FINITE OUTER GALOIS THEORY OF NON-COMMUTATIVE RINGS

By

Yôichi MIYASHITA

Contents

§ 0. Introduction. .................................................. 114
§ 1. Galois extension and normal basis. ....................... 115
§ 2. The first characterization of fixed-subrings. ........ 118
§ 3. The second characterization of fixed-subrings. ....... 121
§ 4. Extension of isomorphisms. ................................ 122
§ 5. Heredity of Galois extensions. ....................... 123
§ 6. Completely outer case. .................................. 126
§ 7. Several results. ........................................... 130

§ 0. Introduction. It is the purpose of this paper to extend the Galois theory of commutative rings given by S. U. Chase, D. K. Harrison and A. Rosenberg [4] to non-commutative case. In what follows, for the sake of simplicity, we shall state main results for directly indecomposable rings: Let \( A \ni 1 \) be a directly indecomposable ring, \( G \) a finite group of automorphisms of \( A \), and \( B = A^G = \{ x \in A ; \sigma(x) = x \text{ for all } \sigma \in G \} \). We call \( A/B \) a \( G \)-Galois extension if there are elements \( a_1, \cdots, a_n; a_1^*, \cdots, a_n^* \) in \( A \) such that \( \sum a_i \cdot \sigma(a_i^*) = \delta_{1,\sigma} \text{ (} \sigma \in G \text{)} \), where \( \delta_{1,\sigma} \) means Kronecker's delta. If \( V_A(B) = C \) (the center of \( A \)), then \( A/B \) is a \( G \)-Galois extension if and only if the mapping \( x \otimes y \rightarrow xy \) from \( A \otimes_A A \) to \( A \) splits as an \( A \)-\( A \)-homomorphism (Th. 1.5). Let \( A/B \) be a \( G \)-Galois extension, and \( A' \) a \( G \)-invariant subring of \( A \), i.e., \( \sigma(A') = A' \) for all \( \sigma \) in \( G \), and put \( B' = A'^G \). If \( A'/B' \) is a \( G \)-Galois extension and \( B''_B \) is a direct summand of \( A''_B \), then there hold the following: (1) For any subgroup \( H \) of \( G \), \( A''_H = B \otimes_B A'' = A'' \otimes_B B \). (2) Let \( \{ T \} \) be the set of all \( G \)-invariant intermediate rings of \( A/A' \), and \( \{ T \} \) the set of all intermediate rings of \( B/B' \) such that \( A'T = TA' \). Then, \( T \rightarrow T \cap B \) and \( T \rightarrow A'T = TA' \) are mutually converse order isomorphisms between \( \{ T \} \) and \( \{ T \} \), and \( T/(T \cap B) \) is a \( G \)-Galois extension (Th. 5.1).

Let \( A/B \) be a \( G \)-Galois extension, \( V_A(B) = C \), and \( B_B \) a direct summand of \( A_B \). Then there hold the following: (1) \( G \) coincides with the set of all \( B \)-automorphisms of \( A \) (Th. 4.2). (2) For any subgroup \( H \) of \( G \), \( \{ \sigma \in G ; \sigma|A'' = 1_{A''} \} = H \). (3) If \( T \) is an intermediate ring of \( A/B \), the following are
equivalent: (a) $T = A^H$ for some subgroup $H$ of $G$. (b) The mapping $x \otimes y \rightarrow xy$ from $T \otimes_B A$ to $A$ splits as a $T$-$T$-homomorphism (Th. 2.6). (c) $A/T$ is a projective Frobenius extension (in the sense of Kasch), and $T_T$ is a direct summand of $A_T$ (Th. 3.2). In case $_B \Re(B)$ is a direct summand of $_BA_B$, the next is also equivalent to (a). (b') The mapping $x \otimes y \rightarrow xy$ from $T \otimes_B T$ to $T$ splits as a $T$-$T$-homomorphism (Th. 2.9). (4) For any subgroup $H$ of $G$, every $B$-isomorphism from $A^H$ to $A$ can be extended to a $B$-ring automorphism of $A$ (Th. 4.2). (5) If $A_B$ is finitely generated and free, and $B$ is a semi-primary ring (i.e. $B/\Re(B)$ satisfies the minimum condition for left ideals, where $\Re(B)$ means the Jacobson radical of $B$), then $A$ has a normal basis (Th. 1.7).

Let $\Delta = \Delta(A, G) = \sum_{\sigma \in \theta} Au_\sigma$ be the trivial crossed product of $A$ with $G$. $G$ is said to be completely outer if $A^\Delta$ and $A^\Delta u_\sigma$ have no isomorphic non-zero subquotients provided $\sigma \neq \tau$. If $G$ is completely outer, then $A/B$ is a $G$-Galois extension and $V_A(B) = C$ (Prop. 6.4). If $A$ is commutative, then $A/B$ is a $G$-Galois extension if and only if $G$ is completely outer (Th. 6.6). In case $A$ is two-sided simple, $G$ is completely outer if and only if $A/B$ is a $G$-Galois extension and $V_A(B) = C$ (Cor. to Prop. 6.4).

The author wishes to express his best thanks to Dr. H. Tominaga for helpful suggestions.

\section{Galois extension and normal basis.}

Throughout the present paper, all rings have identities, modules are unitary. A subring of a ring will mean one containing the same identity. By a ring homomorphism, we mean always a ring homomorphism such that the image of 1 is 1. Let $A$ be a ring, $C$ the center of $A$, $G$ a finite group of automorphisms of $A$ which acts on the left side, and $B = A^G = \{x \in A; \sigma(x) = x \text{ for all } \sigma \in G\}$. For any subgroup $H$ of $G$, $\delta_{H, \sigma}$ means the mapping from $G$ to $\{1, 0\}$ (\$A\$) such that $\delta_{H, \sigma} = 1$ if and only if $\sigma \in H$.

Let $B'$ and $T$ be subrings of a ring $A'$ such that $B' \subseteq T$. $A'$ is said to be $(B', T)$-projective, if the mapping $\sum_j x_j \otimes y_j \rightarrow \sum_j x_j y_j$ from $T \otimes_{B'} A'$ to $A'$ splits as a $T$-$T$-homomorphism. As is easily seen, $A'$ is $(B', T)$-projective if and only if there are elements $t_1, \cdots, t_n \in T$ and $a_1', \cdots, a_n' \in A'$ such that $\sum t_i a_i' = 1$ and $\sum i t_i \otimes a_i' = \sum t_i \otimes a_i' x (\in T \otimes_{B'} A')$ for all $x$ in $T$. When this is the case, $\{(t_i, a_i') \}; i = 1, \cdots, n$ is called a $(B', T)$-projective coordinate system for $A'$. If $A'$ is $(B', A')$-projective, then we call $A'/B'$ a separable extension.

Let $f$ and $g$ be ring homomorphisms from a ring $A'$ to a ring $A''$. $f$ and $g$ are called strongly distinct if, for any non-zero central idempotent $e$ of $A''$, there is an element $x$ in $A'$ such that $f(x)e \neq g(x)e$. Let $\emptyset$ be a set of
ring homomorphisms from $A'$ to $A''$. $\mathcal{S}$ is called \textit{strongly distinct} if any distinct $f$, $g$ in $\mathcal{S}$ are strongly distinct.

$A=\Delta(A, G)$ denotes the trivial crossed product of $A$ with $G$: $A=\sum_{\sigma \in \mathcal{S}} A u_{\sigma}, \ u_{\sigma}u_{\tau}=u_{\sigma \tau} (\sigma, \tau \in G), \ u_{\sigma}x=\sigma(x)u_{\sigma} (x \in A)$. By $j$, we denote the ring homomorphism from $\Delta$ to $\text{Hom} (A_B, A_B)$ defined by $j(\xi u_{\sigma})(y)=x \cdot \sigma(y)$ for $x$, $y$ in $A$ and $\sigma$ in $G$.

$A/B$ is called a \textit{$G$-Galois extension} if there are elements $a_1, \ldots, a_n$; $a_1^*, \ldots, a_n^*$ in $A$ such that $\sum_i a_i \sigma(a_i^*)=\delta_{1, \sigma}$ for all $\sigma$ in $G$. When this is the case, \{$(a_i, a_i^*)$: $i=1, \ldots, n$\} is called a \textit{$G$-Galois coordinate system} for $A/B$. Then the following is known: $A/B$ is a $G$-Galois extension if and only if $A_B$ is finitely generated and projective and $j$ is an onto homomorphism (cf. [6]). When this is the case we identify $\Delta$ with $\text{Hom} (A_B, A_B)$: $\Delta=A_G=AG$, where $A_i$ means the set of all left multiplications by elements of $A$. If $A/B$ is $G$-Galois and $C=V_A(B)$ (the centralizer of $B$ in $A$), it is called \textit{outer $G$-Galois}. If $A/B$ is $G$-Galois (resp. outer $G$-Galois) and $H$ is a subgroup of $G$, then $A/A^H$ is evidently $H$-Galois (resp. outer $H$-Galois).

\textbf{Proposition 1.1.} Let $A'$ and $A''$ be rings, $T$ a subring of $A'$, $f$ a ring homomorphism from $T$ to $A''$, and $g$ a ring homomorphism from $A'$ to $A''$. If there are elements $t_1, \ldots, t_n \in T$ and $a_1, \ldots, a_n \in A'$ such that $\sum_i t_ia_i=1$ and $\sum_i f(t_i)g(a_i)=0$, then $f$ and $g|T$ (the restriction of $g$ to $T$) are strongly distinct.

\textit{Proof.} Let $e$ be a central idempotent of $A''$ such that $f(x)e=g(x)e$ for all $x \in T$. Since $\sum_i t_ia_i=1$, we have $\sum_i g(t_i)g(a_i)=1$, and therefore $e=e1=\sum_i e\cdot g(t_i)g(a_i)=\sum_i e\cdot f(t_i)g(a_i)=0$. Thus, $f$ and $g|T$ are strongly distinct.

\textbf{Proposition 1.2.} Let $B'$ and $T$ be subrings of a ring $A'$ such that $B' \subseteq T$, and $A''$ an extension ring of $B'$ such that $V_{A''}(B')=V_{A''}(A'')$, where $V_{A''}(B')$ means the centralizer of $B'$ in $A''$. Let $A'$ be $(B', T)$-projective, and \{$(t_i, a_i); i=1, \ldots, n$\} a $(B', T)$-projective coordinate system for $A'$. Let $f$ be a $B'$-ring homomorphism from $T$ to $A''$, $g$ and $g'$ $B'$-ring homomorphisms from $A'$ to $A''$. We set $e=\sum_i f(t_i)g(a_i)$ and $e'=\sum_i f(t_i)g'(a_i)$. Then there hold the following:

(1) $e$ is a central idempotent in $A''$.
(2) $f(x)e=g(x)e$ for all $x \in T$.
(3) $ee'=e \sum_i g(t_i)g'(a_i)$.
(4) $f$ and $g'|T$ are strongly distinct if and only if $e=0$.
(5) If $g|T$ and $g'|T$ are strongly distinct, then $ee'=0$.

\textit{Proof.} Since $\sum_i x_t \otimes a_i = \sum_i t_i \otimes a_i x$ ($\in T \otimes_{B'} A'$) for all $x$ in $T$, $\sum_i f(x_t) \otimes g(a_i) = \sum_i f(t_i) \otimes g(a_i x)$ ($\in A'' \otimes_{B'} A''$) for all $x$ in $T$. Therefore,
Finite Outer Galois Theory of Non-Commutative Rings

\[ f(x)e = e \cdot g(x) \] for all \( x \) in \( T \), in particular, \( ye = ey \) for all \( y \) in \( B' \). Hence, by assumption, \( e \) is contained in the center of \( A'' \). Since \( \sum_j f(t_j)(\sum_i f(t_i) \otimes g(a_i))g'(a_j) = (\sum_i f(t_i) \otimes g(a_i)) \sum_j g(t_j)g'(a_j) \), we obtain \( ee' = \sum_j f(t_j)e \cdot g'(a_j) = e \sum_j g(t_j)g'(a_j) \).

