ON SEPARABLE POLYNOMIALS OVER A COMMUTATIVE RING IV

Takasi NAGAHARA and Atsushi NAKAJIMA

Throughout this paper, all rings will be assumed commutative with identity element, B will mean a ring, and all ring extensions of B will be assumed with identity element 1, the identity element of B. Moreover, $B[X]$ will mean the ring of polynomials in an indeterminate X with coefficients in B, and all monic polynomials will be assumed to be of degree $\geqq 1$. Given a monic polynomial f in $B[X]$, a ring extension S of B is called a splitting ring of f (over B) if $S=B[a_1, a_2, \cdots, a_n]$ and $f=(X-a_1)(X-a_2)\cdots(X-a_n)$ (cf. [6, Def.]). A polynomial $f\in B[X]$ is called separable if f is monic and $B[X]/(f)$ is a separable B-algebra. Moreover, a polynomial $f\in B[X]$ is called cyclic if f is separable and f has a splitting ring which is a cyclic extension of B (i. e., a Galois extension with a cyclic Galois group).

This paper is about splitting rings of cyclic polynomials. In § **1**, we shall prove that if f is a cyclic polynomial in $B[X]$ then every splitting ring S of f which is projective over B and with $\mathrm{rank}_B S$ is a cyclic extension of B. In §§ **2-3**, we shall make some remarks on cyclic p^e-extensions and strongly cyclic n-extensions which has been studied in [8] and [9].

As to notations and terminologies used in this paper we follow [6]-[9].

1. Splitting rings of cyclic polynomials. First, we shall prove the following

Lemma 1.1. (cf. [11, p. 183]). *If A is a cyclic extension of B then any finite direct sum $A\oplus\cdots\oplus A$ is a cyclic extension of $B^*=\{(b,\cdots,b);\ b\in B\}$.*

Proof. Let A be a cyclic extension of B with a Galois group (σ) of degree n, and $T=A\oplus\cdots\oplus A$ (m-times direct sum). Then we can construct an automorphism τ of T by demanding that $\tau((x_1,\cdots,x_m))=(\sigma(x_m), x_1,\cdots,x_{m-1})$, where $(x_1,\cdots,x_m)\in T$. It is obvious that τ is of order mn and the fixring of τ in T is B^*. Since A is (σ)-Galois over B, there exist elements $a_1,\cdots, a_s, b_1,\cdots, b_s$ in A so that $\sum_{i=1}^{s} a_i\mu(b_i)=\delta_{1,\mu}$ (Kronecker's delta) for all $\mu\in(\sigma)$ (cf. [2, Th. 1. 3]). Write here

$a_{1,i}=(a_i, 0, \cdots, 0), \cdots, a_{i,m}=(0, \cdots, 0, a_i)$, $b_{i,1}=(b_i, 0, \cdots, 0), \cdots, b_{i,m}=(0, \cdots, 0, b_i)$, where $i=1, \cdots, s$. Then it is easily seen that $\sum_{i,j} a_{i,j}\nu(b_{i,j})=\delta_{1,\nu}$ for all $\nu \in (\tau)$. Hence T is a cyclic extension of B^* with Galois group (τ).

Lemma 1.2. *Let A be a ring extension of B and $\mathfrak{G}$ a finite group. If A is finitely generated, projective over B and A_x is $\mathfrak{G}$-Galois over B_x for all $x \in \operatorname{Spec}\mathscr{B}(B)$ then A is a $\mathfrak{G}$-Galois extension of B, and conversely.*

