ON ABELIAN EXTENSIONS OF RINGS II

Dedicated to Professor Takeshi Inagaki for his 60th birthday

KAZUO KISHIMOTO

Introduction. In [5], the author has studied abelian extensions of an algebra over $GF(p)$ with Galois group of order p^f. In the present paper, as a continuation of [5], we shall continue our study on Kummer case. This paper, as well as [5], depends on [1], [3], [4] and [6], and the reader should consult them for relevant definitions and basic properties of Galois extensions of rings.

In this paper, we assume the following:

1) $\mathfrak{G}$ (resp. $\mathfrak{G}^*$) is a cyclic group of order n with a generator σ (resp. σ^*) or a direct product of cyclic groups (σ_i) (resp. (σ_i^*)) of order n_i, $i=1, 2, \cdots, e$, such that $\Pi_{i=1}^e n_i = n$.

2) B is a ring without proper central idempotents whose center Z contains a primitive n-th root ζ of 1 and n, $1-\zeta^i$, $i=1, 2, \cdots, n-1$, are units in Z.

3) Galois extensions are always Galois extensions without proper central idempotents and the base ring is contained in the extension ring as a right (as well as left) direct summand.

Definition 1. A ring extension T/S will be called *an abelian* $(\mathfrak{H}, \zeta)$-*extension* (resp. *a cyclic* $(\mathfrak{H}, \zeta)$-*extension*) if S is a ring extension of B and T is a Galois extension of S with an abelian Galois group $\mathfrak{H}$ (resp. with a cyclic Galois group $\mathfrak{H}$) such that the center of T contains ζ.

Definition 2. Let $\mathfrak{G}=(\sigma_1)\times(\sigma_2)\times\cdots\times(\sigma_e)$. A ring extension T/S will be called *a strongly abelian* $(\mathfrak{G}, \zeta)$-*extension* (resp. *a strongly cyclic* $(\mathfrak{G}, \zeta)$-*extension*) if T/S is an abelian $(\mathfrak{G}, \zeta)$-extension (resp. a cyclic $(\mathfrak{G}, \zeta)$-extension with $\mathfrak{G}=(\sigma_1)$) and $\{\sum_{k=0}^{n_i-1}\zeta_i^k\sigma_i^k(x)\,|\,x\in S_i\}\cap U(S_i)$[1] $\neq\emptyset$ for each $i=1, 2, \cdots, e$, where $\zeta_i=\zeta^{n/n_i}$, $S_i=T^{\check{\mathfrak{G}}_i}$ and $\check{\mathfrak{G}}_i=(\sigma_1)\times(\sigma_2)\times\cdots\times(\sigma_{i-1})\times(\sigma_{i+1})\times\cdots\times(\sigma_e)$.

The purpose of this paper is to give

1) Let T be a ring. Then, by $U(T)$ we denote the set of unit elements of T.

I) necessary and sufficient conditions for B to have strongly abelian $(\mathfrak{G}, \zeta)$-extensions;

II) necessary and sufficient conditions for an abelian $(\mathfrak{T}, \zeta)$-extension T/B to be embedded in an abelian $(\mathfrak{H}, \zeta)$-extension A/B in such a way that A/T is a strongly abelian $(\mathfrak{G}, \zeta)$-extension, $T=(\tau_1)\times(\tau_2)\times\cdots\times(\tau_e)$, $\mathfrak{H}=(\eta_1)\times(\eta_2)\times\cdots\times(\eta_e)$, $\eta_i|T=\tau_i$ and $\sigma_i=\eta_i^{m_i}$ where m_i is the order of τ_i;

III) sufficient conditions for a cyclic $(\mathfrak{G}, \zeta)$-extension of a commutative ring to be strongly cyclic.

In §1, we restrict our attention to the case that $\mathfrak{G}$ is cyclic.

In §2, as a generalization of §1, we consider the case $\mathfrak{G}=(\sigma_1)\times(\sigma_2)\times\cdots\times(\sigma_e)$.

In §3, we consider a cyclic $(\mathfrak{G}, \zeta)$-extension A of B such that B is a commutative ring and A is an algebra over B. Then A is also commutative ([2, Theorem 11]). Firstly, we shall show that if A has a $\mathfrak{G}$-normal basis then it is strongly cyclic. Moreover, if B is semi-local then the converse is true. As an application of this fact, I) and II) are given for the case of semi-local rings.

§4 deals with an abelian $(\mathfrak{G}, \zeta)$-extension of commutative rings.

The author wishes to express his thanks to Professor H. Tominaga, Professor T. Nagahara and Mr. A. Nakajima for helpful discussion and advice.

1. Cyclic $(\mathfrak{H},\zeta)$-extension with $\mathfrak{H}=(\eta)$ of order nm

Throughout the present section, we assume that $\mathfrak{G}$ is a cyclic group of order n with a generator σ. In a cyclic $(\mathfrak{G}, \zeta)$-extension A of B, an element x will be called *a σ-generator* for A/B if $\sigma(x)=x\zeta^{-1}(=\zeta^{-1}x)$ and x is a unit in A.

Lemma 1.1. *Let A/B be a cyclic $(\mathfrak{G}, \zeta)$-extension. Then there exists a non-zero element x in A with $\sigma(x)=x\zeta^{-1}$. If A/B is strongly cyclic then there exists a σ-generator for A/B, and conversely*[2].

Proof. We set $f(a)=a+\zeta\sigma(a)+\cdots+\zeta^{n-1}\sigma^{n-1}(a)$, $a\in A$. Then there exists an element c in A with $f(c)\neq 0$. Hence $\sigma(f(c))=f(c)\zeta^{-1}$. If $x\in A$ and $\sigma(x)=x\zeta^{-1}$ then $f(x)=nx$. This implies our assertion.

The first theorem of this section is the following

Theorem 1.1. *In order that B have a strongly cyclic $(\mathfrak{G}, \zeta)$-exten-*

---

2) Cf. [7, Theorem 10.6].

sion A, it is necessary and sufficient that there exist an automorphism ρ of B and an element b_0 in $U(B)$ satisfying

(a) $\rho^n=\widetilde{b_0^{-1}}$, $\rho(b_0)=b_0$ *and* $\rho(\zeta)=\zeta$,

(b) X^n-b_0 *is directly indecomposable in* $B[X;\rho]$.

More precisely, if there exist ρ, b_0 satisfying (a) *and* (b), *then* $M=(X^n-b_0)B[X;\rho]=\{(X^n-b_0)f(X)\mid f(X)\in B[X;\rho]\}$ *is a two-sided ideal of* $B[X;\rho]$ *and* $A^*=B[y]=B[X;\rho]/M$ *is a strongly cyclic* $(\mathfrak{G}^*, \zeta)$ *extension of B where y is the residue class of X modulo M and $\mathfrak{G}^*$ is the cyclic group of order n generated by σ^* defined by* $\sigma^*(y)=y\zeta^{-1}$. *Conversely, if A is a strongly cyclic $(\mathfrak{G}, \zeta)$-extension of B, then we can find such ρ, b_0 satisfying* (a) *and* (b) *that there exists a B-isomorphism* $\varphi^*: A^*\longrightarrow A$ *with* $\varphi^*\sigma^*=\sigma\varphi^*$.