If we put \( g = g' \), then we have \( e^2 = e \), and so \( e \) is a central idempotent of \( A'' \) such that \( f(x)e = e \cdot g(x) \) for all \( x \) in \( T \). Therefore \( f \) and \( g \) are strongly distinct if and only if \( e = 0 \) (Prop. 1.1). Now, it is left only to prove (5). If \( g \) and \( g' \) are strongly distinct, then \( \sum_j g(t_j)g'(a_j) = 0 \) by (4), and so \( ee' = e \sum_j g(t_j)g'(a_j) = 0 \).

Evidently, the mapping \( x \otimes y \rightarrow x \sum \mu_x y \) from \( A \otimes_B A \) to \( A \) is an \( A \cdot A \)-homomorphism. We denote this homomorphism by \( h \). One may remark here that \( h \) is a \( A \cdot A \)-homomorphism. In fact, \( u, x \sum \mu_x y = \tau(x)u, \sum \mu_x y = \tau(x) \sum \mu_x y \).

**Proposition 1.3.** Let \( A/B \) be a \( G \)-Galois extension, and let \( \{(a_i, a_i^*); i = 1, \cdots, n\} \) be a \( G \)-Galois coordinate system for \( A/B \). Then \( h \) is a \( A \)-isomorphism, \( h^{-1}(\sum \sigma x \mu_x) = \sum \sigma \sum \sigma x \sigma(a_i) \otimes a_i^* \) for every \( \sum \sigma x \mu_x \) in \( A \), and \( \{(a_i, a_i^*); i = 1, \cdots, n\} \) is a \( (B, A) \)-projective coordinate system for \( A \).

**Proof.** To be easily seen, \( h(\sum \sigma \sum \sigma x \sigma(a_i) \otimes a_i^*) = \sum \sigma x \mu_x \), and hence \( h \) is onto. Let \( x, y \) be in \( A \). Then \( \sum \sigma \sum \sigma x \sigma(y) \sigma(a_i) \otimes a_i^* = x \otimes \sum \sigma \sum \sigma(y) \sigma(a_i) a_i^* = x \otimes y \), whence we can easily see that \( h \) is \( 1-1 \). Hence, \( h \) is a \( A \)-isomorphism. Since \( h(\sum \sigma a_i \otimes a_i^*) = u \), and \( h \) is an \( A \)-isomorphism, \( \sum \sigma a_i \otimes a_i^* = \sum \sigma a_i \otimes a_i^* x \) for any \( x \) in \( A \).

**Proposition 1.4.** Assume \( V_A(B) = C \) (the center of \( A \)), and let \( a_i, a_i^* \) (\( i = 1, \cdots, n \)) be elements of \( A \). Then the following conditions are equivalent:

(i) \( \{(a_i, a_i^*); i = 1, \cdots, n\} \) is a \( G \)-Galois coordinate system for \( A/B \). (ii) \( \{(a_i, a_i^*); i = 1, \cdots, n\} \) is \( (B, A) \)-projective coordinate system for \( A/B \) and \( G \) is strongly distinct.

**Proof.** (i) \( \Rightarrow \) (ii) follows from Prop. 1.3 and Prop. 1.1. (ii) \( \Rightarrow \) (i) follows from Prop. 1.2 (4).

Restating the above proposition we obtain the following theorem.

**Theorem 1.5.** (Cf. [4; Th. 1.3].) Let \( V_A(B) = C \). Then following conditions are equivalent:

(i) \( A/B \) is a \( G \)-Galois extension.
(ii) \( A/B \) is a separable extension and \( G \) is strongly distinct.

Remark. To prove the part (i) \( \Rightarrow \) (ii) we do not need the condition \( V_A(B) = C \).

**Proposition 1.6.** (Cf. [4; Th. 4.2].) If \( A/B \) is a \( G \)-Galois extension and \( B \cong B^n \) for some natural number \( m \), then \( B \cong B^n \).

**Proof.** Let \( A = \sum \sigma Bi \) (\( i = 1, \cdots, n \)), and \( B \cong B^n \) by the correspondence
$y\rightarrow yd_i \ (y \in B)$. Then $A = \sum_i \oplus u_i A = \sum_i \oplus u_i B d_i = \sum_i \oplus (\sum_i u_i d_i)$ and $(\sum_i B d_i) d_i \cong \sum_i B d_i$ as $\sum_i B d_i$-left modules. Hence, $\mathfrak{m}_G A \cong _\mathfrak{m}BG^m$. On the other hand, $A \cong _A \otimes A \cong _A \otimes (B^m) \cong _A \Delta A^m$ (Prop. 1.3). We obtain therefore $\mathfrak{m}_G BG^m \cong _\mathfrak{m}BG^m$.

**Theorem 1.7.** Let $A/B$ be a $G$-Galois extension and $_B A \cong _B A^m$ for some natural number $m$. If $B$ is semi-primary (i.e., $B/\mathfrak{R}(B)$ satisfies the minimal condition for left ideals, where $\mathfrak{R}(B)$ means the Jacobson radical of $B$), then $\mathfrak{m}_G BG \cong _\mathfrak{m}BG^m$, that is, $A$ has a normal basis.

**Proof.** By Prop. 1.6, $\mathfrak{m}_G BG^m \cong _\mathfrak{m}BG^m$. Since $\mathfrak{R}(B)G \cdot BG^m = \mathfrak{R}(B)G^m \hookrightarrow (\mathfrak{R}(B)A)^m$ under the above isomorphism, $(BG/\mathfrak{R}(B)G)^m \cong (A/\mathfrak{R}(B)A)^m$ as $BG/\mathfrak{R}(B)G$-left modules. Since $BG/\mathfrak{R}(B)G$ is $B/\mathfrak{R}(B)$-left finitely generated and $B$ is semi-primary, $BG/\mathfrak{R}(B)G$ satisfies the minimal condition (and the maximal condition) for left ideals. Hence, by Krull-Remak-Schmidt's theorem, we have $BG/\mathfrak{R}(B)G \cong A/\mathfrak{R}(B)A$ as $BG$-left modules. Since $\mathfrak{m}_G BG$ and $\mathfrak{m}_G A$ are finitely generated and projective and $\mathfrak{R}(B)G \subseteq \mathfrak{R}(\mathfrak{m}_G BG)$ and $\mathfrak{R}(B)A \subseteq \mathfrak{R}(\mathfrak{m}_G A)$, $BG \cong A$ as $BG$-left modules by the uniqueness of projective cover (cf. [11]).

§ 2. The first characterization of fixed-subrings. For any subgroup $H$ of $G$, the mapping $x \rightarrow \sum_{\sigma \in H} \tau(x)$ from $A$ to $A^H$ is evidently an $A^H$-$A^H$-homomorphism. We denote this by $t_H$.

Let $A/B$ be a $G$-Galois extension. Then $(\sum_i u_i) A \cong \text{Hom} (A_B, B_B)$ by $j$ (cf. [6]). From this fact, one will easily see that $B_B$ is a direct summand of $A_B$ if and only if there exists an element $c$ in $A$ such that $t_\emptyset (c) = 1$. Further, since $j((\sum_i u_i) V_A (B)) = \text{Hom} (\emptyset_A B_B, \emptyset_B B_B)$, $\emptyset_B B_B$ is a direct summand of $\emptyset_A B_B$ if and only if there exists an element $c$ in $V_A (B)$ such that $t_\emptyset (c) = 1$.

Let $c$ be an element of $A$ such that $t_\emptyset (c) = 1$, $H$ a subgroup of $G$, and $G = H_1 \cup \cdots \cup H_r$ the right coset decomposition of $G$. If we set $\sum_\emptyset (x) c = d$, then $t_H (d) = 1$. Hence, if $A/B$ is $G$-Galois and $B_B$ is a direct summand of $A_B$, then $A_B^H$ is a direct summand of $A_A^H$.

For any $G$-left module $M$ and any subgroup $H$ of $G$, we denote by $M^H\{u \in M; \tau (u) = u \text{ for all } \tau \in H\}$. If $A/B$ is a $G$-Galois extension, then $h: \sigma_A \otimes_B A_B \cong \sigma A_B$ (Prop. 1.3), and evidently $(A \otimes_A) \cong \Delta A^\mu$ under $h$.

**Proposition 2.1.** Let $A/B$ be a $G$-Galois extension. If $H$ is a subgroup of $G$, then $A^H = \{\sum_i u_i x_i; \text{ if } H\sigma = H\tau \text{ then } x_i = x_i\}$ and $(A \otimes_A)^H = A^H \otimes A$.

**Proof.** The first assertion is evident. We shall prove the second one. Evidently $A^H \otimes A \cong (A \otimes A)^H$. Let $\{a_i, a_i^*; i = 1, \cdots, n\}$ be a $G$-Galois coordinate system for $A/B$. If $\rho$ is an element of $G$, then $\sum_i \epsilon H u_i \in A^H$ and $h^{-1}(\sum_i \epsilon H u_i) = \sum_i \epsilon H \sum_i \tau (a_i) \otimes a_i^* = \sum_i (\sum_{\epsilon H} \tau (a_i)) \otimes a_i^* \in A^H \otimes A$. Noting that $h$
is an $A$-right isomorphism, we have $(A\otimes A)^{H} \subseteq A^{H} \otimes A$. Thus $(A\otimes A)^{H} = A^{H} \otimes A$.

**Proposition 2.2.** Let $A/B$ be $G$-Galois. If $H$ is a subgroup of $G$, then there are elements $t_{1}, \cdots, t_{n} \in A^{H}$ and $a_{1}^{*}, \cdots, a_{n}^{*} \in A$ such that $\sum t_{i} \sigma(a_{i}^{*}) = \delta_{H, \sigma}$ for all $\sigma$ in $G$, and $\{\sigma \in G; \sigma | A^{H} = 1_{A^{H}}\} = H$.

**Proof.** Let $\{(a_{i}, a_{i}^{*}); i=1, \cdots, n\}$ be a $G$-Galois coordinate system for $A/B$. If we put $t_{i} = t_{H}(a_{i})$, then $t_{i} \in A^{H}$ and $\sum t_{i} \sigma(a_{i}^{*}) = \delta_{H, \sigma}$. If $\sigma | A^{H} = 1_{A^{H}}$, then $1 = \sum t_{i} \sigma(a_{i}^{*}) = \sum_{\sigma \in H} \sigma \delta_{H, \sigma}$. Hence $\sigma \in H$.

**Theorem 2.3.** Let $A/B$ be $G$-Galois, and $B_{n}$ a direct summand of $A_{n}$. If $H$ is a subgroup of $G$ and $T$ is an intermediate subring of $A/B$ such that $T \subseteq A^{H}$, then the following conditions for $T$ are equivalent.

(i) $T = A^{H}$.

(ii) There are elements $t_{1}, \cdots, t_{n} \in T$ and $a_{1}^{*}, \cdots, a_{n}^{*} \in A$ such that $\sum t_{i} \sigma(a_{i}^{*}) = \delta_{H, \sigma}$ for all $\sigma$ in $G$.

(iii) $T \otimes A = A^{H} \otimes A$ in $A \otimes_{B} A$.

