<table>
<thead>
<tr>
<th>項目</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>タイトル</td>
<td>有限外ガロワ理論の非可換環について</td>
</tr>
<tr>
<td>著者</td>
<td>Miyashita, Yôichi</td>
</tr>
<tr>
<td>引用</td>
<td>Journal of the Faculty of Science Hokkaido University. Ser. 1 Mathematics = 北海道大学理学部紀要, 19(3-4): 114-134</td>
</tr>
<tr>
<td>発行年</td>
<td>1966</td>
</tr>
<tr>
<td>項目</td>
<td>File Information</td>
</tr>
<tr>
<td>項目</td>
<td>JFSHIU_19_N3-4_114-134.pdf</td>
</tr>
</tbody>
</table>

HOKKAIDO UNIVERSITY
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 $A$ be a directly indecomposable ring, $G$ a finite group of automorphisms of $A$, and $B = A^g = \{ x \in A ; \sigma(x) = x \}$ for all $\sigma$ in $G$. We call $A/B$ a $G$-Galois extension if there are elements $a_1, \ldots, a_n; a_1^*, \ldots, a_n^*$ in $A$ such that $\sum_i a_i \cdot \sigma(a_i^*) = \delta_{1,\sigma}(\sigma \in G)$, 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 $A \otimes B A$ 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 $G$, $A'^H = B \otimes_B A'^H = A'^H \otimes_B B$. (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 $T ightarrow A'T = TA'$ 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 $G$, $\{ \sigma \in G ; \sigma|A^H - 1 \} = H$. (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 \( T \) is a direct summand of \( A_T \) (Th. 3.2). In case \( _BA_B \) 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. \( B/\mathfrak{R}(B) \) satisfies the minimum condition for left ideals, where \( \mathfrak{R}(B) \) means the Jacobson radical of \( B \)), then \( A \) has a normal basis (Th. 1.7).

Let \( A = A(A,G) = \sum_{\sigma \in G} \oplus Au_{\sigma} \) be the trivial crossed product of \( A \) with \( G \). \( G \) is said to be completely outer if \( A^{\sigma}A \) and \( A^{\sigma}A^{\tau} \) 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.

§ 1. 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 \( B = A^G = \{ x \in A ; \sigma(x) = x \) for all \( \sigma \) in \( G \} \). For any subgroup \( H \) of \( G \), \( \delta_{H,\sigma} \) means the mapping from \( G \) to \( \{1, 0\} \) (\( \subseteq A \)) 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 \( t_i, \cdots, t_n \in T \) and \( a_i', \cdots, a_n' \in A' \) such that \( \sum_i x_i a_i' = 1 \) and \( \sum_i x_i t_i \otimes a_i' = \sum_i x_i \otimes a_i' x (\in T \otimes_{B'} A') \) 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 \( \mathcal{S} \) be a set of
ring homomorphisms from $A'$ to $A''$. $\mathcal{S}$ is called strongly distinct if any distinct $f$, $g$ in $\mathcal{S}$ are strongly distinct.

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

$A/B$ is called a G-Galois extension if there are elements $a_{1}, \cdots, a_{n}$; $a_{1}^{*}, \cdots, a_{n}^{*}$ in $A$ such that $\sum_{i}a_{i}^{*}\sigma(a_{i}^{*})=\delta_{1, \sigma}$ for all $\sigma$ in $G$. When this is the case, $\{a_{i}, a_{i}^{*} \}: 1=1, \cdots, n$ is called a 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 isomorphism (cf. [6]). When this is the case we identify $A$ with Hom $(A_{B}, A_{B})$: $A=A_{i}G=AG$, 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 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).

**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 $t_{1}, \cdots, t_{n} \in T$ and $a_{1}, \cdots, a_{n} \in A'$ such that $\sum_{i}t_{i}a_{i}=1$ and $\sum_{i}f(t_{i})g(a_{i})=0$, then $f$ and $g|T$ (the restriction of $g$ to $T$) are strongly distinct.

**Proof.** Let $e$ be a central idempotent of $A''$ such that $f(x)e=g(x)e$ for all $x$ in $T$. Since $\sum_{i}t_{i}a_{i}=1$, we have $\sum_{i}g(t_{i})g(a_{i})=1$, and therefore $e=e_{1}=$ $\sum_{i}e\cdot g(t_{i})g(a_{i})=\sum_{i}e\cdot f(t_{i})g(a_{i})=0$. Thus, $f$ and $g|T$ are strongly distinct.

**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 $\{[t_{i}, a_{i}]: i=1, \cdots, n\}$ 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 $ee'=0$.

**Proof.** Since $\sum_{i}xt_{i}a_{i}=\sum_{i}t_{i}a_{i}x$ ($\in T \otimes_{B'} A'$) for all $x$ in $T$, $\sum_{i}f(xt_{i})g(a_{i})=\sum_{i}f(t_{i})g(a_{i}x)$ ($\in A'' \otimes_{B'} A''$) for all $x$ in $T$. Therefore,
$f(x)e = g(x)f(x)$ for all $x$ in $T$, in particular, $y = ey$ for all $y$ in $B'$. Hence, by assumption, $e$ is contained in the center of $A''$. Since $\sum f(t_i)(\sum g(a_i))g'(a_j) = (\sum f(t_i)g(a_i))\sum g(a_j)$, we obtain $e' = \sum f(t_i)e'g'(a_j) = e\sum g(t_j)g'(a_j)$.

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

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

**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 $A$-$A'$-isomorphism, $h^{-1}(\sum x, \mu_i) = \sum x, \sigma(a_i) \otimes a_i^{*}$ for every $\sum x, \mu_i$ 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, $h(\sum x, \sigma(a_i) \otimes a_i^{*}) = \sum x, \mu_i$, and hence $h$ is onto. Let $x, y$ be in $A$. Then $\sum x, \sigma(y) \sigma(a_i) \otimes a_i^{*} = x \otimes \sum x, \sigma(y) \sigma(a_i) \otimes a_i^{*} = x \otimes y$, whence we can easily see that $h$ is 1-1. Hence, $h$ is a $A$-$A'$-isomorphism. Since $h(\sum a_i \otimes a_i^{*}) = u_i$ and $h$ is an $A$-$A'$-isomorphism, $\sum a_i \otimes a_i^{*} = \sum a_i \otimes a_i^{*} x$ 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, ⋯, 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) ⇒ (ii) follows from Prop. 1.3 and Prop. 1.1. (ii) ⇒ (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) ⇒ (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 $a A \cong B^m$ for some natural number $m$, then $BG^m \cong A^m$.