Proof. Necessity: Let A be a strongly cyclic $(\mathfrak{G}, \zeta)$-extension of B. Then there exists a σ-generator x for A/B by Lemma 1.1. Since $\sigma(x^{-1}bx)=x^{-1}bx$ for each $b\in B$, the inner automorphism $\tilde{x}^{-1}$ of A effected by x^{-1} induces an automorphism of B. Now we set $\rho=\tilde{x}^{-1}|B$. Then $\sigma(x^n)=(x\zeta^{-1})^n=x^n$ shows that $b_0=x^n\in U(B)$. Thus ρ, b_0 satisfy (a). If we note that $bx=x\rho(b)$ for each $b\in B$, $T=B+xB+\cdots+x^{n-1}B$ forms a subring of A with $\sigma(T)\subseteq T$. In the following, we shall show $T=B\oplus xB\oplus\cdots\oplus x^{n-1}B=A$. Let $T\ni t=\sum_{i=0}^{n-1}x^id_i=0$ $(d_i\in B)$. Then $\sigma(t)-t=x(\sum_{i=1}^{n-1}x^{i-1}d_i(\zeta^{-i}-1))$, and hence $t_1=\sum_{i=1}^{n-1}x^{i-1}d_i(\zeta^{-i}-1)=0$. Since ζ^i-1 is a unit for each $i=1, 2, \cdots, n-1$, repeating the same procedure, we have $d_{n-1}=d_{n-2}=\cdots=d_1=d_0=0$. Therefore $T=B\oplus xB\oplus\cdots\oplus x^{n-1}B$. To be easily seen, $X^nb_0^{-1}-1$ is central in $B[X;\rho]$, $T^\sigma=B$ and $T\cong B[X;\rho]/(X^n-b_0)B[X;\rho]$. Now, for $\tau\in\mathfrak{G}$ we have

$$\delta_{1,\tau}=\Pi_{j=1}^{n-1}\{(\zeta^{-j}-1)^{-1}x^{-1}\sigma^j(x)-(\zeta^{-j}-1)^{-1}x^{-1}\tau(x)\},$$

whence we obtain $\delta_{1,\tau}=\sum_{k=0}^{n-1}a_k\tau(x^k)$ with some a_k in T. Hence, we see that $\{a_0, a_1, \cdots, a_{n-1}; 1, x, \cdots, x^{n-1}\}$ is a $\mathfrak{G}$-Galois coordinate system for A/B. Since $a_0, a_1, \cdots, a_{n-1}, x$ are elements of T, it follows from [6, Theorem 2.3] that $T=A$ and X^n-b_0 is directly indecomposable in $B[X;\rho]$.

Sufficiency: Assume that there exist an automorphism ρ and an element b_0 satisfying the conditions (a) and (b). Let Ψ be the map of $B[X;\rho]$ defined by $f(X)\longmapsto f(X\zeta^{-1})$. Then Ψ is an automorphism of $B[X;\rho]$ of order n with $\Psi(X^nb_0^{-1}-1)=X^nb_0^{-1}-1$ where $X^nb_0^{-1}-1$ is a central polynomial. Hence Ψ induces an automorphism σ^* of order n in $A^*=B\oplus yB\oplus\cdots\oplus y^{n-1}B=B[X;\rho]/(X^nb_0^{-1}-1)=B[X;\rho]/M$ and $\sigma^*(y)=y\zeta^{-1}$, where y is the residue class of X modulo M. Since $y^n b_0^{-1}=1$, y is a unit in A^*. Noting n is a unit in A^*, we have $\sum_{i=0}^{n-1} \zeta^i \sigma^{*i}(y)=ny\in U(A^*)$. The existence of (σ^*)-Galois coordinate system for A^*/B will be seen in the same way as in the proof of the necessity. The rest of the proof will be almost evident.

Corollary 1.1. *Let A be a strongly cyclic $(\mathfrak{G}, \zeta)$-extension of B. Then A/B has a σ-generator and if x is a σ-generator for A/B then $A=B[x]$ and $\{1, x, x^2, \cdots, x^{n-1}\}$ is a right free B-basis for A.*

Let A/B be a strongly cyclic $(\mathfrak{G}, \zeta)$-extension with $\sigma=\tilde{v}$ for some $v\in A$. Then we have $v\in V=V_A(B)$. Hence $v\in V^{\tilde{v}}=B\cap V=Z$. Further, since $x\zeta^{-1}=\tilde{v}(x)=vxv^{-1}$ for a σ-generator x for A/B, we have $v\zeta^{-1}=x^{-1}vx$. Thus we have proved the necessity in the following

Corollary 1.2. *In order that B have a strongly cyclic $(\mathfrak{G}, \zeta)$-extension with $\sigma=\tilde{v}$, it is necessary and sufficient that there exist an automorphism ρ of B, an element $b_0\in U(B)$ and an element $z\in U(Z)$ satisfying*

(a) $\rho^n=\tilde{b}_0^{-1}$, $\rho(b_0)=b_0$ *and* $\rho(\zeta)=\zeta$,

(b) X^n-b_0 *is directly indecomposable in* $B[X;\rho]$,

(c) $\rho(z)=z\zeta^{-1}$.

Proof. We shall prove the sufficiency. Under the same notations as in the proof of Theorem 1. 1, we set $A^*=B\oplus yB\oplus\cdots\oplus y^{n-1}B=B[X;\rho]/M$. If $\rho(z)=z\zeta^{-1}$ for some $z\in U(Z)$, then $zyz^{-1}=y\rho(z)z^{-1}=y\zeta^{-1}=\sigma^*(y)$, and hence $\sigma^*(a)=zaz^{-1}$ for every $a\in A^*$. This imples $\sigma^*=\tilde{z}$, that is, $(\sigma^*)=(\tilde{z})$.

Now we shall prove the following embedding theorem.

Theorem 1.2. *Let T be a cyclic $(\mathfrak{T}, \zeta)$-extension of B where $\mathfrak{T}$ is of order m and generated by τ. Let $\mathfrak{H}$ be a cyclic group of order nm with a generator η. In order that B have a cyclic $(\mathfrak{H}, \zeta)$-extension A such that $A\supseteqq T$, A/T is a strongly cyclic $(\mathfrak{G}, \zeta)$-extension, $\eta\,|\,T=\tau$, and $\eta^m=\sigma$, it is necessary and sufficient that there exist an automorphism ρ of T and elements t_0, u in $U(T)$ satisfying*

(a) $\rho^n=\widetilde{t_0^{-1}}$, $\rho(t_0)=t_0$ *and* $\rho(\zeta)=\zeta$,

(b) X^n-t_0 *is directly indecomposable in* $T[X;\rho]$,

(c) $\rho\tau\rho^{-1}\tau^{-1}=\tilde{u}$,

(d) $RN_m(u;\tau)(=u\tau(u)\tau^2(u)\cdots\tau^{m-1}(u))=\zeta^{-1}$,

(e) $LN_n(u;\rho)(=\rho^{n-1}(u)\rho^{n-2}(u)\cdots\rho(u)u)=t_0^{-1}\tau(t_0)$.