**Proof.** (i) $\Rightarrow$ (ii) follows from Prop. 2.2. (ii) $\Rightarrow$ (iii) Evidently $T \otimes A \subseteq A^{H} \otimes A$ in $A \otimes_{B} A$. If $\rho$ is in $G$, then $\sum t_{i} \otimes \rho^{-1}(a_{i}^{*}) \in T \otimes A$ and

$$h\left(\sum t_{i} \otimes \rho^{-1}(a_{i}^{*})\right) = \sum_{\sigma \in H} u_{\sigma}.$$ 

Noting that $h$ is an $A$-right homomorphism, we know that $h(T \otimes A) = A^{H}$, and hence $T \otimes A = A^{H} \otimes A$ (Prop. 2.1). (iii) $\Rightarrow$ (i) There is an element $c$ of $A$ such that $t_{0}(c) = 1$. For any $x$ in $A^{H}$, $x \otimes c \in A^{H} \otimes A = T \otimes A$. Therefore, there are elements $x_{j}'s \in T$, $y_{j}'s \in A$ such that $x \otimes c = \sum_{j} x_{j} \otimes y_{j}$. By making use of the mapping $1 \otimes t_{0}$, we can easily see $x = x_{1} \otimes t_{0}(c) = \sum_{j} x_{j} \otimes t_{0}(y_{j}) \in T \cdot B = T$. Hence $T = A^{H}$.

**Proposition 2.4.** Let $A/B$ be a $G$-Galois extension. If $H$ is a subgroup of $G$, then $G|A^{H}$ is strongly distinct and the mapping $x \otimes y \rightarrow xy$ from $A^{H} \otimes_{B} A$ to $A$ splits as an $A^{H}$-$A^{H}$-homomorphism (i.e. $A$ is $(B, A^{H})$-projective).

**Proof.** Let $\{(a_{i}, a_{i}^{*}); i=1, \cdots, n\}$ be a $G$-Galois coordinate system for $A/B$. If we set $t_{i} = t_{H}(a_{i})$, then $t_{i} \in A^{H}$ and $\sum t_{i} \sigma(a_{i}^{*}) = \delta_{H, \sigma}$ for every $\sigma$ in $G$. Therefore, by Prop. 1.1, $G|A^{H}$ is strongly distinct. Now, $t_{H} \otimes 1$ is an $A^{H}$-$A^{H}$-homomorphism from $A \otimes_{B} A$ to $A^{H} \otimes_{B} A$. Since $\sum_{x} x a_{i} \otimes a_{i}^{*} = \sum_{x} a_{i} \otimes a_{i}^{*} x (\in A \otimes_{B} A)$ for all $x$ in $A$ (Prop. 1.3), $\sum_{x} y t_{i} \otimes a_{i}^{*} = \sum_{x} t_{i} \otimes a_{i}^{*} y (\in A^{H} \otimes_{B} A)$ for all $y$ in $A^{H}$. Hence the mapping $x \rightarrow \sum t_{i} \otimes a_{i}^{*} x$ from $A$ to $A^{H} \otimes_{B} A$ is an $A^{H}$-$A^{H}$-homomorphism, and $\sum t_{i} \otimes a_{i}^{*} = x$. Hence the mapping $x \otimes y \rightarrow xy$ from $A^{H} \otimes_{B} A$ to $A$ splits as an $A^{H}$-$A^{H}$-homomorphism.

**Proposition 2.5.** Let $A/B$ be outer $G$-Galois, and $T$ an intermediate ring of $A/B$. If $G|T$ is strongly distinct, and $A$ is $(B, T)$-projective then there are elements $t_{1}, \cdots, t_{n} \in T$ and $a_{1}^{*}, \cdots, a_{n}^{*} \in A$ such that $\sum t_{i} \sigma(a_{i}^{*}) = \delta_{H, \sigma}$
for all \( \sigma \) in \( G \), where \( H = \{ \sigma \in G; \sigma|T = 1_{T} \} \).

**Proof.** Let \( \{(t_{i}, a_{i}^{*}); i=1, \cdots; n\} \) be a \((B, T)\)-projective coordinate system for \( A \). Then, by Prop. 1.2, \( \sum_{i}t_{i}\sigma(a_{i}^{*}) = 0 \) for every \( \sigma \notin H \). Whereas, if \( \sigma \in H \), then \( 1 = \sum_{i}\sigma(t_{i})\sigma(a_{i}^{*}) = \sum_{i}t_{i}\sigma(a_{i}^{*}) \).

Combining Props 2.4, 2.5 with Th. 2.3, we readily obtain the following:

**Theorem 2.6.** Let \( A/B \) be outer \( G\)-Galois, and \( B_{B} \) a direct summand of \( A_{B} \). If \( T \) is an intermediate ring of \( A/B \), then the following conditions are equivalent:

(i) There is a subgroup \( H \) of \( G \) such that \( T = A^{H} \).

(ii) \( A \) is \((B, T)\)-projective and \( G\midT \) is strongly distinct.

**Lemma 2.7.** Let \( S \) and \( T \) be subrings of a ring \( R \) such that \( S \supseteq T \).

1. If \( R\midT \) is separable, then so is \( R\midS \).
2. If \( S\midT \) is separable, then \( R \) is \((T, S)\)-projective.
3. If both \( R\midS \) and \( S\midT \) are separable, then so is \( R\midT \).

**Proof.** (1) will be easily seen. (2) Since \( S \otimes_{T}S \otimes_{R}R \cong S \otimes_{T}R \) and \( S \otimes_{S}R \cong R \), this is obvious. (3) Since the mapping \( s \otimes s' \rightarrow ss' \) from \( S \otimes_{T}S \) to \( S \) splits as an \( S\midS \)-homomorphism, the mapping \( r \otimes r' \rightarrow r \otimes r' \) from \( R \otimes_{T}R \) to \( R \otimes_{S}R \) splits as an \( R\midR \)-homomorphism. Since \( R\midS \) is separable, the mapping \( r \otimes r' \rightarrow rr' \) from \( R \otimes_{S}R \) to \( R \) splits as an \( R\midR \)-homomorphism.

**Proposition 2.8.** Let \( A/B \) be outer \( G\)-Galois, and \( B_{B} \) a direct summand of \( A_{B} \). If \( H \) is a subgroup of \( G \), then \( A^{H} \) is an \( A^{H} \)-\( A^{H} \)-direct summand of \( A \), and \( A^{H}/B \) is a separable extension.

**Proof.** Since \( B_{B} \) is a direct summand of \( A_{B} \), there is an element \( c \) of \( C \) such that \( t_{0}(c) = 1 \). Let \( G = Ha_{1} \cup \cdots \cup Ha_{r} \) be the right coset decomposition of \( G \). If we set \( d = \sum_{k}a_{k}(c) \), then \( t_{B}(d) = 1 \) and \( d \subseteq C \). Hence \( A^{H} \) is an \( A^{H} \)-\( A^{H} \)-direct summand of \( A \). Let \( \{(a_{i}, a_{i}^{*}); i=1, \cdots, n\} \) be a \((B, A)\)-projective coordinate system for \( A/B \). Then, \( \{(a_{i}, a_{i}^{*}); i=1, \cdots, n\} \) is a \( G\)-Galois coordinate system for \( A/B \) (Prop. 1.4). The mapping \( x \rightarrow t_{B}(dx) \) from \( A \) to \( A^{H} \) is an \( A^{H} \)-\( A^{H} \)-homomorphism. We denote this by \( t' \). Then, the mapping \( t_{H} \otimes t' \) from \( A \otimes_{B}A \) to \( A^{H} \otimes_{B}A^{H} \) is evidently an \( A^{H} \)-\( A^{H} \)-homomorphism, and therefore the mapping \( y \rightarrow \sum_{i}t_{H}(ya_{i}) \otimes t'(a_{i}^{*}) = \sum_{i}t_{H}(a_{i}) \otimes t'(a_{i}^{*}y) \) from \( A^{H} \) to \( A^{H} \otimes_{B}A^{H} \) is an \( A^{H} \)-\( A^{H} \)-homomorphism. Since \( \sum_{i}t_{H}(a_{i})t'(a_{i}^{*}y) = \sum_{i}t_{H}(a_{i}) \otimes t'(a_{i}^{*}) \tau(d)y = \sum_{i, \epsilon \in H}t_{H}(a_{i})^{*} \tau(d)y = \sum_{i, \epsilon \in H}t_{H}(a_{i})^{*} \tau(d)y = y \) for all \( y \) in \( A^{H} \), \( A^{H}/B \) is a separable extension.

By Th. 2.6, Lemma 2.7 and Prop. 2.8, we obtain at once the following:

**Theorem 2.9.** (Cf. [4; Th. 2.2]). Let \( A/B \) be outer \( G\)-Galois, and \( B_{B} \) a direct summand of \( A_{B} \). If \( T \) is an intermediate ring of \( A/B \), then the
following conditions are equivalent:

(i) There is a subgroup \( H \) of \( G \) such that \( T = A^H \).

(ii) \( T/B \) is a separable extension and \( G|T \) is strongly distinct.

§ 3. The second characterization of fixed-subrings.

Let \( R \) be a ring, \( S \) a subring of \( R \). \( R/S \) is called a projective Frobenius extension if \( R_S \) is finitely generated and projective and \( _sR_R \cong _s\text{Hom}(R_S, S_R) \) (cf. [10]). If \( A/B \) is a \( G \)-Galois extension, then \( (\sigma \sum \alpha)A_A \cong _s\text{Hom}(A_B, B_A) \) by \( j \). Hence, \( A/B \) is a projective Frobenius extension. Now, we shall state the next lemma without proof.

**Lemma 3.1.** Let \( R/S \) be a projective Frobenius extension, and \( 1 \to t \) under an isomorphism \( _sR_R \cong _s\text{Hom}(R_S, S_R) \). Then \( \text{teHom}(sR_S, sS_R) \), \( \text{Hom}(R_S, S_S)_t = tR \) and \( \text{Hom}(R_S, R_S)_t = R_tR \).

**Theorem 3.2.** Let \( A/B \) be outer \( G \)-Galois, and \( B_B \) a direct summand of \( A_B \). If \( T \) is an intermediate ring of \( A/B \), then the following conditions are equivalent.

(i) There is a subgroup \( H \) of \( G \) such that \( A^H = T \).

(ii) \( A/T \) is a projective Frobenius extension, \( T_T \) is a direct summand of \( A_T \), and \( G|T \) is strongly distinct.

**Proof.** It suffices to prove that (ii) \( \Rightarrow \) (i) (cf. § 2). We identify \( \text{Hom}(A_B, A_B) \) with \( \Delta \), and set \( \Delta_B = \text{Hom}(A_T, A_T) \), which is a subring of \( \Delta \). Let \( t = \sum c_i u_i \) be the image of 1 under the isomorphism \( _A \Delta_A \cong _A \text{Hom}(A_T, T_T)_A \). Then \( tA = \text{Hom}(A_T, T_T), \ A_T = \Delta_B \) and \( t \in \text{Hom}(sA_T, sT_T) \) (Lemma 3.1). Since \( xt = tx \) for all \( x \) in \( T \), we have \( x_{c_i} = c_i \alpha(x) \) for all \( x \) in \( T \) and \( \alpha \) in \( G \), in particular, \( y_{c_i} = c_i y \) for \( y \) in \( B \). Therefore, by assumption, each \( c_i \) is an element of \( C \). Since \( A_T = A_B \), there are elements \( c_i \)'s, \( d_i \)'s in \( A \) such that \( \sum c_i d_i = u_i \). From this fact, \( c_1 \) is an invertible element of \( C \). Now, the mapping \( \alpha : \delta \to \delta c_1^{-1} \) is a \( \Delta \)-\( A \)-homomorphism from \( \Delta_B \) to \( \Delta \), and the mapping \( \beta : \sum x_{c_i} u_i \to \sum x_{c_i} c_i u_i \), is evidently an \( A \)-\( A \)-endomorphism of \( \Delta \). For any \( y \) in \( A \) and \( z \) in \( T \), we have \( \sum x_{c_i} u_i \to \sum x_{c_i} c_i u_i \) is evidently a \( A \)-\( A \)-endomorphism of \( \Delta \). For any \( y \) in \( A \) and \( z \) in \( T \), we have \( \delta(xyt) = \delta(xt(yz)) = \delta(x) \cdot t(yz) = \delta_0(x) \cdot ty(z) \). Thus, \( \beta \) is a \( \Delta \)-\( A \)-homomorphism from \( A \otimes_B A \to \Delta_B \), and so \( \beta \) is a \( \Delta \)-\( A \)-homomorphism from \( A \) to \( \Delta_B \). Since \( \beta \alpha(u_i) = \beta(u_i c_i^{-1}) = u_1, \ \beta \alpha = 1_{\Delta} \). Thus, we have \( \Delta = \text{Im} \alpha \oplus \ker \beta = \Delta \oplus (\sum c_i \text{Ann}_A(c_i) u_i) \), where \( \text{Ann}_A(c_i) = \{ x \in A; xc_i = 0 \} \). Now, let \( \{ (a_i, a_i^*) ; i = 1, \ldots, n \} \) be a \( G \)-Galois coordinate system for \( A/B \). If \( \tau \) is in \( G \), then \( \Delta_B = A \oplus \sum \tau(a_i) ta_i^* = c_i u_i \), and so \( \Delta_B = \sum A c_i u_i \), whence it follows that \( A = A c_i \oplus \text{Ann}_A(c_i) \). Let \( A c_i = A e_i \), with a
central idempotent $e_{r}$ in $A$. Then, $e_{r} \cdot \sigma(y) = e_{r} y$ for any $y$ in $T$. By assumption, if $|T| \neq 1_{T}$ then $e_{r} = 0$, and so $A_{0} = \sum_{r \in H} \mathbb{C} e_{r}$, where $H = \{ \tau \in G ; |\tau| = 1_{T} \}$.

