HOKKAIDO UNIVERSITY

Title	FINITE OUTER GALOIS THEORY OF NON-COMMUTATIVE RINGS
Author(s)	Miyashita, Yōichi
Citation	Journal of the Faculty of Science Hokkaido University. Ser. 1 Mathematics, 19(3-4), 114-134
Issue Date	1966
Doc URL	https://hdl.handle.net/2115/56076
Type	departmental bulletin paper
File Information	JFSHIU_19_N3-4_114-134.pdf

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

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 $B=A^G=\{x\in A;\ \sigma(x)=x \text{ for all } \sigma \text{ in } G.\}$. 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 $\sum_i a_i\cdot\sigma(a_i^*)=\delta_{1,\sigma}(\sigma\in G)$, 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 $x\otimes y\to xy$ 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 σ 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 $\{\bar{T}\}$ 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, $\bar{T}\to\bar{T}\cap B$ and $T\to A'T=TA'$ are mutually converse order isomorphisms between $\{\bar{T}\}$ and $\{T\}$, and $\bar{T}/(\bar{T}\cap B)$ 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, $\{\sigma\in G;\ \sigma|A^H=1_{A^H}\}=H$. (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 $x\otimes y\to xy$ 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 sence of Kasch), and T_T is a direct summand of A_T (Th. 3.2). In case ${}_BB_B$ is a direct summand of ${}_BA_B$, the next is also equivalent to (a). (b′) The mapping $x\otimes y\to xy$ 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 $\Delta=\Delta(A,G)=\sum_{\sigma\in G}\oplus Au_\sigma$ be the trivial crossed product of A with G. G is said to be completely outer if ${}_AAu_{\sigma A}$ and ${}_AAu_{\tau A}$ 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 auther 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 σ 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 $\sum_j x_j\otimes y_j\to\sum_j x_jy_j$ 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 $\sum_i t_ia'_i=1$ and $\sum_i xt_i\otimes a'_i=\sum_i t_i\otimes a'_ix$ $(\in T\otimes_{B'}A')$ 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 $\mathfrak{S}$ be a set of

ring homomorphisms from A' to A''. $\mathfrak{S}$ is called *strongly distinct* if any distinct f, g in $\mathfrak{S}$ are strongly distinct.

$\Delta=\Delta(A, G)$ denotes the trivial crossed product of A with G: $\Delta=\sum_{\sigma\in G}\oplus Au_\sigma$, $u_\sigma u_\tau=u_{\sigma\tau}$ $(\sigma, \tau\in G)$, $u_\sigma x=\sigma(x)u_\sigma$ $(x\in A)$. By j, we denote the ring homomorphism from Δ to Hom (A_B, A_B) defined by $j(xu_\sigma)(y)=x\cdot\sigma(y)$ for x, y in A and σ 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 $\sum_i a_i\cdot\sigma(a_i^*)=\delta_{1,\sigma}$ for all σ in G. When this is the case, $\{(a_i, a_i^*): i=1, \cdots, n\}$ 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 Δ with Hom (A_B, A_B): $\Delta=A_lG=AG$, where A_l 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 $e=e1=\sum_i e\cdot g(t_i)g(a_i)=\sum_i e\cdot f(t_i)g(a_i)=0$. Thus, f and $g|T$ are strongly distinct.

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) *$f(x)e=e\cdot g(x)$ 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 $\sum_i xt_i\otimes a_i=\sum_i t_i\otimes a_i x$ $(\in T\otimes_{B'}A')$ for all x in T, $\sum_i f(xt_i)\otimes g(a_i)=\sum_i f(t_i)\otimes g(a_i x)$ $(\in A''\otimes_{B'}A'')$ for all x in T. Therefore,

$f(x)e=e\cdot g(x)$ 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 $g|T$ 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 $\sum_j g(t_j)g'(a_j)=0$ by (4), and so $ee'=e\sum_j g(t_j)g'(a_j)=0$.

Evidently, the mapping $x\otimes y\to x\sum_\sigma u_\sigma y$ from $A\otimes_B A$ to Δ is an A-A-homomorphism. We denote this homomorphism by h. One may remark here that h is a Δ-A-homomorphism. In fact, $u_\tau x\sum_\sigma u_\sigma y=\tau(x)u_\tau\sum_\sigma u_\sigma y=\tau(x)\sum_\sigma u_\sigma y$.

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 Δ-A-isomorphism, $h^{-1}(\sum_\sigma x_\sigma u_\sigma)=\sum_\sigma\sum_i x_\sigma\cdot\sigma(a_i)\otimes a_i^*$ for every $\sum_\sigma x_\sigma u_\sigma$ in Δ, and $\{(a_i, a_i^*);\ i=1,\cdots,n\}$ is a (B, A)-projective coordinate system for A.*

Proof. To be easily seen, $h(\sum_\sigma\sum_i x_\sigma\cdot\sigma(a_i)\otimes a_i^*)=\sum_\sigma x_\sigma u_\sigma$, and hence h is onto. Let x, y be in A. Then $\sum_\sigma\sum_i x\cdot\sigma(y)\sigma(a_i)\otimes a_i^*=x\otimes\sum_\sigma\sum_i\sigma(y)\sigma(a_i)a_i^*=x\otimes y$, whence we can easily see that h is 1-1. Hence, h is a Δ-A-isomorphism. Since $h(\sum_i a_i\otimes a_i^*)=u_1$ and h is an A-A-isomorphism, $\sum_i xa_i\otimes a_i^*=\sum_i a_i\otimes a_i^*x$ 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)-projcetive 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 ${}_BA\cong{}_BB^m$ for some natural number m, then ${}_{BG}BG^m\cong{}_{BG}A^m$.*

Proof. Let $A=\sum_i\oplus Bd_i$ $(i=1,\cdots,n)$, and ${}_BB\cong{}_BBd_i$ by the correspondence

$y \to yd_i$ $(y \in B)$. Then $\Delta = \sum_\sigma \oplus u_\sigma A = \sum_{\sigma,i} \oplus u_\sigma B d_i = \sum_{\sigma,i} \oplus B u_\sigma d_i = \sum_i \oplus (\sum_\sigma B u_\sigma) d_i$ and $(\sum_\sigma B u_\sigma) d_i \cong \sum_\sigma B u_\sigma$ as $\sum_\sigma B u_\sigma$-left modules. Hence, ${}_{BG}\Delta \cong {}_{BG}BG^m$. On the other hand, ${}_A\Delta \cong {}_AA \otimes_B A \cong {}_AA \otimes_B (B^m) \cong {}_AA^m$ (Prop. 1.3). We obtain therefore ${}_{BG}BG^m \cong {}_{BG}A^m$.

