Math. J. Okayama Univ. 32 (1990), 25-42

ON G-EXTENSIONS OF A SEMI-CONNECTED RING

Dedicated to Professor Hiroyuki Tachikawa on his 60th birthday

KAZUO KISHIMOTO and TAKASI NAGAHARA

0. Introduction. Throughout this note, A will mean a ring with an identity 1 which is not necessarily commutative. By C_A and $\mathfrak{B}(C_A)$, we denote the center of A and the set of all idempotents of C_A respectively. Then A is said to be *connected* (resp. *disconnected*) if the cardinality $|\mathfrak{B}(C_A)|=2$ (resp. $|\mathfrak{B}(C_A)|>2$). Moreover, A will be called to be *semi-connected* if $|\mathfrak{B}(C_A)|<\infty$. Let B/A be a ring extension with an identity 1 which is the common identity of B and A. B/A will be called to be *a G-extension* if there exists a finite group G of automorphisms of B such that A is the fixring of G in B. A G-extension B/A will be called to be a *G-Galois extension* if there exists a subset $\{u_i, v_i;\ i=1, \dots, r\}$ in B such that $\sum_{i=1}^{r} u_i\sigma(v_i)=\delta_{1,\sigma}$ (Kronecker's delta) for any $\sigma\in G$. This subset will be called to be a *G-Galois coordinate system* for B/A.

In [8], O. E. Villamayor and D. Zelinsky presented a Galois theory for separable G-extensions of commutative semi-connected rings.

In this note, we shall study about a G-extension B of a semi-connected ring A and $\mathfrak{B}(C_B)$. In § 1 and § 2, we shall prove that any G-extension of a semi-connected ring is also semi-connected (Theorem 5 and Theorem 8), and any G-extension of a connected ring A is A-isomorphic to a direct sum of some finite copies of a connected H-extension of A (Theorems 11 and 11′). In § 3, we shall present a Galois theory for G-extensions of semi-connected rings which is a partial generalization of [8, Theorem] to non-commutative rings (Theorem 13).

In what follows, for a G-extension B/A and any subset S (resp. H) of B (resp. G), we shall use the following conventions:

$|S|$ = the cardinality of S.

$S(H)$ (= S^H as an abbreviation) $=\{a\in S;\ \sigma(a)=a$ for all $\sigma\in H\}$.

$H(S)$ (= H_S as an abbreviation) $=\{\sigma\in H;\ \sigma(a)=a$ for all $a\in S\}$.

$HS=\{\sigma(a);\ \sigma\in H,\ a\in S\}$.

$H|S$ = the restriction of H to S.

It is obvious that for any $a\in B$, $G\{a\}=\{\sigma(a);\ \sigma\in G\}$ and $|G\{a\}|=(G: G_a)$ (the index of G_a in G).

Moreover, for e and f in $\mathfrak{B}(C_B)$, if $e \neq f$ and $ef = f$ then we write $e > f$; and further, if $e \neq 0$ and $\{f \in \mathfrak{B}(C_B);\ e > f\} = \{0\}$ then e will be called to be a *primitive idempotent* in C_B (or in $\mathfrak{B}(C_B)$).

1. On G-extensions of commutative rings. In this section, let A be a commutative ring, and B a commutative ring which is a G-extension of A. If e_i $(i = 1, 2)$ are primitive idempotents in $\mathfrak{B}(B)$ and $e_1e_2 \neq 0$ then $e_1e_2 \in \mathfrak{B}(B)$ and $e_i \geqq e_1e_2 > 0$ $(i = 1, 2)$, which implies $e_1 = e_1e_2 = e_2$. If e is a primitive idempotent in $\mathfrak{B}(B)$ and σ is an arbitrary element of G then $\sigma(e)$ is also a primitive idempotent in $\mathfrak{B}(B)$ and whence, there holds either $\sigma(e) = e$ or $e\sigma(e) = 0$.

By $O(\mathfrak{B}(B);G)$, we denote the set of non-zero elements e of $\mathfrak{B}(B)$ such that there holds either $\sigma(e) = e$ or $e\sigma(e) = 0$ for each $\sigma \in G$. By the preceeding remarks, any primitive idempotent in $\mathfrak{B}(B)$ belongs to $O(\mathfrak{B}(B);G)$. Since $O(\mathfrak{B}(B);G) \ni 1$, this is non-empty. Moreover, we denote $\mathrm{Max}_{e\in O(\mathfrak{B}(B);G)}|G\{e\}|$ by $m_{O(\mathfrak{B}(B);G)}$.

Now, let e be an element of $O(\mathfrak{B}(B);G)$, and

$$G\{e\} = \{\sigma_1(e), \sigma_2(e), \dots, \sigma_m(e)\} \quad \text{where } m = |G\{e\}|.$$

Then $G = \sigma_1G_e \cup \cdots \cup \sigma_mG_e$ (disjoint) where $G_e = \{\sigma \in G;\ \sigma(e) = e\}$. Moreover, since $\sigma_i(e)\sigma_j(e) = \delta_{ij}\sigma_i(e)$ for each $i \neq j$, $e' = \sum_{i=1}^m \sigma_i(e)$ is an idempotent of B, that is $e' \in \mathfrak{B}(B)$. Noting $\sigma(e') = e'$ for all $\sigma \in G$, we see that $e' \in \mathfrak{B}(B^G)$ and $e' \neq 0$. Hence, if B^G is connected then $e' = 1$, the identity of $B^G = A$.

