ON ABELIAN EXTENSIONS OF RINGS I

KAZUO KISHIMOTO

Introduction. In [1], M. Auslander and O. Goldman introduced the notion of a Galois extension of a commutative ring. Further, Galois theory of general rings, were developed in [2], [3], [4], [5], [8] and others.

While, in [6] and [7] the author generalized the notion of abelian extensions of fields and gave necessary and sufficient conditions for a simple ring to have an abelian simple ring extension.

In this paper, combining the method used in [6] and [7] with results of [4] and [8], we shall give the conditions for an algebra over $GF(p)$ to have a Galois extension with an abelian Galois group of order p^f.

Let B be a ring with the identity 1, A an extension ring of B with the same identity, and $\mathfrak{G}$ a finite group of automorphisms of A. Then, following [1], A is called *a Galois extension of B with a Galois group* $\mathfrak{G}$ (or a *$\mathfrak{G}$-Galois extension of* B) if the following is satisfied:

1) *$A^{\mathfrak{G}}$, the fixsubring of A of $\mathfrak{G}$, is B,*

2) *A is a finitely generated, projective B-module and the map j of $D(A, \mathfrak{G})=\sum_{\rho\in\mathfrak{G}}Au_\rho$ (the trivial crossed product of A with $\mathfrak{G}$) to* Hom(A_B, A_B) *defined by $j(au_\rho)(x)=a\rho(x)(x\in A)$ is an isomorphism.*

As is well known, 2) is equivalent to the following

2′) *there exist elements $x_1, x_2, \cdots, x_n$; $y_1, y_2, \cdots, y_n$ of A such that* $\sum_{i=1}^n x_i\rho(y_i)=\delta_{\rho,1}$ $(\rho\in\mathfrak{G})$.

A subset $\{x_1, x_2, \cdots, x_n;\ y_1, y_2, \cdots, y_n\}$ of A satisfying 2′) is called a *$\mathfrak{G}$-Galois coordinate system* for A/B.

Throughout the present paper, we assume that the base ring B is an algebra over $GF(p)$ without proper central idempotents containing the identity 1, a Galois extension is one without proper central idempotents containing the base ring as a direct summand considered as a module over the base ring.

In § **0**, for the convenience of the later discussion, we state some properties of polynomials over a ring.

In § **1**, we shall show that if A is a Galois extension of B with a cyclic Galois group $\mathfrak{G}$ of order p, then A is a residue class ring $B[X; D]/(X^p-X-b)B[X; D]$ where D is a derivation in B, X^p-X-b is a central polynomial of $B[X; D]$, and conversely (Corollary 1. 1). Next, we shall give a necessary and sufficient condition that there holds an embedding theorem for a Galois extension (Theorem 1. 2).

In § 2, we shall give a necessary and sufficient condition for B to have a $\mathfrak{G}$-Galois extension A, where $\mathfrak{G}=(\sigma_1)\times(\sigma_2)\times\cdots\times(\sigma_t)$ (a direct product of cyclic groups (σ_i) of order p with a generator σ_i) (Corollary 2. 1). Combining this with Theorem 1. 2, we obtain an extension of Theorem 1. 2 (Theorem 2. 2).

In §§ 3—5, we assume that B is commutative.

In § 3, by the aid of the fact that every cyclic algebra over B is commutative [3, Theorem 11[1]], we shall show that if A is a $\mathfrak{G}$-Galois algebra over B with a cyclic Galois group of order p, then A is a splitting ring of a separable polynomial X^p-X-b_0 in $B[X]$ (Theorem 3. 1). Next, let T and B be local rings and T a Galois algebra over B with a cyclic Galois group $\mathfrak{R}$ of order p with a generator τ. Then, for each positive integer e, there exists an $\mathfrak{H}$-Galois algebra A over B with a cyclic Galois group $\mathfrak{H}$ of order p^e with a generator σ such that $A\supseteq T$, $\sigma|T=\tau$ and A is local (Theorem 3. 3).

In § 4, we shall deal with the commutative case. Namely, if A is a commutative Galois extension of B with a Galois group $\mathfrak{G}=(\sigma_1)\times(\sigma_2)\times\cdots\times(\sigma_t)$, then we can see that $A=B_1\otimes_B B_2\otimes\cdots\otimes_B B_t$, where each B_i is a (σ_i)-Galois algebra over B (Theorem 4. 1).

In § 5, we assume that B is a domain, and consider a Galois algebra A over B with a cyclic Galois group $\mathfrak{G}$ of order p. Then, a necessary and sufficient condition for B to have A is that there exists an element b_0 in B such that $b^p-b\neq b_0$ for all $b\in B$ (Theorem 5. 1). Moreover, if A is a domain, we can see that there holds the embedding theorem without any restriction (Theorem 5. 2).

As to notations and terminologies used in this paper, we follow [2] and [7].

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

0. Preliminary results on polynomials

Let D be a derivation of B. Then, by $B[X;D]$ we denote the ring of polynomials $\{\sum_i X^i b_i\,;\, b_i\in B\}$, where the multiplication is defined by

1) Cf. [5].

the distributive law and the rule $bX=Xb+Db$ ($b\in B$). If $D=0$, we denote it by $B[X]$.

Let $\mathfrak{B}=B[X;D]$, and $f(X)$ a monic polynomial of $\mathfrak{B}$.

1) $f(X)$ is called *directly indecomposable* if the residue class ring $\mathfrak{B}/(f(X))$ is a ring without proper central idempotents.

2) $f(X)$ is called *irreducible* if each proper factor of $f(X)$ is contained in B.

3) (Janusz) Let B be commutative and $\mathfrak{B}$ be $B[X]$. Then $f(X)$ is called *separable* if $\mathfrak{B}/(f(X))$ is a separable B-algebra [4, § 2].

The next is well known.

Lemma 1. *Let B be a domian*[2] *with the quotient field K, and $f(X)$ a monic polynomial of $B[X]$. Then $(f(X))=f(X)B[X]$ is prime if and only if $f(X)$ is irreducible in $K[X]$.*

By [4, Corollary 2. 10], we readily obtain

Lemma 2. *Let B be a commutative ring. If $f(X)$ is separable and irreducible in $B[X]$, then $f(X)$ is directly indecomposable.*

Lemma 3. *Let b_0 be an element of B, and $\mathfrak{p}$ a maximal ideal of B. If $b^p-b-d\neq b_0$ whenever $b\in B$ and $d\in\mathfrak{p}$, then X^p-X-b_0 is irreducible in $B[X]$.*

Proof. Since $b^p-b-d\neq b_0$, X^p-X-b_0 is irreducible modulo $\mathfrak{p}[X]$. Now, suppose that $X^p-X-b_0=g(X)h(X)$, where $g(X), h(X)\in B[X]$ are monic and deg $g(X)$, deg $h(X)<p$. Then $g(X)-b$ or $h(X)-c$ are contained in $\mathfrak{p}[X]$ for some b or c in B, and we have a contradiction $(g(X)-b)(h(X)-c)=X^p-X-b_0-bh(X)-cg(X)+bc\in\mathfrak{p}[X]$.