Theorem 1.7. *Let A/B be a G-Galois extension and ${}_BA \cong {}_BB^m$ 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 ${}_{BG}BG \cong {}_{BG}A$, that is, A has a normal basis.*

Proof. By Prop. 1.6, ${}_{BG}BG^m \cong {}_{BG}A^m$. Since $\mathfrak{R}(B)G \cdot BG^m = (\mathfrak{R}(B)G)^m \leftrightarrow (\mathfrak{R}(B)A)^m$ 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 ${}_{BG}BG$ and ${}_{BG}A$ are finitely generated and projective and $\mathfrak{R}(B)G \subseteq \mathfrak{R}({}_{BG}BG)$ and $\mathfrak{R}(B)A \subseteq \mathfrak{R}({}_{BG}A)$, $BG \cong A$ 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 $x \to \sum_{\tau \in H} \tau(x)$ 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 $(\sum_\sigma u_\sigma)A \cong \mathrm{Hom}\,(A_B, B_B)$ 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 $t_G(c) = 1$. Further, since $j((\sum_\sigma u_\sigma)\mathrm{V}_A(B)) = \mathrm{Hom}\,({}_BA_B, {}_BB_B)$, ${}_BB_B$ is a direct summand of ${}_BA_B$ if and only if there exists an element c in $\mathrm{V}_A(B)$ such that $t_G(c) = 1$.

Let c be an element of A such that $t_G(c) = 1$, H a subgroup of G, and $G = H\sigma_1 \cup \cdots \cup H\sigma_r$ the right coset decomposition of G. If we set $\sum_i \sigma_i(c) = d$, then $t_H(d) = 1$. Hence, if A/B is G-Galois and B_B is a direct summand of A_B, then $A^H_{A^H}$ 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 $\{u \in M;\ \tau(u) = u \text{ for all } \tau \text{ in } H\}$. If A/B is a G-Galois extension, then h: ${}_GA \otimes_B A_A \cong {}_G\Delta_A$ (Prop. 1.3), and evidently $(A \otimes A)^H \leftarrow \Delta^H$ under h.

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

Proof. The first assertion is evident. We shall prove the second one. Evidently $A^H \otimes A \subseteq (A \otimes A)^H$. Let $\{(a_i, a_i^*);\ i = 1, \cdots, n\}$ be a G-Galois coordinate system for A/B. If ρ is an element of G, then $\sum_{\sigma \in H\rho} u_\sigma \in \Delta^H$ and $h^{-1}(\sum_{\sigma \in H\rho} u_\sigma) = \sum_{\tau \in H} \sum_i \tau\rho(a_i) \otimes a_i^* = \sum_i (\sum_{\tau \in H} \tau\rho(a_i)) \otimes a_i^* \in A^H \otimes A$. 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 $\sum_i t_i\cdot\sigma(a_i^*)=\delta_{H,\sigma}$ for all σ 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 $\sum_i t_i\cdot\sigma(a_i^*)=\delta_{H,\sigma}$. 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_B a direct summand of A_B. 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 $\sum_i t_i\cdot\sigma(a_i^*)=\delta_{H,\sigma}$ for all σ 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 ρ is in G, then $\sum_i t_i\otimes\rho^{-1}(a_i^*)\in T\otimes A$ and $h(\sum_i t_i\otimes\rho^{-1}(a_i^*))=\sum_{\sigma\in H\rho}u_\sigma$. Noting that h is an A-right homomorphism, we know that $h(T\otimes A)=\Delta^H$, and hence $T\otimes A=A^H\otimes A$ (Prop. 2.1). (iii)$\Rightarrow$(i) There is an element c of A such that $t_G(c)=1$. 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 $1\otimes t_G$, we can easily see $x=x\cdot t_G(c)=\sum_j x_j\cdot t_G(y_j)\in T\cdot B=T$. 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 $x\otimes y\to xy$ 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 $\sum_i t_i\cdot\sigma(a_i^*)=\delta_{H,\sigma}$ for every σ in G. Therefore, by Prop. 1.1, $G|A^H$ is strongly distinct. Now, $t_H\otimes 1$ is an A^H-A-homomorphism from $A\otimes_B A$ to $A^H\otimes_B A$. Since $\sum_i xa_i\otimes a_i^*=\sum_i a_i\otimes a_i^*x$ $(\in A\otimes_B A)$ for all x in A (Prop. 1.3), $\sum_i yt_i\otimes a_i^*=\sum_i t_i\otimes a_i^*y$ $(\in A^H\otimes_B A)$ for all y in A^H. Hence the mapping $x\to\sum_i t_i\otimes a_i^*x$ from A to $A^H\otimes_B A$ is an A^H-A-homomorphism, and $\sum_i t_i a_i^*x=x$. Hence the mapping $x\otimes y\to xy$ from $A^H\otimes_B A$ to A splits as an A^H-A-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 $\sum_i t_i\cdot\sigma(a_i^*)=\delta_{H,\sigma}$*

for all σ 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, $\sum_i t_i\cdot\sigma(a_i^*)=0$ for every $\sigma\notin H$. Whereas, if $\sigma\in H$, then $1=\sum_i\sigma(t_i)\sigma(a_i^*)=\sum_i t_i\cdot\sigma(a_i^*)$.

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 $G|T$ 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 $S\otimes_T S\otimes_S R\cong S\otimes_T R$ and $S\otimes_S R\cong R$, this is obvious. (3) Since the mapping $s\otimes s'\to ss'$ from $S\otimes_T S$ to S splits as an S-S-homomorphism, the mapping $r\otimes r'\to r\otimes r'$ from $R\otimes_T R$ to $R\otimes_S R$ splits as an R-R-homomorphism. Since R/S is separable, the mapping $r\otimes r'\to rr'$ from $R\otimes_T R$ to R splits as an R-R-homomorphism.

Proposition 2.8. *Let A/B be outer G-Galois, and ${}_BB_B$ a direct summand of ${}_BA_B$. 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 ${}_BB_B$ is a direct summand of ${}_BA_B$, there is an element c of C such that $t_G(c)=1$. Let $G=H\sigma_1\cup\cdots\cup H\sigma_r$ be the right coset decomposition of G. If we set $d=\sum_k\sigma_k(c)$, then $t_H(d)=1$ and $d\in C$. 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 $x\to t_H(dx)$ 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-homomoryhism, and therefore the mapping $y\to\sum_i t_H(ya_i)\otimes t'(a_i^*)=\sum_i t_H(a_i)\otimes t'(a_i^*y)$ from A^H to $A^H\otimes_B A^H$ is an A^H-A^H-homomorphism. Since $\sum_i t_H(a_i)t'(a_i^*y)=\sum_i\sum_{\sigma,\tau\in H}\sigma(a_i)\tau(a_i^*)\tau(d)y$ $=\sum_{\sigma,\tau\in H}\sum_i\sigma(a_i)\tau(a_i^*)\tau(d)y=\sum_{\tau\in H}\tau(d)y=y$ 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 ${}_BB_B$ a direct summand of ${}_BA_B$. 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 ${}_SR_R \cong {}_S\mathrm{Hom}(R_S, S_S)_R$ (cf. [10]). If A/B is a G-Galois extension, then $({}_BA_A \cong)\ {}_B(\sum_\sigma u_\sigma)A_A \cong {}_B\mathrm{Hom}(A_B, B_B)_A$ 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 ${}_SR_R \cong {}_S\mathrm{Hom}(R_S, S_S)_R$. Then $t \in \mathrm{Hom}({}_SR_S\ {}_SS_S)$, $\mathrm{Hom}(R_S, S_S)=tR$ and $\mathrm{Hom}(R_S, R_S)=RtR$.*