**Proof.** Let $A = \sum a_i \otimes a_i^{*}$ (i = 1, ⋯, n), and $a B \cong a B^m$ by the correspondence
$y \rightarrow yd_{i}(y \in B)$. Then $A = \sum_{a_{i}}u_{a}A = \sum_{a_{i}}u_{Bd_{i}} = \sum_{a_{i}}u_{Bd_{i}} = \sum_{a_{i}}(\sum_{Bd_{i}})d_{i}$ and $(\sum_{Bd_{i}})d_{i} = \sum_{a_{i}Bd_{i}}$ as $a_{i}Bd_{i}$-left modules. Hence, $\eta_{A}A = \eta_{BG}A$. On the other hand, $\Delta = \sum_{A \otimes B \Delta}A \otimes B \Delta = \sum_{A \otimes B \Delta}A \otimes B \Delta \cong A^{m}(\text{Prop. 1.3})$. We obtain therefore $\eta_{BG}A \cong \eta_{BA}A$.

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

**Proof.** By Prop. 1.6, $\eta_{BG}A \cong \eta_{BA}A$. Since $\Re(B)A \cong \Re(B)G = \Re(B)A^{m}$ under the above isomorphism, $(BG/\Re(B)A)^{m} \cong (A/\Re(B)A)^{m}$ as $BG/\Re(B)A$-G-left modules. Since $BG/\Re(B)A$ is $B/\Re(B)A$-left finitely generated and $B$ is semi-primary, $BG/\Re(B)A$ satisfies the minimal condition (and the maximal condition) for left ideals. Hence, by Krull-Remak-Schmidt’s theorem, we have $BG/\Re(B)A \cong A/\Re(B)A$ as $BG$-left modules. Since $\eta_{BG}A$ and $\eta_{BA}A$ are finitely generated and projective and $\Re(B)A \subseteq \Re(\eta_{BG}A)$ and $\Re(B)A \subseteq \Re(\eta_{BA}A)$, $BG \cong A$ 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 $x \rightarrow \sum_{x \in H} \tau(x)$ from $A$ to $A^{\mu}$ is evidently an $A^{\mu}$-A-homomorphism. We denote this by $t_{H}$.

Let $A/B$ be a $G$-Galois extension. Then $(\sum_{a}u_{a})A \cong \text{Hom}(A_{B}, B_{B})$ 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 $t_{H}(c) = 1$. Further, since $j((\sum_{a}u_{a})V_{A}(B)) = \text{Hom}(\eta_{A_{B}}, \eta_{B_{B}})$, $B_{B}$ is a direct summand of $\text{Hom}(\eta_{A_{B}}, \eta_{B_{B}})$ and only if there exists an element $c$ in $V_{A}(B)$ such that $t_{H}(c) = 1$.

Let $c$ be an element of $A$ such that $t_{H}(c) = 1$, $H$ a subgroup of $G$, and $G = H_{1} \cup \cdots \cup H_{r}$ the right coset decomposition of $G$. If we set $\sum_{a}a_{H}(c) = 1$, then $t_{H}(d) = 1$. Hence, if $A/B$ is $G$-Galois and $B_{B}$ is a direct summand of $A_{B}$, then $A^{\mu}$ is a direct summand of $A_{A^{H}}$.

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

**Proposition 2.1.** Let $A/B$ be a $G$-Galois extension. If $H$ is a subgroup of $G$, then $A^{\mu} = \{\sum_{a}u_{a}x_{a}a_{a}; \text{ if } Ha = H_{a} \text{ then } x_{a} = x_{a}\}$ and $(A \otimes A)^{\mu} = A^{\mu} \otimes A$.

**Proof.** The first assertion is evident. We shall prove the second one. Evidently $A^{\mu} \otimes A \subseteq (A \otimes A)^{\mu}$. 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 $\sum_{a \in H}u_{a} \in A^{\mu}$ and $h^{-1}(\sum_{a \in H}u_{a}) = \sum_{a \in H} \tau(a_{i}) \otimes a_{i}^{*} = \sum_{i}h(\sum_{a \in H} \tau(a_{i}) \otimes a_{i}^{*} \in A^{\mu} \otimes A$. 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 $t_{1}, \ldots, t_{n} \in A^{H}$ and $a_{1}^{*}, \ldots, a_{n}^{*} \in A$ such that $\sum_{i} t_{i} \cdot \sigma(a_{i}^{*}) = \delta_{H, \sigma}$ for all $\sigma \in G$, and $\{ \sigma \in G \mid \sigma | A^{H} = 1_{A^{H}} \} = H$.

**Proof.** Let $\{(a_{i}, a_{i}^{*}) ; i = 1, \ldots, n\}$ 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 $\sum_{i} t_{i} \cdot \sigma(a_{i}^{*}) = \delta_{H, \sigma}$. If $\sigma | A^{H} = 1_{A^{H}}$, then $1 = \sum_{i} \sigma(t_{i}) \sigma(a_{i}^{*}) = \sum_{i} t_{i} \cdot \sigma(a_{i}^{*}) = \delta_{H, \sigma}$. Hence $\sigma \in H$.