Proof. Let A be a cyclic $(\mathfrak{H}, \zeta)$-extension of B such that $A \supseteqq T$, A/T is a strongly cyclic $(\mathfrak{G}, \zeta)$-extension, $\eta | T = \tau$ and $\eta^m = \sigma$. Then there exists a η^m-generator x for A/T. Set $t_0 = x^n$. Then $x^n \in U(T)$. Since $\eta^m(x^{-1}tx) = x^{-1}tx$ for each $t \in T$, $\rho = \widetilde{x^{-1}}$ is an automorphism of T with $\rho(t_0) = t_0$. Set $u = x^{-1}\eta(x)$. Then $\eta^m(u) = x^{-1}\zeta\eta(x)\zeta^{-1} = x^{-1}\eta(x) = u$ shows that $u \in U(T)$. For $t \in T$, $\rho\tau\rho^{-1}\tau^{-1}(t) = \rho\tau(x\tau^{-1}(t)x^{-1}) = \rho(\eta(x)t\eta(x^{-1})) = x^{-1}\eta(x)t$ $\eta(x)x = \tilde{u}(t)$. This implies $\rho\tau\rho^{-1}\tau^{-1} = \tilde{u}$. Further, $RN_m(u, \tau) = (x^{-1}\eta(x))\eta(x^{-1}$ $\eta(x))\eta^2(x^{-1}\eta(x)) \cdots \eta^{m-1}(x^{-1}\eta(x)) = x^{-1}\eta^m(x) = \zeta^{-1}$. Next, $LN_n(u ; \rho) = \rho^{n-1}(x^{-1}$ $\eta(x))\rho^{n-2}(x^{-1}\eta(x)) \cdots \rho(x^{-1}\eta(x))x^{-1}\eta(x) = x^{-n}\eta(x^n) = t_0^{-1}\tau(t_0)$. Consequently, we can see that there exist an automorphism ρ and elements t_0, u satisfying the conditions (a)—(e).

Conversely, assume that there exist an automorphism ρ and elements t_0, u satisfying the conditions (a)—(e). Then the map Ψ of $T[X ; \rho]$ defined by $\sum_i X^i u_i \longmapsto \sum_i (Xu)^i \tau(u_i)$ $(u_i \in T)$ is an automorphism of order nm. For, $\Psi(tX) = \Psi(X\rho(t)) = Xu\tau\rho(t)$ and $\Psi(t)\Psi(X) = \tau(t)Xu = X\rho\tau(t)u$ show that Ψ is a homomorphism if and only if there holds (c). Noting that $\Psi^m(X) = XRN_m(u ; \tau)$, (d) implies that $\Psi^{nm} = 1$, and hence Ψ is an automorphism. $\Psi(X^n - t_0) = (Xu)^n - \tau(t_0) = X^n LN_n(u ; \rho) - \tau(t_0) = (X^n - t_0)LN_n$ $(u ; \rho)$ by (e). Thus Ψ induces an automorphism η^* of order nm in $T[X ; \rho]/(X^n - t_0) = T \oplus yT \oplus \cdots \oplus y^{n-1}T = A^*$, where y is the residue class of X modulo $(X^n - t_0)$. By Theorem 1. 1, it is clear that $(\eta^*)_T \equiv \{\nu \in (\eta^*) | \nu(t) = t$ for all $t \in T\} = (\eta^{*m})$, A^*/B is a cyclic $((\eta^*), \zeta)$-extension by [5, Lemma 1. 1].

2. Abelian $(\mathfrak{H}, \zeta)$-extension with $\mathfrak{H} = (\eta_1) \times (\eta_2) \times \cdots \times (\eta_e)$

In this section, we assume that $\mathfrak{G} = (\sigma_1) \times (\sigma_2) \times \cdots \times (\sigma_e)$ where every (σ_i) is a cyclic group of order n_i generated by σ_i and $n = \prod_{i=1}^e n_i$. Firstly, we shall state several remaks without proofs.

Let ρ_i $(i = 1, 2, \cdots, e)$ be automorphisms of B, b_i $(i = 1, 2, \cdots, e)$ elements of $U(B)$ and b_{ij} $(i, j = 1, 2, \cdots, e)$ elements of $U(B)$ with $b_{ij} = b_{ji}^{-1}$ and $b_{ii} = 1$. If they satisfy

$$\rho_i\rho_j\rho_i^{-1}\rho_j^{-1} = \tilde{b}_{ij} \quad \text{and}$$
$$b_{ij}(\rho_j b_{ik})b_{jk} = \rho_i(b_{jk})b_{ik}\rho_k(b_{ij}),$$

then the set of polynomials of e indeterminates $\mathscr{B} \equiv B[X_1, X_2, \cdots, X_e ; \rho_1, \rho_2, \cdots, \rho_e] = \{\sum X_1^{\nu_1} X_2^{\nu_2} \cdots X_e^{\nu_e} b_{\nu_1 \cdots \nu_e} | b_{\nu_1 \cdots \nu_e} \in B\}$ forms a ring if we define the multiplication by the distributive law and the rules $bX_i = X_i\rho_i(b)$ $(b \in B)$ and $X_iX_j = X_jX_ib_{ij}$ [4, Proposition 2. 2]. Further, if there holds

$$\rho_i^{n_i}=\tilde{b}_i^{-1},\ \ \rho_i(b_i)=b_i \ \text{ and}$$
$$RN_{n_i}(b_{ji}\,;\,\rho_i)=\rho_j(b_i^{-1})b_i\,,$$

then the polynomials $X_i^{n_i}b_i^{-1}-1$ are central in $\mathscr{B}$.

Let $k\leqq e$, and π an arbitrary permutation of $\{1, 2, \cdots, k\}$. Then $B[X_1, X_2, \cdots, X_k\,;\,\rho_1, \rho_2, \cdots, \rho_k]\cong B[X_{\pi(1)}, X_{\pi(2)}, \cdots, X_{\pi(k)}\,;\,\rho_{\pi(1)}, \rho_{\pi(2)}, \cdots, \rho_{\pi(k)}]$ ([4, Proposition 2. 2]).

Let $M_{k-1}=(X_1^{n_1}-b_1, X_2^{n_2}-b_2, \cdots, X_{k-1}^{n_{k-1}}-b_{k-1})$. Then $B[X_1, X_2, \cdots, X_{k-1}\,;\,\rho_1, \rho_2, \cdots, \rho_{k-1}]/M_{k-1}=B[y_1, y_2, \cdots, y_{k-1}]=\bigoplus_{0\leqq\nu_i<n_i} y_1^{\nu_1}y_2^{\nu_2}\cdots y_{k-1}^{\nu_{k-1}}B$, where y_i is the residue class of X_i modulo M_{k-1}. Further, $B[y_1, y_2, \cdots, y_{k-1}][X_k\,;\,\rho_k]=\{\sum X_k^{\nu}a_\nu\,|\,a_\nu\in B[y_1, y_2, \cdots, y_{k-1}]\}$ forms a ring if we define the multiplication by the distributive law and the rule $aX_k=X_kP_k(a)$ $(a_\nu\in B[y_1, y_2, \cdots, y_{k-1}])$, where P_k is an automorphism of $B[y_1, y_2, \cdots, y_{k-1}]$ defined by $P_k|B=\rho_k$ and $P_k(y_i)=y_ib_{ik}$. Moreover, the polynomial $X_k^{n_k}b_k^{-1}-1$ is a central polynomial of $B[y_1, y_2, \cdots, y_{k-1}][X_k\,;\,\rho_k]$ and $B[y_1, y_2, \cdots, y_k]\cong B[y_1, y_2, \cdots, y_{k-1}][X_k\,;\,\rho_k]/(X_k^{n_k}-b_k)B[y_1, y_2, \cdots, y_{k-1}][X_k\,;\,\rho_k]$. We denote this residue class ring by A_k.