Since $T_{\tau}$ is a direct summand of $A_{\tau}$, $\text{End} (t_{\tau} A) = T_{\tau}$, the set of all right multiplications by elements of $T$ (see [1; Th. A. 2]). On the other hand, since $A_{0} = \sum_{r \in H} \mathbb{C} e_{r}$, $\text{End} (t_{\tau} A) = (A^{H})_{\tau}$. Hence, $T = A^{H}$.

§ 4. Extension of isomorphisms.

Theorem 4.1. Let $A/B$ be G-Galois, and $A'$ an extension ring of $B$ such that $V_{A'}(b) = V_{A'}(A')$. Assume that there exists at least one B-ring homomorphism from $A$ to $A'$.

(1) If $H$ is a subgroup of $G$ such that $A_{A^{H}}^{H}$ is a direct summand of $A_{A^{H}}$. Then every B-ring homomorphism from $A^{H}$ to $A'$ can be extended to a (B-)ring homomorphism from $A$ to $A'$.

(2) If $f$ and $g$ are B-ring homomorphisms from $A$ to $A'$. Then $A'$ contains orthogonal central idempotents $e_{\sigma}(\sigma \in G)$ such that $\sum_{e} e_{r} = 1$ and $f(x) = \sum_{e} e_{\sigma} g(x) e_{r}$ for all $x$ in $A$. (Cf. [4; Th. 3.1].)

Proof. There are elements $a_{i}$, $a_{i}^{*} (i = 1, \ldots, n)$ in $A$ such that $\sum_{i} x a_{i} \otimes a_{i}^{*} = \sum_{i} a_{i} \otimes a_{i}^{*} x (\in A \otimes_{B} A)$ for all $x$ in $A$ and $\sum_{i} a_{i} \cdot \sigma(a_{i}^{*}) = \delta_{i, r}$ for all $\sigma$ in $G$ (Prop. 1.3). If we set $t_{i} = t_{H}(a_{i})$, then $t_{i} \in A^{H}$, $\sum_{i} t_{i} \cdot \sigma(a_{i}^{*}) = \delta_{i, r}$, for all $\sigma$ in $G$ and $\sum_{i} x t_{i} \otimes a_{i}^{*} = \sum_{i} x t_{i} \otimes a_{i}^{*} x (\in A^{H} \otimes_{B} A)$ for all $x$ in $A^{H}$. Let $f$ be a B-ring homomorphism from $A^{H}$ to $A'$, and $g$ a B-ring homomorphism from $A$ to $A'$. If we set $e_{r} = \sum_{i} f(t_{i}) g_{\sigma}(a_{i}^{*})$, then each $e_{r}$ is a central idempotent in $A'$ (Prop. 1.2). By Prop. 1.2 (3), $e_{r} = e_{\sigma} g(\sum_{\tau} \sigma(t_{i}) \tau a_{i}^{*})$ for any $\sigma$, $\tau$ in $G$. Therefore, if $\sigma^{-1} \tau \not\in H$ then $e_{\sigma r} = 0$, and if $\sigma^{-1} \tau \in H$ then $e_{\sigma r} = e_{r}$. Recalling that $A_{A^{H}}^{H}$ is a direct summand of $A_{A^{H}}$ there is an element $d$ of $A$ such that $t_{H}(d) = 1$. Since $\sum_{i} \sum_{t_{i} \cdot \sigma(a_{i}^{*})} x (\in A \otimes_{B} A)$, $\sum_{i} a_{i} \cdot \sigma(a_{i}^{*}) = \delta_{i, r}$, for all $\sigma$ in $G$ (Prop. 1.3). If we set $t_{i} = t_{H}(a_{i})$, then $t_{i} \in A^{H}$, $\sum_{i} t_{i} \cdot \sigma(a_{i}^{*}) = \delta_{i, r}$, for all $\sigma$ in $G$ and $\sum_{i} x t_{i} \otimes a_{i}^{*} = \sum_{i} x t_{i} \otimes a_{i}^{*} x (\in A^{H} \otimes_{B} A)$ for all $x$ in $A^{H}$. Let $f$ be a B-ring homomorphism from $A^{H}$ to $A'$, and $g$ a B-ring homomorphism from $A$ to $A'$. If we set $e_{r} = \sum_{i} f(t_{i}) g_{\sigma}(a_{i}^{*})$, then each $e_{r}$ is a central idempotent in $A'$ (Prop. 1.2). By Prop. 1.2 (3), $e_{r} = e_{\sigma} g(\sum_{\tau} \sigma(t_{i}) \tau a_{i}^{*})$ for any $\sigma$, $\tau$ in $G$. Therefore, if $\sigma^{-1} \tau \not\in H$ then $e_{\sigma r} = 0$, and if $\sigma^{-1} \tau \in H$ then $e_{\sigma r} = e_{r}$. Recalling that $A_{A^{H}}^{H}$ is a direct summand of $A_{A^{H}}$ there is an element $d$ of $A$ such that $t_{H}(d) = 1$. Since $\sum_{i} \sum_{t_{i} \cdot \sigma(a_{i}^{*})} x (\in A \otimes_{B} A)$, $\sum_{i} a_{i} \cdot \sigma(a_{i}^{*}) = \delta_{i, r}$, for all $\sigma$ in $G$ (Prop. 1.3). If we set $t_{i} = t_{H}(a_{i})$, then $t_{i} \in A^{H}$, $\sum_{i} t_{i} \cdot \sigma(a_{i}^{*}) = \delta_{i, r}$, for all $\sigma$ in $G$ and $\sum_{i} x t_{i} \otimes a_{i}^{*} = \sum_{i} x t_{i} \otimes a_{i}^{*} x (\in A^{H} \otimes_{B} A)$ for all $x$ in $A^{H}$. Let $G = \sigma H \cup \cdots \cup \sigma H$ be the left coset decomposition of $G$. Then, $1 = \sum_{s} \sum_{t} f(t_{i}) g_{\sigma}(a_{i}^{*}) = \sum_{k} \sum_{x e_{r}} g_{e_{r}} t_{H}(d) = \sum_{k} e_{r} \cdot g_{e_{r}} t_{H}(d) = \sum_{k} e_{r} \cdot g_{e_{r}} x (\in A^{H} \otimes_{B} A)$ for all $x$ in $A^{H} (\text{Prop. 1.2})$, we have $f(x) e_{r} = e_{r} \cdot g_{\sigma}(x)$ for all $x$ in $A^{H} (\text{Prop. 1.2})$, we have $f(x) e_{r} = e_{r} \cdot g_{\sigma}(x)$ for all $x$ in $A^{H}$. Evidently, the mapping $z \mapsto \sum_{k} e_{r} \cdot g_{e_{r}} z$ is a B-ring homomorphism from $A$ to $A'$, and an extension of $f$.

Now, the following theorem will follow at once from Th. 4.1.

Theorem 4.2. Let $A/B$ be an outer G-Galois extension, and let $A$ be directly indecomposable. If $H$ is a subgroup of $G$ such that $A_{A^{H}}^{H}$ is a direct summand of $A_{A^{H}}$, then every B-ring homomorphism from $A^{H}$ to $A$ can be extended to an element of $G$. In particular, $G$ is the set of all B-ring automorphisms of $A$. 

Y. Miyashita

**Theorem 5.1.** Let $A/B$ be $G$-Galois, $A'$ a $G$-invariant subring of $A$, and $B' = A''$. Assume that there are elements $a_i, a_i^*$, $i = 1, \ldots, n$ and $c$ in $A'$ such that $\sum t_{l} a_t \sigma(a_{t}^*) = \delta_{1,n}$, and $t_0(c) = 1$.

1. Let $A'/B'$ be a $G$-Galois extension, and $A'' = B \otimes_B A'' = A'' \otimes_B B$ for any subgroup $H$ of $G$, in particular, $A = B \otimes_B A' = A' \otimes_B A'$.

2. Let $\{ \overline{X} \}$ be the set of all $A'$-left submodules of $A$, and $\{ X \}$ the set of all $B'$-left submodules of $B$. Then, $\overline{X} \rightarrow \overline{X} \cap B$ and $X \rightarrow A'X = A' \otimes_B X$ are mutually converse order isomorphisms between $\{ \overline{X} \}$ and $\{ X \}$.

3. Let $\{ \overline{Y} \}$ be the set of all $G$-invariant intermediate rings of $A'/A'$, and $\{ Y \}$ the set of all intermediate rings of $B'/B'$ such that $A'Y = YA'$. Then, $\overline{Y}/(\overline{Y} \cap B)$ is $G$-Galois, and $\overline{Y} \rightarrow \overline{Y} \cap B$ and $Y \rightarrow A'Y = YA'$ are mutually converse order isomorphisms between $\{ \overline{Y} \}$ and $\{ Y \}$.

**Proof.** (1) Evidently, $G \cong G|A'$, and $G$ may be regarded as a finite group of automorphisms of $A'$. Hence, $A'/B'$ is $G$-Galois. Let $G = H_1 \cup \cdots \cup H_r$, be the right coset decomposition of $G$. If we put $d = \sum t_i \sigma(a_i^*)$ and $t_0 = t_0(a_i^*)$, then $t_0(d) = 1$ and $\sum t_i \sigma(a_i^*) = \delta_{H_i}$. If $x$ is in $A''$, then $A''B \ni \sum t_i t_0(a_i^* dy) = \sum (\sum t_i \sigma(a_i^*)) \sigma(dx) = t_0(dx) = t_0(d)x = x$. Thus, we obtain $A'' = A''B$. To be easily seen, the mapping $\sum_j x_j \otimes y_j \rightarrow \sum_j x_j y_j$ from $A'' \otimes B'$ to $A''B = A''$ is well-defined and $\sum_j x_j \otimes t_0(a_i^* d \sum_j x_j y_j) = \sum_j x_j \otimes y_j$. Hence, $A'' \otimes B' = A''B = A''$ by the mapping $\sum_j x_j \otimes y_j \rightarrow \sum_j x_j y_j$. Symmetrically, it follows $A'' = B \otimes_B A''$. (2) Let $X$ be an $A'$-left submodule of $A$. Evidently, $\overline{X} \supseteq A'(\overline{X} \cap B)$, and $\overline{X} \cap B$ is a $B'$-left submodule of $B$. If $x$ is in $\overline{X}$, then $t_0(a_i^* x)$ is in $\overline{X} \cap B$, and hence $x = \sum_i a_i t_0(a_i^* x) \in A'(\overline{X} \cap B)$. Hence, $\overline{X} = A'(\overline{X} \cap B)$, and the mapping $\sum_j x_j \otimes y_j \rightarrow \sum_j x_j y_j$ from $A' \otimes_B (\overline{X} \cap B)$ to $A'(\overline{X} \cap B) = \overline{X}$ is onto. Moreover, to be easily seen, $\sum_i a_i \otimes t_0(a_i^* \sum_j x_j y_j) = \sum_j x_j \otimes y_j$. Hence, $\overline{X} = A' \otimes_B (\overline{X} \cap B)$. Now, let $X$ be a $B'$-left submodule of $B$. Then, $A'X$ is an $A'$-left submodule of $A$, and $A'X \cap B \supset X$. If $\sum_j x_j y_j (x_j \in A', y_j \in X)$ is in $A'X \cap B$, then $\sum_j x_j y_j = t_0(c)(\sum_j x_j y_j) = \sum \sigma(c) \sum_j x_j y_j = \sum_j t_0(c x_j) y_j \in X$. Hence, $A'X \cap B \subseteq X$, namely, $A'X \cap B = X$. (3) Evidently, $(\overline{Y}/\overline{Y} \cap B)$ is $G$-Galois. Hence $\overline{Y} = A'((\overline{Y} \cap B)) = (\overline{Y} \cap B)A'$ by (1), and then our assertion is an easy consequence of (2).

