If $n=m$ then the assertion is obvious. Hence we assume that $n>m$. We shall here distinguish two cases:

Case 1. K has at least n elements. In this case, we can find $n-m$ elements $a_{m+1},\cdots,a_n$ in K so that $\alpha, a_{m+1},\cdots,a_n$ are distinct. If we set $g(X)=f(X)(X-a_{m+1})\cdots(X-a_n)$ then $g(X)$ is a monic polynomial in $K[X]$ of degree n so that $g(\alpha)=0$ and $g(X)$ has no multiple roots. If L is Galois over K then L is the splitting field of $f(X)$, and so, L is the splitting field of $g(X)$.

Case 2. K has at most n elements. In this case, K is a finite field. Hence we may write $K=\mathrm{GF}(p^k)$ where p is the characteristic of K. For any positive integer t, $\mathrm{GF}(p^{kt})$ is a separable extension of $\mathrm{GF}(p^k)$ of rank t, and whence there exists a monic polynomial $q(X)$ in $K[X]$ of degree t which is irreducible over K; the set of such polynomials will be denoted by $K[X]_{\mathrm{irr}.t}$. Now, if $n=2$ and $m=1$ then for $a\neq\alpha\in K$, set $g(X)=f(X)(X-a)$ $(=(X-\alpha)(X-a))$. If $n=4$ and $m=2$ then set $g(X)=f(X)X(X-1)$. If $n=2m$ and $m>2$ then, for a polynomial $q(X)$ in $K[X]_{\mathrm{irr}.m-1}$, set $g(X)=f(X)q(X)X$. If $n\neq 2m$ then, for a polynomial $q(X)$ in $K[X]_{\mathrm{irr}.n-m}$, set $g(X)=f(X)q(X)$. Then $g(X)$ is a monic polynomial in $K[X]$ of degree n so that $g(\alpha)=0$ and $g(X)$ has no multiple roots. This completes the proof.

As in [6, (2.1)], Spec $B(R)$ will mean the Boolean spectrum of R which is the Stone space consisting of all prime ideals of $B(R)$, where the family of the subsets $U_e=\{y\in \operatorname{Spec} B(R)\,;\, e\in y\}$ $(e\in B(R))$ forms a base of the open subsets of $B(R)$. Given an element $x\in\operatorname{Spec} B(R)$ and a ring extension S of R, we denote by S_x the ring of residue classes of S modulo the ideal $\sum_{d\in x} Sd$, and for any element $\alpha\in S$, we denote by α_x the image of α under the canonical homomorphism $S\to S_x$. Obviously, S_x is a ring extension of R_x.

Now, we shall prove the following theorem which contains an improvement on the result of F. DeMeyer [3, Theorem 2.7].

Theorem. *Let R be a regular ring, and let S be a finite separable extension of R with $B(S)=B(R)$, and $n=\operatorname{Max}\{\operatorname{rank}_{R_x} S_x\,;\, x\in\operatorname{Spec} B(R)\}$. Then there is an element $\alpha\in S$ with $S=R[\alpha]$. In this case, there is a separable polynomial $p(X)\in R[X]$ of degree n with $p(\alpha)=0$. Moreover, if S is a weakly Galois extension of R and if S has* $\operatorname{rank}_R S$ *or the each R_x $(x\in\operatorname{Spec} B(R))$ is an infinite ring then the polynomial $p(X)$ can be chosen to be uniform and $S=$a splitting ring of $p(X)$.*

Proof. Let $x \in \operatorname{Spec} B(R)$. Then R_x is a field and S_x is a finite separable extension of R_x which is a field (cf. [6, (2.13)]). Hence there is an element $\xi_x \in S_x$ so that $S_x = R_x[\xi_x] = R[\xi]_x$. By [6, (2.11)], we can find an open neighborhood $U_e(=\{y \in \operatorname{Spec} B(R); e \in y\})$ of x such that $S_y = R[\xi]_y$ for all $y \in U_e$. Then, it follows that $S(1-e) = R[\xi](1-e)$. Applying the usual compactness argument, one can find orthogonal non-zero idempotents $e_1, \cdots, e_s$ in R and elements $\xi_1, \cdots, \xi_s$ in S such that $e_1 + \cdots + e_s = 1$ and $Se_i = R[\xi_i]e_i$ $(i=1, \cdots, s)$. Then we see that if $\alpha = \xi_1 e_1 + \cdots + \xi_s e_s$ then $S = R[\alpha]$.