Now the set of polynomials $\{X_1^{n_1}-b_1, X_2^{n_2}-b_2, X_3^{n_3}-b_3, \cdots, X_e^{n_e}-b_e\}$ of $\mathscr{B}$ will be called *a system of directly indecomposable polynomials* if $X_k^{n_k}-b_k$ is directly indecomposable in $B[y_1, y_2, \cdots, y_{k-1}][X_k\,;\,\rho_k]$.

Corresponding to Theorem 1. 1, we shall prove the following

Theorem 2.1. *In order that B have a strongly abelian $(\mathfrak{G}, \zeta)$-extension A such that for every $\mathfrak{G}_i=(\sigma_{i+1})\times(\sigma_{i+2})\times\cdots\times(\sigma_e)$ $(0\leqq i\leqq e-1)$, $A^{\mathfrak{G}_i}$ has no proper central idempotents, it is necessary and sufficient that there exist automorphisms $\{\rho_i\,;\, i=1, 2, \cdots, e\}$ of B, and elements $\{b_i, b_{ij}\,|\,i, j=1, 2, \cdots, e\}$ in $U(B)$ with $b_{ij}=b_{ji}^{-1}$ and $b_{ii}=1$ such that*

(a) $\rho_i\rho_j\rho_i^{-1}\rho_j^{-1}=\tilde{b}_{ij}$,

(b) $b_{ij}(\rho_jb_{ik})b_{jk}=\rho_i(b_{jk})b_{ik}\rho_k(b_{ij})$,

(c) $\rho_i^{n_i}=\tilde{b}_i^{-1}$, $\rho_i(b_i)=b_i$ *and* $\rho_i(\zeta)=\zeta$,

(d) $RN_{n_i}(b_{ji}\,;\,\rho_i)=\rho_j(b_i^{-1})b_i$,

(e) $\{X_i^{n_i}-b_i\,|\,i=1, 2, \cdots, e\}$ *is a system of directly indecomposable polynomials.*

More precisely, if there exist automorphisms $\{\rho_i\,|\,i=1, 2, \cdots, e\}$, elements $\{b_i, b_{ij}\,|\,i, j=1, 2, \cdots, e\}$ with $b_{ij}=b_{ji}^{-1}$ and $b_{ii}=1$ satisfying (a)−(e), *then $M_i=(X_1^{n_1}-b_1, X_2^{n_2}-b_2, \cdots, X_i^{n_i}-b_i)B[X_1, X_2, \cdots, X_i\,;\,\rho_1, \rho_2, \cdots, \rho_i]$ is a two sided ideal of $B[X_1, X_2, \cdots, X_i\,;\,\rho_1, \rho_2, \cdots, \rho_i]$ and $A_i^*=B[y_1, y_2, \cdots, y_i]=B[X_1, X_2, \cdots, X_i\,;\,\rho_1, \rho_2, \cdots, \rho_i]/M_i$ is a strongly abelian*

$(\mathfrak{G}_i^*, \zeta^{n_1\cdots n_i})$-extension with $\mathfrak{G}_i^*=(\sigma_{i+1}^*)\times(\sigma_{i+2}^*)\times\cdots\times(\sigma_e^*)$, where y_j is the residue class of X_j modulo M_i and σ_s^* is defined by $\sigma_s^*(y_s)=y_s\zeta^{n/n_s}$, $\sigma_s^*(y_j)=y_j$ for $j\neq s$.

Conversely, if A is a strongly abelian $(\mathfrak{G}, \zeta)$-extension of B such that $A^{\mathfrak{G}_i}$ has no proper central idempotents, then we can find such $\{\rho_i|i=1, 2, \cdots, e\}$, $\{b_i, b_{ij}|i, j=1, 2, \cdots, e\}$ with $b_{ij}=b_{ji}^{-1}$, $b_{ii}=1$ satisfying (a)—(e) *that there exists a B-isomorphism $\varphi_i^*: A_i^*\longrightarrow A^{\mathfrak{G}_i}$ with $\varphi_i^*\sigma_j^*=\sigma_j\varphi_i^*$ for every $i, j=1, 2, \cdots, e$.*

Proof. Necessity: Let A be a strongly abelian $(\mathfrak{G}, \zeta)$-extension of B such that $A^{\mathfrak{G}_i}$ has no proper central idempotents for $i=1, 2, \cdots, e$. By Definition 2 and by making use of the same method as in the proof of Lemma 1. 1, we obtain elements $x_i\in U(B_i)$ $(1\leqq i\leqq e)$ such that $\sigma_i(x_i)=x_i\zeta_i^{-1}$ and $\sigma_i(x_j)=x_j$ for $i\neq j$ where $\zeta_i=\zeta^{n/n_i}$ and $B_i=A^{\mathfrak{G}_i}$. Then it is clear that $x_i^{-1}bx_i\in B (b\in B)$ and $x_i^{n_i}, x_ix_jx_i^{-1}x_j^{-1}\in U(B)$. We set $\rho_i=\tilde{x}_i^{-1}$, $b_i=x_i^{n_i}$ and $b_{ij}=x_i^{-1}x_j^{-1}x_ix_j$. Then they satisfy (c).

(a) $\rho_i\rho_j\rho_i^{-1}\rho_j^{-1}(b)=x_i^{-1}x_j^{-1}x_ix_jbx_j^{-1}x_i^{-1}x_jx_i=b_{ij}bb_{ij}^{-1}=\tilde{b}_{ij}(b)$.

(b) $$\begin{aligned} b_{ij}\rho_j(b_{ik})b_{jk} &= x_i^{-1}x_j^{-1}x_ix_j(x_j^{-1}x_i^{-1}x_k^{-1}x_ix_kx_j)\cdot x_j^{-1}x_k^{-1}x_jx_k \\ &= x_i^{-1}x_j^{-1}x_k^{-1}x_ix_jx_k=(x_i^{-1}x_j^{-1}x_k^{-1}x_jx_kx_i)(x_i^{-1}x_k^{-1}x_ix_k)\cdot \\ &\quad (x_k^{-1}x_i^{-1}x_j^{-1}x_ix_jx_k)=\rho_i(b_{jk})b_{ik}\rho_k(b_{ij}). \end{aligned}$$

(d) $$\begin{aligned} RN_{n_i}(b_{ji}; \rho_i) &= (x_j^{-1}x_i^{-1}x_jx_i)x_i^{-1}(x_j^{-1}x_i^{-1}x_jx_i)x_ix_i^2(x_j^{-1}x_i^{-1}x_jx_i)x_i^2\cdots \\ &\quad x_i^{1-n_i}(x_j^{-1}\cdot x_i^{-1}x_jx_i)x_i^{n_i-1}=x_jx_i^{-n_i}x_jx_i^{n_i}=\rho_j(b_i^{-1})b_i. \end{aligned}$$