Lemma 4. *Let B be a domain, and b_0 an element of B. If X^p-X-b_0 is not irreducible in $B[X]$, then $X^p-X-b_0=(X-b)(X-(b+1))\cdots(X-(b+p-1))$ for some $b\in B$.*

In all that follows, by $X^{\mathfrak{p}}-b$ we denote X^p-X-b.

1. Cyclic extension with a Galois group of order p

Throughout this section, by $\mathfrak{G}$ we denote a cyclic group of order p with a generator σ. Firstly, we shall prove the following

Theorem 1. 1. *Let A be a $\mathfrak{G}$-Galois extension of B. Then there exist an element b_0 in B, a derivation D in B such that $D^p-D=I_{b_0}$*

2) A domain means a commutative integral domian.

and $Db_0=0$, and then X^p-b_0 is a central polynomial of $B[X;D]$ and A is isomorphic to $B[X;D]/(X^p-b_0)B[X;D]$.

Proof. Since $A_B=B_B\oplus B'_B$, there exists an element a in A with $t_{\mathfrak{G}}(a)=1$. Hence, there exists an element $x\in A$ with $\sigma(x)=x+1$ [9, Theorem 10. 1]. Then it is clear that $x^p-x\in B$ and $bx-xb\in B$ for each $b\in B$. Now, we set $b_0=x^p-x$, $D=I_x$. Then $D^p-D=I_{b_0}$ and $Db_0=0$. Let $T=B+xB+\cdots+x^{p-1}B$ ($\subseteqq A$). Then T is a subring of A and $\sigma(T)\subseteqq T$. Now for $0<j<p$, we set $a_j=\sigma^j(x)(j^{-1})$, $b_j=(-j^{-1})x$. Then $\prod_{j=1}^{p-1}(a_j+b_j)=1$ and $\prod_{j=1}^{p-1}(a_j+\sigma^k(b_j))=0$ for $k=1,2,\cdots,p-1$. Comparing the expansions of those above, we can easily see that the existence of a $\mathfrak{G}$-Galois coordinate system $\{x_1,x_2,\cdots,x_n;\ y_1,y_2,\cdots,y_n\}$ for T/B. Hence $T=A$ [8, Theorem 2. 3]. If $a=\sum_{i=0}^{p-1}x^id_i$ ($d_i\in B$) is 0, then we have $\sigma(a)-a=x^{p-2}(p-1)d_{p-1}+\cdots=0$. Repeating the same procedure, we can easily see that $d_{p-1}=d_{p-2}=\cdots=d_0=0$. Thus $A=B\oplus xB\oplus\cdots\oplus x^{p-1}B$. To be easily verified $D^p-D=I_{b_0}$ and $Db_0=0$ mean that X^p-b_0 is central in $B[X;D]$. *Let* φ^* be the map of $B[X;D]$ to A defined by $f(X)\longmapsto f(x)$. Since $f(X)=(X^p-b_0)g(X)+r(X)$ with deg $r(X)<p$, Ker $\varphi^*=(X^p-b_0)B[X;D]$.

Corollary 1. 1. *In order that B have a $\mathfrak{G}$-Galois extension A, it is necessary and sufficient that there exist an element b_0 in B and a derivation D in B such that*

(*a*) $D^p-D=I_{b_0}$, $Db_0=0$,

(*b*) *X^p-b_0 is directly indecomposable in $B[X;D]$.*

Proof. By Theorem 1. 1, it remains only to prove the sufficiency.

As was noted above, X^p-b_0 is central in $B[X;D]$ and $X^p-b_0=(X+1)^p-b_0$. Thus the automorphism ϕ of order p of $B[X:D]$ defined by $f(X)\longmapsto f(X+1)$ induces an automorphism σ^* of $A^*=B[X;D]/(X^p-b_0)B[X;D]=B\oplus yB\oplus\cdots\oplus y^{p-1}B$ with $\sigma^*(y)=y+1$, where y is the residue class of X modulo $(X^p-b_0)B[X;D]$. Let $a=\sum_{i=0}^{p-1}y^id_i\in A^*$ with $\sigma(a)=a(d_i\in B)$. Then $\sum_{i=0}^{p-1}(y+1)^id_i=\sigma(a)=a=\sum_{i=0}^{p-1}y^id_i$ yields $(p-1)d_{p-1}+d_{p-2}=d_{p-2}$, and hence, $d_{p-1}=0$. Repeating the same procedure, we have $a=d_0\in B$, that is, $A^{*\sigma^*}=B$. Now, the existence of a (σ^*)-Galois coordinate system for A^*/B will be seen as same argument as in the proof of Theorem 1. 1. Thus A^* is a Galois extension of B with a Galois group (σ^*) of order p.

Corollary 1. 2. *If A is a $\mathfrak{G}$-Galois extension of B, then A is B-*

free.

Let A be a $\mathfrak{G}$-Galois extension of B. Since the order of $\mathfrak{G}$ is p, it is either inner or contains no inner automorphisms except identity. Now, we consider the case $\sigma=\tilde{v}$, an inner automorphism generated by a unit $v\in V=V_A(B)$. Then $\sigma(V)\subseteq V$ and $V^{\sigma}=V\cap B=Z$, the center of B. Therefore, $v\in Z$ and hence $V=V^{\sigma}=Z$. Under the same notations in the proof of Theorem 1. 1, $\sigma(x)=vxv^{-1}=x+1$ yields at once $vx-xv=v$, that is, $Dv=v$. Thus we have proved only if part of the following

Corollary 1. 3. *There exists a $\mathfrak{G}$-Galois extension A of B such that $\mathfrak{G}=(\tilde{v})$, $v\in V$, if and only if there exist an element b_0 in B, a derivation D in B and an element z in $U(Z)$ such that*

(*a*) $D^p-D=I_{b_0}$, $Db_0=0$,

(b) X^p-b_0 *is directly indecomposable in* $B[X;D]$,

(*c*) $Dz=z$.

Proof. We shall prove the if part. Under the notations in the proof of Corollary 1. 1, we set $A^*=B\oplus yB\oplus\cdots\oplus y^{p-1}B=B[X;D]/(X^p-b_0)B[X;D]$. Then $Dz=z=zy-yz$ means $zyz^{-1}=y+1$ and hence $z^pyz^{-p}=y$ which implies $z^p\in V_{A^*}(A^*)$. Thus in the proof of Corollary 1. 1, we may set $(\sigma^*)=(\tilde{z})$.