**Corollary.** Let $A/B$ be $G$-Galois, and $B' = V_B(B)$. Assume that there are elements $a_i, a_i^*$, $i = 1, \ldots, n$ in $V_A(B)$ such that $\sum t_i a_t \sigma(a_{t}^*) = \delta_{1,n}$.

1. $V_A(B)/B'$ is $G$-Galois, $A'' = B \otimes_B V_A(B)''$ for any subgroup $H$ of $G$, and the center of $A''$ coincides with the center of $V_A(B)''$. In particular, $A = B \otimes_B V_A(B)$, and $B' \subseteq C$.

2. Let $\{ \overline{Y} \}$ be the set of all $G$-invariant intermediate rings of $A/V_A(B)$,
and \( \{Y\} \) the set of all intermediate rings of \( B/B' \). Then \( \overline{Y} \to \overline{Y} \cap B \) and \( Y \to V_A(B) \) \( Y = V_A(B) \times B \cdot A \) are mutually converse order isomorphisms between \( \{\overline{Y}\} \) and \( \{Y\} \).

(3) \( A/V_A(B) \) is separable if and only if \( B \) is a separable \( B' \)-algebra.

Proof. If remains to prove (3). If \( B/B' \) is separable, then \( A/B' \) is separable, because both \( A/B \) and \( B/B' \) are separable (Lemma 2.7). Hence \( A/V_A(B) \) is separable. Conversely, assume that \( A/V_A(B) \) is separable. Then, since both \( A/V_A(B) \) and \( V_A(B)/B' \) are separable, \( A/B' \) is separable, or equivalently, \( A \) is a separable \( B' \)-algebra (Lemma 2.7). Since \( A = B \times B', V_A(B) \), by [2; Prop. 1.7 and its Remark], \( B \) is a separable \( B' \)-algebra.

Remark. The above corollary contains Kanzaki [8; Th. 5].

Let \( A, A' \) be \( R \)-algebras over a commutative ring \( R \) such that \( A \times_R A' \neq 0 \). Assume that \( A/B \) is a \( G \)-Galois extension such that \( R \cdot 1 \subseteq B \) and \( B_B \) is a direct summand of \( A_B \), and assume that \( A/B' \) is a \( G' \)-Galois extension such that \( R \cdot 1 \subseteq B' \) and \( B'_{B'} \) is a direct summand of \( A'_{B'} \). Let \( \{(a_i, a_i^*) ; i = 1, \cdots, n\} \) and \( \{(d_j, d_j^*) ; j = 1, \cdots, m\} \) be a \( G \)-Galois coordinate system for \( A/B \) and a \( G' \)-Galois coordinate system for \( A'/B' \), respectively. For any \( \sigma \times \tau \in G \times G' \), we can define \( \sigma \times \tau \cdot \sum_j x_j \otimes y_j = \sum_j \sigma(x_j) \otimes \tau(y_j) \) \( (x_j \in A, y_j \in A') \). Then, since \( \sum_i (a_i \otimes d_j) \cdot (\sigma \times \tau)(a_i^* \otimes d_j^*) = (\sum_i a_i \sigma(a_i^*)) \otimes (\sum_j d_j \tau(d_j^*)) \), \( (A \otimes_R A')/(A \otimes A')^{\sigma \times \tau} \) is a \( G \times G' \)-Galois extension. Now, let \( H \) and \( H' \) be subgroups of \( G \) and \( G' \), respectively. Then, by assumption, there are elements \( c, c' \) in \( A \) and \( A' \), respectively such that \( \sum_{c \in H} c = 1 \) and \( \sum_{c' \in H'} c' = 1 \). If \( \sum_k x_k \otimes y_k \) is in \( (A \otimes A')^{H \times H'} \), then \( \sum_k x_k \otimes y_k = (\sum_{c \in H} c) \otimes (\sum_{c' \in H'} c') \). \( \sum_k x_k \otimes y_k = \sum_{c \in H} \sum_{c' \in H'} c \otimes c' \cdot (\sigma \times \tau)(\sum_k x_k \otimes y_k) = \sum_{c \in H} (\sum_{c' \in H'} c x_k) \otimes \sum_{c' \in H'} c' y_k) \in A^H \otimes A^H \). Hence, \( (A \otimes A')^{H \times H'} = A^H \otimes A^H \). Thus, we have the following:

Theorem 5.2. Let \( A \) and \( A' \) be algebras over a commutative ring \( R \) such that \( A \otimes_R A' \neq 0 \). If \( A/B \) is a \( G \)-Galois extension such that \( R \cdot 1 \subseteq B \) and \( B_B \) is a direct summand of \( A_B \), and \( A'/B' \) a \( G' \)-Galois extension such that \( R \cdot 1 \subseteq B' \) and \( B'_{B'} \) is a direct summand of \( A'_{B'} \), then \( (A \otimes_R A')/(B \otimes B') \) is a \( G \times G' \)-Galois extension, and \( (A \otimes A')^{H \times H'} = A^H \otimes A^{H'} \) for any subgroup \( H \) of \( G \) and any subgroup \( H' \) of \( G' \) (cf. [2; Th. A. 8]).

Corollary. Let \( A/B \) be a \( G \)-Galois extension such that \( B \subseteq C \). If \( A' \) is a \( B \)-algebra, then \( (A' \otimes_R A)/(A' \otimes 1) \) is a \( G \)-Galois extension, and \( (A' \otimes A)^H = A' \otimes A^H \) for any subgroup \( H \) of \( G \).

Proposition 5.3. Let \( A/B \) be a \( G \)-Galois extension. If \( H, K \) are subgroups of \( G \), and \( A^{H \cap K} \) is an \( A^{H \cap K} \)-left direct summand of \( A \), then \( A^{H \cap K} = A^H \cdot A^K = A^K \cdot A^H \).

Proof. By assumption, there is an element \( c \) in \( A \) such that \( t_{H \cap K}(c) = 1 \).
Evidently, $A^{H\cap K} \supseteq A^{H}. A^{K}$. Let $\{(a_{i}, a_{i}^*) ; i = 1, \cdots, n\}$ be a G-Galois coordinate system for $A/B$. If $x$ is in $A^{H\cap K}$, then $A^{H} \cdot A^{K} \ni \sum_{i} t_{H}(a_{i}) t_{K}(a_{i}^{*}cx) = \sum_{i\in H} \sum_{j\in K} \rho(a_{i}) \sigma(a_{i}^*) \sigma(cx) = t_{H\cap K}(c)x = x$. Hence $A^{H\cap K} = A^{K}. A^{H}$. Symmetrically we have $A^{H\cap K} = A^{H}. A^{K}$.

**Corollary.** Let $A/B$ be a G-Galois extension. If $H$ and $K$ are subgroups of $G$ such that $H \cap K = \{1\}$, then $A = A^{H}. A^{K} = A^{K}. A^{H}$.

**Theorem 5.4.** Let $A/B$ be a G-Galois extension, and $B$ a direct summand of $A$. If $G = KH$ and $K \cap H = \{1\}$ for a normal subgroup $K$ and a subgroup $H$, then there hold the following:

1. $A = A^{K} \otimes_{B} A^{H} = A^{H} \otimes_{B} A^{K}$.
2. $A^{K}/B$ is an $H$-Galois extension.
3. For any subgroup $H_0$ of $H$ and any subgroup $K_0$ of $K$ such that $N(K_0) \supseteq H$ (where $N(K_0)$ means the normalizer of $K_0$ in $G$), $A^{K_0} = A^{K_0} \otimes_{B} A^{K_0} = A^{K_0} \otimes_{B} A^{K_0}$ and $A^{K_0} \otimes_{B} A^{K_0}$ is an $H$-Galois extension.

**Proof.** Let $\{(a_{i}, a_{i}^*) ; i = 1, \cdots, n\}$ be a G-Galois coordinate system for $A/B$. Since $B$ is a direct summand of $A$, there is an element $c$ in $A$ such that $t_{0}(c) = 1$. Put $t_{e} = t_{H}(a_{e})$, $t_{e}^{*} = t_{K}(a_{e}^{*})$, and $d = t_{K}(c)$. Then, $t_{H}(d) = 1$ and $\sum_{\tau} t_{\tau}(t_{e}^{*}) = \delta_{1, e}$, for $\tau$ in $H$. $N(K_0) \supseteq H$ implies that $\tau(A^{K_0}) = A^{K_0}$ for all $\tau$ in $H$. Hence, by Th. 5.1, $A^{K}/A^{H}$ is an H-Galois extension. By Th. 5.1, $A^{B} = A^{H} \otimes_{B} A^{K_0} = A^{K_0} \otimes_{B} A^{H}$. Since $K_0 \cap H = K_0 \cap H$, $A^{K_0} = A^{K_0} \otimes_{B} A^{K_0}$ (Prop. 5.3). Since $A^{B} \supseteq A^{K_0}$ and $A^{K_0}$ is a right direct summand of $A$, $A^{K_0} = A^{K_0} \otimes_{B} A^{K_0}$. Similarly, we have $A^{K_0} \otimes_{B} A^{K_0}$.

**Corollary.** Let $A/B$ be a G-Galois extension, $B$ a direct summand of $A$, and $G = N_1 \times \cdots \times N_r$. If $H = N_1 \times \cdots \times N_{i} \times \cdots \times N_r (i = 1, \cdots, r)$, then $A^{B}/B$ is $N$-Galois, $A = A^{H} \otimes_{B} \cdots \otimes_{B} A^{H_r}$, and $A^{K_1} \cdots A^{K_r} = A^{H_1} \otimes_{B} \cdots \otimes_{B} A^{H_r}$ for each subgroup $K_i$ of $N_i$.

**Proposition 5.5.** Let $A/B$ be outer G-Galois. $B$ a direct summand of $A$, and $A$ directly indecomposable. Let $T$ and $T'$ be intermediate rings of $A/B$ such that $A = T \otimes_{B} T'$. If $H = \{a \in G ; \delta|T = 1_T\}$ and $H' = \{a \in G ; \delta|T' = 1_{T'}\}$, then $T = A^{H}$ and $T' = A^{H'}$.

**Proof.** Since $T \otimes_{B} T' = A$, we have $T \otimes_{B} A^{A} \equiv T \otimes_{B} A_{A}$. Since $A/T'$ is a separable extension, $A$ is $(B, T')$-projective. Hence, by Th. 2.6, $T = A^{H}$. Symmetrically we have $T' = A^{H'}$.