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 $\mathrm{Hom}(A_B, A_B)$ with Δ, and set $\Delta_0=\mathrm{Hom}(A_T, A_T)$, which is a subring of Δ. Let $t=\sum_\sigma c_\sigma u_\sigma$ be the image of 1 under the isomorphism ${}_TA_A \cong {}_T\mathrm{Hom}(A_T, T_T)_A$. Then, $tA=\mathrm{Hom}(A_T, T_T)$, $AtA=\Delta_0$ and $t \in \mathrm{Hom}({}_TA_T, {}_TT_T)$ (Lemma 3.1). Since $xt=tx$ for all x in T, we have $xc_\sigma=c_\sigma \cdot \sigma(x)$ for all x in T and σ in G, in particular, $yc_\sigma=c_\sigma y$ for y in B. Therefore, by assumption, each c_σ is an element of C. Since $AtA=\Delta_0$, there are elements c_i's, d_i's in A such that $\sum_i c_i t d_i = u_1$. From this fact, c_1 is an inversible element of C. Now, the mapping α: $\delta \to \delta c_1^{-1}$ is a Δ_0-A-homomorphism from Δ_0 to Δ, and the mapping β: $\sum_\sigma x_\sigma u_\sigma \to \sum_\sigma x_\sigma c_\sigma u_\sigma$ is evidently an A-A-endomorphism of Δ. For any y in A and z in T, we have $\sum_\sigma x_\sigma c_\sigma u_\sigma(yz)=\sum_\sigma x_\sigma c_\sigma \cdot \sigma(y)\sigma(z)=\sum_\sigma x_\sigma \cdot \sigma(y)c_\sigma \cdot \sigma(z)=\sum_\sigma x_\sigma \cdot \sigma(y)zc_\sigma=\sum_\sigma x_\sigma c_\sigma \cdot \sigma(y)z=(\sum_\sigma x_\sigma c_\sigma u_\sigma(y))z$, which means $\beta(\Delta)\subseteq\Delta_0$. If $x\otimes y$ is in $A\otimes_B A$, then $\beta h(x\otimes y)=\beta(x(\sum_\sigma u_\sigma)y)=\beta(\sum_\sigma x\cdot\sigma(y)u_\sigma)=\sum_\sigma x\cdot\sigma(y)c_\sigma u_\sigma=x\sum_\sigma c_\sigma u_\sigma y=xty$. For any δ_0 in Δ_0 and any z in A, we have $\delta_0 xty(z)=\delta_0(xt(yz))=\delta_0(x)\cdot t(yz)=\delta_0(x)ty(z)$. Thus, βh is a Δ_0-A-homomorphism from $A\otimes_B A$ to Δ_0, and so β is a Δ_0-A-homomorphism from Δ to Δ_0. Since $\beta\alpha(u_1)=\beta(u_1c_1^{-1})=u_1$, $\beta\alpha=1_{\Delta_0}$. Thus, we have $\Delta=\mathrm{Im}\,\alpha\oplus\mathrm{Ker}\,\beta=\Delta_0\oplus(\sum_\sigma\oplus\mathrm{Ann}_A(c_\sigma)\cdot u_\sigma)$, where $\mathrm{Ann}_A(c_\sigma)=\{x\in A;\ xc_\sigma=0\}$. Now, let $\{(a_i, a_i^*);\ i=1, \cdots, n\}$ be a G-Galois coordinate system for A/B. If τ is in G, then $\Delta_0=AtA \ni \sum_i \tau(a_i)ta_i^*=c_\tau u_\tau$, and so $\Delta_0=\sum Ac_\sigma u_\sigma$, whence it follows that $A=Ac_\sigma\oplus\mathrm{Ann}_A(c_\sigma)$. Let $Ac_\sigma=Ae_\sigma$ with a

central idempotent e_σ 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 $\Delta_0 = \sum_{\tau \in H} \oplus Au_\tau$, where $H = \{\tau \in G;\ \tau|T = 1_T\}$. Since T_T is a direct summand of A_T, End $({}_{\Delta_0}A) = T_r$ the set of all right multiplications by elements of T (see [1; Th. A. 2]). On the other hand, since $\Delta_0 = \sum_{\tau \in H} \oplus Au_\tau$, End $({}_{\Delta_0}A) = (A^H)_r$. 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 $A^H_{A^H}$ 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 $\sum_\sigma e_\sigma = 1$ and $f(x) = \sum_\sigma g\sigma(x)e_\sigma$ for all x in A.* (Cf. [4; Th. 3.1].)

Proof. There are elements a_i, a_i^* $(i = 1, \cdots, n)$ in A such that $\sum_i xa_i \otimes a_i^* = \sum_i a_i \otimes a_i^* x (\in A \otimes_B A)$ for all x in A and $\sum_i a_i \cdot \sigma(a_i^*) = \delta_{1,\sigma}$ for all σ in G (Prop. 1.3). If we set $t_i = t_H(a_i)$, then $t_i \in A^H$, $\sum_i t_i \cdot \sigma(a_i^*) = \delta_{H,\sigma}$ $(\sigma \in G)$ and $\sum_i xt_i \otimes a_i^* = \sum_i t_i \otimes a_i^* x$ $(\in A^H \otimes_B A)$ 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 $e_\sigma = \sum_i f(t_i) g\sigma(a_i^*)$, then each e_σ is a central idempotent in A' (Prop. 1.2). By Prop. 1.2 (3), $e_\sigma e_\tau = e_\sigma g(\sum_j \sigma(t_j)\tau(a_j^*))$ for any σ, τ in G. Therefore, if $\sigma^{-1}\tau \notin H$ then $e_\sigma e_\tau = 0$, and if $\sigma^{-1}\tau \in H$ then $e_\sigma = e_\tau$. Recalling that $A^H_{A^H}$ is a direct summand of A_{A^H} there is an element d of A such that $t_H(d) = 1$. Since $\sum_q \sum_i t_i \otimes \sigma(a_i^* d) = \sum_i t_i \otimes t_G(a_i^* d) = \sum_i t_i \cdot t_G(a_i^* d) \otimes 1 = \sum_\sigma (\sum_i t_i \cdot \sigma(a_i^*))\sigma(d) \otimes 1 = t_H(d) \otimes 1 = 1 \otimes 1$ in $A^H \otimes_B A$, we have $\sum_\sigma \sum_i f(t_i) \otimes g\sigma(a_i^* d) = 1 \otimes 1$ $(\in A' \otimes A')$, and therefore $\sum_\sigma \sum_i f(t_i) g\sigma(a_i^* d) = 1$ $(\in A')$. Let $G = \sigma_1 H \cup \cdots \cup \sigma_r H$ be the left coset decomposition of G. Then, $1 = \sum_\sigma \sum_i f(t_i) g\sigma(a_i^* d) = \sum_k \sum_{\tau \in H} e_{\sigma_k \tau} g\sigma_k\tau(d) = \sum_k e_{\sigma_k} \cdot g\sigma_k \cdot t_H(d) = \sum_k e_{\sigma_k}$. Since $f(x)e_\sigma = e_\sigma \cdot g\sigma(x)$ for all x in A^H (Prop. 1.2), we have $f(x) = \sum_k f(x)e_{\sigma_k} = \sum_k g\sigma_k(x)e_{\sigma_k}$ for all x in A^H. Evidently, the mapping $z \to \sum_k g\sigma_k(z)e_{\sigma_k}$ 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 $A^H_{A^H}$ 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.*