Lemma 1. 1. *Let $\mathfrak{H}$ be a finite group of automorphisms of a ring A with $A^{\mathfrak{H}}=B$. If an intermediate ring T is an $\mathfrak{H}|T$-Galois extension of B, and A/T is an $\mathfrak{N}$-Galois extension for some normal subgroup $\mathfrak{N}$ of $\mathfrak{H}$ with $\mathfrak{H}_T=\{\rho\in\mathfrak{H};\rho(t)=t$ for all $t\in T\}=\mathfrak{N}$, then A is an $\mathfrak{H}$-Galois extension of B.*

Proof. Let $\{x_1, x_2, \cdots, x_n; y_1, y_2, \cdots, y_n\}$ be an $\mathfrak{N}$-Galois coordinate system for A/T, and $\{w_1, w_2, \cdots, w_m; z_1, z_2, \cdots, z_m\}$ an $\mathfrak{H}|T$-Galois coordinate system for T/B. Then $\sum_i x_i(\sum_j w_j\rho(z_j))\rho(y_i)=\delta_{\rho,1}$.

Let T be a Galois extension of B with a cyclic Galois group $\mathfrak{N}$ of order p^e with a generator τ. For a derivation D in T and an element t of T, we set $\mathfrak{D}_0(t)=1$ and $\mathfrak{D}_k(t)=D(\mathfrak{D}_{k-1}(t))+(\mathfrak{D}_{k-1}(t))t$, then $(X+t)^n=\sum_{k=0}^{n}\binom{n}{k}X^{n-k}\mathfrak{D}_k(t)$ in $T[X;D]$ [7, § 1, I, (ii)]. Now we shall prove

Theorem 1. 2. *In order that B have a cyclic $\mathfrak{H}$-Galois extension ($\mathfrak{H}=(\sigma)$ of order p^{e+1}) such that $A\supseteq T$, and $\sigma|T=\tau$, it is necessary and sufficient that there exist a derivation D in T and elements u_0, u_1 in T such that*

(a) $D^p - D = I_{u_0}$, $Du_0 = 0$,
(b) $X^p - u_0$ *is directly indecomposable in* $T[X; D]$,
(c) $T_{\mathfrak{N}}(u_1) = 1$,
(d) $\tau D \tau^{-1} - D = I_{u_1}$,
(e) $\mathfrak{D}_p(u_1) - u_1 = \tau(u_0) - u_0$.

Proof. Let A be the extension cited in Theorem 1. 2. Then $A^{\sigma^{p^e}} \supseteq T$. If $\{x_1, x_2, \cdots, x_n; y_1, y_2, \cdots, y_n\}$ is an $\mathfrak{N}$-Galois coordinate system for T/B, then $\sum_i x_i \rho(y_i) = \delta_{(\sigma^{p^e}), \rho}$ for each $\rho \in \mathfrak{H}$. Hence $A = A^{\sigma^{p^e}}$ by [8, Theorem 2. 3], that is, A/T is a (σ^{p^e})-Galois extension. Hence $A = T \oplus xT \oplus \cdots \oplus x^{p-1}T \cong T[X; D]/(X^p - u_0)T[X; D]$, where $\sigma^{p^e}(x) = x+1$, $u_0 = x^p - x$ and $D = I_x | T$ (Theorem 1. 1). Then it is clear that D, u_0 satisfy (a) and (b). We set $u_1 = \sigma(x) - x$ which is contained in T by $\sigma^{p^e}(x) = x+1$. Then (c)—(e) can be checked as follows:

$$t_{\mathfrak{N}}(u_1) = \sum_{i=0}^{p^e-1} \sigma^i(\sigma(x) - x) = \sigma^{p^e}(x) - x = 1.$$
$$(\tau D \tau^{-1} - D)(t) = \tau(\sigma^{-1}(t) x - x\sigma^{-1}(t)) - tx + xt = t\sigma(x) - \sigma(x)t - tx + xt$$
$$= t(\sigma(x) - x) - (\sigma(x) - x)t = tu_1 - u_1 t = I_{u_1}(t).$$
$$\sigma(u_0) - u_0 = \sigma(x^p - x) - (x^p - x) = (x + u_1)^p - (x + u_1) - x^p + x = \mathfrak{D}_p(u_1) - u_1.$$

Conversely, assume that there exist a derivation D in T and elements u_0, u_1 in T satisfying (a)—(e). Let ϕ be the map of $T[X; D]$ defined by $\sum_i X^i t_i \longrightarrow \sum_i (X + u_1)^i \tau(t_i)$. Then ϕ is an automorphism of $T[X; D]$ of order p^{e+1} by (c) and (d). By (a), $X^p - u_0$ is central and $T[X; D]/(X^p - u_0) = T[y] = T \oplus yT \oplus \cdots \oplus y^{p-1}T = A^*$, where y is the residue class of X modulo $(X^p - u_0)$. (e) show that $\phi(X^p - u_0) = X^p - u_0$. Hence ϕ induces an automorphism σ^* of order p^{e+1} in A^* with $\sigma^*(y) = y + u_1$ and $\sigma^* | T = \tau$.

If $(\sum_{i=0}^{p-1} y^i t_i)$ is left invariant by σ^{*p^e}, then $\sigma^{*p^e}(\sum_{i=0}^{p-1} y^i t_i) = \sum_{i=0}^{p-1}(y + t_{\mathfrak{N}}(u_1))^i t_i = \sum_{i=0}^{p-1}(y+1)^i t_i$. Therefore the argument used in Corollary 1. 1 will be proved A^*/T is a (σ^{*p^e})-Galois extension. Then it is clear that $(\sigma^*)_T = \{\rho \in (\sigma^*); \rho(t) = t$ for all $t \in T\} = (\sigma^{*p^e})$. Thus A^*/B is a Galois extension with a Galois group (σ^*) of order p^{e+1} by Lemma 1. 1.

2. Abelian extension with a Galois group of order p^f

Throughout this section, we assume that $\mathfrak{G} = (\sigma_1) \times (\sigma_2) \times \cdots \times (\sigma_e)$, a direct product of cyclic groups (σ_i) of order p with a generator σ_i.

We shall state several remarks without proof.

Let D_i $(i = 1, 2, \cdots, e)$ be derivations in B, b_i $(i = 1, 2, \cdots, e)$ elements of B and $b_{ij}(i, j=1, 2, \cdots, e)$ elements of B with $b_{ij}=-b_{ji}$ and $b_{ii}=0$. If they satisfy

$$[D_i, D_j]=D_iD_j-D_jD_i=I_{b_{ji}}$$
$$D_kb_{ij}+D_ib_{jk}+D_jb_{ki}=0$$

then the set of polynomials of e-indeterminates $\mathfrak{B}=B[X_1, X_2, \cdots, X_e; D_1, D_2, \cdots, D_e]=\{\sum X_1^{\nu_1}X_2^{\nu_2}\cdots X_e^{\nu_e}b_{\nu_1\nu_2\cdots\nu_e}; b_{\nu_1\nu_2\cdots\nu_e}\in B\}$ forms a ring whose multiplication is defined by the distributive law and the rule $bX_i=X_ib+D_ib$ $(b\in B)$ and $X_iX_j=X_jX_i+b_{ji}$ [7, Proposition 2. 1].

Further, if there holds

$$D_i^p-D_i=I_{b_i},\ D_ib_i=0,$$
$$D_j^{p-1}b_{ji}+b_{ij}+D_ib_j=0,$$

the polynomial $X_i^p-b_i$ is central in $\mathfrak{B}$ [7, Theorem 3. 1].