As to (e), we first consider $T=B[x_1, x_2, \cdots, x_e]=\sum_{0\leq\nu_i<n_i}x_1^{\nu_1}x_2^{\nu_2}\cdots x_e^{\nu_e}B$. Then T is a $\mathfrak{G}$-(setwise) invariant subring of A with $T^{\mathfrak{G}}=B$. By the similar method as in the proof of [4, Theorem 2. 1], we can easily see that $\{x_1^{\nu_1}x_2^{\nu_2}\cdots x_e^{\nu_e}|0\leqq\nu_i<n_i\}$ is a B-right linearly independent set. Let $\tau=\sigma_1^{l_1}\sigma_2^{l_2}\cdots\sigma_i^{l_i}\cdots\sigma_e^{l_e}$ be an arbitrary element of $\mathfrak{G}$. Then by making use of the same method as in the proof of Theorem 1. 1, we can easily see the existence of elements $\{c_1^{(i)}, c_2^{(i)}, \cdots, c_t^{(i)}; d_1^{(i)}, d_2^{(i)}, \cdots, d_t^{(i)}\}$ in $B[x_i]$ such that

$$\delta_{1,\tau_i}=\sum_j c_j^{(i)}\tau_i(d_j^{(i)}) \text{ for } \tau_i=\sigma_i^{l_i}.$$

Since $\sum_j c_j^{(i)}\tau(d_j^{(i)})=\sum_j c_j^{(i)}\sigma_i^{l_i}(d_j^{(i)})$, it follows that

$$\delta_{1,\tau}=\sum_{(j_e, j_{e-1},\cdots,j_1)} c_{j_e}^{(e)}c_{j_{e-1}}^{(e-1)}\cdots c_{j_1}^{(1)}\tau(d_{j_1}^{(1)}d_{j_2}^{(2)}\cdots d_{j_e}^{(e)}).$$

This means the existence of a $\mathfrak{G}$-Galois coordinate system for T/B. Thus we obtain $T=A$. Noting here that $A^{\mathfrak{G}_i}/B$ is $(\sigma_1)\times(\sigma_2)\times\cdots\times(\sigma_i)$-Galois, the above argument enables us to see $A^{\mathfrak{G}_i}=B[x_1, x_2, \cdots, x_i]$. While,

$B[X_1, X_2, \cdots, X_i; \rho_1, \rho_2, \cdots, \rho_i]/M_i \cong A_{i-1}[X_i; \rho_i]/(X_i^{n_i}-b_i)A_{i-1}[X_i; \rho_i] \cong A^{\mathfrak{G}_i}$. Hence there holds (e).

Let φ^* be the map of $\mathscr{B}$ to $A=B[x_1, x_2, \cdots, x_e]$ defined by $f(X_1, X_2, \cdots, X_e) \longmapsto f(x_1, x_2, \cdots, x_e)$. Then φ^* is a B-(ring) epimorphism and its kernel contains M_e. On the other hand, we can write $f(X_1, X_2, \cdots, X_e) = (X_1^{n_1}-b_1)\, g_1(X_1, X_2, \cdots, X_e) + (X_2^{n_2}-b_2)\, g_2(X_1, X_2, \cdots, X_e) + \cdots + (X_e^{n_e}-b_e)\, g_e(X_1, X_2, \cdots, X_e) + r(X_1, X_2, \cdots, X_e)$ with a polynomial $r(X_1, X_2, \cdots, X_e)$ whose degree with respect to each X_i is smaller than n_i. Hence we have $\mathscr{B}/M_e \cong A$.

Sufficiency: Assume that there exist automorphisms $\{\rho_i \mid i=1, 2, \cdots, e\}$ and $\{b_i, b_{ij} \mid i, j=1, 2, \cdots, e\}$ with $b_{ij}=b_{ji}^{-1}$ and $b_{ii}=1$ satisfying (a)—(e). Then, by (e), $A^* = \bigoplus_{0 \leq \nu_i < n_i} y_1^{\nu_1} y_2^{\nu_2} \cdots y_e^{\nu_e} B \cong \mathscr{B}/M_e$ has no proper central idempotents, where y_i is the residue class of X_i modulo M_e. By (c), the map Ψ_i of $\mathscr{B}$ defined by $f(X_1, X_2, \cdots, X_i, \cdots, X_e) \longmapsto f(X_1, X_2, \cdots, X_i\zeta_i^{-1}, \cdots, X_e)$ is an automorphism of order n_i and each $X_j^{n_j} b_j^{-1}-1$ is central by (d), Ψ_i induces an automorphism σ_i^* of order n_i of A^*. If $\mathfrak{G}^*$ is the group generated by $\sigma_1^*, \sigma_2^*, \cdots, \sigma_e^*$, then $\mathfrak{G}^* = (\sigma_1^*) \times (\sigma_2^*) \times \cdots \times (\sigma_e^*)$ and $A^{*\mathfrak{G}^*} = B$. Since $B_i^* = A^{*\mathfrak{G}_i^*} = B[y_i]$, $y_i + \zeta_i \sigma_i^*(y_i) + \cdots + \zeta_i^{n_i-1} \sigma_i^{*n_i-1}(y_i) = n_i y_i$ is a unit. The existence of a $\mathfrak{G}^*$-Galois coordinate system for A^*/B will be seen as in the necessity part. Finally, $A^{*\mathfrak{G}_i^*} = B[y_1, y_2, \cdots, y_i] \cong B[y_1, y_2, \cdots, y_{i-1}][X_i; \rho_i]/(X_i^{n_i}-b_i)\, B[y_1, y_2, \cdots, y_{i-1}][X_i; \rho_i]$, which contains no proper central idempotents by (e). The rest of the proof will be almost evident.

Corollary 2.1. *If A is a strongly abelian $(\mathfrak{G}, \zeta)$-extension of B such that $A^{\mathfrak{G}_i}$ has no proper central idempotents for each $i=1, 2, \cdots, e$, then A is B-free.*

Now, corresponding to Theorem 1. 2, we shall prove the following

Theorem 2.2. *Let T be an abelian $(\mathfrak{T}, \zeta)$-extension of B where $\mathfrak{T} = (\tau_1) \times (\tau_2) \times \cdots \times (\tau_e)$ is a direct product of cyclic groups (τ_i) of order m_i. Let $\mathfrak{H} = (\eta_1) \times (\eta_2) \times \cdots \times (\eta_e)$ a direct product of cyclic groups (η_i) of order $n_i m_i$, and $\prod_{i=1}^{e} n_i = n$. Then, in order that B have an abelian $(\mathfrak{H}, \zeta)$-extension A such that $A \supseteqq T$, A/T is a strongly abelian $(\mathfrak{G}, \zeta)$-extension, $\eta_i \mid T = \tau_i$, $\eta_i^{m_i} = \sigma_i$ and the fixring of $\mathfrak{G}_i = (\sigma_{i+1}) \times (\sigma_{i+2}) \times \cdots \times (\sigma_e)$ in A has no proper central idempotents $(i=1, 2, \cdots, e)$, it is necessary and sufficient that there exist automorphisms $\{\rho_i \mid i=1, 2, \cdots, e\}$ of T, elements $\{t_i, t_{ij} \mid i, j=1, 2, \cdots, e\}$ in $U(T)$ with $t_{ij}=t_{ji}^{-1}$, $t_{ii}=1$ satisfying the conditions* (a)—(e) *of Theorem* 2. 1 *(T replacing B) and there exist* *elements* $\{u_{ij}\,;\, i, j=1, 2, \cdots, e\}$ *in* $U(T)$ *satisfying*