Proof. Assume that A is finitely generated, projective over B and A_x is $\mathfrak{G}$-Galois over B_x for all $x \in \operatorname{Spec}\mathscr{B}(B)$. Then by [7, Lemma 3. 1] we see that for each $x \in \operatorname{Spec}\mathscr{B}(B)$, there exists an open neighborhood $U_e(=\{y \in \operatorname{Spec}\mathscr{B}(B); e \in y\})$ of x such that $A(1-e)$ is $\mathfrak{G}$-Galois over $B(1-e)$. Hence, employing the compactness of $\operatorname{Spec}\mathscr{B}(B)$, we can find orthogonal non-zero idempotents $e_1, \cdots, e_m$ in B so that $\sum_{i=1}^m e_i=1$ and the each Ae_i is $\mathfrak{G}$-Galois over Be_i. Now, for each $\sigma \in \mathfrak{G}$, we construct an automorphism $\bar{\sigma}$ of A by demanding that $\bar{\sigma}$ restricted to Ae_i be σ for $i=1, \cdots, m$, and set $\overline{\mathfrak{G}}=\{\bar{\sigma}; \sigma \in \mathfrak{G}\}$. Then $\overline{\mathfrak{G}}$ is a group of automorphisms of A which is isomorphic to $\mathfrak{G}$, and the fixring of $\mathfrak{G}$ in A is B. Since the each Ae_i is $\mathfrak{G}$-Galois over Be_i, this contains elements $a_{i1}, \cdots, a_{i\alpha_i}$, $b_{i1}, \cdots, b_{i\alpha_i}$ such that $\sum_j a_{ij}\sigma(b_{ij})=e_i\delta_{1,\sigma}$ for all $\sigma \in \mathfrak{G}$. We may here write $n=\alpha_1=\cdots=\alpha_s$. If we set $u_j=\sum_i a_{ij}$ and $v_j=\sum_i b_{ij}$ $(j=1, \cdots, n)$ then there holds that $\sum_j u_j\bar{\sigma}(v_j)=\delta_{1,\bar{\sigma}}$ for all $\bar{\sigma} \in \overline{\mathfrak{G}}$. Hence A is *a* $\overline{\mathfrak{G}}$-Galois extension of B. Since $\overline{\mathfrak{G}} \cong \mathfrak{G}$, A is $\mathfrak{G}$-Galois over B. The converse is easily seen by using the result of [2, Th. 1.3].

Corollary 1.1. *Let A be a weakly Galois extension of B with* $\operatorname{rank}_B A$. *If* $\operatorname{rank}_B A$ *is prime then A is a cyclic extension of B.*

Proof. Let $p=\operatorname{rank}_B A$ be prime. Then, for each $x \in \operatorname{Spec}\mathscr{B}(B)$, A_x is a Galois extension of B_x of rank p, and whence A_x is a cyclic extension of B_x of rank p (cf. [12, (3. 15)]). Therefore by Lemma 1.2, A is a cyclic extension of B, completing the proof.

Now, let f be a separable polynomial in $B[X]$, and $x \in \operatorname{Spec}\mathscr{B}(B)$. By [7, Lemma 2.1], f_x has a splitting ring N_x which is projective over B_x and connected; and then N_x is a Galois extension of B_x with a Galois group $\mathfrak{G}$, which is unique up to isomorphism. The uniquely determined group $\mathfrak{G}$ will be denoted by $\mathfrak{G}(f_x)$.

Lemma 1. 3. *Let f be a separable polynomial in $B[X]$, and S a splitting ring of f which is projective over B and has $\mathrm{rank}_B S$. Then, S is a cyclic extension of B if and only if $\mathfrak{G}(f_x)$ is cyclic for all $x \in$* Spec $\mathscr{B}(B)$.