**Theorem 2.3.** Let $A/B$ be $G$-Galois, and $B_{H}$ a direct summand of $A_{H}$. 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 $t_{1}, \ldots, t_{n} \in T$ and $a_{1}^{*}, \ldots, a_{n}^{*} \in A$ such that $\sum_{i} t_{i} \cdot \sigma(a_{i}^{*}) = \delta_{H, \sigma}$ 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 $\sum_{i} t_{i} \otimes \rho^{-1}(a_{i}^{*}) \in T \otimes A$ and $h(\sum_{i} t_{i} \otimes \rho^{-1}(a_{i}^{*})) = \sum_{i} h_{\rho}(t_{i}) u_{i}$. 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 $x_{j} \in T$, $y_{j} \in A$ 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 $x = x \cdot t_{0}(c) = \sum_{j} x_{j} t_{0}(y_{j}) \in T \cdot B = T$. 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 $\{(a_{i}, a_{i}^{*}) ; i = 1, \ldots, n\}$ 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 $\sum_{i} t_{i} \cdot \sigma(a_{i}^{*}) = \delta_{H, \sigma}$ for every $\sigma$ in $G$. Therefore, by Prop. 1.1, $G | A^{H}$ is strongly distinct. Now, $t_{H} \otimes 1$ is an $A^{H}$-homomorphism from $A \otimes_{B} A$ to $A^{H} \otimes_{B} A$. Since $\sum_{i} x a_{i} \otimes a_{i}^{*} x = (\sum_{i} x a_{i} \otimes a_{i}^{*} x) (\in A \otimes_{B} A)$ for all $x$ in $A$ (Prop. 1.3), $\sum_{i} y t_{i} \otimes a_{i}^{*} x = \sum_{i} t_{i} \otimes a_{i}^{*} y$ (in $A^{H} \otimes_{B} A$) for all $y$ in $A^{H}$. Hence the mapping $x \rightarrow \sum_{i} t_{i} \otimes a_{i}^{*} x$ from $A$ to $A^{H} \otimes_{B} A$ is an $A^{H}$-homomorphism, and $\sum_{i} t_{i} a_{i}^{*} x = x$. Hence the mapping $x \otimes y \rightarrow xy$ from $A^{H} \otimes_{B} A$ to $A$ splits as an $A^{H}$-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 $t_{1}, \ldots, t_{n} \in T$ and $a_{1}^{*}, \ldots, a_{n}^{*} \in A$ such that $\sum_{i} t_{i} \cdot \sigma(a_{i}^{*}) = \delta_{H, \sigma}$.
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, \(\sum t_i \sigma(a_i^*) = 0\) for every \(\sigma \notin H\). Whereas, if \(\sigma \in H\), then \(1 = \sum t_i \sigma(t_i) \sigma(a_i^*) = \sum t_i \sigma(a_i^*)\).

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 \(G\mid T\) is strongly distinct.

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

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

**Proof.** (1) will be easily seen. (2) Since \(S \otimes_T S \cong S \otimes_R R\) and \(S \otimes_R R \cong R\), this is obvious. (3) Since the mapping \(s \otimes s' \rightarrow ss'\) from \(S \otimes_T S\) to \(S\) splits as an \(S\)-\(S\)-homomorphism, the mapping \(r \otimes r' \rightarrow r \otimes r'\) from \(R \otimes_T R\) to \(R \otimes_S R\) splits as an \(R\)-\(R\)-homomorphism. Since \(R/S\) is separable, the mapping \(r \otimes r' \rightarrow rr'\) from \(R \otimes_T R\) to \(R\) splits as an \(R\)-\(R\)-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 \(A^B\)-\(A^B\)-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 \(G = H_{a_1} \cup \cdots \cup H_{a_r}\) be the right coset decomposition of \(G\). If we set \(d = \sum_i s_i(c)\), then \(t_H(d) = 1\) and \(d \in C\). Hence \(A^H\) is an \(A^B\)-\(A^B\)-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 \(x \rightarrow t_H(dx)\) from \(A\) to \(A^H\) is an \(A^B\)-\(A^B\)-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 \(A^B\)-\(A^B\)-homomorphy, and therefore the mapping \(y \rightarrow \sum t_H(ya_i) \otimes t'(a_i^*) = \sum t_H(a_i) \otimes t'(a_i^*)y\) from \(A^H\) to \(A^H \otimes_B A^H\) is an \(A^B\)-\(A^B\)-homomorphism. The mapping \(y \rightarrow \sum t_H(ya_i) \otimes t'(a_i^*)\tau(d)y = \sum t_H(ya_i) \otimes t'(a_i^*)\tau(d)\) from \(A^B\) to \(A^B \otimes_B A^B\) 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 $sR_R \cong s\text{Hom}(R_S, S_S)_R$ (cf. [10]). If $A/B$ is a $G$-Galois extension, then $(\mathcal{A}_A \cong t) \mathcal{A}(\sum u_\sigma)A_A \cong \mathcal{A}\text{Hom}(A_B, B_B)_A$ 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 $1 \leftarrow t$ under an isomorphism $sR_R \cong s\text{Hom}(R_S, S_S)_R$. Then $t\text{Hom}(sR_S, S_S)_R$ and $\text{Hom}(R_S, S_S)_R = tR$. 