Let π be an arbitrary permutation of $\{1, 2, \cdots, k\}$, $k\leqq e$. Then $\mathfrak{B}=B[X_{\pi(1)}, X_{\pi(2)}, \cdots, X_{\pi(e)}; D_{\pi(1)}, D_{\pi(2)}, \cdots, D_{\pi(e)}]$ [7, Proposition 2. 1].

We set $B[X_1, X_2, \cdots, X_{k-1}; D_1, D_2, \cdots, D_{k-1}]/M_{k-1}=B[x_1, x_2, \cdots, x_{k-1}]=\sum_{0\leq\nu_i<p}x_1^{\nu_1}x_2^{\nu_2}\cdots x_{k-1}^{\nu_{k-1}}B$, where $M_{k-1}=(X_1^p-b_1, X_2^p-b_2, \cdots, X_{k-1}^p-b_{k-1})$ and x_i is the residue class of X_i modulo M_{k-1}. Then,

$B[x_1, x_2, \cdots, x_{k-1}][X_k; D_k]=\{\sum X_k^i a_i;\ a_i\in B[x_1, x_2, \cdots, x_{k-1}]\}$ forms a ring whose multiplication is defined by the distributive law and the rule $bX_k=X_kb+D_kb(b\in B)$ and $x_iX_k=X_kx_i+b_{ki}$ [7, Lemma 2. 3], moreover $X_k^p-b_k$ is a central polynomial of $B[x_1, x_2, \cdots x_{k-1}][X_k; D_k]$ if we reduce the coefficents modulo M_{k-1}, and,

$B[X_1, X_2, \cdots, X_k; D_1, D_2, \cdots, D_k]/M_k=B[x_1, x_2, \cdots, x_k]\cong B[x_1, x_2, \cdots, x_{k-1}][X_k; D_k]/(X_k^p-b_k)B[x_1, x_2, \cdots, x_{k-1}][X_k; D_k]$ [7, Lemma 2. 3].

We denote this residue class ring by A_k.

Now, a set of polynomials $\{X_1^p-b_1, X_2^p-b_2, \cdots, X_e^p-b_e\}$ of $\mathfrak{B}$ will be called *a system of directly indecomposable polynomials* if $X^p_{\pi(i)}-b_{\pi(i)}$ is directly indecomposable in $A_{\pi(i-1)}[X_{\pi(i)}; D_{\pi(i)}]$ for every permutation π of $\{1, \cdots, i\}$, $i\leqq e$.

We shall prove the following which corresponds to Theorem 1. 1.

Theorem 2. 1. *Let A be a $\mathfrak{G}$-Galois extension of B. Then there exist derivations D_i $(i=1, 2, \cdots, e)$ elements b_i $(i=1, 2, \cdots, e)$ and b_{ij} $(i, j=1, 2, \cdots, e)$ with $b_{ij}=-b_{ji}$ and $b_{ii}=0$ in B such that*

(a) $[D_i, D_j]=I_{b_{ji}}$,

(b) $D_kb_{ij}+D_ib_{jk}+D_jb_{ki}=0$,

(c) $D_i^p-D_i=I_{b_i}$, $D_ib_i=0$,

(d) $D_j^{p-1}b_{ji}+b_{ij}+D_ib_j=0$,
and then $X_i^p-b_i$ $(i=1, 2, \cdots, e)$ *are central polynomials of* $\mathfrak{B}$ *and* A *is isomorphic to* $\mathfrak{B}/M_e$.

Proof. Since $A_B=B_B\oplus B'_B$, there exists an element $a\in A$ with $t_{\mathfrak{G}}(a)=1$. Hence there exist elements $x_1, x_2, \cdots, x_e$ in A with $\sigma_i(x_j)=x_j+\delta_{ij}$ [9, Theorem 10]. Then $x_i^p-x_i=b_i\in B$, $x_ix_j-x_jx_i=b_{ji}\in B$ and $bx_i-x_ib\in B$ for each $b\in B$. Hence if we set $D_i=I_{x_i}|B$, D_i, b_i and b_{ij} satisfy the conditions (a)—(d) [cf. 7, Theorem 3. 1].

Let $T=\sum_{0\leq\nu_i<p}x_1^{\nu_1}x_2^{\nu_2}\cdots x_e^{\nu_e}B$. Then T is a subring of A such that $\mathfrak{G}(T)\subseteq T$ and $T^{\mathfrak{G}}=B$.

Let $\rho=\sigma_1^{l_1}\cdots\sigma_i^{l_i}\cdots\sigma_e^{l_e}$ be an arbitrary element of $\mathfrak{G}$.

For each σ_i^k, we set

$a_k^{(i)}=\sigma_i^k(x_i)k^{-1}$, $b_k^{(i)}=(-k)^{-1}x_i$.

Then $\prod_{k=1}^{p-1}(a_k^{(i)}+b_k^{(i)})=1$ and $\prod_{k=1}^{p-1}(a_k^{(i)}+\rho(b_k^{(i)}))=\begin{cases}0 \text{ if } \sigma_i^{l_i}\neq 1\\ 1 \text{ if } \sigma_i^{l_i}=1\end{cases}$.

Comparing the expansions of those above, we can easily see the existence of elements $\{c_1^{(i)}, c_2^{(i)}, \cdots, c_n^{(i)}; d_1^{(i)}, d_2^{(i)}, \cdots, d_n^{(i)}\}$ in A such that

$$\sum_j c_j^{(i)}d_j^{(i)}=1$$
$$\sum_j c_j^{(i)}\rho(d_j^{(i)})=\begin{cases}0 & \text{if } \sigma_i^{l_i}\neq 1\\ 1 & \text{if } \sigma_i^{l_i}=1\end{cases}$$

for each $i=1, 2, \cdots, e$.

Hence if we set

$$W_1=\sum_j c_j^{(1)}d_j^{(1)},\ W_1^{(\rho)}=\sum_j c_j^{(1)}\rho(d_j^{(1)}),$$
$$W_2=\sum_j c_j^{(2)}W_1d_j^{(2)},\ W_2^{(\rho)}=\sum_j c_j^{(2)}W_1^{(\rho)}\rho(d_j^{(2)})$$

and

$$W_k=\sum_j c_j^{(k)}W_{k-1}d_j^{(k)},\ W_k^{(\rho)}=\sum_j c_j^{(k)}W_{k-1}^{(\rho)}\rho(d_j^{(k)}),$$

we have

$$W_e=\sum x_my_m=1,\ W_e^{(\rho)}=\sum x_m\rho(y_m)=0 \text{ for each } \rho\neq 1.$$

This means the existence of a $\mathfrak{G}$-Galois coordinate system for T/B. Thus we obtain $T=A$.