Proof. Let $x \in \mathrm{Spec}\,\mathscr{B}(B)$. As is easily seen, we have $S_x = \sum_{i=1}^{t} S_i$, a direct decomposition of S into connected B_x-algebras. Then the S_i are faithful B_x-modules, and so, the each S_i is a splitting ring of f_x which is projective over B_x. Since f_x is a separable polynomial in $B_x[X]$, it follows that the S_i are all isomorphic as B_x-algebras. For each i, let e_i be the identity element of S_i. Then the each S_i is a Galois extension of $B_x e_i$ ($\cong B_x$, $b_x e_i \longleftrightarrow b_x$) with Galois group $\mathfrak{G}_i$ ($\cong \mathfrak{G}(f_x)$), and $\{e_1, \cdots, e_t\}$ coincides with the set of all primitive idempotents in S_x. Now, assume that S is a cyclic extension of B with Galois group (τ). Then S_x is a cyclic extension of B_x with Galois group (τ). Hence we have $\{e_1 = \tau^t(e_1), \tau(e_1), \cdots, \tau^{t-1}(e_1)\} = \{e_1, \cdots, e_t\}$. This implies that the each S_i is a cyclic extension of $B_x e_i$ with Galois group (τ^t). Thus we obtain that $\mathfrak{G}(f_x) \cong (\tau^t)$ and is cyclic. To see the converse, we assume that $\mathfrak{G}(f_x)$ is cyclic for all $x \in \mathrm{Spec}\,\mathscr{B}(B)$. Then S_1 is a cyclic extension of $B_x e_1$, and S_x is B_x-algebra isomorphic to the t-times direct sum of S_1. Hence by Lemma 1. 1, S_x is a cyclic extension of B_x with a Galois group (τ) of order $s = \mathrm{rank}_B S$. Therefore, it follows from Lemma 1. 2 that S is a cyclic extension of B. This completes the proof.

By using of the result of Lemma 1. 3, we obtain the following

Theorem 1. 1 *Let f be a cyclic polynomial in $B[X]$, and T any splitting ring of f which is projective over B. If T has* $\mathrm{rank}_B T$ *then T is a cyclic extension of B, and conversely.*

As a direct consequence of Th. 1. 1 and [1, Th. 2. 5. 1], we obtain the following

Corollary 1. 2. *Let f be a cyclic polynomial in $B[X]$, and T any splitting ring of f which is projective over B. Then there exists a finite set of orthogonal non-zero idempotents $\{e_1, \cdots, e_n\}$ in T such that $\sum_{i=1}^{n} e_i = 1$, the each Se_i is a cyclic extension of Be_i, and* $\mathrm{rank}_{Be_i} Se_i \neq \mathrm{rank}_{Be_j} Se_j$ *if $1 \leqq i \neq j \leqq n$.*

Remark 1. 1. Let $f = X^2 - X \in B[X]$. Then, by using the result of [6, Th. 2. 3], we see that f is a cyclic polynomial. If B is not connected then, by [8, Remark 2. 1], we see that f has a splitting ring which is projective over B but has not $\text{rank}_B S$.

Next, we shall present an example which implies that in Th. 1. 1, the condition of "cyclic" cannot take the place of the condition of "Galois". Let Q be the field of rational numbers and ζ a primitive 4-th root of 1. Moreover, let $B = Q[\zeta] \oplus Q$ and $S = Q[\zeta, \sqrt[4]{5}] + Q[\sqrt{2}, \sqrt{3}]$. Then $f(X) = (1, 0)(X^4 - 5) + (0, 1)(X^2 - 2)(X^2 - 3)$ is a separable polynomial in $B[X]$ and S is a splitting ring of $f(X)$. Since $[Q[\zeta, \sqrt[4]{5}] : Q[\zeta]] = [Q[\sqrt{2}, \sqrt{3}] : Q] = 4$, we have $\text{rank}_B S = 4$. However, the Galois group of the Galois extension $Q[\zeta, \sqrt[4]{5}]/Q[\zeta]$ is not isomorphic to the Galois group of the Galois extension $Q[\sqrt{2}, \sqrt{3}]/Q$. This implies that S is not Galois over B.

1. On cyclic p^e-extensions. Throughout this section, B will mean a ring which contains the prime field $GF(p)$ where $p \neq 0$ and $GF(p) \ni 1$, the identity element of B. Then, by the results of [8, Lemma 1. 1, Ths. 1. 1, 1. 2], [7, Th. 3. 1] and Cor. 1. 1, we see that for every $b \in B$, the polynomial $X^p - X - b \in B[X]$ is cyclic, and for a ring extension A/B, the following conditions are equivalent:

(a) A is a weakly Galois extension of B with $\text{rank}_B A = p$.