§ 5. Heredity of Galois extensions.

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

(1) *A'/B' is a G-Galois extension, and $A^H=B\otimes_{B'}A'^H=A'^H\otimes_{B'}B$ 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 $A'G$-left submodules of A, and $\{X\}$ the set of all B'-left submodules of B. Then, $\overline{X}\to\overline{X}\cap B$ and $X\to A'X=A'\otimes_{B'}X$ are muturally 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 $\overline{Y}\to\overline{Y}\cap B$ and $Y\to A'Y=YA'$ 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 $G=H\sigma_1\cup\cdots\cup H\sigma_r$ be the right coset decomposition of G. If we put $d=\sum_k\sigma_k(c)$ and $t_i=t_H(a_i)$, then $t_H(d)=1$ and $\sum_i t_i\cdot\sigma(a_i^*)=\delta_{H,\sigma}$ $(\sigma\in G)$. If x is in A^H, then $A'^H\cdot B\ni\sum_i t_i\cdot t_G(a_i^*dy)=\sum_\sigma(\sum_i t_i\cdot\sigma(a_i^*))\sigma(dx)=t_H(dx)=t_H(d)x=x$. Thus, we obtain $A^H=A'^H\cdot B$. To be easily seen, the mapping $\sum_j x_j\otimes y_j\to\sum_j x_jy_j$ from $A'^H\otimes_{B'}B$ to $A'^H\cdot B=A^H$ is well-defined and $\sum_i t_i\otimes t_G(a_i^*d\sum_j x_jy_j)=\sum_j x_j\otimes y_j$. Hence, $A'^H\otimes_{B'}B\cong A'^H\cdot B=A^H$ by the mapping $\sum_j x_j\otimes y_j\to\sum_j x_jy_j$. Symmetrically, it follows $A^H=B\otimes_{B'}A'^H$. (2) Let X be an $A'G$-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 $t_G(a_i^*x)$ is in $\overline{X}\cap B$, and hence $x=\sum_i a_i\cdot t_G(a_i^*x)\in A'(\overline{X}\cap B)$. Hence, $\overline{X}=A'(\overline{X}\cap B)$, and the mapping $\sum_j x_j\otimes y_j\to\sum_j x_jy_j$ from $A'\otimes_{B'}(\overline{X}\cap B)$ to $A'(\overline{X}\cap B)=\overline{X}$ is onto. Moreovr, to be easily seen, $\sum_i a_i\otimes t_G(a_i^*\sum_j x_jy_j)=\sum_j x_j\otimes y_j$. 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 $A'G$-left submodule of A, and $A'X\cap B\supseteq X$. If $\sum_j x_jy_j$ $(x_j\in A',\ y_j\in X)$ is in $A'X\cap B$, then $\sum_j x_jy_j=t_G(c)(\sum_j x_jy_j)=\sum_\sigma\sigma(c)\sum_j\sigma(x_j)y_j=\sum_j t_G(cx_j)y_j\in X$. 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 $B'=\mathrm{V}_B(B)$. Assume that there are elements a_i, a_i^* $(i=1,\cdots,n)$ in $\mathrm{V}_A(B)$ such that $\sum_i a_i\cdot\sigma(a_i^*)=\delta_{1,\sigma}$.*

(1) *$V_A(B)/B'$ is G-Galois, $A^H=B\otimes_{B'}\mathrm{V}_A(B)^H$ for any subgroup H of G, and the center of A^H coincides with the center of $\mathrm{V}_A(B)^H$. In particular, $A=B\otimes_{B'}\mathrm{V}_A(B)$, and $B'\subseteq C$.*

(2) *Let $\{\overline{Y}\}$ be the set of all G-invariant intermediate rings of $A/\mathrm{V}_A(B)$,*

and $\{Y\}$ *the set of all intermediate rings of* B/B'. *Then* $\overline{Y}\to\overline{Y}\cap B$ *and* $Y\to V_A(B)Y=V_A(B)\otimes_{B'}Y$ *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 $A=B\otimes_{B'}V_A(B)$, 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 $A\otimes_R A'\neq 0$. 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 $\{(a_i, a_i^*);\ i=1,\cdots,n\}$ 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 $\sum_{i,j}(a_i\otimes d_j)\cdot(\sigma\times\tau)(a_i^*\otimes d_j^*)=(\sum_i a_i\cdot\sigma(a_i^*))\otimes(\sum_j d_j\cdot\tau(d_j^*))$, $(A\otimes_R A')/(A\otimes A')^{G\times G'}$ 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 $\sum_{\sigma\in H}\sigma(c)=1$ and $\sum_{\tau\in H'}\tau(c')=1$. If $\sum_k x_k\otimes y_k$ is in $(A\otimes A')^{H\times H'}$, then $\sum_k x_k\otimes y_k=(\sum_{\sigma\in H}\sigma(c))\otimes(\sum_{\tau\in H'}\tau(c'))\cdot\sum_k x_k\otimes y_k=\sum_{\sigma\in H}\sum_{\tau\in H'}\sigma(c)\otimes\tau(c')\cdot(\sigma\times\tau)(\sum_k x_k\otimes y_k)=\sum_k(\sum_{\sigma\in H}\sigma(cx_k)\otimes\sum_{\tau\in H'}\tau(c'y_k))\in A^H\otimes A^{H'}$. 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, $A^{H\cap K}\supseteq A^H\cdot A^K$. 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 $A^H\cdot A^K\ni\sum_i t_H(a_i)t_K(a_i^*cx)=\sum_{\rho\in H}\sum_{\sigma\in K}\sum_i\rho(a_i)\sigma(a_i^*)\sigma(cx)=t_{H\cap K}(c)x=x$. Hence $A^{H\cap K}=A^K\cdot A^H$. Symmetrically 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_B a direct summand of A_B. 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 $\mathrm{N}(K_0)\supseteq H$ (where $\mathrm{N}(K_0)$ means the normalizer of K_0 in G), $A^{K_0H_0}=A^{K_0H}\otimes_B A^{KH_0}=A^{KH_0}\otimes_B A^{K_0H}$ and A^{K_0}/A^{K_0H} is an H-Galois extension.*