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 $\mathcal{A}$, and set $\mathcal{A}/A = \text{Hom}(A_T, A_T)$, which is a subring of $\mathcal{A}$. Let $t = \sum c_\sigma u_\sigma$ be the image of 1 under the isomorphism $sA_A \cong s\text{Hom}(A_T, T_T)_A$. Then, $tA = \text{Hom}(A_T, T_T)$, $AtA = \mathcal{A}/A$ and $t \in \text{Hom}(sA_T, sT_T)$ (Lemma 3.1). Since $xt = tx$ for all $x$ in $T$, we have $x_c = c_\sigma \sigma(x)$ for all $x$ in $T$ and $\sigma$ in $G$, in particular, $yc = c_\sigma y$ for $y$ in $B$. Therefore, by assumption, each $c_\sigma$ is an element of $C$. Since $AtA = \mathcal{A}/A$, there are elements $c_i's, d_i's$ in $A$ such that $\sum c_i'td_i = u_1$. From this fact, $c_1$ is an invertible element of $C$. Now, the mapping $\alpha: \delta \rightarrow \delta c_1^{-1}$ is a $\mathcal{A}_0$-A-homomorphism from $\mathcal{A}_0$ to $\mathcal{A}$, and the mapping $\beta: \sum x_u \rightarrow \sum x_c u_\sigma$ is evidently an A-A-endomorphism of $\mathcal{A}$. For any $y$ in $A$ and $z$ in $T$, we have $\sum x_c u_\sigma(yz) = \sum x_c u_\sigma(y) \sigma(z) = \sum x_c u_\sigma(y) c_\sigma(z) = \sum x_c u_\sigma(y) x_c = \sum x_c u_\sigma(y) z = \sum x_c u_\sigma(y) z$, which means $\beta(\mathcal{A}) \subseteq \mathcal{A}_0$. If $x \otimes y$ is in $A \otimes_B A$, then $\beta h(x \otimes y) = \beta(x(\sum u_\sigma) y) = \beta(\sum x \cdot \sigma(y) u_\sigma) = \sum x \cdot \sigma(y) c_\sigma u_\sigma = x \sum c_\sigma u_\sigma y = xty$. For any $a_\delta$ in $\mathcal{A}$ and any $z$ in $A$, we have $\delta_0 xty(a_\delta) = \delta_0(xt(yz)) = \delta_0(x)t(yz) = \delta_0(x)ty(z)$. Thus, $\beta h$ is a $\mathcal{A}_0$-A-homomorphism from $A \otimes_B A$ to $\mathcal{A}_0$, and so $\beta$ is a $\mathcal{A}_0$-A-homomorphism from $A$ to $\mathcal{A}_0$. Since $\beta \alpha(u_i) = \beta(u_i c_1^{-1}) = u_i$, $\beta \alpha = 1_{\mathcal{A}_0}$. Thus, we have $\mathcal{A} = \text{Im} \alpha \otimes \text{Ker} \beta = \mathcal{A}_0 \otimes (\sum \Gamma \text{Ann}(c_i) \cdot u_\sigma)$, where $\text{Ann}(c_i) = \{x \in A; xc_\sigma = 0\}$. 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 $\delta_\tau = AtA \sum \tau(a_i) a_i^* = c_\tau u_\tau$, and so $\mathcal{A}_0 = \sum A c_\tau u_\tau$, whence it follows that $A = Ac_\tau \text{Ann}(c_i)$. Let $Ac_\tau = Ae_\tau$ with a
central idempotent \( e_\sigma \) in \( A \). Then, \( e_\sigma \cdot \sigma(y) = e_\sigma y \) for any \( y \) in \( T \). By assumption, if \( \sigma | T \neq 1_T \) then \( e_\sigma = 0 \), and so \( A_0 = \sum_{\sigma \in \mathcal{H}} A_{\sigma} \), where \( H = \{ \tau \in G \mid \tau | T = 1_T \} \). Since \( T_T \) is a direct summand of \( A_T \), \( \text{End} (A_T) = T_T \) the set of all right multiplications by elements of \( T \) (see [1; Th. A. 2]). On the other hand, since \( A_0 = \sum_{\sigma \in \mathcal{H}} A_{\sigma} \), \( \text{End} (A_T) = (A^H)_T \). 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 \( A^H_A \) is a direct summand of \( A^H \). 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 \( \sum e_\sigma = 1 \) and \( f(x) = \sum e_\sigma f(x) e_\sigma \) 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 \( \sum_\sigma a_\sigma \otimes a^*_\sigma = \sum_\sigma a_\sigma \otimes a^*_\sigma x (\in A \otimes_B A) \) for all \( x \) in \( A \) and \( \sum_\sigma a_\sigma = \delta_{1,\sigma} \) for all \( \sigma \) in \( G \) (Prop. 1.3). If we set \( t_i = t_i^H(a_i) \), then \( t_i \in A^H, \sum t_i \cdot \sigma(a^*_i) = \delta_{\alpha_i,\sigma} (\sigma \in G) \) and \( \sum_\sigma x t_i \otimes a^*_\sigma = \sum_\sigma t_i \otimes a^*_\sigma x = (\in A^H \otimes_B A) \) 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 \( e_\sigma = \sum \sigma f(t_i) g \sigma(a^*_i) \), then each \( e_\sigma \) is a central idempotent in \( A' \) (Prop. 1.2). By Prop. 1.2 (3), \( e_\sigma = e_\sigma f(\sum \sigma(t_i) \tau a^*_i) \) for any \( \sigma, \tau \) in \( G \). Therefore, if \( \sigma^{-1} \tau \notin H \) then \( e_\sigma = 0 \), and if \( \sigma^{-1} \tau \in H \) then \( e_\sigma = e_\tau \). Recalling that \( A^H_A \) is a direct summand of \( A_{A^H} \) there is an element \( d \) of \( A \) such that \( t^H(d) = 1 \). Since \( \sum_\sigma \sum_i t_i \otimes \sigma(a^*_i d) = \sum_\sigma t_i \otimes a^*_i d = \sum_\sigma t_i \otimes a^*_i = \sum_\sigma e_\sigma \cdot a^*_i d = 1 \) in \( A^H \otimes_B A \), we have \( \sum_\sigma \sum_i f(t_i) \otimes \sigma(a^*_i d) = 1 \otimes 1 \) \((\in A' \otimes A')\) and therefore \( \sum_\sigma \sum_i f(t_i) e_\sigma \otimes a^*_i d = 1 \) \((\in A')\). Let \( G = \sigma, H \cup \cdots \cup \sigma, H \) be the left coset decomposition of \( G \). Then, \( 1 = \sum_\sigma \sum_i f(t_i) g \sigma(a^*_i d) = \sum_\sigma \sum_i e_\sigma \cdot g \sigma(a^*_i d) = \sum_\sigma e_\sigma \cdot t^H(d) \) \(= 1 \). Since \( f(x) e_\sigma = e_\sigma f(x) \) for all \( x \) in \( A^H \) (Prop. 1.2), we have \( f(x) = \sum_\sigma f(x) e_\sigma = \sum_\sigma g \sigma(x) e_\sigma \) for all \( x \) in \( A^H \). Evidently, the mapping \( z \rightarrow \sum_\sigma g \sigma(z) e_\sigma \) 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 \( A^H_A \) is a direct summand of \( A^H \), 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 \( A \).

Theorem 5.1. Let $A/B$ be $G$-Galois, $A'$ a $G$-invariant subring of $A$, and $B'=A''$. Assume that there are elements $a_1, \ldots, a_n; a_1^*, \ldots, a_n^*$ and $c$ in $A'$ such that $\sum_i a_i \sigma(a_i^*)=\delta_{1,n}$, and $t_0(c)=1$.

(1) $A'|B'$ is a $G$-Galois extension, and $A''=B\otimes_B A''=A''\otimes_B B$ for any subgroup $H$ of $G$, in particular, $A=B\otimes_B A'=A'\otimes_B B$.