(b) A is a cyclic p-extension of B.

(c) A is a B-algebra isomorphic to $B[X]/(X^p - X - b)$, the ring of residue classes of $B[X]$ modulo $(X^p - X - b)$ for some polynomial $X^p - X - b$ in $B[X]$.

(d) A is a splitting ring of some polynomial $X^p - X - b$ in $B[X]$ which is projective over B and with $\text{rank}_B A = p$.

Now we shall prove first the following

Lemma 2. 1. *Let B be connected, and A a splitting ring of a polynomial $f(X) = X^p - X - b$ in $B[X]$ which is projective over B and connected. Then $\text{rank}_B A = p$ or 1. Moreover, $\text{rank}_B A = p$ if and only if $f(b') \neq 0$ for all $b' \in B$, which is equivalent to that $f(X)$ is irreducible over B.*

Proof. Since A is a splitting ring of $f(X)$, there exists an element a in A so that $f(a) = 0$, and then $f(X) = (X - a)(X - a - 1) \cdots (X - a - p + 1)$ (cf. [8, Lemma 1. 1]). Hence by [5, Cor. 6], we have $A = B[a]$. By Th. 1. 1, A is a cyclic extension of B with Galois group (σ). Since $\sigma(a)$ is a root of $f(X)$, we have $\sigma(a) = a + i$ for some $0 \leqq i \leqq p - 1$ (cf. [5, Cor. 6]). If $i = 0$ then (σ) is of order 1, and so, $\text{rank}_B A = 1$. If $i \neq 0$ then (σ) is of order p, and so, $\text{rank}_B A = p$. Hence

$\operatorname{rank}_B A = p$ if and only if $a+i \notin B$ for $i=0, 1, \cdots, p-1$, which is equivalent to that $f(b') \neq 0$ for all $b' \in B$. The other assertion follows from [8, Lemma 1.2].

In [3], F. DeMeyer introduced the notion of uniform separable polynomials. By [7, Th. 3.3], we see that a separable polynomial $f(X)$ in $B[X]$ is uniform if and only if $f(X)$ has a splitting ring S which is projective over B and with $\mathscr{B}(S) = \mathscr{B}(B)$.

Proposition 2.1. *Let* $f(X) = X^p - X - b \in B[X]$. *Then,* $f(X)$ *is uniform if and only if* $E = \{x \in \operatorname{Spec} \mathscr{B}(B)\,;\ f(b')_x \neq 0_x$ *for all* b' *in* $B\}$ *is an open set.*

Proof. Given an element $x \in \operatorname{Spec}\mathscr{B}(B)$, the result of Lemma 2.1 implies that the order of $G(f(X)_x) = p$ if and only if $f(b')_x \neq 0$ for all $b' \in B$. Hence E coincides with the set $\{x \in \operatorname{Spec}\mathscr{B}(B)\,;$ the order of $\mathfrak{G}(f(X)_x) = p\}$. Therefore, if $f(X)$ is uniform then E is open by [7, Th. 3.3]. To see the converse, we assume that E is open. By Lemma 2.1, the complement E^C of E in $\operatorname{Spec}\mathscr{B}(B)$ coincides with the set $\{x \in \operatorname{Spec}\mathscr{B}(B)\,;$ the order of $\mathfrak{G}(f(X)_x) = 1\}$. Hence by {7, Th. 3.3], it suffices to prove that E^C is open. Let $E^C \neq \Phi$ and $x \in E^C$. Then there exists an element b' in B such that $f(b')_x = 0_x$. Hence by [12, (2.9)], there exists an open neighborhood U of x such that for every $y \in U$, $f(b')_y = 0_y$; whence the order of $\mathfrak{G}(f(X)_y) = 1$. Thus E^C is an open set.

Proposition 2.2. *For a ring extension* A/B, *the following conditions are equivalent.*

(a) A *is a cyclic* p*-extension of* B *with* $\mathscr{B}(A) = \mathscr{B}(B)$.