Let $A/B$ be a G-Galois extension, $B$ a direct summand of $A$, and $\mathfrak{N}$ a G-invariant proper ideal of $A$. Let $\{(a_{i}, a_{i}^*) ; i = 1, \cdots, n\}$ be a G-Galois coordinate system for $A/B$. For any $x$ in $A$ we denote $x + \mathfrak{N}$ (in $A/\mathfrak{N}$) by $\bar{x}$. If we define $\sigma(\bar{x}) = \bar{\sigma(x)}$, then $\sum_{i} a_{i} \cdot \sigma(a_{i}^*) = \delta_{1, *}$ for $\sigma$ in $G$, and therefore
\[(A/\mathfrak{M})(A/\mathfrak{M})^g\] is a G-Galois extension. By assumption, for any subgroup \(H\) of \(G\) there is an element \(c\) in \(A\) such that \(t_H(c)=1\). If \(\bar{x}\) is in \((A/\mathfrak{M})^g\), then 
\[\bar{x}=\bar{x}\sum e_H\tau(\bar{e})=\sum e_H\tau(\bar{x}\bar{e})=t_H(xc)\in(A^H+\mathfrak{M})/\mathfrak{M}.\] Thus, we prove the following:

**Theorem 5.6.** Let \(A/B\) be a G-Galois extension, \(B_0\) a direct summand of \(A_0\), and \(\mathfrak{M}\) a G-invariant proper ideal of \(A\). Then \((A/\mathfrak{M})/(B+\mathfrak{M})/\mathfrak{M}\) is a G-Galois extension, and \((A/\mathfrak{M})^g=(A^H+\mathfrak{M})/\mathfrak{M}\) for any subgroup \(H\) of \(G\).

**Corollary.** Let \(A/B\) be a G-Galois extension, and \(B_0\) a direct summand of \(A_0\). If \(B\) contains a non-zero central idempotent \(e\) of \(A\), then \(Ae/Be\) is a G-Galois extension, and \((Ae)^g=A^g.e\) for any subgroup \(H\) of \(G\).

**Proposition 5.7.** Let \(A/B\) be a G-Galois extension. If \(N\) is a normal subgroup of \(G\) such that \(A^N\) is an \(A^N\)-right direct summand of \(A\), then \(A^N/B\) is a G/N-Galois extension.

**Proof.** Let \(\{(a_i, a_i^\ast)\}; i=1, \ldots, n\) be a G-Galois coordinate system for \(A/B\). By assumption, there is an element \(c\) of \(A\) such that \(t^N(c)=1\). If we put \(t_N(a_i)=t_i\) and \(t_N(a_i^\ast c)=t_i^\ast\), then \(t_i\) and \(t_i^\ast\) are \(A^N\), and \(\sum t_i\cdot t_i^\ast=\delta_{N,*}\) for all \(\sigma\) in \(G\). Hence, \(A^N/B\) is a G/N-Galois extension (Prop. 2.2).

Let \(A/B\) be a G-Galois extension, and \(m\) a natural number. Then, every \(\sigma\) in \(G\) induces a ring automorphism in the \(m \times m\) complex matrix ring \((A)_m\).

Accordingly, \(G\) may be regarded as a finite group of automorphisms of \((A)_m\) such that \((A)_m^g=(B)_m\). Let \(E\) be the identity of \((A)_m\), and let \(\{(a_i, a_i^\ast)\}; i=1, \ldots, n\) be a G-Galois coordinate system for \(A/B\). Then \(\sum a_iE\cdot \sigma(a_i^\ast E)=\delta_{1,*}\) for all \(\sigma\) in \(G\). Thus \((A)_m/(B)_m\) is a G-Galois extension. (Remark. This may be considered as a special case of Th. 5.2).

**Theorem 5.8.** Let \(A/B\) be a G-Galois extension, and \(\{e_{ij}; i, j=1, \ldots, m\}\) a system of matrix units contained in \(B\). If \(A_0=\sum\{e_{ij}\}\), then \(A_0/A_0^g\) is a G-Galois extension, and \(B=\sum A_0^g e_{ij}\).

**Proof.** Obviously, \(G\) induces an automorphism group of \(A_0\) and \(B=\sum A_0^g e_{ij}\). Let \(\{(A_i, A_i^\ast)\}; i=1, \ldots, n\) be a G-Galois coordinate system for \(A/B\). Let \(A_i=\sum d_{ijk} e_{jk}\), \(A_i^\ast=\sum d_{ijk}^* e_{jk}\) \((a_{ijk}, d_{ijk} \in A_0)\). Then, \(\sigma(A_i^\ast)=\sum d_{ijk}^* \sigma(d_{ijk}) e_{jk}\) and therefore \(\sum a_{i1k}\cdot \sigma(d_{ikk})=\delta_{1,*}\) for \(\sigma\) in \(G\). Thus \(A_0/A_0^g\) is a G-Galois extension.

§ 6. Completely outer case.

Let \(R\) be a ring. If non-zero \(R\)-left modules \(M\) and \(N\) have no non-zero isomorphic subquotients, we say that \(\_\_\_\_M\) and \(\_\_\_\_N\) are unrelated.

**Proposition 6.1.** Let \(M\) be a non-zero \(R\)-left module, and \(M=M_1 \oplus \cdots \oplus M_s\) with non-zero \(R\)-submodules \(M_i\)'s of \(M\).

(1) If \(M_i\)'s are unrelated to each other, then each \(M_i\) is \(\text{End}(\_\_\_\_M)\)-
admissible and $X=\sum_{i}(X\cap M_{i})$ for every submodule $X$ of $\mathfrak{U}M$.

(2) If $X=\sum_{i}(X\cap M_{i})$ for every submodule $X$ of $\mathfrak{U}M$, then $M_{i}$'s are unrelated to each other.

Proof. (1) will be rather familiar. We shall prove here (2). To our end, it suffices to prove that if $M=M_{1}\oplus M_{2}$ and $X=(X\cap M_{1})+(X\cap M_{2})$ for every submodule $X$ of $\mathfrak{U}M$ then $M_{1}$ and $M_{2}$ are unrelated. Let $M_{i}/N_{i}$ and $M_{j}/N_{j}$ be non-zero subquotients of $M_{1}$ and $M_{2}$, respectively. If there exists an $R$-isomorphism $\alpha; M_{i}/N_{i}\cong M_{j}/N_{j}$, we can define an $R$-homomorphism $\varphi; M_{i}\oplus M_{2}\rightarrow M_{2}/N_{2}$ by the following rule: $(m_{i}'+m_{2}')\varphi=(m_{i}'+N_{i})\alpha+(m_{2}'+N_{2})$. Then, our assumption yields $\text{Ker}\varphi=(M_{1}\cap\text{Ker}\varphi)+(M_{2}\cap\text{Ker}\varphi)$, and so $(M_{1}+M_{2})\varphi=M_{1}\varphi\oplus M_{2}\varphi=M_{2}/N_{2}\oplus M_{2}/N_{2}$, which is a contradiction.

$G$ is said to be completely outer, if each $A$-$A$-modules $Au_{\sigma}$, $Au_{\tau}$ $(\sigma\neq\tau)$ are unrelated.

To be easily seen, $Au_{\sigma}$ and $Au_{\tau}$ $(\sigma, \tau\in G)$ are $A$-$A$-isomorphic if and only if $\sigma^{-1}$ is an inner automorphism of $A$, and every $A$-$A$-submodule of $Au_{\sigma}$ is written as $\mathfrak{U}u_{\sigma}$ with some ideal $\mathfrak{U}$ of $A$. Therefore, if $G$ is completely outer, then $G$ contains no inner automorphism of $A$, and in case $A$ is two-sided simple, the converse is true. Now, for $\sigma$ in $G$ we set $J_{\sigma}={a\in A; \sigma(x)a=ax \text{ for all } x \in A}$. Then each $J_{\sigma}$ is a $C$-submodule of $A$, and $J_{1}=C$. In his paper [9], T. Kanzaki proved the following: Let $A/B$ be a $G$-Galois extension. Then $V_{A}(B)=\sum_{\sigma}J_{\sigma}$. Therefore, if $A/B$ is $G$-Galois, then $V_{A}(B)=C$ if and only if $J_{\sigma}=0$ for all $\sigma$ in $G$ such that $\sigma\neq1$.

**Proposition 6.2.** $J_{\sigma}=0$ if and only if $\text{Hom} (\_Au_{\sigma}, A)\cong A=0$.

Proof. Assume $J_{\sigma}=0$. If $f$ is in $\text{Hom} (\_Au_{\sigma}, A)$, then $\sigma(x)f(u_{\sigma})=f(\sigma(x)u_{\sigma})=f(u_{\sigma})x$ for $x$ in $A$. Hence $f(u_{\sigma})=0$, and so $f=0$. Conversely, assume that $\text{Hom} (\_Au_{\sigma}, A)=0$. If $a$ is in $J_{\sigma}$, then we can easily see that the mapping $xu_{\sigma}\rightarrow xa$ $(x\in A)$ is an $A$-$A$-homomorphism from $Au_{\sigma}$ to $A$. Hence, by assumption, $a=0$.

Prop. 6.2 together with Kanzaki's result cited above yields at once the following:

**Proposition 6.3.** If $A/B$ is a $G$-Galois extension, then the following are equivalent. (i) $V_{A}(B)=C$. (ii) $\text{Hom} (\_Au_{\sigma}, A)=0$ for every $\sigma\neq1$ in $G$.

The following proposition will play a fundamental role in our study.

**Proposition 6.4.** If $G$ is completely outer, then $A/B$ is a $G$-Galois extension and $V_{A}(B)=C$.

Proof. At first, $V_{A}(B)=C$ is evident by Prop. 6.3. Since $u_{i}\in A(\sum_{\sigma}u_{\sigma})A$ (Prop. 6.1.), there are elements $a_{i}, a_{i}^{*}$ $(i=1, \cdots, n)$ in $A$ such that $u_{i}=$
\[ \sum_i a_i (\sum_u a^*_i) = \sum_i (\sum_i a_i \cdot \sigma(a^*_i)) u_i. \] Hence \( \sum_i a_i \cdot \sigma(a^*_i) = \delta_{1,i} \) for \( \sigma \) in \( G \).

**Corollary.** If \( A \) is two-sided simple, then the following conditions are equivalent: (i) \( G \) is completely outer. (ii) \( G \) contains no inner automorphisms. (iii) \( A/B \) is an outer \( G \)-Galois extension.

**Proposition 6.5.** If there are elements \( a_i, a'_i \) \( (i=1, \ldots, n) \) in \( A \) such that \( \sum_i a_i x \cdot \sigma(a'_i) = \delta_{1,i} x \) for each \( x \) in \( A \) \( (\sigma \in G) \), then \( G \) is completely outer.

**Proof.** Let \( X \) be any \( A\)-\( A \)-submodule of \( A \). If \( \sum_i x_u \) is in \( X \), then \( X \ni \sum_i a_i (\sum_u a^*_i) \tau^{-1}(a'_i) = x_u \) for each \( \tau \) in \( G \). Hence, by Prop. 6.1, \( G \) is completely outer.

Combining Prop. 6.4 with Prop. 6.5, we readily obtain the following:

**Theorem 6.6.** Let \( A \) be a commutative ring. If \( A/B \) is \( G \)-Galois, then \( G \) is completely outer, and conversely.

**Proposition 6.7.** Let \( A/B \) be a \( G \)-Galois extension, \( H \) a subgroup of \( G \), and \( a \) an element of \( A \). If \( \sigma \in G \) is not contained in \( H \), and \( ax = a \cdot \sigma(a_0) x \) for all \( x \) in \( A^H \), then \( a = 0 \).

**Proof.** There are elements \( t_i, \ldots, t_n \in A^H \) and \( a^*_1, \ldots, a^*_n \in A \) such that \( \sum_i t_i \cdot \sigma(a^*_i) = \delta_{1,i} \) for any \( \sigma \) in \( G \) (Prop. 2.2). Hence, \( a = a \sum_i t_i a^*_i = \sum_i a \cdot \sigma_0(t_i) a^*_i = \sigma_0(a^{-1}(a)) \sum_i t_i \sigma_0^{-1}(a^*_i) = 0 \).