(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 $G=H_{\alpha_1} \cup \cdots \cup H_{\alpha_r}$ be the right coset decomposition of $G$. If we put $d=\sum_i \sigma_i(c)$ and $t_0(a_i)$, then $t_0(d)=1$ and $\sum_i t_i \sigma(a_i^*)=\delta_{H,\sigma}$ ($\sigma \in G$). If $x$ is in $A''$, then $A''\sim B \sum_i t_i \sigma_i(a_i^*dy)=\sum_i (\sum_i t_i \sigma(a_i^*) \sigma(dx)=t_0(dx)=t_0(d)x=x$. Thus, we obtain $A''=A''\sim B$. To be easily seen, the mapping $\sum_j x_j \otimes y_j \rightarrow \sum_j x_j y_j$ from $A''\sim B$ to $A''\sim B$ is well-defined and $\sum_i t_i \otimes t_i(a_i^*d \sum_j x_j y_j)=\sum_j x_j y_j$. Hence, $A''\sim B \cong A''\sim B=A''$ 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, $\overline{X} \cong A'(\overline{X} \cap B)$, 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 $x=\sum_i a_i x \in A'(\overline{X} \cap B)$. Hence, $\overline{X} \cong A'(\overline{X} \cap B)$, and the mapping $\sum_j x_j \otimes y_j \rightarrow \sum_j x_j y_j$ from $A''\sim B(\overline{X} \cap B)$ to $A'(\overline{X} \cap B)=\overline{X}$ is onto. Moreover, it is easily seen, $\sum_i a_i x \otimes y_j=\sum_j x_j y_j$. Hence, $\overline{X} \cong A''\sim B(\overline{X} \cap B)$. Now, let $X$ be a $B'$-left submodule of $B$. Then, $A'X$ is an $A'$-left submodule of $A$, and $A'X \cap B \supseteq X$. If $x \in A', y \in X$ is in $A'X \cap B$, then $\sum_j x_j y_j=t_0(c)(\sum_j x_j y_j)=\sum_i \sigma(c) \sum_j x_j y_j=t_0(\delta_{1,n})y_j \subseteq X$. 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 $a_1, a_1^*$ ($i=1, \cdots, n$) in $V_A(B)$ such that $\sum_i a_i \sigma(a_i^*)=\delta_{1,n}$.

(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 \(Y\rightarrow \bar{Y}\cap B\) and \(Y\rightarrow V_{\alpha}(B)Y=V_{\alpha}(B)\otimes_{B'}Y\) are mutually converse order isomorphisms between \{\bar{Y}\} and \{Y\}.

(3) \(A/V_{\alpha}(B)\) 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 \(A/V_{\alpha}(B)\) is separable. Conversely, assume that \(A/V_{\alpha}(B)\) is separable. Then, since both \(A/V_{\alpha}(B)\) and \(V_{\alpha}(B)/B'\) are separable, or equivalently, \(A\) is a separable \(B'\)-algebra (Lemma 2.7). Since \(A=B\otimes_{B'}V_{\alpha}(B)\), 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 \(A\otimes_{R}A'\neq 0\). 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 \((a_{t}, a_{t}')\); \(i=1, \cdots, n\) 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 \(\sigma\times\tau\cdot\sum_{j}x_{j}\otimes y_{j} = \sum_{j}x_{j}\otimes\tau(y_{j})\) \((x_{j}\in A, y_{j}\in A')\). Then, since \(\sum_{i,j}(a_{i}\otimes d_{j})\cdot(\sigma\times\tau)(a_{i}'\otimes d_{j}') = (\sum_{i}a_{i}\cdot\sigma(a_{i}'))\otimes(\sum_{j}d_{j}\cdot\tau(d_{j}'))\), \((A\otimes_{R}A')/(A\otimes A')^{G\times G'}\) 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 \(\sum_{i\in H}\sigma(c)=1\) and \(\sum_{e\in H'}\tau(c')=1\). If \(\sum_{k}x_{k}\otimes y_{k}\) is in \((A\otimes A')^{H\times H'}\), then \(\sum_{k}x_{k}\otimes y_{k} = (\sum_{e\in H}\sigma(c))\otimes(\sum_{e\in H'}\tau(c'))\cdot\sum_{k}x_{k}\otimes y_{k} = \sum_{k}\sum_{e\in H}\sigma(c)\otimes\tau(c')\cdot(\sigma\times\tau)(\sum_{k}x_{k}\otimes y_{k}) = \sum_{k}(\sum_{e\in H}\sigma(c)\otimes(\sum_{e\in H'}\tau(c')y_{k})\in A\otimes A'.\) Hence, \((A\otimes A')^{H\times H'}=A\otimes A'.\) 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 \(B'_{B'}\) a direct summand of \(A'_{B'}\), then \((A\otimes_{R}A')/(B\otimes B')\) is a \(G\times G'\)-Galois extension, and \((A\otimes A')^{H\times H'}=A\otimes A'\) 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 \(A^{H\cap K}=A^{K}\cdot A^{H}\).

Proof. By assumption, there is an element \(c\) in \(A\) such that \(t_{H\cap K}(c)=1\).
Evidently, \( A^{H \cap K} \supseteq A^{H} \cdot A^{K} \). 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 \( A^{H} \cdot A^{K} \supseteq \sum_{i} t_{i}(a_{i}) t_{i}(a_{i}^* cx) \) is a summand of \( A^{H} \cdot A^{K} \). Therefore we have \( A^{H \cap K} = A^{H} \cdot A^{K} \).

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

**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 \( G \)), \( A^{K_{0}H_{0}} = A^{K_{0}B} \otimes_{B} A^{K_{0}H} \) and \( A^{K_{0}H_{0}} \) 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 \( t_{c}(c) = 1 \). Put \( t_{c} = t_{K}(a_{c}) \), \( t_{c}^{*} = t_{K}(a_{c}^{*}) \), and \( d = t_{K}(c) \). Then, \( B = A^{K} \otimes_{B} A^{H} \) is an \( H \)-Galois extension. By Th. 5.1, \( A^{H} \otimes_{B} A^{K} \) is a summand of \( A \). If \( H_{0} \) is a subgroup of \( H \), then \( A^{K_{0}H_{0}} \supseteq A^{K_{0}H} \cdot A^{KH_{0}} \). Hence, by Th. 5.1, \( A^{K_{0}H_{0}} = A^{K_{0}B} \otimes_{B} A^{K_{0}H} \) and \( A^{K_{0}H_{0}} \) is an \( H \)-Galois extension.

**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 \( H_{i} = N_{i} \times \cdots \times N_{i} \times N_{i} \times \cdots \times N_{r} \) (\( i = 1, \cdots, r \)), then \( A^{H_{i}B} = A^{H_{i}H} \cdot A^{KH_{i}} \cdot A^{K_{0}H_{0}} \cdot A^{KH_{0}} \cdot A^{K_{0}H_{0}} \) 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 \( H = \{\sigma \in G; \delta|T = 1_{T}\} \) and \( H' = \{\sigma \in G; \sigma|T' = 1_{T'}\} \), then \( T = A^{H} \) and \( T' = A^{H'} \).