If $a=\sum_{i=0}^{p-1}x_1^if_i(x_2, x_3, \cdots, x_e)=0$. Then $\sigma_1(a)-a=\sum_{i=0}^{p-1}(\sum_{j=0}^{i}\binom{i}{j}x_1^j$ $f_i(x_2, x_3, \cdots, x_e))=0$. Repeating the same procedure, we can easily see that $f_0(x_2, x_3, \cdots, x_e)=f_1(x_2, x_3, \cdots, x_e)=\cdots=f_{p-1}(x_2, x_3, \cdots, x_e)=0$. Next, we consider $f_i(x_2, x_3, \cdots, x_e)=\sum_{j=0}^{p-1}x_2^jg_{ij}(x_3, x_4, \cdots, x_e)=0$ and $\sigma_2(f_i(x_2, x_3, \cdots, x_e))$. Then we can see that $g_{ij}(x_3, x_4, \cdots, x_e)=0$ for each $j=0, 1, 2, \cdots, p-1$.

Continuing similary, we can see eventually $\{x_1^{\nu_1}x_2^{\nu_2}\cdots x_e^{\nu_e}; 0\leqq\nu_i<p\}$ is a linearly independent right B-basis for A.

Let φ^* be the map of $\mathfrak{B}$ 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. Since $f(X_1, X_2, \cdots, X_e)=(X_1^p-b_1)g_1(X_1, X_2, \cdots, X_e)+(X_2^p-b_2)g_2(X_1, X_2, \cdots, X_e)+\cdots+(X_e^p-b_e)g_e(X_1, X_2, \cdots, X_e)+r(X_1, X_2, \cdots, X_e)$, where each degree X_i of $r(X_1, X_2, \cdots, X_e)$ is smaller than p, $f(x_1, x_2, \cdots, x_e)=r(x_1, x_2, \cdots, x_e)$ yields that $\mathrm{Ker}\,\varphi^*=(X_1^p-b_1, X_2^p-b_2, \cdots, X_e^p-b_e)$.

Corollary 2. 1. *In order that B have a $\mathfrak{G}$-Galois extension A such that $A^{\mathfrak{G}_i}(\mathfrak{G}_i=(\sigma_{i+1})\times\cdots\times(\sigma_e))$ has no proper central idempotents, it is necessary and sufficient that there exist derivations $D_i(i=1, 2, \cdots, e)$ in B, elements $b_i(i=1, 2, \cdots, e)$ and $b_{ij}(i, j=1, 2, \cdots, e)$ of B with $b_{ij}=-b_{ji}$ and $b_{ii}=0$ such that*

(a) $[D_i, D_j]=I_{b_{ji}}$,

(b) $D_kb_{ij}+D_ib_{jk}+D_jb_{ki}=0$,

(c) $D_i^p-D_i=I_{b_i}$, $D_ib_i=0$,

(d) $D_j^{p-1}b_{ji}+b_{ij}+D_ib_j=0$,

(e) $\{X_1^p-b_1, X_2^p-b_2, \cdots, X_e^p-b_e\}$ *is a system of directly indecomposable polynomials.*

Proof. Let A be the extension cited in Corollary 2. 1. Then, as was shown in Theorem 2. 1, there exist derivations D_i, elements b_i and $b_{ij}(i, j=1, 2, \cdots, e)$ satisfying (a)–(d). Since $A^{\mathfrak{G}_i}$ is a $(\sigma_1)\times(\sigma_2)\times\cdots\times(\sigma_i)$-Galois extension over B, $A^{\mathfrak{G}_i}=B[x_1, x_2, \cdots, x_i]$ by Theorem 2. 1. While by the remark state just before Theorem 2. 1, $B[x_1, x_2, \cdots, x_i]\cong B[x_1, x_2, \cdots, x_{i-1}][X_i; D_i]/(X_i^p-b_i)B[x_1, x_2, \cdots, x_{i-1}][X_i; D_i]$. Hence (e) is clear.

Conversely, assume that there exist derivations D_i, elements b_i and b_{ij} $(i, j=1, 2, \cdots, e)$ satisfying (a)–(e). Then (e) yields that $A^*=B[y_1, y_2, \cdots, y_e]=B[X_1, X_2, \cdots, X_e; D_1, D_2, \cdots, D_e]/M_e$ contains no proper central idempotents, where each y_i is the residue class of X_i modulo M_e. Now, let ϕ_i be the map of $\mathfrak{B}$ into itself defined by $f(X_1, X_2, \cdots, X_i, \cdots, X_e)\longmapsto f(X_1, X_2, \cdots, X_i+1, \cdots, X_e)$. Then ϕ_i is an automorphism and further, it induces an automorphism σ_i^* of order p in $B[y_1, y_2, \cdots, y_e]$ for $\phi_i(X_j^p-b_j)=X_j^p-b_j(j=1, 2, \cdots, e)$. The group generated by $\sigma_1^*, \sigma_2^*, \cdots, \sigma_e^*$ coincides with $\mathfrak{G}^*=(\sigma_1^*)\times(\sigma_2^*)\times\cdots\times(\sigma_e^*)$, a direct product of each (σ_i^*). Then it is clear that $A^{\mathfrak{G}^*}=B$. The existence of a $\mathfrak{G}^*$-Galois coordinate system will be seen as for that of Theorem 2. 1.

Corollary 2. 2. *If A is a $\mathfrak{G}$-Galois extension of B satisfying the conditions of Corollary 2. 1, then A is B-free.*

Combining Theorem 2. 1 with Corollary 2. 1, we can state the following fact corresponding to Theorem 1. 2. The proof is quite similar as that of [7, Theorem 3. 2], and it may be left to readers.

Theorem 2. 2. *Let T/B be a Galois extension with an abelian group $\mathfrak{N}=(\tau_1)\times(\tau_2)\times\cdots\times(\tau_e)$, a direct product of cyclic groups (τ_i) of order p^{f_i} with a generator τ_i. In order that B have a Galois extension A with a Galois group $\mathfrak{H}=(\sigma_1)\times(\sigma_2)\times\cdots\times(\sigma_e)$, a direct product of cyclic groups (σ_i) of order p^{f_i+1} with a generator σ_i such that $A\supseteqq T$, $A^{\mathfrak{H}_i}(\mathfrak{H}_i=(\sigma_1^{f_1})\times\cdots\times(\sigma_e^{f_e}))$ has no proper central idempotents and $\sigma_i|T=\tau_i$, it is necessary and sufficient that there exist derivations $D_i(i=1, 2, \cdots, e)$ in T, elements t_i, t_{ij} $(i, j=1, 2, \cdots, e)$ such that $t_{ij}=-t_{ji}$ and $t_{ii}=0$ in T satisfying (a)—(e) of Corollary 2. 1 (in T) and there exist elements $u_{ij}(i, j=1, 2, \cdots, e)$ in T such that*

(a) $D_i\tau_j-\tau_jD_i=I_{u_{ij}}\tau_j$,

(b) $t_{\tau_j}(u_{ij})=\delta_{ij}$,

(c) $\mathfrak{D}_p^{(i)}(u_{ij})-u_{ij}=\tau_j(b_i)-b_i$[3],

(d) $\tau_k(t_{ij})-t_{ij}=\tau_kD_j\tau_k^{-1}(u_{ik})-D_iu_{jk}$,

(e) $\tau_k(u_{ij})-u_{ij}=\tau_j(u_{ik})-u_{ik}$.