(f) $\tau_i\rho_j\tau_i^{-1}\rho_j^{-1}=\tilde{u}_{ji}^{-1}$,

(g) $RN_{m_i}(u_{ii}\,;\,\tau_i)=\zeta_i^{-1},\quad RN_{m_j}(u_{ij}\,;\,\tau_j)=1\quad (i\neq j)$,

(h) $LN_{n_j}(u_{ji}\,;\,\rho_j)=t_j^{-1}\tau_i(t_j)$,

(i) $t_{ij}(\rho_j u_{ik})u_{jk}=(\rho_i u_{jk})\tau_k(t_{ij})$,

(j) $u_{ki}\tau_i(u_{ik})=u_{kj}\tau_i(u_{ki})$.

Proof. Necessity: Let A be an extension requested in the theorem. Then there exist elements $x_1, x_2, \cdots, x_e$ in $U(T)$ such that $\eta_i^{m_i}(x_i)=x_i\zeta_i^{-1}$ and $\eta_i^{m_i}(x_j)=x_j$ for each $i\neq j$ where $\rho_i=\zeta^{m_i}$ (see the proof of Theorem 2. 1). We set $t_i=x_i^{n_i}\in U(T)$, $t_{ij}=x_i^{-1}x_j^{-1}x_ix_j\in U(T)$ and $\rho_i=\tilde{x}_i^{-1}$. Then they satisfy the conditions (a)$-$(e), and $A=T[x_1, x_2, \cdots, x_e]\cong\mathscr{T}/M$ by $x_i\longmapsto X_i+M$ where $\mathscr{T}=T[X_1, X_2, \cdots, X_e\,;\,\rho_1, \rho_2, \cdots, \rho_e]$ and $M=(X_1^{n_1}-t_1, X_2^{n_2}-t_2, \cdots, X_e^{n_e}-t_e)$. Now, we set $u_{ij}=x_i^{-1}\eta_j(x_i)$. Then $\eta_k^{m_k}(u_{ij})=u_{ij}$ for each $k=1, 2, \cdots, e$. Hence $u_{ij}\in U(T)$. In the following, we shall show that u_{ij} satisfies the conditions (f)$-$(j).

(f) $\tau_i\rho_j\tau_i^{-1}\rho_j^{-1}(t)=\tau_i\rho_j(t_i^{-1}(x_j)\eta_i^{-1}(t)\eta_i^{-1}(x_j^{-1}))=\tau_i(x_j^{-1}\eta_i^{-1}(x_j)\eta_i^{-1}(t)$ $\eta_i^{-1}(x_j^{-1})x_j)=\eta_i(x_j^{-1})x_jtx_j^{-1}\eta_i(x_j)=\tilde{u}_{ji}^{-1}(t)$.

(g) $RN_{m_i}(u_{ii}\,;\,\tau_i)=x_i^{-1}\eta_i(x_i)\eta_i(x_i^{-1})\eta_i^2(x_i)\cdots\eta_i^{m_i-1}(x_i^{-1})\eta_i^{m_i}(x_i)=x_i^{-1}$ $\eta_i^{m_i}(x_i)=\zeta_i^{-1}$.

$RN_{m_j}(u_{ij}\,;\,\tau_j)=(x_i^{-1}\eta_j(x_i))(\eta_j(x_i^{-1})\eta_j^2(x_i))\cdots(\eta_j^{m_j-1}(x_i^{-1})\eta_j^{m_j}(x_i))=x_i^{-1}$ $\eta_j^{m_j}(x_i)=1$.

(h) $LN_{n_j}(u_{ji}\,;\,\rho_j)=x_j^{1-n_j}x_j^{-1}\eta_i(x_j)x_j^{n_j-1}x_j^{-1}\eta_i(x_j)x_j^{n_j-1}\cdots x_j^{-1}x_j^{-1}\eta_i(x_j)$ $x_jx_j^{-1}\eta_i(x_j)=x_j^{-n_j}\eta_i(x_j^{n_j})=t_j^{-1}\tau_i(t_j)$.

(i) $t_{ij}(\rho_ju_{ik})u_{jk}=x_i^{-1}x_j^{-1}x_ix_j(x_j^{-1}x_i^{-1}\eta_k(x_i)x_j)x_j^{-1}\eta_k(x_j)=\rho_i(u_{jk})u_{ik}(\tau_k(t_{ij}))$.

(j) $u_{ki}(\tau_iu_{kj})=x_k^{-1}\eta_i(x_k)\eta_i(x_k^{-1}\eta_j(x_k))=x_k^{-1}\eta_i\eta_j(x_k)=x_k^{-1}\eta_j\eta_i(x_k)=x_k^{-1}$ $\eta_j(x_k)\eta_j(x_k^{-1}\eta_i(x_k))=u_{kj}\tau_j(u_{ki})$.

Sufficiency: Assume there exist $\{\rho_i, t_i, t_{ij}$ and $u_{ij}\,|\,i, j=1, 2, \cdots, e\}$ satisfying the conditions (a)$-$(j). Then the map Ψ_i of $\mathscr{T}$ defined by $\sum X_1^{\nu_1}X_2^{\nu_2}\cdots X_e^{\nu_e}t_{\nu_1\cdots\nu_e}\longmapsto\sum(X_1u_{1i})^{\nu_1}(X_2u_{2i})^{\nu_2}\cdots(X_eu_{ei})^{\nu_e}\tau_i(t_{\nu_1\cdots\nu_e})$ is an automorphism by (f) and (h), and its order is n_im_i by (g) ([4, Theorem 4. 2]). Next, $\Psi_i(X_j^{n_j}-t_j)=X_j^{n_j}LN_{n_j}(u_{ji}\,;\,\rho_j)-\tau_i(t_j)$ implies $\Psi_i(X_j^{n_j}-t_j)=(X_j^{n_j}-t_j)t_j^{-1}\tau_i(t_j)$ by (h). Hence each Ψ_i induces respectively τ_i and an automorphism η_i^* of order n_im_i on T and $A^*=\bigoplus_{0\leq\nu_i<n_i}y_1^{\nu_1}y_2^{\nu_2}\cdots y_e^{\nu_e}T=\mathscr{T}/M_e$,