**Proof.** Since \( T \otimes_{B} T' = A \), we have \( \tau T \otimes_{B} A^{A} \equiv \tau A \otimes_{T} A_{A} \). 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 \( \mathfrak{A} \) 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 \( x + \mathfrak{A} \) (\( \in A/\mathfrak{A} \)) by \( \overline{x} \). If we define \( \sigma(\overline{x}) = \sigma(\overline{x}) \), then \( \sum_{i} a_{i} \cdot \sigma(a_{i}^{*}) = \delta_{i, \sigma} \) for \( \sigma \in G \), and therefore
If $\mathfrak{A}$ 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 $(A/\mathfrak{A})^H$, then $\bar{x} = \bar{x} \sum_{e \in H} \tau(e) = \sum_{e \in H} \tau(\bar{x}e) = t_H(xc) \in (A^H + \mathfrak{A})/\mathfrak{A}$. Thus, we prove the following:

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

**Corollary.** Let $A/B$ be a $G$-Galois extension, and $B_B$ a direct summand of $A_B$. If $B$ contains a non-zero central idempotent $e$ of $A$, then $Ae/Be$ is a $G$-Galois extension, and $(Ae)^H = A^H \cdot e$ 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 $\{(a_i, a_i^*) ; i = 1, \cdots, n\}$ 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 $t_N(a_i^* e) = t_i^*$, then $t_i$ and $t_i^*$ are $A^N$, and $\sum_i t_i \sigma(t_i^*) = \delta_{N, \sigma}$ 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 $m \times m$ complete 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 $\{(a_i, a_i^*) ; i = 1, \cdots, n\}$ be a $G$-Galois coordinate system for $A/B$. Then $\sum_i a_i E \cdot \sigma(a_i^* E) = \delta_{1, \sigma}$ 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 $\{e_{ij} ; i, j = 1, \cdots, m\}$ a system of matrix units contained in $B$. If $A_0 = \bigvee_A \{e_{ij}\}$, then $A_0/A_0^G$ is a $G$-Galois extension, and $B = \sum_{i, j} A_0^G e_{ij}$.

**Proof.** Obviously, $G$ induces an automorphism group of $A_0$ and $B = \sum_{i, j} A_0^G e_{ij}$. Let $\{(A_i, A_i^*) ; i = 1, \cdots, n\}$ be a $G$-Galois coordinate system for $A/B$. Let $A_i = \sum_{j, k} a_{ijk} e_{jk}$, $A_i^* = \sum_{j, k} d_{ijk} e_{jk}$ $(a_{ijk}, d_{ijk} \in A_i)$. Then, $\sigma(A_i^*) = \sum_{j, k} \sigma(d_{ijk}) e_{jk}$ and therefore $\sum_{i, k} a_{ik} \cdot \sigma(d_{ik}) = \delta_{1, \sigma}$ 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 $R M$ and $R N$ 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 $\text{End}_R(M)$-
admissible and $X=\sum_{i}(X\cap M_{i})$ for every submodule $X$ of $\kappa M$.

(2) If $X=\sum_{i}(X\cap M_{i})$ for every submodule $X$ of $\kappa M$, 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 $\kappa M$ 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 $\varphi; M_{i}\oplus M_{j}\rightarrow M_{j}/N_{j}$ by the following rule: $(m_{i}+m_{j})\varphi=(m_{i}+N_{i})\alpha+(m_{j}+N_{j})$. Then, our assumption yields $\text{Ker}\varphi=(M_{i}\cap\text{Ker}\varphi)+(M_{j}\cap\text{Ker}\varphi)$, and so $(M_{i}+M_{j})\varphi=M_{i}\varphi\oplus M_{j}\varphi=M_{i}/N_{i}\oplus M_{j}/N_{j}$, 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 $\mathfrak{A}u_{\sigma}$ with some ideal $\mathfrak{A}$ 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 $J_{\sigma}={a\in A; \sigma(x)a=ax}$ 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 $\text{Hom}(A_{u_{\sigma}}, A_{A})=0$.

Proof. Assume $J_{\sigma}=0$. If $f$ is in $\text{Hom}(A_{u_{\tau}}, A_{A})$, 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 $\text{Hom}(A_{u_{\sigma}}, A_{A})=0$. If $a$ is in $J_{\sigma}$, then we can easily see that the mapping $xu_{\tau}\rightarrow xa$ $(x\in A)$ 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) $\text{Hom}(A_{u_{\sigma}}, A_{A})=0$ 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 $u_{1}\in A(\sum_{*}u_{\tau})A$ (Prop. 6.1.), there are elements $a_{i}, a_{i}^{*}$ $(i=1, \cdots, n)$ in $A$ such that $u_{1}=$
\[ \sum_{t}a_{t}(\sum_{u_{t}}a_{t}^{*})a_{t}^{*} = \sum_{\sigma}(\sum_{t}a_{t}^{*}\sigma(a_{t}^{*}))u_{t}. \] Hence \[ \sum_{t}a_{t}^{*}\sigma(a_{t}^{*}) = \delta_{1,\sigma} \] 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 \( a, a' \) \((i=1, \cdots, n)\) in \( A \) such that \( \sum_{t}a_{t}x=\sigma(a't)\) for each \( x \) in \( A \) \((\sigma \in G)\), then \( G \) is completely outer.

**Proof.** Let \( X \) be any \( A \)-module of \( A \). If \( \sum_{t}a_{t}x_{u} \) is in \( X \), then \( X \ni \sum_{t}a_{t}(\sum_{x}x_{u})\tau^{-1}(a_{t}) = x_{u} \) 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 \( ax = a\cdot\sigma_{0}(x) \) for all \( x \) in \( A^{u} \), then \( a = 0 \).

**Proof.** There are elements \( t_{1}, \cdots, t_{n} \in A^{u} \) and \( a_{1}^{*}, \cdots, a_{n}^{*} \in A \) such that \( \sum_{t}t_{i}\cdot\sigma(a_{i}^{*}) = \delta_{1,\sigma} \) for any \( \sigma \) in \( G \) (Prop. 2.2). Hence, \[ a = a\sum_{i}t_{i}a_{i}^{*} = \sum_{i}a\cdot\sigma_{0}(t_{i})a_{i}^{*} = \sigma_{0}(a^{-1}(a))\sum_{i}t_{i}\cdot\sigma_{0}^{-1}(a_{i}^{*}) = 0. \]

**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 \( a_{i} \in R, f_{i} \in \text{Hom}(R/S, S) \) \((i=1, \cdots, n)\) 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 \( * \)-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 \( G/A^{u} \) is \( * \)-strongly distinct for any subgroup \( H \) of \( G \) (Prop. 6.7).