3. Cyclic Galois algebras

In this section, we assume that B is a commutative ring, $\mathfrak{G}$ a cyclic group of order p with a generator σ. If A is a $\mathfrak{G}$-Galois extension of B, then $A=B\oplus xB\oplus\cdots\oplus x^{p-1}B$ (Theorem 1. 1). Hence, if A is an algebra over B, then A is commutative. This is a special case of [3, Theorem 11].

Theorem 3. 1. (1) *Let A be a $\mathfrak{G}$-Galois algebra over B. Then there exists an element $b_0\in B$ such that $b^p-b\neq b_0$ for each $b\in B$. Moreover, if this is the case, X^p-b_0 is a separable polynomial in $B[X]$ and A is a splitting ring of X^p-b_0.*

(2) *Let $\mathfrak{p}$ be a maximal ideal of B. If there exists an element $b_0\in B$ such that $b^p-b-d\neq b_0$ for each $b\in B$ and $d\in\mathfrak{p}$, then there exists a Galois algebra A^* over B with a cyclic Galois group $\mathfrak{G}^*$ of order p. Moreover, if this is the case, X^p-b_0 is a separable polynomial in $B[X]$ and A^* is a splitting ring of X^p-b_0.*

3) $\mathfrak{D}_k^{(i)}(t)$ means $D_i(\mathfrak{D}_{k-1}^{(i)}(t))+\mathfrak{D}_{k-1}^{(i)}(t)t$, where $\mathfrak{D}_0^{(i)}(t)=1$.

Proof. (1) If A is a $\mathfrak{G}$-Galois algebra over B, then, as is shown in Corollary 1.1, there exists an element $x\in A$ with $\sigma(x)=x+1$, $b_0=x^p-x\in B$ and $A=B\oplus xB\oplus\cdots\oplus x^{p-1}B\cong B[X]/(X^p-b_0)$. Hence X^p-b_0 is a separable polynomial of $B[X]$ and $\{x, x+1, \cdots, x+(p-1)\}$ is the set of roots of X^p-b_0 [4, Lemma 2.1]. Consequently, $b^p-b\neq b_0$ for each $b\in B$. Furthermore, it is clear that $X^p-b_0=(X-x)(X-(x+1))\cdots(X-(x+(p-1))$ in $A[X]$.

(2) Let $A^*=B\oplus yB\oplus\cdots\oplus y^{p-1}B=B[X]/[X^p-b_0)$, where y is the residue class of X modulo (X^p-b_0). Then the map defined by $\sigma^*(y)=y+1$ is an automorphism of order p of A^* with $A^{*\sigma^*}=B$. Since $j=\sigma^{*j}(y)-y$ for each $0<j<p$, A^* is a separable B-algebra [2, Theorem 1.3]. Hence X^p-b_0 is a separable polynomial. Furthermore, by Lemma 3, X^p-b_0 is irreducible. Thus it is directly indecomposable by Lemma 2.

Corollary 3.1. *In order that there exist a $\mathfrak{G}$-Galois algebera A over B such that $A/\mathfrak{p}A$ has no proper idempotents for each maximal ideal $\mathfrak{p}$ of B, it is necessary and sufficient that there exist an element $b_0\in B$ satisfying $b^p-b-d\neq b_0$ for* each $b\in B$ and $d\in B\backslash U(B)$.

Proof. Let A be the extension cited in Corollary 3.1. Then there exists an element x in A such that $\sigma(x)=x+1$, $b_0=x^p-x\in B$ and $A=B\oplus xB\oplus\cdots\oplus x^{p-1}B\cong B[X]/(X^p-b_0)$ (Theorem 3.1 (1)). Further, for each maximal ideal $\mathfrak{p}$ of B, $A/\mathfrak{p}A$ is a (σ)-Galois algebra over the field $(B+\mathfrak{p}A)/\mathfrak{p}A\cong B/\mathfrak{p}$. Hence $A/\mathfrak{p}A$ is a field ($A/\mathfrak{p}A$ is semi-simple artinian without proper idempotents), and since $A/\mathfrak{p}A\cong(B/\mathfrak{p})[X]/(X^p-\bar{b}_0)(B/\mathfrak{p})[X]$, where $\bar{b}_0$ is the residue class of b_0 modulo $\mathfrak{p}$, $X^p-\bar{b}_0$ is irreducible in $(B/\mathfrak{p})[X]$ for each $\mathfrak{p}$. Thus $b^p-b-d\neq b_0$ for each $b\in B$ and $d\in B\backslash U(B)$.

Conversely, if there exists an element $b_0\in B$ satisfying $b^p-b-d\neq b_0$ for each $b\in B$ and $d\in B\backslash U(B)$, we have seen that $A^*=B\oplus yB\oplus\cdots\oplus y^{p-1}B=B[X]/(X^p-b_0)$ is a (σ^*)-Galois algebra over B with $\sigma^*(y)=y+1$ (Theorem 3.1 (2)). Noting that $X^p-\bar{b}_0$ is irreducible in $(B/\mathfrak{p})[X]$ for each maximal ideal $\mathfrak{p}$ of B, $A^*/\mathfrak{p}A^*\cong(B/\mathfrak{p})[X]/(X^p-\bar{b}_0)$ yields that $A^*/\mathfrak{p}A^*$ is a field. Thus $A^*/\mathfrak{p}A^*$ has no proper idempotents.

Corollary 3.2. *Let B be a local ring. In order that there exist a $\mathfrak{G}$-Galois algebra A over B that A is local, it is neceseary and sufficient that there exist an element $b_0\in B$ with $b^p-b-r\neq b_0$ for each $b\in B$ and $r\in J(B)$, the Jacobson radical of B.*

Proof. Let A be the extension cited in Corollary 3.2. Then there exists an element x in A such that $\sigma(x)=x+1$, $b_0=x^p-x\in B$ and $A=B\oplus xB\oplus\cdots\oplus x^{p-1}B\cong B[X]/(X^p-b_0)$ by Theorem 3.1 (1). Since $J(A)=J(B)A$, $A/J(B)A$ is a field. Thus $b^p-b-r\neq b_0$ for each $b\in B$, $r\in B\setminus U(B)=J(B)$ by Corollary 3.1.

Conversely, if there exists $b_0\in B$ such that $b^p-b-r\neq b_0$ for each $b\in B$, $r\in J(B)$, $A^*=B\oplus yB\oplus\cdots\oplus y^{p-1}B=B[X]/(X^p-b_0)$, where y is the residue class of X modulo (X^p-b_0), is a Galois algebra over B with a Galois group (σ^*) of order p such that $\sigma^*(y)=y+1$, and $A^*/J(B)A^*$ is a field by Corollary 3.1. Since $J(B)A^*=J(A^*)$, $J(A^*)$ is a maximal ideal of A^*, that is, A^* is local.