Proof. Let $\{(a_i, a_i^*); i=,\cdots,n\}$ be a G-Galois coordinate system for A/B. Since B_B is a direct summand of A_B, there is an element c in A such that $t_G(c)=1$. Put $t_i=t_K(a_i)$, $t_i^*=t_K(a_i^*)$, and $d=t_K(c)$. Then, $t_H(d)=1$ and $\sum_i t_i\cdot\tau(t_i^*)=\delta_{1,\tau}$ for τ in H. $\mathrm{N}(K_0)\supseteq H$ implies that $\tau(A^{K_0})=A^{K_0}$ for all τ in H. Hence, by Th. 5.1, A^{K_0}/A^{K_0H} is an H-Galois extension. By Th. 5.1, $A^{H_0}=A^H\otimes_B A^{KH_0}=A^{KH_0}\otimes_B A^H$. Since $K_0H_0=K_0H\cap KH_0$, $A^{K_0H_0}=A^{K_0H}\cdot A^{KH_0}=A^{KH_0}\cdot A^{K_0H}$ (Prop. 5.3). Since $A^H\supseteq A^{K_0H}$ and A^{K_0H} is an A^{K_0H}-right direct summand (of A, and so) of A^H, $A^{K_0H_0}=A^{K_0H}\otimes_B A^{KH_0}$. Similarly, we have $A^{K_0H_0}=A^{KH_0}\otimes_B A^{K_0H}$.

Corollary. *Let A/B be a G-Galois extension, B_B a direct summand of A_B, and $G=N_1\times\cdots\times N_r$. If $H_i=N_1\times\cdots\times\check{N}_i\times\cdots\times N_r$ $(i=1,\cdots,r)$, then A^{H_i}/B is N_i-Galois, $A=A^{H_1}\otimes_B\cdots\otimes_B A^{H_r}$, and $A^{K_1\cdots K_r}=A^{H_1K_1}\otimes_B\cdots\otimes_B A^{H_rK_r}$ for each subgroup K_i of N_i.*

Proposition 5.5. *Let A/B be outer G-Galois. B_B a direct summand of A_B, and A directly indecomposale. 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 ${}_TT\otimes_B A^A\cong{}_TA\otimes_{T'}A_A$. 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_B a direct summand of A_B, 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 $\bar{x}$. If we define $\sigma(\bar{x})=\overline{\sigma(x)}$, then $\sum_i\bar{a}_i\cdot\sigma(\overline{a_i^*})=\delta_{1,\sigma}$ for σ in G, and therefore

$(A/\mathfrak{A})/(A/\mathfrak{A})^G$ 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 $(A/\mathfrak{A})^H$, then $\bar{x}=\bar{x}\sum_{\tau\in H}\tau(\bar{c})=\sum_{\tau\in H}\tau(\bar{x}\bar{c})=\overline{t_H(xc)}\in(A^H+\mathfrak{A})/\mathfrak{A}$. 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 $t_N(a_i^*c)=t_i^*$, then t_i and t_i^* are A^N, and $\sum_i t_i\cdot\sigma(t_i^*)=\delta_{N,\sigma}$ for all σ 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 σ 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 $\sum_i a_iE\cdot\sigma(a_i^*E)=\delta_{1,\sigma}$ for all σ 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 $A_0=\mathrm{V}_A(\{e_{ij}\})$, then A_0/A_0^G is a G-Galois extension, and $B=\sum_{i,j}\oplus A_0^Ge_{ij}$.*

Proof. Obviously, G induces an automorphism group of A_0 and $B=\sum_{i,j}A_0^Ge_{ij}$. Let $\{(A_i.A_i^*);\ i=1,\cdots,n\}$ be a G-Galois coordinate system for A/B, Let $A_i=\sum_{j,k}a_{ijk}e_{jk}$, $A_i^*=\sum_{j,k}d_{ijk}e_{jk}$ $(a_{ijk}, d_{ijk}\in A_0)$. Then, $\sigma(A_i^*)=\sum_{j,k}\sigma(d_{ijk})e_{jk}$ and therefore $\sum_{i,k}a_{i1k}\cdot\sigma(d_{ik1})=\delta_{1,\sigma}$ for σ 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 ${}_RM$ and ${}_RN$ 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* $\mathrm{End}({}_RM)$-

admissible and $X=\sum_i(X\cap M_i)$ *for every submodule* X *of* ${}_RM$.

(2(*If* $X=\sum_i(X\cap M_i)$ *for every submodule* X *of* ${}_RM$, *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 ${}_RM$ then M_1 and M_2 are unrelated. Let M_1'/N_1 and M_2'/N_2 be non-zero subquotients of M_1 and M_2, respectively. If there exists an R-isomorphism α; $M_1'/N_1\cong M_2'/N_2$, we can define an R-homomorphism φ; $M_1'\oplus M_2'\to M_2'/N_2$ by the following rule: $(m_1'+m_2')\varphi=(m_1'+N_1)\alpha+(m_2'+N_2)$. Then, our assumption yields $\mathrm{Ker}\,\varphi=(M_1'\cap\mathrm{Ker}\,\varphi)+(M_2'\cap\mathrm{Ker}\,\varphi)$, 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_σ, Au_τ $(\sigma\neq\tau)$ are unrelated.

To be easily seen, Au_σ and Au_τ $(\sigma,\tau\in G)$ are A-A-isomorphic if and only if $\sigma\tau^{-1}$ is an inner automorphism of A, and every A-A-submodule of Au_σ 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 σ in G we set $J_\sigma=\{a\in A;\ \sigma(x)a=ax$ for all x in $A\}$. Then each J_σ 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 $V_A(B)=\sum_\sigma\oplus J_\sigma$. Therefore, if A/B is G-Galois, then $V_A(B)=C$ if and only if $J_\sigma=0$ for all σ in G such that $\sigma\neq 1$.

Proposition 6.2. $J_\sigma=0$ *if and only if* $\mathrm{Hom}\,({}_AAu_{\sigma A},\ {}_AA_A)=0$.