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

(i) \( T = A^{u} \) for some subgroup \( H \) of \( G \).

(ii) \( A^{u} \) is finitely generated and projective, and \( T/_{T} \) is a direct summand
of $A_T$, and $G|T$ is\*-strongly distinct.

\textbf{Proof.} Since $A/A^H$ is $H$-Galois, it remains to prove (ii) $\Rightarrow$ (i). If we put $\mathcal{A}_0 = \text{End}(A_T)$, then $\mathcal{A}_0$ is a subring of $\mathcal{A}$. Since $\mathcal{A}_0$ is an $A$-$A$-submodule of $\mathcal{A}$, $\mathcal{A}_0 = \sum \mathfrak{A}_\sigma u_\sigma$ with some ideals $\mathfrak{A}_\sigma$ of $A$. By Lemma 6.8, $\mathcal{A}_0$ is a direct summand of $\mathcal{A}$, so that each $\mathfrak{A}_\sigma u_\sigma$ is a direct summand of $\mathcal{A}$. Therefore each $\mathfrak{A}_\sigma u_\sigma$ is a direct summand of $A_T u_\sigma$. Hence $\mathfrak{A}_\sigma$ is a direct summand of $\mathcal{A}$. Let $\mathfrak{A}_\sigma = A e_\sigma$ with an idempotent $e_\sigma$ in $A$. Then, since $e_\sigma u_\sigma$ is in $\mathcal{A}_0$, $e_\sigma \sigma(x y) = e_\sigma \sigma(x) y$ 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 $\mathfrak{A}_\sigma = A$ for each $\sigma$ in $H$. We obtain therefore $\mathcal{A}_0 = \sum e H \oplus A u_\sigma$, and hence $\text{End}(A) = (A^H)_T$. On the other hand, since $T_T$ is a direct summand of $A_T$, $\text{End}(A) = T_T$ (cf. [1]). 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:

\textbf{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 $T_T$ is a direct summand of $A_T$, $G|T$ is strongly distinct.

\textbf{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 $a_i, a'_i$ $(i = 1, \ldots, n)$ in $A$ such that $\sum_i a_i \cdot x a'_i = x$ and $\sum_i a_i y \cdot \sigma(a'_i) = 0$.

\textbf{Proof.} (i) $\Rightarrow$ (ii) Let $x, y$ be in $A$, and $\sigma$ any element of $G$ such that $\sigma \neq 1$. We set $X = A (x u_1 + y u_2) A$, which is an $A$-$A$-submodule of $Au_1 + Au_2$. By Prop. 6.1, $x u_1 \in A$, and hence there are elements $a_i, a'_i$ $(i = 1, \ldots, n)$ in $A$ such that $\sum_i a_i (x u_1 + y u_2) a'_i = x u_1$. Then, $\sum_i a_i x a'_i = x$ and $\sum_i a_i y \cdot \sigma(a'_i) = 0$.

(ii) $\Rightarrow$ (i) Let $\sigma, \tau$ be distinct elements in $G$, and $X$ any $A$-$A$-submodule of $Au_1 + Au_2$. Let $x u_1 + y u_2$ be any element of $X$. For $\sigma^{-1}(x)$ and $\sigma^{-1}(y)$, there are elements $a_i, a'_i$ $(i = 1, \ldots, n)$ in $A$ such that $\sum_i a_i \cdot x^{-1}(a'_i) = \sigma^{-1}(x)$ and $\sum_i a_i \cdot x^{-1}(y) \cdot \tau(a'_i) = 0$. Then, $\sum_i \sigma(a_i) \cdot x \cdot \sigma(a'_i) = x$ and $\sum_i \sigma(a_i) \cdot y \cdot \tau(a'_i) = 0$, and so $x \in \sum_i \sigma(a_i) (x u_1 + y u_2) a'_i = x u_1$. Thus, by Prop. 6.1, $Au_1$ and $Au_2$ are unrelated.

\textbf{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 $xu_1 \in A(\sum_{i \in \mathcal{N}} xu_1 + \sum_{i \in \mathbb{N}} yu_1) A$ (Prop. 6.1), there are elements $x_i$, $y_i$ ($i = 1, \ldots, n$) in $A$ such that $\sum_i x_i (\sum_{\mathcal{N}} xu_1 + \sum_{\mathbb{N}} yu_1) y_i = xu_1$. Then $\sum_i x_i \cdot \tau(y_i) = \delta_1, x \ (\tau \in \mathcal{N})$ and $\sum_i x_i \cdot \sigma(y_i) = 0 \ (\sigma \in G \setminus N)$. 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 $x_i', y_i' (i = 1, \ldots, n)$ are in $A^N$. To be easily seen, $\sum_i x_i' y_i' = x$ and $\sum_i x_i' \rho(y_i') = 0$ 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 $R \cap S = 1$ 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 $n$ 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 $R_S$ is finitely generated and projective. If $S$ is semi-primary, then so is $R$.

Proof. (1) Let $\{I_i; i = 1, \ldots, n\}$ be a $d$-independent set of maximal left ideals of $S$ (cf. [11]). Then, $\{RI_i; i = 1, \ldots, n\}$ is a $d$-independent set of proper left ideals of $R$ (Lemma 7.1). Since each $RI_i$ is contained in a maximal left ideals of $R$, $n \leq \text{max-dim}_R R =$ 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, \( \text{End}(R_S) \) is semi-primary. By Lemma 6.8, \( R_I R_I \) (the set of all left multiplications by elements of \( R \)) is a direct summand of \( R, \text{End}(R_S) \). 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 \( s R_R \cong s \text{Hom}(R_S, S_R) \) (Kasch [10]).

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

1. \( \text{End}(R_S)/R_I \) 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 \( \text{End}(R_S) \) is \( \text{End}(R_S) \)-right injective. Let \( R_S \cong S_S^m \). Then, \( \text{End}(R_S) \cong (S)_m \), 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 \( \Re(R) \cap S + 1 = S \) for some maximal left ideal \( I \) of \( S \). Since \( R(\Re(R) \cap S) + Rl = R \) and \( R(\Re(R) \cap S) \subseteq \Re(R) \), we have \( Rl = R \). If follows then a contradiction \( 1 = Rl \cap S = S \) (Lemma 7.1).