Let B be local, T a Galois algebra over B with a cyclic Galois group $\mathfrak{N}=(\tau)$ of order p^e with a generator τ, and T be local. Then,

Lemma 3.1. *Assume that there exist elements x, y in T such that $\tau(x)-x=y^p-y$ and $t_\tau(y)=1$. Then $t^p-t-r\neq x$ for each $t\in T$, $r\in J(T)$. Further, if this is the case, $T[X]/(X^p-x)$ is a Galois algebra over B with a cyclic Galois group $\mathfrak{H}$ of order p^{e+1} with a generator σ such that $\sigma|T=\tau$.*

Proof. Suppose that $t^p-t-r=x$ for some $t\in T$ and $r\in J(T)$. Then $y^p-y=\tau(x)-x=(\tau(t)-t)^p-(\tau(t)-t)-(\tau(r)-r)$. Hence $(\tau(t)-t-y)^p=(\tau(t)-t-y)-(\tau(r)-r)$ and $t_\tau(\tau(t)-t-y)=t_\tau(-y)=-1$ imply $z=\tau(t)-t-y\in U(T)$ and $z^p\equiv z(\neq 0)$ modulo $J(T)$. This means that the residue class of z modulo $J(T)$ is contained in the prime field of $T/J(T)$, and hence, that of $B/J(B)$. Consequently, we have $z=b+s$ for some $b\in B$ and $s\in J(T)$. But this is a contradiction since $-1=t_\tau(z)=t_\tau(s)\in J(T)$. This means that $t^p-t-r\neq x$ for each $t\in T$ and $r\in J(T)$, namely, X^p-x is irreducible in $T[X]$. Thus $A^*=T[X]/(X^p-x)=T[w]=T\oplus wT\oplus\cdots\oplus w^{p-1}T$, where w is the residue class of X modulo (X^p-x), is a ring without proper idempotents by Theorem 3.1 (2). Let σ^* be the map of A^* defined by $\sigma^*(\sum_{i=0}^{p-1}w^it_i)=\sum_{i=0}^{p-1}(w+y)^i\tau(t_i)$. Then $\sigma^*(w^p-w)=(w+y)^p-(w+y)=w^p-w+y^p-y=x+\tau(x)-x=\tau(x)$. Hence σ^* is an automorphism of A^* of order p^{e+1} with $A^{\sigma^*}=B$ and $\sigma^*|T=\tau$. Furthermore, $\sigma^{*p^e}(w)=w+t_\tau(y)=w+1$ shows that A^* is a (σ^{*p^e})-Galois algebra over T. Thus A^* is a (σ^*)-Galois algebra over B by Lemma 1.1.

Theorem 3.2. *Let B be a local ring. If T is a Galois algebra over B with a cyclic Galois group $\mathfrak{N}=(\tau)$ of order p^e with a generator τ and T is local, then there exists a Galois algebra A^* over B contain-*

ing T with a cyclic Galois group $\mathfrak{H}=(\sigma^*)$ of order p^{e+1} with a generator σ^* such that $\sigma^*|T=\tau$ and A^* is local. More generally, for each positive integer f, there exists a Galois algebra A^* over B containing T with a cyclic Galois group $\mathfrak{H}=(\sigma^*)$ of order p^{e+f} with a generator σ^* such that $\sigma^*|T=\tau$ and A^* is local.

Proof. Since $T_B=B_B\oplus B'_B$, there exists an element $y\in T$ such that $t_{\mathfrak{N}}(y)=1$. Hence $t_{\mathfrak{N}}(y^p)=(t_{\mathfrak{N}}(y))^p=1$, then, $t_{\mathfrak{N}}(y^p-y)=0$. Thus there exists an element x in T such that $\tau(x)-x=y^p-y$. Then by Lemma 3.1 and Corollary 3.2, $A^*=T[X]/(X^p-x)$ is a requested extension.

4. Commutative abelian extension

Throughout the present section, we assume that B is a commutative ring, $\mathfrak{G}=(\sigma_1)\times(\sigma_2)\times\cdots\times(\sigma_e)$, an abelian group which is a direct product of cyclic groups (σ_i) of order p.

Theorem 4.1. (1) *Let A be a commutative $\mathfrak{G}$-Galois algebra over B. Then there exist elements b_i $(i=1, 2, \cdots, e)$ in B with $b^p-b\neq b_i$ for each $b\in B$. Further, there exists an element x_k in A such that $\sigma_i(x_k)=x_k+\delta_{ik}$, $x_k{}^p-x_k=b_k\in B$, $B_k=B\oplus x_kB\oplus\cdots\oplus x_k{}^{p-1}B\cong B[X_k]/(X_k^p-b_k)$ and $A=B_1\otimes_B B_2\otimes\cdots\otimes_B B_e$.*

(2) *If there exist elements b_i $(i=1, 2, \cdots, e)$ in B with $x^p_{i-1}-x_{i-1}-d_{i-1}\neq b_i$ for each $x_{i-1}\in A_{i-1}$, $d_{i-1}\in\mathfrak{p}_{i-1}$, where $A_{i-1}=B[X_1, \cdots, X_{i-1}]/(X_1^p-b_1, \cdots, X_{i-1}{}^p-b_{i-1})$ and $\mathfrak{p}_{i-1}$ is a maximal ideal of A_{i-1}, then there exists a commutative $\mathfrak{G}^*$-Galois algebra A^* over B, where $\mathfrak{G}^*=(\sigma_1^*)\times(\sigma_2^*)\times\cdots\times(\sigma_e^*)$, an abelian group which is a direct product of cyclic groups (σ_i^*) of order p.*

Proof. (1) As is shown in Theorem 2.1, there exist elements $x_1, x_2, \cdots, x_e$ in A with $\sigma_i(x_j)=x_j+\delta_{ij}$, $b_i=x_i{}^p-x_i\in B$. Let $B_i=B[x_i]=B\oplus x_iB\oplus\cdots\oplus x_{i-1}{}^{p-1}B(\subseteq A)$. Then $B_i\cong B[X_i]/(X_i^p-b_i)$. Further, B_i is a (σ_i)-Galois algebra over B by Theorem 1.1. Hence $b^p-b\neq b_i$ for each $b\in B$ by Theorem 3.1 (1). Since $\{x_1^{\nu_1}x_2^{\nu_2}\cdots x_e^{\nu_e};\ 0\leqq\nu_i<p\}$ is a linearly independent B-basis for A, it is clear that $A=B_1\otimes_B B_2\otimes\cdots\otimes_B B_e(\cong\mathfrak{B}/M_e)$.