(b) $A \cong B[X]/(f(X))$ (*as* B*-algebras*) *for some polynomial* $f(X) = X^p - X - b \in B[X]$ *so that* $f(b')_x \neq 0_x$ *for all* $b' \in B$ *and for all* $x \in \operatorname{Spec}\mathscr{B}(B)$.

Proof. By [8, Ths. 1.1, 1.2], it suffices to prove that for a polynomial $f(X) = X^p - X - b \in B[X]$, $\mathscr{B}(B[X]/(f(X))) = \mathscr{B}(B)$ if and only if $f(b')_x \neq 0_x$ for all $b' \in B$ and for all $x \in \operatorname{Spec}\mathscr{B}(B)$. We set $S = B[X]/(f(X))$. Then S is a splitting ring of $f(X)$ which is projective over B and with $\operatorname{rank}_B S = p$. If $\mathscr{B}(S) = \mathscr{B}(B)$ then, by [12, (2.13)], for every $x \in \operatorname{Spec}\mathscr{B}(B)$, S_x is a connected ring, and this a splitting ring of $f(X)_x$ which is projective over B_x and with $\operatorname{rank}_{B_x} S_x = p$, whence by Lemma 2.1, $f(b')_x \neq 0_x$ for all $b' \in B$. Conversely, if $f(b')_x \neq 0_x$ for all $b' \in B$ and for all $x \in \operatorname{Spec}\mathscr{B}(B)$ then, by

[8, Th. 1. 6], S_x is a connected ring for all $x \in \operatorname{Spec} \mathscr{B}(B)$. Hence, if $e^2 = e \in S$ then $B_x + (eB)_x = B_x$ for all $x \in \operatorname{Spec} \mathscr{B}(B)$, and so, by [12, (2. 11)], $B + eB = B$, that is, $e \in B$. This implies that $\mathscr{B}(S) = \mathscr{B}(B)$.

Proposition 2. 3. *Let B be a regular ring* (*in the sense of* Von Neumann). *Then, for a ring extension A/B, the following conditions are equivalent.*

(a) *A is a cyclic p-extension of B with $\mathscr{B}(A) = \mathscr{B}(B)$.*

(b) *$A \cong B[X]/(f(X))$ (as B-algebras) for some polynomial $f(X) = X^p - X - b \in B[X]$ so that for every $b' \in B$, $f(b')$ is inversible in B.*

Moreover, if there hold the conditions then A is a regular ring.

Proof. Since B is a regular ring, B_x is a field for all $x \in \operatorname{Spec} \mathscr{B}(B)$. Hence, if there holds (a) then the each A_x is a field, and this implies that A is a regular ring. Now we shall prove that (a)$\Leftrightarrow$(b). By Prop. 2. 2, it suffices to prove that $f(b')_x \neq 0_x$ for all $b' \in B$ and for all $x \in \operatorname{Spec} \mathscr{B}(B)$ if and only if $f(b')$ is inversible in B for all $b' \in B$. Let b' be an arbitrary element of B, and assume that $f(b')_x \neq 0_x$ for all $x \in \operatorname{Spec} \mathscr{B}(B)$. Then, we have that for every $x \in \operatorname{Spec} \mathscr{B}(B)$, $f(b')_x$ is inversible in B_x, and so, $f(b')B_x = B_x$. Hence by [12, (2. 11)], we obtain $f(b')B = B$. Thus $f(b')$ is inversible in B. The converse is obvious.