Proof. Assume $J_\sigma=0$. If f is in $\mathrm{Hom}\,({}_AAu_{\sigma A},\ {}_AA_A)$, then $\sigma(x)\cdot f(u_\sigma)=f(\sigma(x)u_\sigma)=f(u_\sigma x)=f(u_\sigma)x$ for x in A. Hence $f(u_\sigma)=0$, and so $f=0$. Conversely, assume that $\mathrm{Hom}\,({}_AAu_{\sigma A},\ {}_AA_A)=0$. If a is in J_σ, then we can easily see that the mapping $xu_\sigma\to xa$ $(x\in A)$ is an A-A-homomorphism from Au_σ 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) $\mathrm{Hom}\,({}_AAu_{\sigma A},\ {}_AA_A)=0$ *for every* $\sigma\neq 1$ *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 $u_1\in A(\sum_\sigma u_\sigma)A$ (Prop. 6.1.), there are elements a_i, a_i^* $(i=1,\cdots,n)$ in A such that $u_1=$

$\sum_i a_i(\sum_\sigma u_\sigma)a_i^* = \sum_\sigma(\sum_i a_i \cdot \sigma(a_i^*))u_\sigma$. Hence $\sum_i a_i \cdot \sigma(a_i^*) = \delta_{1,\sigma}$ for σ 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' $(i=1, \cdots, n)$ in A such that $\sum_i a_i x \cdot \sigma(a_i') = \delta_{1,\sigma} x$ for each x in A $(\sigma \in G)$, then G is completely outer.*

Proof. Let X be any A-A-submodule of Δ. If $\sum_\sigma x_\sigma u_\sigma$ is in X, then $X \ni \sum_i a_i(\sum_\sigma x_\sigma u_\sigma)\tau^{-1}(a_i') = x_\tau u_\tau$ for each τ 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 $\sigma_0 \in G$ is not contained in H, and $ax = a \cdot \sigma_0(x)$ for all x in A^H, then $a=0$.*

Proof. There are elements $t_1, \cdots, t_n \in A^H$ and $a_1^*, \cdots, a_n^* \in A$ such that $\sum_i t_i \cdot \sigma(a_i^*) = \delta_{H,\sigma}$ for any σ in G (Prop. 2.2). Hence, $a = a\sum_i t_i a_i^* = \sum_i a \cdot \sigma_0(t_i)a_i^*$ $= \sigma_0(\sigma_0^{-1}(a)\sum_i t_i \cdot \sigma_0^{-1}(a_i^*)) = 0$.

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

Proof. As is well known, there are elements $a_i \in R$, $f_i \in \mathrm{Hom}\,(R_S, S_S)$ $(i=1, \cdots, n)$ such that $\sum_i a_i \cdot f_i(x) = x$ for every x in R (cf. [3]). If g is in End (R), then $\sum_i g(a_i)f_i$ is in End (R_S), and so the mapping $g \to \sum_i g(a_i)f_i$ is an End (R_S)-left homomorphism from End (R) to End (R_S). To be easily seen, if g is in End (R_S) then $\sum_i g(a_i)f_i = g$. This implies that End (R_S) is an End (R_S)-left direct summand of 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 σ, τ 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 $G|A^H$ is *-strongly distinct for any subgroup H of G (Prop. 6.7).

Theorem 6.9. *Let G be completely outer, B_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, and $G|T$ is-strongly distinct.*

Proof. Since A/A^H is H-Galois, it remains to prove (ii)$\Rightarrow$(i). If we put $\Delta_0=\mathrm{End}\,(A_T)$, then Δ_0 is a subring of Δ. Since Δ_0 is an A-A-submodule of Δ, $\Delta_0=\sum_\sigma\oplus\mathfrak{A}_\sigma u_\sigma$ with some ideals $\mathfrak{A}_\sigma$ of A. By Lemma. 6.8, ${}_A\Delta_0$ is a direct summand of ${}_A\Delta$, so that each ${}_A\mathfrak{A}_\sigma u_\sigma$ is a direct summand of ${}_A\Delta$. Therefore each ${}_A\mathfrak{A}_\sigma u_\sigma$ is a direct summand of ${}_AA_\sigma u_\sigma$. Hence $\mathfrak{A}_\sigma$ is a direct summand of ${}_AA$. Let $\mathfrak{A}_\sigma=Ae_\sigma$ with an idempotent e_σ in A. Then, since $e_\sigma u_\sigma$ is in Δ_0, $e_\sigma\cdot\sigma(xy)=e_\sigma\cdot\sigma(x)y$ for each x in A and y in T, in particular, $e_\sigma\cdot\sigma(y)=e_\sigma y$ for each y in T. Therefore, if we set $H=\{\sigma\in G;\ \sigma|T=1_T\}$, then $e_\sigma=0$ for σ not contained in H. Evidently $\mathfrak{A}_\sigma=A$ for each σ in H. We obtain therefore $\Delta_0=\sum_{\tau\in H}\oplus Au_\tau$, and hence $\mathrm{End}\,({}_{\Delta_0}A)=(A^H)_r$. On the other hand, since T_T is a direct summand of A_T, $\mathrm{End}\,({}_{\Delta_0}A)=T_r$ (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:

Theorem 6.10. *Let A be a semi-prime ring. If G is completely outer, B_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.*

Proposition 6.11. *The following are equivalent:*

(i) *G is completely outer.*

(ii) *For any x, y in A and any σ in G such that $\sigma\neq1$, there are elements a_i, a_i' $(i=1,\cdots,n)$ in A such that $\sum_i a_ixa_i'=x$ and $\sum_i a_iy\cdot\sigma(a_i')=0$.*