where each y_i is the residue class of X_i modulo M_e. Now $\eta_i^*\eta_j^*(y_k) = \eta_i^*(y_k u_{kj}) = y_k u_{ki}\tau_i(u_{kj})$ and $\eta_j^*\eta_i^*(y_k) = \eta_j^*(y_k u_{ki}) = y_k u_{kj}\tau_j(u_{ki})$ show that $\eta_i^*\eta_j^* = \eta_j^*\eta_i^*$ by (j). By a brief computation, we can see that the group $\mathfrak{H}^*$ generated by $\eta_1^*, \eta_2^*, \cdots, \eta_e^*$ is $(\eta_1^*)\times(\eta_2^*)\times\cdots\times(\eta_e^*)$ and $A^{*\mathfrak{H}^*} = B$. Let $\mathfrak{G}^* = (\eta_1^{*m_1})\times(\eta_2^{*m_2})\times\cdots\times(\eta_e^{*m_e})$. Then by (g), we have $\eta_i^{*m_i}(y_i) = y_i\zeta_i^{-1}$ and $\eta_i^{*m_i}(y_j) = y_j$ for $i \neq j$. Hence A^*/T is a strongly abelian $(\mathfrak{G}^*, \zeta)$-extension. Since $\mathfrak{H}^* | T = \mathfrak{T}$ and $\mathfrak{H}^*_T = \mathfrak{G}^*$, A^*/B is an abelian $(\mathfrak{H}^*, \zeta)$-extension ([5, Lemma 1. 1]).

3. Cyclic extensions of commutative rings

In this section, $\mathfrak{G}$ will be a cyclic group of order n generated by σ. As has been observed in §1, if A is a strongly cyclic $(\mathfrak{G}, \zeta)$-extension of B, then $A = B[x]$ for some $x \in A$ (Corollary 1. 1). Hence, if an algebra A is a strongly cyclic $(\mathfrak{G}, \zeta)$-extension over B, then A is commutative. However, DeMeyer proved that any cyclic Galois algbera is commutative ([2, Theorem 11]). In the rest we assume that rings are commutative.

The following lemma gives a sufficient condition for a cyclic $(\mathfrak{G}, \zeta)$-extension to be strongly cyclic.

Lemma 3.1. *Let A be a cyclic $(\mathfrak{G}, \zeta)$-extension of B, and x an element of A with $\sigma(x) = x\zeta^{-1}$. Then the following conditions are equivalent*:

(1) *$B[x]$ is separable over B.*

(2) *x is a unit.*

(3) *$\{1, x, x^2, \cdots, x^{n-1}\}$ is a free B-basis for A.*

Proof. (2) → (3) is already shown in Corollary 1. 1 and (3) → (1) is obvious. If $B[x]$ is separable over B then, by [3, Lemma 2. 1 and Lemma 2. 7], $x - \sigma(x) = x - x\zeta^{-1} = x(1-\zeta^{-1})$ is a unit in A and hence so is x.

Remark. In [3, Definition 5], a strongly separable B algebra A without proper idempotents is called a splitting ring for the separable polynomial $f(X)$ if $f(X)$ is a product of linear factors from $A[X]$ and if A is generated over B by the roots of $f(X)$. By [3, Proposition 2. 6] and Lemma 3. 1, we can see that A is a strongly cyclic $(\mathfrak{G}, \zeta)$-extension of B if and only if A is a splitting ring for a directly indecomposable separable polynomial $X^n - b_0$ with $b_0 \in U(B)$.

Lemma 3.2. *Let A be a cyclic $(\mathfrak{G}, \zeta)$-extension of B. If B has a $\mathfrak{G}$-normal basis then it is strongly cyclic.*

Proof. Let a be a normal basis element of A. Then $A=aB\oplus\sigma(a)B \oplus\cdots\oplus\sigma^{n-1}(a)B$ shows that an element y of A is contained in $\mathfrak{p}A$, where $\mathfrak{p}$ is a maximal ideal of B, if and only if $y=\sum_{i=0}^{n-1}\sigma^i(a)p_i$, $p_i\in\mathfrak{p}$. Let $x=a+\zeta\sigma(a)+\cdots+\zeta^{n-1}\sigma^{n-1}(a)$. Then $\sigma(x)=x\zeta^{-1}$ and $x\notin\mathfrak{p}A$ for each maximal ideal $\mathfrak{p}$ of B. While $A/\mathfrak{p}A$ is a Galois extension of the field $(B+\mathfrak{p}A)/\mathfrak{p}A\cong B/\mathfrak{p}$, $A/\mathfrak{p}A$ is a direct sum of a finite number of fields. Thus it contains no non-zero nilpotent element. Now, if we assume that $x^n\in\mathfrak{p}$ for some $\mathfrak{p}$, it yields a contradiction $x\in\mathfrak{p}A$. Thus $x^n\notin\mathfrak{p}$. Consequently, x^n and hence x is a unit.

Since a Galois extension of a semi-local ring is semi-local, the following result is a direct consequence of Lemma 3. 2 and Theorem 1. 1. (Cf. the necessity part of the proof of Theorem 1. 1.)

Corollary 3.1. *Let B be semi-local. In order that B have a cyclic $(\mathfrak{G}, \zeta)$-extension, it is necessary and sufficient that there exists an element b_0 in $U(B)$ such that X^n-b_0 is directly indecomposable in $B[X]$.*

Theorem 3.1. *Let T be a cyclic $(\mathfrak{T}, \zeta)$-extension of a semi-local ring B where $\mathfrak{T}$ is of order m and is generated by τ. Let $\mathfrak{H}$ be a cyclic group of order nm with a generator η. In order that B have a cyclic $(\mathfrak{H}, \zeta)$-extension A with $A\supseteqq T$, $\eta|T=\tau$ and $\eta^m=\sigma$, it is necessary and sufficient that there exist elements t_0 and u in $U(T)$ satisfying*

(a) X^n-t_0 *is directly indecomposable in* $T[X]$

(b) $N_\tau(u)(=u\tau(u)\tau^2(u)\cdots\tau^{m-1}(u))=\zeta^{-1}$

(c) $\tau(t_0)=t_0u^n$

Proof. Assume first that there exist elements t_0, u in $U(T)$ satisfying the conditions (a), (b) and (c). Then $\rho=1$, t_0 and u satisfy the conditions (a)−(e) of Theorem 1. 2.

Conversely, we assume that A is a cyclic $(\mathfrak{H}, \zeta)$-extension of B with $A\supseteqq T$ and $\eta|T=\tau$. Then A/T is a cyclic $((\eta^m), \zeta)$-extension. Hence by Lemma 3. 2, A/T is a strongly cyclic $((\eta^m), \zeta)$-extension. Now, the rest is clear from the proof of Theorem 1. 2.

As an immediate consequence of [3, Corollary 2. 10], we see that if a separable polynomial is irreducible then it is directly indecomposable. Now, we shall prove the following

Theorem 3.2. *Let B be a domain. In order that B have a strongly cyclic $(\mathfrak{G}, \zeta)$-extension A which is a domain, it is necessary and sufficient that there exists an element b_0 in $U(B)$ such that $X^n - b_0$ is irreducible in $K[X]$ where K is the quotient field of B.*

Proof. Let A be a strongly cyclic $(\mathfrak{G}, \zeta)$-extension of B which is a domain. Then by Theorem 1. 1, we have $A \cong B[X]/(X^n - b_0)$ for some $b_0 \in U(B)$. Since A is a domain, it follows that $X^n - b_0$ is irreducible in $K[X]$. The converse is almost evident.