**Lemma 6.8.** Let \( S \) be a subring of a ring \( R \). If \( R_S \) is finitely generated and projective, then \( \text{End}(R_S) \) is an \( \text{End}(R_S) \)-left direct summand of \( \text{End}(R) \), where \( \text{End}(R_S) \) and \( \text{End}(R) \) act on the left side.

**Proof.** As is well known, there are elements \( a_i \in R \), \( f_i \in \text{Hom}(R_S, S_S) \) \( (i=1, \ldots, n) \) such that \( \sum_i a_i f_i(x) = x \) for every \( x \) in \( R \) (cf. [3]). If \( g \) is in \( \text{End}(R) \), then \( \sum_i g(a_i) f_i \) is in \( \text{End}(R_S) \), and so the mapping \( g \rightarrow \sum_i g(a_i) f_i \) is an \( \text{End}(R_S) \)-left homomorphism from \( \text{End}(R) \) to \( \text{End}(R_S) \). To be easily seen, if \( g \) is in \( \text{End}(R_S) \) then \( \sum_i g(a_i) f_i = g \). This implies that \( \text{End}(R_S) \) is an \( \text{End}(R_S) \)-left direct summand of \( \text{End}(R) \).

Let \( T \) be an intermediate ring of \( A/B \). \( G|T \) is said to be \( \ast \)-strongly distinct if, for any non-zero idempotent \( e \) in \( A \) such that \( eA \subseteq Ae \) and any distinct \( \sigma, \tau \) in \( G \), there is at least an element \( x \) in \( T \) such that \( e \cdot \sigma(x) \neq e \cdot \tau(x) \).

If \( A/B \) is a \( G \)-Galois extension, then \( G|A^\pi \) is \( \ast \)-strongly distinct for any subgroup \( H \) of \( G \) (Prop. 6.7).

**Theorem 6.9.** Let \( G \) be completely outer, \( B_\pi \) a direct summand of \( A_\pi \), and \( T \) an intermediate ring of \( A/B \). Then the following conditions are equivalent.

(i) \( T = A^\pi \) for some subgroup \( H \) of \( G \).
(ii) \( A^\pi \) is finitely generated and projective, and \( T \) is a direct summand
of $A_T$, and $G|T$ is*-strongly distinct.

Proof. Since $A/A^H$ is $H$-Galois, it remains to prove $(ii) \Rightarrow (i)$. If we put $A_0=\text{End}(A_T)$, then $A_0$ is a subring of $A$. Since $A_0$ is an $A$-$A$-submodule of $A$, $A_0=\sum_+ \mathfrak{U} u_\sigma$ with some ideals $\mathfrak{U}_\sigma$ of $A$. By Lemma. 6.8, $A_0$ is a direct summand of $A$, so that each $\mathfrak{U}_\sigma u_\sigma$ is a direct summand of $A$. Therefore each $\mathfrak{U}_\sigma u_\sigma$ is a direct summand of $A u_\sigma$. Hence $\mathfrak{U}_\sigma$ is a direct summand of $A$. Let $\mathfrak{U}_\sigma=A e_\sigma$ with an idempotent $e_\sigma$ in $A$. Then, since $e_\sigma u_\sigma$ is in $A_0$, $e_\sigma \sigma(x)=e_\sigma \sigma(x)y$ for each $x$ in $A$ and $y$ in $T$, in particular, $e_\sigma \sigma(y)=e_\sigma y$ for each $y$ in $T$. Therefore, if we set $H=\{\sigma \in G; \sigma | T=1_T\}$, then $e_\sigma=0$ for $\sigma$ not contained in $H$. Evidently $\mathfrak{U}_\sigma=A$ for each $\sigma$ in $H$. We obtain therefore $A_0=\sum_+ e \mathfrak{U} A u_\sigma$, and hence $\text{End}(A)=\text{End}(A^H)$. On the other hand, since $T_\tau$ is a direct summand of $A_T$, $\text{End}(A)=(A^H)_\tau$. Hence we obtain $T=A^H$.

Now, if $A$ is a semi-prime ring (i.e., $A$ has no nilpotent ideals) and $e$ is an idempotent in $A$ such that $eA \subseteq Ae$, then $eA=Ae$ so that $e$ is a central idempotent in $A$. Noting this fact, Th. 6.9 yields at once the following:

Theorem 6.10. Let $A$ be a semi-prime ring. If $G$ is completely outer, $B$ a direct summand of $A_B$, and $T$ an intermediate ring of $A/B$, then the following conditions are equivalent:

(i) $T=A^H$ for some subgroup $H$ of $G$.
(ii) $A_T$ is finitely generated and projective, and $T_\tau$ is a direct summand of $A_T$, $G|T$ is strongly distinct.

Proposition 6.11. The following are equivalent:

(i) $G$ is completely outer.
(ii) For any $x, y$ in $A$ and any $\sigma$ in $G$ such that $\sigma \neq 1$, there are elements $a_i, a'_i$ $(i=1, \cdots, n)$ in $A$ such that $\sum_i a_i x a'_i = x$ and $\sum_i a_i y \sigma(a'_i) = 0$.

Proof. $(i) \Rightarrow (ii)$ Let $x, y$ be in $A$, and $\sigma$ any element of $G$ such that $\sigma \neq 1$. We set $X=A(xu_1+yu_2)A$, which is an $A$-$A$-submodule of $Au_1+Au_2$. By Prop. 6.1, $xu_1 \in X$, and hence there are elements $a_i, a'_i$ $(i=1, \cdots, n)$ in $A$ such that $\sum_i a_i(xu_1+yu_2)a'_i = xu_1$. Then, $\sum_i a_i x a'_i = x$ and $\sum_i a_i y \sigma(a'_i) = 0$.

$(ii) \Rightarrow (i)$ Let $\sigma, \tau$ be distinct elements in $G$, and $X$ any $A$-$A$-submodule of $Au_1+Au_2$. Let $xu_1+yu_2$ be any element of $X$. For $\sigma^{-1}(x)$ and $\sigma^{-1}(y)$, there are elements $a_i, a'_i$ $(i=1, \cdots, n)$ in $A$ such that $\sum_i a_i(xu_1+yu_2)a'_i = xu_1$ and $\sum_i a_i y \sigma^{-1}\tau(a'_i) = 0$. Then, $\sum_i a_i(xu_1+yu_2)a'_i = xu_1$ and $\sum_i a_i y \sigma^{-1}\tau(a'_i) = 0$, and so $X \ni \sum_i a_i(xu_1+yu_2)a'_i = xu_1$. Thus, by Prop. 6.1, $Au_1$ and $Au_2$ are unrelated.

Theorem 6.12. Let $G$ be completely outer, and $N$ a proper normal subgroup of $G$ such that $A^N$ is an $A^N$-right direct summand of $A$. Then,
$G/N$ is completely outer as an automorphism group of $A^n$.

Proof. Let $x, y$ be in $A^n$. Since $xu_i \in A(\sum_{\tau \in N} xu_i + \sum_{\tau \in \Theta} yu_i) A$ (Prop. 6.1), there are elements $x_i, y_i$ $(i = 1, \cdots, n)$ in $A$ such that $\sum_{\tau \in N} x_i (\sum_{\tau \in N} xu_i + \sum_{\tau \in \Theta} yu_i) y_i = xu_1$. Then $\sum_{\tau \in N} x_i x_\tau y_i = \delta_{1, \tau} x \ (\tau \in N)$ and $\sum_{\tau \in N} x_i y_i - \sigma(y_i) = 0 \ s \in G \setminus N$. By assumption, there is an element $c$ in $A$ such that $t_N(c) = 1$. We set $t_N(x_i) = x_i'$ and $t_N(y_i) = y_i'$, then $x_i', y_i' \ (i = 1, \cdots, n)$ are in $A^n$. To be easily seen, $\sum_{\tau} x_i x_\tau y_i = x$ and $\sum_{\tau} x_i y_i - \rho(y_i) = 0$ for any $\rho \in G \setminus N$. Thus, by Prop. 6.11, $G/N$ is completely outer as an automorphism group of $A^n$.

§ 7. Several results.

The following lemma is well known.

Lemma 7.1. Let $S$ be a subring of a ring $R$. If $S_S$ is a direct summand of $R_S$, then $R_S \cap S = 1$ for any left ideal $1$ of $S$.

Lemma 7.2. Let $S$ be a subring of a ring $R$ such that $S_S$ is a direct summand of $R_S$ and $S R$ is finitely generated. If $R$ satisfies the minimal condition (resp. the maximal condition) for left ideals, then so does $S$, and conversely.

Proof. If $R$ satisfies the minimal condition (resp. the maximal condition) for left ideals, then so does $S$ (Lemma 7.1). Conversely, if $S$ satisfies the minimal condition (resp. the maximal condition) for left ideals then $S R$ satisfies the minimal condition (resp. the maximal condition) for $S$-left submodules, so that $R$ satisfies the minimal condition (resp. the maximal condition) for left ideals.

A ring $R$ is called a semi-primary ring if $R/\Re(R)$ satisfies the minimal condition for left ideals, where $\Re(R)$ means the Jacobson radical of $R$. If $R$ is semi-primary, then $(R)_n$ and $eRe$ are semi-primary rings, where $e$ is a natural number and $e$ is a non-zero idempotent in $R$ (cf. [7]). Therefore, in case $R$ is semi-primary, if an $R$-right module $M$ is finitely generated and projective then $\text{End}(M_R)$ is semi-primary. As to notations and terminologies used in below, we follows [11].

Proposition 7.3. (1) Let $R$ be a semi-primary ring, and $S$ a subring of $R$. If $S_S$ is a direct summand of $R_S$, then $S$ is a semi-primary ring.

(2) Let $R$ be a ring, and $S$ a subring of $R$ such that $S_S$ is finitely generated and projective. If $S$ is semi-primary, then so is $R$.

Proof. (1) Let $\{I_i; i = 1, \cdots, n\}$ be a $d$-independent set of maximal left ideals of $S$ (cf. [11]). Then, $\{RL_i; i = 1, \cdots, n\}$ is a $d$-independent set of proper left ideals of $R$ (Lemma 7.1). Since each $RL_i$ is contained in a maximal left ideals of $R$, $n \leq \max \dim_R d-dim \ nR = d-dim R$ (cf. [11]). Thus $d-dim S \leq d-dim R < S_0$, and hence $S$ is semi-primary ([11; Prop. 5.14]. (2) Since $S$
is semi-primary, End \((R_S)\) is semi-primary. By Lemma 6.8, \(R_i R_R\) (the set of all left multiplications by elements of \(R\)) is a direct summand of \(R_i \text{End} (R_S)\). Hence, by (1), \(R (\cong R_i)\) is semi-primary.

**Remark.** Let \(A/B\) be a \(G\)-Galois extension, and \(B_B\) a direct summand of \(A_B\). If \(A\) is a semi-primary ring, then so is \(B\), and conversely (cf. Th. 1.7).

Let \(R\) be a ring, and \(S\) a subring of \(R\). \(R/S\) is called a free Frobenius extension if \(R_S\) is finitely generated and free and \(_sR_R \cong _s\text{Hom} (R_S, S_S)\) (Kasch [10]).

**Lemma 7.4.** Let \(R/S\) be a free Frobenius extension.

1. End \((R_S)/R_i\) is a free Frobenius extension.
2. If \(R_R\) is injective, then so is \(S_S\), and conversely.

**Proof.** (1) and the if part of (2) are given in [10]. Assume that \(R_R\) is injective. By (1) and the if part, we can easily see that End \((R_S)\) is End \((R_S)\)-right injective. Let \(R_S \cong S_S^m\). Then, End \((R_S)\) \(\cong (S)_m\), and hence we readily see that \(S_S\) is injective (cf. [11]).

**Proposition 7.5.** Let \(R\) be a ring, and \(S\) a subring of \(R\). If \(S_S\) is a direct summand of \(R_S\), then \(\Re(R) \cap S \subseteq \Re(S)\).