Proof. (i)$\Rightarrow$(ii) Let x, y be in A, and σ any element of G such that $\sigma\neq1$. We set $X=A(xu_1+yu_\sigma)A$, which is an A-A-submodule of Au_1+Au_σ. 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 $\sum_i a_i(xu_1+yu_\sigma)a_i'=xu_1$. Then, $\sum_i a_ixa_i'=x$ and $\sum_i a_iy\cdot\sigma(a_i')=0$. (ii)$\Rightarrow$(i) Let σ, τ be distinct elements in G, and X any A-A-submodule of $Au_\sigma+Au_\tau$. Let $xu_\sigma+yu_\tau$ 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 $\sum_i a_i\cdot\sigma^{-1}(x)a_i'=\sigma^{-1}(x)$ and $\sum_i a_i\cdot\sigma^{-1}(y)\sigma^{-1}\tau(a_i')=0$. Then, $\sum_i\sigma(a_i)x\cdot\sigma(a_i')=x$ and $\sum_i\sigma_i(a_i)y\cdot\tau(a_i')=0$, and so $X\ni\sum_i\sigma(a_i)(xu_\sigma+yu_\tau)a_i'=xu_\sigma$. Thus, by Prop. 6.1, Au_σ and Au_τ 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 $xu_1 \in A(\sum_{\tau\in N} xu_\tau + \sum_{\tau\in G\setminus N} yu_\sigma)A$ (Prop. 6.1), there are elements x_i, y_i $(i=1,\cdots,n)$ in A such that $\sum_i x_i(\sum_{\tau\in N} xu_\tau + \sum_{\sigma\in G/N} yu_\sigma)y_i = xu_1$. Then $\sum_i x_i x\cdot\tau(y_i) = \delta_{1,\tau}x$ $(\tau\in N)$ and $\sum_i x_i y\cdot\sigma(y_i) = 0$ $\sigma\in G\setminus N)$. By assumption, there is an element c in A such that $t_N(c)=1$. We set $t_N(x_i)=x_i'$ and $t_N(y_ic)=y_i'$, then x_i', y_i' $(i=1,\cdots,n)$ are in A^N. To be easily seen, $\sum_i x_i' x y_i' = x$ and $\sum_i x_i' y\cdot\rho(y_i')=0$ 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 $R\mathfrak{l}\cap S=\mathfrak{l}$ for any left ideal $\mathfrak{l}$ 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 ${}_SR$ 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 ${}_SR$ 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 $R/\mathfrak{N}(R)$ satisfies the minimal condition for left ideals, where $\mathfrak{N}(R)$ 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 $\mathrm{End}(M_R)$ 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 $\{\mathfrak{l}_i;\ i=1,\cdots,n\}$ be a d-independent set of maximal left ideals of S (cf. [11]). Then, $\{R\mathfrak{l}_i;\ i=1,\cdots,n\}$ is a d-independent set of proper left ideals of R (Lemma 7.1). Since each $R\mathfrak{l}_i$ is contained in a maximal left ideals of R, $n\leqslant$ max-dim ${}_RR=$d-dim ${}_RR$ (cf. [11]). Thus d-dim ${}_SS\leqslant$ d-dim ${}_RR<\aleph_0$, and hence S is semi-primary ([11; Prop. 5.14]. (2) Since S

is semi-primary, $\mathrm{End}(R_S)$ is semi-primary. By Lemma 6.8, ${}_{R_l}R_l$ (the set of all left multiplications by elements of R) is a direct summand of ${}_{R_l}\mathrm{End}(R_S)$. Hence, by (1), $R(\cong R_l)$ 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 ${}_SR_R \cong {}_S\mathrm{Hom}(R_S, S_S)_R$ (Kasch [10]).

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

(1) *$\mathrm{End}(R_S)/R_l$ 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 $\mathrm{End}(R_S)$ is $\mathrm{End}(R_S)$-right injective. Let $R_S \cong S_S^m$. Then, $\mathrm{End}(R_S) \cong (S)_m$, and hence we readily see that S_S is injective (cf. [11]).

Proposition 7.5. *Let R be a ring, and S a subiing of R. If S_S is a direct summand of R_S,* then $\mathfrak{N}(R) \cap S \subseteq \mathfrak{N}(S)$.

Proof. If $\mathfrak{N}(R) \cap S \not\subseteq \mathfrak{N}(S)$, then $(\mathfrak{N}(R) \cap S) + \mathfrak{l} = S$ for some maximal left ideal $\mathfrak{l}$ of S. Since $R(\mathfrak{N}(R) \cap S) + R\mathfrak{l} = R$ and $R(\mathfrak{N}(R) \cap S) \subseteq \mathfrak{N}(R)$, we have $R\mathfrak{l} = R$. If follows then a contradiction $\mathfrak{l} = R\mathfrak{l} \cap S = S$ (Lemma 7.1).

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

Proof. Let X be a maximal Δ-A-submodule of A. Take a maximal ideal $\mathfrak{P}_1$ such that $\mathfrak{P}_1 \supseteq X$. Then, $\cap_\sigma \sigma(\mathfrak{P}_1) \supseteq X$, and so $\cap_\sigma \sigma(\mathfrak{P}_1) = X$. Now, let $\mathfrak{P}$ be a maximal ideal of A, and Y a maximal Δ-A-submodule of A such that $Y \supseteq \cap_\sigma \sigma(\mathfrak{P})$. Then $Y = \cap \sigma(\mathfrak{P}_2)$ for some maximal ideal $\mathfrak{P}_2$ of A. If $\cap_\sigma \sigma(\mathfrak{P}_2) \supsetneqq \cap_\sigma \sigma(\mathfrak{P})$, then $\mathfrak{P} \not\supseteq \cap_\sigma \sigma(\mathfrak{P}_2)$, and so $\mathfrak{P} + \cap_\sigma \sigma(\mathfrak{P}_2) = A$, whence it follows a contradiction $\cap_\sigma \sigma(\mathfrak{P}) + \cap_\sigma \sigma(\mathfrak{P}_2) = A$.

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 Δ-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 $A \cdot \mathfrak{N}(B)$ is an ideal of A, then $\mathfrak{N}(A) = A \cdot \mathfrak{N}(B)$.*

Proof. By Prop. 7.7 and Prop. 7.5, $\mathfrak{N}(A) = A(\mathfrak{N}(A) \cap B) \subseteq A \cdot \mathfrak{N}(B)$.