4. Abelian extensions of commutative rings

In this section, we assume that $\mathfrak{G} = (\sigma_1) \times (\sigma_2) \times \cdots \times (\sigma_e)$, where every (σ_i) is a cyclic group of order n_i generated by σ_i and $n = \Pi_{i=1}^{e} n_i$.

Corresponding to Theorem 2. 1, we shall prove the following

Theorem 4.1. *In order that B have a strongly abelian $(\mathfrak{G}, \zeta)$-extension A, it is necessary and sufficient that there exist elements $b_1, b_2, \cdots, b_e$ in $U(B)$ such that $\{X_1^{n_1} - b_1, X_2^{n_2} - b_2, \cdots, X_e^{n_e} - b_e\}$ is a system of indecomposable polynomials in $B[X_1, X_2, \cdots, X_e]$. Moreover, if this is the case, $A = A^{\mathfrak{G}_1} \otimes_B A^{\mathfrak{G}_2} \otimes \cdots \otimes_B A^{\mathfrak{G}_e}$.*

Proof. Let A be a strongly abelian $(\mathfrak{G}, \zeta)$-extension of B. Then, as is shown in Theorem 2. 1, there exist elements $x_1, x_2, \cdots, x_e$ in $U(A)$ such that $\sigma_i(x_i) = x_i \zeta_i^{-1}$, $\sigma_i(x_j) = x_j$ for $i \neq j$ and $A = B[x_1, x_2, \cdots, x_e]$. Set $B_i = B[x_i]$. Then $B_i = B \oplus x_i B \oplus \cdots \oplus x_i^{n_i - 1} B$, $b_i = x_i^{n_i} \in U(B)$, $A^{\mathfrak{G}_i} = B_i$, B_i/B is a strongly cyclic $((\sigma_i), \zeta)$-extension and $A^{\mathfrak{G}_i} = B[x_1, x_2, \cdots, x_i] \cong B[x_1, x_2, \cdots, x_{i-1}][X_i]/(X_i^{n_i} - b_i)B[x_1, x_2, \cdots, x_{i-1}][X_i]$. By the same argument as in the proof of [5, Theorem 4. 1], we can easily see that $A = B_1 \otimes_B B_2 \otimes \cdots \otimes_B B_e$.

Conversely, assume that there exist elements $b_1, b_2, \cdots, b_e$ in $U(B)$ satisfying the condition. If we set $\rho_i = 1$, $b_{ij} = 1$, $i, j = 1, 2, \cdots, e$, $\{\rho_i, b_i$ and $b_{ij} \mid i, j = 1, 2, \cdots, e\}$ satisfies the conditions (a)—(e) of Theorem 2. 1. Hence $A^* = B[X_1, X_2, \cdots, X_e]/M_e$ is a requested extension.

Now, corresponding to Theorem 2. 2, we shall give a necessary and sufficient condition that there holds the embedding theorem for abelian extensions of commutative rings.

First we have the following theorem which is a direct consequence of Theorem 2. 2.

Theorem 4.2. *Let T be an abelian $(\mathfrak{T}, \zeta)$-extension of B where*

$\mathfrak{T}=(\tau_1)\times(\tau_2)\times\cdots\times(\tau_e)$ is a direct product of cyclic groups (τ_i) of order m_i. Let $\mathfrak{H}=(\eta_1)\times(\eta_2)\times\cdots\times(\eta_e)$ be a direct product of cyclic groups of (η_i) of order $n_i m_i$, and $\Pi_{i=1}^{e} n_i=n$. Then, in order that $A\supseteqq T$, A/T is a strongly abelian $(\mathfrak{G},\zeta)$-extension and $\eta_i|T=\tau_i$, $\eta_i^{m_i}=\sigma_i$ it is necessary and sufficient that there exist elements $\{t_i, u_{ij}\mid i, j=1, 2, \cdots, e\}$ in $U(T)$ satisfying

(a) $N_{\tau_i}(u_{ii})=\zeta_i^{-1}$, $N_{\tau_j}(u_{ij})=1$,

(b) $u_{ij}^{n_i}=t_i^{-1}\tau_j(t_i)$,

(c) $u_{ki}\tau_i(u_{kj})=u_{kj}\tau_j(u_{ki})$,

(d) $\{X_i^{n_i}-t_i\mid i=1, 2, \cdots, e\}$ *is a system of directly indecomposable polynomials in* $T[X_1, X_2, \cdots, X_e]$.

Combining Theorem 3. 2 with Theorem 4. 2, we have the following

Theorem 4.3. *Let T be an abelian $(\mathfrak{T},\zeta)$-extension of B such that T is a domain and $\mathfrak{T}=(\tau_1)\times(\tau_2)\times\cdots\times(\tau_e)$ is a direct product of cyclic groups (τ_i) of order m_i. Let $\mathfrak{H}=(\eta_1)\times(\eta_2)\times\cdots\times(\eta_e)$ be a direct product of cyclic groups (η_i) of order $n_i m_i$, and $\Pi_{i=1}^{e} n_i=n$. Then, in order that B have an abelian $(\mathfrak{H},\zeta)$-extension domian A such that $A\supseteqq T$, A/T is a strongly abelian $(\mathfrak{G},\zeta)$-extension, $\eta_i|T=\tau_i$ and $\eta_i^{m_i}=\sigma_i$, it is necessary and sufficient that there exist elements $\{t_i, u_{ij}\mid i, j=1, 2, \cdots, e\}$ in $U(T)$ satisfying*

(a) $N_{\tau_i}(u_{ii})=\zeta_i^{-1}$, $N_{\tau_j}(u_{ij})=1$,

(b) $u_{ij}^{n_i}=t_i^{-1}\tau_j(t_i)$,

(c) $u_{ki}\tau_i(u_{kj})=u_{kj}\tau_j(u_{ki})$,

(d) $X_i^{n_i}-t_i$ *is irreducible in* $K_{i-1}[X_i]$, *where* K_{i-1} *is the quotient field of* $B[X_1, X_2, \cdots, X_{i-1}]/(X_1^{n_1}-t_1, X_2^{n_2}-t_2, \cdots, X_{i-1}^{n_{i-1}}-t_{i-1})$.

REFERENCES

[1] S. U. CHASE, D. K. HARRISON and A. ROSENBERG: Galois theory and Galois cohomology of commutative rings, Mem. Amer. Math. Soc., **52** (1965), 15—33.

[2] F. R. DEMEYER: Some notes on the general Galois theory of rings. Osaka Math. J., **2** (1965), 117—127.

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

[4] K. KISHIMOTO: On abelian extensions of simple rings, J. Fac. Sci. Hokkaido Univ., **19** (1967), 74—85.

[5] K. KISHIMOTO: On abelian extensions of rings I, Math. J. of Okayama Univ., **14** (1970), 159—174.

[6] Y. MIYASHITA: Finite outer Galois theory of non-commutative rings. J. Fac. Sci. Hokkaido univ., **19** (1966), 114—134.

[7] T. NAGAHARA and H. TOMINAGA: Galois theory of simple rings, Okayama Math. Lecture, Dept. of Math., Okayama Univ., (1970).

DEPARTMENT OF MATHEMATICS
SHINSHU UNIVERSITY

(Received January 1, 1971)