Now, let $S = R[\alpha]$. Then, given any element $x \in \operatorname{Spec} B(R)$, we have $S_x = R_x[\alpha_x]$ and $n \geqq \operatorname{rank}_{R_x} S_x$. Hence by Lemma, there exists a separable polynomial $g_x(X)$ in $R_x[X]$ of degree n so that α_x is a root of $g_x(X)$. We write

$$(*) \qquad g_x(X) = X^n + (a_{n-1})_x X^{n-1} + \cdots + (a_1)_x X + (a_0)_x$$

where $a_i \in R$ $(i=0, 1, \cdots, n-1)$, and set

$$g(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0.$$

Then $g(\alpha)_x = 0$. We now denote by $\delta(g(X))$ the discriminant of $g(X)$ in the sense of [4, pp. 152–153] (, which is a polynomial in $a_0, a_1, \cdots, a_{n-1}$ with coefficients in the ring generated by 1). Since $g_x(X)$ is separable over R_x, it follows from [4, Corollary 1.3 and Theorem 2.3] that $\delta(g_x(X)) = \delta(g(X))_x$ and is inversible in R_x, that is, $\delta(g(X))R_x = R_x$. Hence by [6, (2.9) and (2.11)], we can find an open neighborhood U_d $(=\{y \in \operatorname{Spec} B(R); d \in y\})$ of x such that for every $y \in U_d$, $g(\alpha)_y = 0$, and $\delta(g(X))R_y = R_y$. Then $g(\alpha)(1-d) = 0$, $\delta(g(X))R(1-d) = R(1-d)$, and whence $\delta(g(X))(1-d) = \delta(g(X)(1-d))$ is inversible in $R(1-d)$. Thus $\alpha(1-d)$ is a root of $g(X)(1-d)$, and $g(X)(1-d)$ is a separable polynomial in $R[X](1-d)$ of degree n. Applying the usual compactness argument, we can find orthogonal non-zero idempotents $d_1, \cdots, d_r$ in R and monic polynomials $g_1(X), \cdots, g_r(X)$ in $R[X]$ of degree n such that $d_1 + \cdots + d_r = 1$, and the each $g_i(X)d_i$ is a separable polynomial in $R[X]d_i$ with $g_i(\alpha)d_i = 0$. Then $p(X) = g_1(X)d_1 + \cdots + g_r(X)d_r$ is a monic polynomial in $R[X]$ of degree n which is separable over R, and α is a root of $p(X)$.

Next we assume that S is a weakly Galois extension of R and that S has $\operatorname{rank}_R S$ or the each R_x $(x \in \operatorname{Spec} B(R))$ is an infinite field. Then for any $x \in \operatorname{Spec} B(R)$, S_x is a Galois extension of R_x. Hence by Lemma, $g_x(X)$ of $(*)$ can be chosen to be $S_x =$ the splitting field of $g_x(X)$. We write

$$g_x(X) = (X - (\alpha_1)_x) \cdots (X - (\alpha_n)_x)$$

where $\alpha_i \in S$ $(i=1, \cdots, n)$, $\alpha_1 = \alpha$, and set

$$h(X) = (X - \alpha_1) \cdots (X - \alpha_n).$$

Then, by [6, (2.11)] and [4, Corollary 1.3, Theorem 2.3], there exists an open neighborhood U_c $(=\{y \in \operatorname{Spec} B(R)\,;\, c \in y\})$ of x such that for every $y \in U_c$, $h(X)_y \in R_y[X]$ and $\delta(h(X))R_y = (\delta(h(X))R + R)_y = R_y$. Then $h(X)(1-c) \in R[X](1-c)$, $\delta(h(X))R(1-c) = (\delta(h(X))R + R)(1-c) = R(1-c)$, and whence $\delta(h(X))(1-c) = \delta(h(X)(1-c))$ is inversible in $R(1-c)$. Hence $h(X)(1-c)$ is a separable polynomial in $R[X](1-c)$ of degree n so that

$$h(X)(1-c) = (X(1-c) - \alpha_1(1-c)) \cdots (X(1-c) - \alpha_n(1-c)).$$

Applying the usual compactness argument, we obtain a separable polynomial $q(X)$ in $R[X]$ of degree n such that $q(\alpha) = 0$ and S is a splitting ring of $q(X)$. Since S is projective over R and with $B(S) = B(R)$, it follows from [5, Theorem 3.3] that $q(X)$ is uniform. This completes the proof.

Remark. Let $R = \mathrm{GF}(p) \oplus \mathrm{GF}(p)$, and $S = \mathrm{GF}(p^n) \oplus \mathrm{GF}(p)$, where $p > 0$ is a prime number and $n > p$ is an integer. Then R is a regular ring and S is a weakly Galois extension of R with $B(S) = B(R)$. However, there is no separable polynomials f in $R[X]$ so that S is a splitting ring of f.

References

[1] N. Bourbaki: Algèbre commutative. Chapitres I-II, Actualités Sci. Ind., No. 1290, Hermann, Paris (1961).

[2] S. U. Chase, D. K. Harrison, and Alex Rosenberg: Galois theory and Galois cohomology of commutative rings. Mem. Amer. Math. Soc., **52**, 15–33 (1965). MR 33 #4118.

[3] F. DeMeyer: Separable polynomials over a commutative ring. Rocky Mt. J. Math., **2**, 299–310 (1972). MR 45 #3391.

[4] T. Nagahara: On separable polynomials over a commutative ring. II. Math. J. of Okayama Univ., **15**, 149–162 (1972).

[5] ——: On separable polynomials over a commutative ring. III (to appear in Math. J. of Okayama Univ., **16**).

[6] O. E. Villamayor and D. Zelinsky: Galois theory with infinitely many idempotents. Nagoya Math. J., **35**, 83–93 (1969). MR 39 #5555.