For cyclic p^e-extensions, we have the following

Proposition 2. 4. *Let A be a cyclic p^e-extension of B with a Galois group (σ), where $e > 0$. Let A_1 be the fixring of (σ^p) in A. Then*

(1) *A_1 is a cyclic p-extension of B.*

(2) *$\mathscr{B}(A_1) = \mathscr{B}(B)$ if and only if $\mathscr{B}(A) = \mathscr{B}(B)$.*

(3) *If B is a regular ring and $\mathscr{B}(A_1) = \mathscr{B}(B)$ then A is a regular ring.*

Proof. The first assstion is obvious. Now, let $x \in \operatorname{Spec} \mathscr{B}(B)$. Then A_x is a cyclic p^e-extension of B_x with Galois group (σ_x), and A_{1x} is the fixring of (σ_x^p) in A_x, where σ_x is a B_x-algebra automorphism of A_x induced by σ. Hence, by [8, Th. 1. 8], A_{1x} is connected if and only if A_x is connected. If $\mathscr{B}(A_1) = \mathscr{B}(B)$ then A_{1x} is connected for all $x \in \operatorname{Spec} \mathscr{B}(B)$, and conversely. Therefore, it follows that $\mathscr{B}(A_1) = \mathscr{B}(B)$ if and only if $\mathscr{B}(A) = \mathscr{B}(B)$. If B is a regular ring and $\mathscr{B}(A_1) = \mathscr{B}(B)$ then A_x is a field for all $x \in \operatorname{Spec} \mathscr{B}(B)$, which implies that A is a regular ring.

Now, we shall prove the following

Theorem 2. 1. *Let* e *be any positive integer. Then*

(1) *there is a cyclic* p*-extension* A_1 *of* B *with* $\mathscr{B}(A_1)=\mathscr{B}(B)$ *if and only if there is a cyclic* p^e*-extension* A *of* B *with* $\mathscr{B}(A)=\mathscr{B}(B)$.

(2) *Let* B *be a regular ring. If there is a cyclic* p*-extension* A_1 of B *with* $\mathscr{B}(A_1)=\mathscr{B}(B)$ *then there is a cyclic* p^e*-extension* A *of* B *which is a regular ring and with* $\mathscr{B}(A)=\mathscr{B}(B)$.

Proof. We assume that there exists a cyclic p-extension A_1 of B. Then, by [8, Th. 1. 3], there exists a cyclic p^e-extension A of B with Galois group (σ) such that A contains $A_1 \supset B$ and A_1 is the fixring of (σ^p) in A. Hence our assertion follows from the result of the preceding proposition.

In virtue of [8, Th. 2. 3], we have the following proposition, which is proved by making use of the same methods as in the proof of Prop. 2. 4.

Proposition 2. 5. *Let* A *be an abelian* $(p^{e_1}, \cdots, p^{e_s})$*-extension with a Galois group* $(\sigma_1)\times\cdots\times(\sigma_s)$, *where* $e_i > 0$, $i=1, \cdots, s$. *Let* A_1 *be the fixring of* $(\sigma_1{}^p)\cdots(\sigma_s{}^p)$ *in* A. *Then*

(1) A_1 *is an abelian* $(\overbrace{p, \cdots, p}^{s})$*-extension of* B.

(2) $\mathscr{B}(A_1)=\mathscr{B}(B)$ *if and only if* $\mathscr{B}(A)=\mathscr{B}(B)$.

(3) *If* B *is a regular ring and* $\mathscr{B}(A_1)=\mathscr{B}(B)$ *then* A *is a regular ring*.

By [8, Ths. 1. 3, 2. 1, 2. 2] and Prop. 2. 5, we obtain the following

Theorem 2. 2. *Let* e_i $(1\leqq i\leqq s)$ *be positive integers. Then*

(1) *there is an abelian* $(\overbrace{p, \cdots, p}^{s})$*-extension* A_1 *of* B *with* $\mathscr{B}(A_1)=\mathscr{B}(B)$ *if and only if there is an abelian* $(p^{e_1}, \cdots, p^{e_s})$*-extension* A *of* B *with* $\mathscr{B}(A)=\mathscr{B}(B)$.

(2) *Let* B *be a regular. If there is an abelian* $(\overbrace{p, \cdots, p}^{s})$*-extension* A_1 *of* B *with* $\mathscr{B}(A_1)=\mathscr{B}(B)$ *then there is an abelian* $(p^{e_1}, \cdots, p^{e_s})$*-extension* A *of* B *which is a regular ring and with* $\mathscr{B}(A)=\mathscr{B}(B)$.