**Proof.** If \(\Re(R) \cap S \not\subseteq \Re(S)\), then \(\Re(R) \cap S + I = S\) for some maximal left ideal \(I\) of \(S\). Since \(R(\Re(R) \cap S) + RI = R\) and \(R(\Re(R) \cap S) \subseteq \Re(R)\), we have \(RI = R\). If follows then a contradiction \(I = RI \cap S = S\) (Lemma 7.1).

**Proposition 7.6.** The set of all maximal \(A\)-A-submodules of \(A\) coincides with \(\{\bigcap \sigma(\mathfrak{P}); \mathfrak{P} \text{ ranges over all maximal ideals of } A\}\).

**Proof.** Let \(X\) be a maximal \(A\)-A-submodule of \(A\). Take a maximal ideal \(\mathfrak{P}_1\) such that \(\mathfrak{P}_1 \supseteq X\). Then, \(\cap \sigma(\mathfrak{P}_1) \supseteq X\), and so \(\cap \sigma(\mathfrak{P}_1) = X\). Now, let \(\mathfrak{P}\) be a maximal ideal of \(A\), and \(Y\) a maximal \(A\)-A-submodule of \(A\) such that \(Y \supseteq \cap \sigma(\mathfrak{P})\). Then \(Y = \cap \sigma(\mathfrak{P})\) for some maximal ideal \(\mathfrak{P}_2\) of \(A\). If \(\cap \sigma(\mathfrak{P}_2) \supseteq \cap \sigma(\mathfrak{P})\), then \(\mathfrak{P}_2 \supseteq \cap \sigma(\mathfrak{P}_2)\), and so \(\mathfrak{P} + \cap \sigma(\mathfrak{P}_2) = A\), whence it follows a contradiction \(\cap \sigma(\mathfrak{P}) + \cap \sigma(\mathfrak{P}_2) = A\).

**Proposition 7.7.** Let \(A/B\) be a \(G\)-Galois extension, and \(B_B\) a direct summand of \(A_B\). Let \(\{\overline{X}\}\) be the set of all \(A\)-submodules of \(A\) and \(\{X\}\) be the set of all left ideals of \(B\). Then \(\overline{X} \rightarrow \overline{X} \cap B\) and \(X \rightarrow AX = A \otimes_B X\) are mutually converse order isomorphisms between \(\{\overline{X}\}\) and \(\{X\}\).

**Proof.** This is a special case of Th. 5.1 (2).

**Proposition 7.8.** Let \(A/B\) be a \(G\)-Galois extension, and \(B_B\) a direct summand of \(A_B\). If \(A \cdot \Re(B)\) is an ideal of \(A\), then \(\Re(A) = A \cdot \Re(B)\).

**Proof.** By Prop. 7.7 and Prop. 7.5, \(\Re(A) = A(\Re(A) \cap B) \subseteq A \cdot \Re(B)\).
Since $A_B$ is finitely generated, $A \cdot \Re(B)$ is d-dense in $A_B$, and so d-dense in $A_A$ (cf. [11]). Hence $A \cdot \Re(B) \subseteq \Re(A)$.

**Theorem 7.9.** Let $A/B$ be a G-Galois extension such that $B \subseteq C$. If $A'$ is a $B$-algebra, then $\Re(A' \otimes_B A) = \Re(A') \otimes A$.

**Proof.** By Cor. to Th. 5.2, $(A' \otimes_B A)/(A' \otimes 1)$ is a G-Galois extension. Since $(A' \otimes A) (\Re(A') \otimes 1) = \Re(A') \otimes A$ is an ideal of $A' \otimes A$, $\Re(A' \otimes A) = \Re(A') \otimes A$ by Prop. 7.8.

Now, assume that $G$ is completely outer and $B_B$ is a direct summand of $A_B$. If $A$ is an $A$-$A$-submodule (resp. $A$-$A$-submodule) of $A$, then $A = \sum u_i \mathfrak{A}$, for some ideals $\mathfrak{A}$ of $A$ (resp. $A = \mathfrak{A} = \sum u_i \mathfrak{A}$ for some ideal $\mathfrak{A}$ of $A$), and conversely. In particular, if $A$ is an ideal of $A$, then $A = \mathfrak{A} = \mathfrak{A} = \mathfrak{A}$ for some $G$-invariant ideal $\mathfrak{A}$ of $A$, and conversely (cf. §6 and [13]). Now, let $\{a\}$ be the set of all ideals of $A$, $\{a\}$ the set of all ideals of $B$, and $\{\mathfrak{A}\}$ the set of all $G$-invariant ideals of $A$. Then, there exists an order isomorphism $A \rightarrow a$ between $\{A\}$ and $\{a\}$ such that $A(\Lambda) = Aa$ (cf. [1; Prop. A. 5]). Consequently, there exists an order isomorphism $\mathfrak{A} \rightarrow Aa$ between $\{\mathfrak{A}\}$ and $\{a\}$ (cf. Th. 5.1 (2)). Accordingly, if $A$ is semi-prime, (prime, two-sided simple) then so is $B$. Since $A \cdot \Re(B) = \Re(B)A$ is an ideal of $A$, Prop. 7.8 implies $\Re(A) = A \cdot \Re(B) = \Re(B)A$. Next, we shall consider $\Re(\Lambda)$. There exists $\mathfrak{A} \in \{\mathfrak{A}\}$ such that $\Re(\Lambda) = \mathfrak{A} = \mathfrak{A}$. Since $\mathfrak{A} u_i = \Re(\Lambda) \cap A u_i \subseteq \Re(A u_i) = \Re(A) u_i$ by Prop. 7.5, we obtain $\Re(\Lambda) = \Re(\Lambda \cap A \mathfrak{A}) = \Re(A \mathfrak{A})$. On the other hand, noting that $A = \mathfrak{A}$ is finitely generated and $A \cdot \Re(A)$ is an ideal of $A$, we see that $A \cdot \Re(A) \subseteq \Re(\Lambda)$ (cf. the proof of Prop. 7.8). Hence, we have $\Re(\Lambda) = A \cdot \Re(A) = A \cdot \Re(A)$. Since $\Re(\mathfrak{A} A) = \Re(\mathfrak{A} A) = \Re(\mathfrak{A} A)$, $A \cdot \Re(B_B) = \Re(B_B)A$, $\Re(\mathfrak{A} A) \cap B = \Re(B_B)B$, $\Re(\Lambda) = A \cdot \Re(B_B)$, and $\Re(\mathfrak{A} A) \cap B = \Re(B_B)$, $\Re(\Lambda) = A \cdot \Re(B_B)$, $\Re(\Lambda) = A \cdot \Re(B_B)$, and $\Re(\mathfrak{A} A) \cap B = \Re(B_B)$. Summarizing the above, we state the following theorem.

**Theorem 7.10.** If $G$ is completely outer and $B_B$ a direct summand of $A_B$, then $\Re(A) = A \cdot \Re(B) = \Re(B)A$, $\Re(A) \cap B = \Re(B)$, $\Re(\mathfrak{A} A) = \Re(B_B)A$, $\Re(\mathfrak{A} A) \cap B = \Re(B_B)$, $\Re(\Lambda) = A \cdot \Re(B_B)$, and $\Re(\mathfrak{A} A) \cap B = \Re(B_B)$.

**Proposition 7.11.** Let $B$ be directly indecomposable, and let $A = \mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_r$ be a direct sum of minimal ideals. If $\mathfrak{A}$ is a minimal ideal of $A$, then $\{\sigma(\mathfrak{A}); \sigma \in G\} = \{\mathfrak{A}_1, \ldots, \mathfrak{A}_r\}$, and $n$ divides $|G : 1|$. If $\mathfrak{P}$ is a maximal ideal of $A$, $\{\sigma(\mathfrak{P}); \sigma \in G\}$ coincides with the set of all maximal ideals of $A$.

**Proof.** Note that $\{\mathfrak{A}_1, \ldots, \mathfrak{A}_r\}$ coincides with the set of all minimal ideals of $A$. For any $\mathfrak{A}_i$, we set $\sum \sigma(\mathfrak{A}_i) = \mathfrak{B}$. Then, $\mathfrak{B} = A \alpha$ with some non-zero
central idempotent \( e \) of \( A \). Since \( \sigma(\mathfrak{B})=\mathfrak{B} \) for all \( \sigma \) in \( G \), \( \sigma(e)=e \) for all \( \sigma \) in \( G \), so that \( e \in B \), which means \( e=1 \). Hence \( \mathfrak{B}=A \), which implies that \( \{\sigma(\mathfrak{U}_{i});\sigma\in G\} = \{\mathfrak{U}_{1}, \cdots, \mathfrak{U}_{8}\} \). If we set \( H=\{\sigma\in G; \sigma(\mathfrak{U}_{i})=\mathfrak{U}_{i}\} \), then \( \#\{\sigma(\mathfrak{U}_{i}); \sigma\in G\} = (G:H) \), which divides \((G:1)\). Let \( \mathfrak{P} \) and \( \mathfrak{P}' \) be maximal ideals of \( A \). Then \( A=\mathfrak{U}\oplus \mathfrak{P}=\mathfrak{U}'\oplus \mathfrak{P}' \) with some minimal ideals \( \mathfrak{U}, \mathfrak{U}' \) of \( A \). There is an element \( \sigma \) in \( G \) such that \( \sigma(\mathfrak{U})=\mathfrak{U}' \). Then \( A=\mathfrak{U}'\oplus \sigma(\mathfrak{P})=\mathfrak{U}'\oplus \mathfrak{P}' \), so that \( \sigma(\mathfrak{P})=\mathfrak{P}' \).

**Corollary 1.** Let \( G \) be completely outer, and \( B_{h} \) a direct summand of \( A_{B} \). If \( B \) is a two-sided simple rings, then \( A \) is a direct sum of isomorphic two-sided simple rings, and the number of components divides \((G:1)\).

**Proof.** Let \( \mathfrak{P} \) be a maximal ideal of \( A \). Then \( \cap_{\sigma}\sigma(\mathfrak{P}) \) is a \( \Delta \)-\( A \)-submodule of \( \mathfrak{P} \). As we remarked above, \( A \) is \( \Delta \)-\( A \)-simple, and so we have \( \cap_{\sigma}\sigma(\mathfrak{P})=0 \). Hence \( A \) is a direct sum of two-sided simple rings.

**Corollary 2.** Let \( A/B \) be a \( G \)-Galois extension, and \( B \) a division ring. Then \( A \) is a direct sum of isomorphic (Artinian) simple rings.

**Proof.** Let \( \mathfrak{P} \) be a maximal left ideal of \( A \). Then \( \cap_{\sigma}\sigma(\mathfrak{P}) \) is a \( \Delta \)-submodule of \( A \). Since \( \Delta A \) is simple (Prop. 7.7), \( \cap_{\sigma}\sigma(\mathfrak{P})=0 \). Hence, as is easily seen, \( \Delta A \) is completely reducible, so that \( A \) is a direct sum of simple rings. Let \( A/B \) be a \( G \)-Galois extension, \( A \) a commutative ring, and \( A' \) a \( B \)-algebra. Then, by Prop. 6.5 and Th. 5.2, \((A'\otimes_{B}A)/(A'\otimes 1) \) is \( G \)-Galois and \( G \) is completely outer (as an automorphism group of \( A'\otimes A \)). Further, if \( A' \) is two-sided simple, then \( A'\otimes_{B}A \) is a direct sum of isomorphic two-sided simple rings (Cor. 1. to Prop. 7.11). Thus we have the following:

**Theorem 7.12.** Let \( A/B \) be a \( G \)-Galois extension, \( A \) commutative, and \( A' \) a \( B \)-algebra. If \( A' \) is two-sided simple, then \( A'\otimes_{B}A \) is a direct sum of isomorphic two-sided simple rings, and the number of components devides \((G:1)\).

**References**


Y. Miyashita


Department of Mathematics,
Hokkaido University

(Received June 10, 1966)