(2) Let $B_i^*=B[X_i]/(X_i^p-b_i)B[X_i]=B\oplus y_iB\cdots\oplus y_i{}^{p-1}B$, where y_i is the residue class of X_i modulo $(X_i^p-b_i)B[X_i]$, then B_i^* is a (σ_i^*)-Galois algebra over B by $\sigma_i^*(y_i)=y_i+1$ (Theorem 3.1 (2)). Now, we extend σ_i^* to an automorphism of $A^*=B_1^*\otimes_B B_2^*\otimes\cdots\otimes_B B_e^*$ defining $\sigma_i^*(y_j)=y_j+\delta_{ij}$. Then as is easily seen $\mathfrak{G}^*$, the group generated by $\sigma_1^*, \sigma_2^*, \cdots, \sigma_e^*$, is a direct product of (σ_i^*), and $A^{*\mathfrak{G}^*}=B$. We can easily prove the existence of a $\mathfrak{G}^*$-Galois coordinate system for A^*/B. Since

$B_1^*[X_2]/(X_2^p-b_2)B_1^*[X_2]\cong(B_1^*\otimes_B B[X_2])/(B_1^*\otimes_B B(X_2^p-b_2)B[X_2])\cong B_1^*\otimes_B(B[X_2]/(X_2^p-b_2)B[X_2])\cong B_1^*\otimes_B B_2^*$, $A_k^*=B[y_1, y_2, \cdots, y_k]\cong B_1^*\otimes_B B_2^*\otimes\cdots\otimes_B B_e^*\cong B[y_1, y_2, \cdots, y_{k-1}][X_k]/[X_k^p-b_k)B[y_1, y_2, \cdots, y_{k-1}][X_k]$, A_k^* has no proper idempotents.

5. The case of domain

Throughout the present section, we assume that B is a domian with the quotient field K, $\mathfrak{G}$ a cyclic group of order p with a generator σ.

Theorem 5.1. *In order that there exist a $\mathfrak{G}$-Galois algebra over B, it is necessary and sufficient that there exists an element $b_0\in B$ with $b^p-b\neq b_0$ for each $b\in B$.*

Proof. Let b_0 be an element of B with $b^p-b\neq b_0$ for each $b\in B$. Then X^p-b_0 is irreducible in $B[X]$ by Lemma 4. Thus, as was observed in Theorem 3.1(2), $A^*=B\oplus yB\oplus\cdots\oplus y^{p-1}B=B[X]/(X^p-b_0)$, where y is the residue class of X modulo (X^p-b_0), has an automorphism σ^* with $\sigma^*(y)=y+1$. Since $\sigma^{*i}(y)-y\notin\mathfrak{P}$ for each maximal ideal $\mathfrak{P}$ of A, A/B is separable ([2, Theorem 1.3]), that is, X^p-b_0 is separable. Consequently, it is directly indecomposable by Lemma 2. The necessity has been shown in Theorem 3.1 (1).

Corollary 5.1. *In order that there exist a domain A that is a $\mathfrak{G}$-Galois algebra over B, it is necessary and sufficient that there exists an element $b_0\in B$ satisfying $b^p-u^{p-1}b\neq u^p b_0$ for each elements $b, u\ (\neq 0)\in B$.*

Proof. Let A be a domain and A/B be a $\mathfrak{G}$-Galois algebra. Then $A\cong B[X]/(X^p-b_0)$ for some $b_0\in B$ by Theorem 3.1 (1). Since A is a domain, (X^p-b_0) is a prime ideal. Thus it is irreducible in $K[X]$ by Lemma 1. Hence $(b/u)^p-(b/u)\neq b_0$ for each b and $u\neq 0$ in B.

Conversely, if $b^p-u^{p-1}b\neq u^p b_0$ for each b and $u\neq 0$ in B, by setting $u=1$, we have $b^p-b\neq b_0$. Thus there exists a $\mathfrak{G}$-Galois algebra $A^*=B[X]/(X^p-b_0)$ over B by Theorem 5.1. Further X^p-b_0 is irreducible in $K[X]$. Hence A^* is a domain.

Corollary 5.2. *Let B be integrally closed in K. If A is a $\mathfrak{G}$-Galois algebra over B, then A is a domain.*

Proof. By Theorem 5.1, $A\cong B[X]/(X^p-b_0)$ for some irreducible polynomial X^p-b_0 in $B[X]$. Then, X^p-b_0 is irreducible in $K[X]$, Since B is integrally closed in K. Hence $(X^p - b_0)$ is a prime ideal of $B[X]$ by Lemma 1.

Lemma 5. 1. *Let $\mathfrak{N}$ be a cyclic group of order p^e with a generator τ, T a domain that is an $\mathfrak{N}$-Galois algebra over B. If t_1, t_2 are elements of T with $\tau(t_1) - t_1 = t_2^p - t_2$ and $t_\tau(t_2) = 1$, then $X^p - t_1$ is irreducible in $L[X]$, where L is the quotient field of T.*

Proof. Let y be an arbitrary element of L. We shall regard τ as an automorphism of L. If $(v/u)^p - v/u = t_1$ for some $v/u \in L(v, u \in T)$, then $t_2^p - t_2 = \tau(t_1) - t_1 = (\tau(v/u) - (v/u))^p = (\tau(v/u) - v/u)$ implies that $(\tau(v/u) - v/u - t_2)^p = (\tau(v/u) - v/u - t_2)$. Consequently, $x = (\tau(v/u) - v/u - t_2)$ is contained in the prime field of K and $t_\tau(x) = 0$. On the other hand, $t_\tau(x) = t_\tau(-t_2) = -1$. This is a contradiction.

Theorem 5. 2. *Let T be a domain that is an $\mathfrak{N}$-Galois algebra over B, where $\mathfrak{N}$ is a cyclic group of order p with a generator τ. Then, for each positive integer e, there exists a Galois algebra $A \supseteqq T$ over B with a cyclic Galois group $\mathfrak{H}$ of order p^e with a generator σ such that $\sigma | T = \tau$ and A is a domain.*

Proof. Since $T_B = B_B \oplus B'_B$, there exists an element t_2 in T with $t_\tau(t_2) = 1$. Hence $t_\tau(t_2^p) = 1$. Thus there exists an element t_1 in T with $\sigma(t_1) - t_1 = t_2^p - t_2$. The rest follows from Lemma 5. 1 and the making use of the same method as in the proof of Theorem 3. 2.

REFERENCES

[1] M. AUSLANDER and O. GOLDMAN: The Brauer group of a commutative ring, Trans. Amer. Math. Scc.. 97 (1960), 367—409.

[2] 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.

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

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

[5] T. KANZAKI: On Galois algebra over a commutative ring, Osaka Math. J., 2 (1965), 309—317.

[6] K. KISHIMOTO: On cyclic extensions of simple rings, J. Fac. Sci. Hokkaido Univ., 19 (1966), 74—85.

[7] ———: On abelian extensions of simple rings, J. Fac. Sci. Hokkaido Univ., 20 (1967), 53—78.

[8] Y. MIYASHITA: Finite outer Galois theory of noncommutative rings, J. Fac. Sci. Hokkaido Univ., 19 (1966), 114—134.
[9] H. TOMINAGA and T. NAGAHARA: Galois theory of simple rings, Okayama Math. Lectures, Dept. of Math., Okayama Univ., 1970.

DEPARTMENT OF MATHEMATICS
SHINSHU UNIVERSITY

(*Received January 7, 1970*)
(*Revised July 1, 1970*)