3. **On strongly cyclic n-extensions.** Throughout this section, B will mean a ring which contains a primitive n-th root ζ of 1 such that n and $1-\zeta^i$ $(i=1, 2, \cdots, n-1)$ are inversible in B. Then by [9, Lemmas 1. 1, 1. 2, Th. 1. 1], we see that for any divisor k of n, $X^k-b\in B[X]$ is separable if and only if b is inversible in B, and in this case, the

polynomial $X^k - b$ is cyclic. The results in this section are similar to those of §2, and the proofs proceed as in those of §2. Hence the details may be omitted.

Our first lemma follows from the results of [9, Lemma 1.2], [5, Cor. 6], Th. 1.1 and [9, Lemma 1.4].

Lemma 3.1. (cf. Lemma 2.1). *Let B be connected, q a prime divisor of n and A a splitting ring of a separable polynomial $f(X) = X^q - b$ in $B[X]$ which is projective over B and connected. Then* $\mathrm{rank}_B A = q$ *or* 1. *Moreover,* $\mathrm{rank}_B A = q$ *if and only if $f(b') \neq 0$ for all $b' \in B$, which is equivalent to that $f(X)$ is irreducible over B.*

In virtue of Lemma 3.1, we have the following proposition which is proved by making use of the same methods as in the proof of Prop. 2.1.

Proposition 3.1. (cf. Prop. 2.1). *Let q be a prime divisor of n and $f(X) = X^q - b$ a separable polynomial in $B[X]$. Then $f(X)$ is uniform if and only if $E = \{x \in \mathrm{Spec}\mathscr{B}(B)\,;\ f(b')_x \neq 0$ for all $b' \in B\}$ is an open set.*

The next propositition is a consequence of the results of [9, Ths. 1.1, 1.2], Lemma 3.1 and [9, Lemma 1.4, Th. 1.8].

Proposition 3.2. (cf. Prop. 2.2). *Let q be a prime divisor of n. Then, for a ring extension A/B, the following conditions are equivalent.*

(a) *A is a strongly cyclic q-extension of B with $\mathscr{B}(A) = \mathscr{B}(B)$.*

(b) *$A \cong A[X]/(f(X))$ (as B-algebras) for some separable polynomial $f(X) = X^q - b \in B[X]$ so that $f(b')_x \neq 0_x$ for all $b' \in B$ and for all $x \in$* $\mathrm{Spec}\,\mathscr{B}(B)$.

By virtue of Prop. 3.2, we have the following

Proposition 3.3. (cf. Prop. 2.3). *Let B be a regular ring, and q a prime divisor of n. Then, for a ring extension A/B, the following conditions are equivalent.*

(a) *A is a strongly cyclic q-extension of B with $\mathscr{B}(A) = \mathscr{B}(B)$.*

(b) *$A \cong B[X]/(f(X))$ (as B-algebras) for some separable polynomial $f(X) = X^q - b \in B[X]$ so that for every $b' \in B$, $f(b')$ is inversible in B.*

Moreover, if there hold the conditions then A is a regular ring.

The next proposition follows from the result of [9, Ths. 1.4, 1.12].

Proposition 3.4. (cf. Prop. 2.4). *Let A be a strongly cyclic (σ, n)-extension of B, k the product of all different prime divisors of n, and A_1 the fixring of (σ^k) in A. Then*

(1) *A_1 is a strongly cyclic k-extension of B.*

(2) *$\mathscr{B}(A_1)=\mathscr{B}(B)$ if and only if $\mathscr{B}(A)=\mathscr{B}(B)$.*

(3) *If B is a regular ring and $\mathscr{B}(A_1)=\mathscr{B}(B)$ then A is a regular ring.*

Now, by [9, Th. 1. 3] and Prop. 3. 4, we obtain the following

Theorem 3.1. (cf. Th. 2. 1). *Let k be the product of all different prime divisors of n. Then*

(1) *there is a strongly cyclic k-extension A_1 of B with $\mathscr{B}(A_1)=\mathscr{B}(B)$ if and only if there is a strongly cyclic n-extension A of B with $\mathscr{B}(A)=\mathscr{B}(B)$.*

(2) *Let B be a regular ring. If there is a strongly cyclic k-extension A_1 of B with $\mathscr{B}(A_1)=\mathscr{B}(B)$, then there is a strongly cyclic n-extension A of B which is a regular ring and with $\mathscr{B}(A)=\mathscr{B}(B)$.*

The following proposition can be proved by making use of the same methods as in the proof of [9, Th. 2. 3].