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

**Proof.** Let \( X \) be a maximal \( \Delta \)-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 \( \Delta \)-submodule of \( A \) such that \( Y \supseteq \cap \sigma(\mathfrak{P}) \). Then \( Y = \cap \sigma(\mathfrak{P}_2) \) for some maximal ideal \( \mathfrak{P}_2 \) of \( A \). If \( \cap \sigma(\mathfrak{P}_2) \supseteq \cap \sigma(\mathfrak{P}) \), then \( \mathfrak{P} \not\supseteq \cap \sigma(\mathfrak{P}_2) \), 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 \( \Delta \)-submodules of \( A \) and \( \{ X \} \) be the set of all left ideals of \( B \). Then \( \overline{X} \to \overline{X} \cap B \) and \( X \to AX = A \otimes_B X \) 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 $A_{S}$ is finitely generated, $A \cdot \mathfrak{R}(B)$ is d-dense in $A_{B}$, and so d-dense in $A_{A}$ (cf. [11]). Hence $A \cdot \mathfrak{R}(B) \subseteq \mathfrak{R}(A)$.

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

**Proof.** By Cor. to Th. 5.2, $(A' \otimes_{B} A)/(A' \otimes 1)$ is a $G$-Galois extension. Since $(A' \otimes A) (\mathfrak{R}(A') \otimes 1) = \mathfrak{R}(A') \otimes A$ is an ideal of $A' \otimes A$, $\mathfrak{R}(A' \otimes A) = \mathfrak{R}(A') \otimes A$ 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 $A = \sum_{u} \mathfrak{U}$, for some ideals $\mathfrak{U}$, of $A$ (resp. $A = \sum_{u} \mathfrak{U}$ for some ideal $\mathfrak{U}$ of $A$), and conversely. In particular, if $A$ is an ideal of $A$, then $A = A \mathfrak{U} = \mathfrak{U} \mathfrak{A}$ for some $G$-invariant ideal $\mathfrak{U}$ 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 $\{\mathfrak{U}\}$ the set of all $G$-invariant ideals of $A$. Then, there exists an order isomorphism $\mathfrak{U} \leftrightarrow a$ between $\{A\}$ and $\{a\}$ such that $A(A) = Aa$ (cf. [1; Prop. A. 5]). Consequently, there exists an order isomorphism $\mathfrak{U} \leftrightarrow A \leftrightarrow a$ between $\{\mathfrak{U}\}$ and $\{a\}$ (cf. Th. 5.1 (2)). Accordingly, if $A$ is semi-prime, (prime, two-sided simple) then so is $B$. Since $A \cdot \mathfrak{R}(B) = \mathfrak{R}(B) \cdot A$ is an ideal of $A$, Prop. 7.8 implies $\mathfrak{R}(A) = A \cdot \mathfrak{R}(B) = \mathfrak{R}(B) \cdot A$. Next, we shall consider $R(A)$. There exists $\mathfrak{W} \in \{\mathfrak{W}\}$ such that $R(A) = \mathfrak{W} \cdot A = \mathfrak{A} \cdot A$. Since $\mathfrak{W} = \mathfrak{W} \cdot A \subseteq \mathfrak{R}(\mathfrak{W}) = \mathfrak{W} \cdot A$ by Prop. 7.5, we obtain $R(A) = \mathfrak{W} \cdot A = \mathfrak{W} \cdot R(A) = \mathfrak{W} \cdot R(A) \cdot A$. On the other hand, noting that $\Delta_{A}$ is finitely generated and $A \cdot R(A)$ is an ideal of $A$, we see that $A \cdot R(A) \subseteq R(A)$ (cf. the proof of Prop. 7.8). Hence, we have $R(A) = A \cdot R(A) = A \cdot R(A) \cdot A$. Since $R(A) = A \cdot R(B) = A \cdot R(B) \cdot A$, $R(A) \cap B = R(B)$, $R(A) = A \cdot R(B) = A \cdot R(B) \cdot A$, $R(A) \cap B = R(B)$, $R(A) = A \cdot R(A) = A \cdot R(A) \cdot A$, and $R(A) = A \cdot R(A) = A \cdot R(A) \cdot A$.

**Theorem 7.10.** If $G$ is completely outer and $B$ a direct summand of $A_{B}$, then $R(A) = A \cdot R(B) = R(B) \cdot A$, $R(A) \cap B = R(B)$, $R(A) = R \cdot R(B) = R \cdot R(B) \cdot A$, $R(A) \cap B = R(B)$, $R(A) = A \cdot R(A) = R(A) \cdot A$, and $R(A) = A \cdot R(A) = A \cdot R(A) \cdot A$.

**Proposition 7.11.** Let $B$ be directly indecomposable, and let $A = \mathfrak{U}_{1} \oplus \cdots \oplus \mathfrak{U}_{s}$ be a direct sum of minimal ideals. If $\mathfrak{U}$ is a minimal ideal of $A$, then $\{ \sigma(\mathfrak{U}); \sigma \in G \} = \{ \mathfrak{U}_{1}, \ldots, \mathfrak{U}_{s} \}$, and $n$ divides $\langle G : 1 \rangle$. If $\mathfrak{B}$ is a maximal ideal of $A$, $\{ \sigma(\mathfrak{B}); \sigma \in G \}$ coincides with the set of all maximal ideals of $A$. For any $\mathfrak{U}_{i}$, we set $\sum_{i} \sigma(\mathfrak{U}_{i}) = \mathfrak{B}$. Then, $\mathfrak{B} = A e$ 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

$$\left\{ \sigma(\mathfrak{U}_{i}); \sigma \in G \right\} = \left\{ \mathfrak{U}_{1}, \cdots, \mathfrak{U}_{8} \right\}.$$

If we set $H = \left\{ \sigma \in G ; \sigma(\mathfrak{U}_{i})=\mathfrak{U}_{i} \right\}$, then $\#\left\{ \sigma(\mathfrak{U}_{i}); \sigma \in G \right\} = (G : H)$, 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 $B_{n}$ a direct summand of $A_{n}$. 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 $\mathfrak{U}$. 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**


Department of Mathematics,
Hokkaido University

(Received June 10, 1966)