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 Δ is an A-A-submodule (resp. Δ-A-submodule) of Δ, then $\Delta=\sum_\sigma u_\sigma\mathfrak{A}_\sigma$ for some ideals $\mathfrak{A}_\sigma$ of A (resp. $\Delta=\Delta\mathfrak{A}=\sum_\sigma u_\sigma\mathfrak{A}$ for some ideal $\mathfrak{A}$ of A), and conversely. In particular, if Δ is an ideal of Δ, then $\Delta=\Delta\mathfrak{A}=\mathfrak{A}\Delta$ for some G-invariant ideal $\mathfrak{A}$ of A, and conversely (cf. §6 and [13]). Now, let $\{\Delta\}$ be the set of all ideals of Δ, $\{\mathfrak{a}\}$ 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 $\Delta\leftarrow\mathfrak{a}$ between $\{\Delta\}$ and $\{\mathfrak{a}\}$ such that $\Delta(A)=A\mathfrak{a}$ (cf. [1; Prop. A. 5]). Consequently, there exists an order isomorphism $\mathfrak{A}\leftarrow\Delta\leftarrow\mathfrak{a}$ between $\{\mathfrak{A}\}$ and $\{\mathfrak{a}\}$ such that $(\Delta\mathfrak{A})\,(A)=A\mathfrak{a}$, namely, $\mathfrak{A}=A\mathfrak{a}$. Hence, $\mathfrak{A}\rightarrow B\cap\mathfrak{A}$ and $\mathfrak{a}\rightarrow A\mathfrak{a}=\mathfrak{a}A$ are mutually converse order isomorphisms between $\{\mathfrak{A}\}$ and $\{\mathfrak{a}\}$ (cf. Th. 5.1 (2)). Accordingly, if A is semi-prime, (prime, two-sided simple) then so is B. Since $A\cdot\mathfrak{R}(B)=\mathfrak{R}(B)A$ is an ideal of A, Prop. 7.8 implies $\mathfrak{R}(A)=A\cdot\mathfrak{R}(B)=\mathfrak{R}(B)A$. Next, we shall consider $\mathfrak{R}(\Delta)$. There exists $\mathfrak{A}'\in\{\mathfrak{A}\}$ such that $\mathfrak{R}(\Delta)=\mathfrak{A}'\Delta=\Delta\mathfrak{A}'$. Since $\mathfrak{A}'u_1=\mathfrak{R}(\Delta)\cap Au_1\subseteq\mathfrak{R}(Au_1)=\mathfrak{R}(A)u_1$ by Prop. 7.5, we obtain $\mathfrak{R}(\Delta)=\Delta\mathfrak{A}'\subseteq\Delta\cdot\mathfrak{R}(A)=\mathfrak{R}(A)\Delta$. On the other hand, noting that Δ_A is finitely generated and $\Delta\cdot\mathfrak{R}(A)$ is an ideal of Δ, we see that $\Delta\cdot\mathfrak{R}(A)\subseteq\mathfrak{R}(\Delta)$ (cf. the proof of Prop. 7.8). Hence, we have $\mathfrak{R}(\Delta)=\Delta\cdot\mathfrak{R}(A)=\mathfrak{R}(A)\Delta$. Since $\mathfrak{R}({}_AA_A)=\mathfrak{R}({}_\Delta A_A)=(\mathfrak{R}({}_\Delta A_A)\Delta)\,(A)=\mathfrak{R}({}_\Delta\Delta_\Delta)\,(A)=A\cdot\mathfrak{R}({}_BB_B)$ by Prop. 7.6, we have $\mathfrak{R}({}_AA_A)=A\cdot\mathfrak{R}({}_BB_B)=\mathfrak{R}({}_BB_B)A$ and $\mathfrak{R}({}_AA_A)\cap B=\mathfrak{R}({}_BB_B)$. 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 $\mathfrak{R}(A)=A\cdot\mathfrak{R}(B)=\mathfrak{R}(B)A$, $\mathfrak{R}(A)\cap B=\mathfrak{R}(B)$, $\mathfrak{R}({}_AA_A)=R\cdot\mathfrak{R}({}_BB_B)=\mathfrak{R}({}_BB_B)A$, $\mathfrak{R}({}_AA_A)\cap B=\mathfrak{R}({}_BB_B)$, $\mathfrak{R}(\Delta)=\Delta\cdot\mathfrak{R}(A)=\mathfrak{R}(A)\Delta$, and $\mathfrak{R}({}_\Delta\Delta_\Delta)=\Delta\cdot\mathfrak{R}({}_AA_A)=\mathfrak{R}({}_AA_A)\Delta$.*

Proposition 7.11. *Let B be directly indecomposable, and let $A=\mathfrak{A}_1\oplus\cdots\oplus\mathfrak{A}_s$ be a direct sum of minimal ideals. If $\mathfrak{A}$ is a minimal ideal of A, then $\{\sigma(\mathfrak{A});\ \sigma\in G\}=\{\mathfrak{A}_1,\cdots,\mathfrak{A}_s\}$, 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.*

Proof. Note that $\{\mathfrak{A}_1,\cdots,\mathfrak{A}_s\}$ coincides with the set of all minimal ideals of A. For any $\mathfrak{A}_i$, we set $\sum_\sigma\sigma(\mathfrak{A}_i)=\mathfrak{B}$. Then, $\mathfrak{B}=Ae$ with some non-zero

central idempotent e of A. Since $\sigma(\mathfrak{B})=\mathfrak{B}$ for all σ in G, $\sigma(e)=e$ for all σ in G, so that $e\in B$, which means $e=1$. Hence $\mathfrak{B}=A$, which implies that $\{\sigma(\mathfrak{A}_i);\ \sigma\in G\}=\{\mathfrak{A}_1,\cdots,\mathfrak{A}_s\}$. If we set $H=\{\sigma\in G;\ \sigma(\mathfrak{A}_i)=\mathfrak{A}_i\}$, then $\#\{\sigma(\mathfrak{A}_i);\ \sigma\in G\}=(G:\ H)$, which divides $(G:\ 1)$. Let $\mathfrak{P}$ and $\mathfrak{P}'$ be maximal ideals of A. Then $A=\mathfrak{A}\oplus\mathfrak{P}=\mathfrak{A}'\oplus\mathfrak{P}'$ with some minimal ideals $\mathfrak{A}$, $\mathfrak{A}'$ of A. There is an element σ in G such that $\sigma(\mathfrak{A})=\mathfrak{A}'$. Then $A=\mathfrak{A}'\oplus\sigma(\mathfrak{P})=\mathfrak{A}'\oplus\mathfrak{P}'$, so that $\sigma(\mathfrak{P})=\mathfrak{P}'$.

Corollary. 1. *Let G be completely outer, and B_B 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 Δ-A-submodule of $\mathfrak{A}$. As we remarked above, A is Δ-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 $\mathfrak{L}$ be a maximal left ideal of A. Then $\cap_\sigma\sigma(\mathfrak{L})$ is a Δ-submodule of A. Since ${}_\Delta A$ is simple (Prop. 7.7), $\cap_\sigma\sigma(\mathfrak{L})=0$. Hence, as is easily seen, ${}_A A$ 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

[1] M. AUSLANDER and O. GOLDMAN, Maximal orders, Trans. Amer. Math. Soc., 97 (1960), 1–24.

[2] M. AUSLANDER and O. GOLDMAN, The Brauer group of a commutative ring, Trans. Amer. Math. Soc., 97 (1960), 367–409.

[3] H. CARTAN and S. EILENBERG, Homological algebra, princeton, 1956.

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

[5] F. R. DEMEYER, Galois theory in algebras over commutative rings, to appear in Ill. J. Math.

[6] F. R. DEMEYER, Some notes on the general Galois theory of rings, Osaka Math.

J., 2 (1965), 117–127.

[7] N. JACOBSON, Structure of rings, Amer. Math. Soc. Colloquium Publ., 37, 1964.

[8] T. KANZAKI, On commutor rings and Galois theory of separable algebras, Osaka Math. J., 1 (1964), 103–115.

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

[10] F. KASCH, Projektive Frobenius Erweiterungen, Sitzungsber. Heidelberger Acad., 1960/1961, 89–109.

[11] Y. MIYASHITA, Quasi-projective modules, perfect modules, and a theorem for modular lattices, J. Fac. Sci. Hokkaido Univ., Ser. I, 19 (1966), 86–110.

[12] T. NAGAHARA, A note on Galois theory of commutative rings, to appear in Proc. Amer. Soc.

]13] T. NAKAYAMA, Galois theory for general rings with minimum condition, J. Math. Soc. Japan, 1 (1949), 203–216.

[14] T. NAKAYAMA and G. AZUMAYA, Algebra II (Theory of rings), Tokyo, 1954 (in Japanese).

Department of Mathematics,
Hokkaido University

(Received June 10, 1966)