Proposition 3.5. (cf. Prop. 2. 5). *Let n_i $(1\leqq i\leqq s)$ be divisors of n and k_i the product of all different prime divisors of n_i. Let A be a strongly abelian $(\sigma_1, \cdots, \sigma_s; n_1, \cdots, n_s)$-extension of B and A_1 the fixring of $(\sigma_1^{k_1})\times\cdots\times(\sigma_s^{k_s})$ in A. Then*

(1) *A_1 is a strongly abelian $(k_1, \cdots, k_s)$-extension of B.*

(2) *$\mathscr{B}(A_1)=\mathscr{B}(B)$ if and only if $\mathscr{B}(A)=\mathscr{B}(B)$.*

(3) *If B is a regular ring and $\mathscr{B}(A_1)=\mathscr{B}(B)$ then A is a regular ring.*

Finally, we shall present the following theorem which follows from the results of [9, Ths. 1. 3, 2. 1, 2. 2] and Prop. 3. 5.

Theorem 3.2. (cf. Th. 2. 2). *Let n_i $(1\leqq i\leqq s)$ be divisors of n and k_i the product of all different prime divisors of n_i. Then*

(1) *there is a strongly abelian $(k_1, \cdots, k_s)$-extension A_1 of B with $\mathscr{B}(A_1)=\mathscr{B}(B)$ if and only if there is a strongly abelian $(n_1, \cdots, n_s)$-extension A of B with $\mathscr{B}(A)=\mathscr{B}(B)$.*

(2) *Let B be a regular ring. If there is a strongly abelian $(k_1, \cdots, k_s)$-extension A_1 of B with $\mathscr{B}(A_1)=\mathscr{B}(B)$ then there is a strongly abelian $(n_1, \cdots, n_s)$-extension A of B which is a regular ring with $\mathscr{B}(A)=\mathscr{B}(B)$.*

REFERENCES

[1] N. BOURBAKI: Algèbre commutative, Chapitres I-II, Actualites Sci. Ind. No. 1290,

Hermann, Paris, 1962.

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

[3] F. DEMEYER: Separable polynomials over a commutative ring, Rocky Mt. J. Math., **2** (1972), 299—310.

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

[5] T. NAGAHARA: On separable polynomials over a commutative ring, Math. J. Okayama Univ., **14** (1970), 175—181.

[6] T. NAGAHARA: On separable polynomials over a commutative ring II, Math. J. Okayama Univ., **15** (1972), 149—162.

[7] T. NAGAHARA: On separable polynomials over a commutative ring III, Math. J. Okayama Univ., **16** (1974), 189—197.

[8] T. NAGAHARA and A. NAKAJIMA: On cyclic extensions of commutative rings, Math. J. Okayama Univ., **15** (1971), 81—90.

[9] T. NAGAHARA and A. NAKAJIMA: On strongly cyclic extensions of commutative rings, Math. J. Okayama Univ., **15** (1971), 91—100.

[10] A. NAKAJIMA: On a group of cyclic extensions over commutative rings, Math. J. Okayama Univ., **15** (1972), 163—172.

[11] A. NAKAJIMA: On a group of cyclic extensions over commutative ring II, Math. J. Okayama Univ., **16** (1974), 177—187.

[12] O. E. VILLAMAYOR and D. ZELINSKY: Galois theory with infinitely many idempotents, Nagoya Math. J., **35** (1969), 83—93.

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY

(Received August 13, 1973)