First, we shall prove the following lemma which plays an important rôle in our considerations.

Lemma 1. *Let A be a connected ring and B/A a G-extension. Then, for $e \in \mathfrak{B}(B)$, the following conditions are equivalent.*

(a) *$e \in O(\mathfrak{B}(B);G)$ and $|G\{e\}| = m_{O(\mathfrak{B}(B);G)}$.*

(b) *e is a primitive idempotent in $\mathfrak{B}(B)$.*

Proof. (a) $\Rightarrow$ (b): We assume (a) and that e is not primitive in $\mathfrak{B}(B)$. Then, there is an element f in $\mathfrak{B}(B)$ such that $e > f \neq 0$, that is, $ef = f \neq e, 0$. Since $|G\{f\}| < \infty$, there is a maximal subset $\{a_1, \dots, a_s\}$ in $G\{f\}$ such that $a_1a_2\cdots a_s \neq 0$. We set here $g = a_1a_2\cdots a_s$. Since $\sigma(g) \neq 0$ for all $\sigma \in G$, we may set $a_1 = f$. Now, let $g \neq \sigma(g)$ for some $\sigma \in G$. Then

$$\{a_1, \dots, a_s\} \not\supset \{\sigma(a_1), \dots, \sigma(a_s)\},$$

Since $G\{f\} \supset \{\sigma(a_1), \dots, \sigma(a_s)\}$, by the maximality of $\{a_1, \dots, a_s\}$ we have

$$a_1a_2\cdots a_s\sigma(a_i) = 0 \quad \text{if} \quad \sigma(a_i) \notin \{a_1, a_2, \dots, a_s\}.$$

This implies that $g\sigma(g) = 0$. Hence, it follows that $g \in O(\mathfrak{B}(B); G)$. We set

$$f_0 = e-f,\ G\{e\} = \{\sigma_1(e), \sigma_2(e), \dots, \sigma_m(e)\} \quad \text{and} \quad h = \textstyle\sum_{i=1}^{m} \sigma_i(g),$$

where $\sigma_1 = 1$ and $m = |G\{e\}| = m_{O(\mathfrak{B}(B);\,G)}$. Noting $f_0 e = f_0$ and $e\sigma_i(e) = 0$ for all $i \geqq 2$, we see that

$$f_0\sigma_i(e) = (f_0 e)\sigma_i(e) = 0\ (i \geqq 2),$$
$$f_0\sigma_i(f) = f_0\sigma_i(ef) = f_0\sigma_i(e)\sigma_i(f) = 0\ (i \geqq 2)$$

and so

$$f_0\sigma_i(g) = f_0\sigma_i(fa_2\cdots a_s) = f_0\sigma_i(f)\sigma_i(a_2\cdots a_s) = 0\ (i \geqq 1).$$

This implies $f_0 h = 0$ and so $h \neq 1$. Now, for any $i \neq j$, we have $\sigma_i^{-1}\sigma_j = \sigma_k\tau$ for some $\tau \in G_e\ (= \{\sigma \in G;\ \sigma(e) = e\})$ and $k > 1$. Hence

$$\sigma_i^{-1}(\sigma_i(g) - \sigma_j(g)) = g + \sigma_k\tau(g) = g + \sigma_k\tau(efa_2\cdots a_s)$$
$$= g + \sigma_k(e)\,\sigma_k\tau(fa_2\cdots a_s)$$

From this, we obtain $e\sigma_i^{-1}(\sigma_i(g) - \sigma_j(g)) = eg = g \neq 0$. Therefore, it follows that $\sigma_i(g) - \sigma_j(g) \neq 0$ for each $i \neq j$. Since $g \in O(\mathfrak{B}(B); G)$, we have $|G\{g\}| = m$, and so $h \in \mathfrak{B}(A)\setminus\{0\} = \{1\}$, which is a contradiction. Hence e is a primitive idempotent in $\mathfrak{B}(B)$. Thus, we obtain (a) $\Rightarrow$ (b).

(b) $\Rightarrow$ (a): We set $m = m_{O(\mathfrak{B}(B);\,G)}$. Let f be an element in $O(\mathfrak{B}(B); G)$ such that $|G\{f\}| = m$, and $G\{f\} = \{f_1, \dots, f_m\}$. Then, since A is connected, we have $1 = \sum_{i=1}^{m} f_i$. Now, let e be an arbitrary primitive idempotent in $\mathfrak{B}(B)$. Then $e \in O(\mathfrak{B}(B); G)$ (which has been noted already). Since $e = \sum_{i=1}^{m} ef_i$, we have $ef_u \neq 0$ for some u in $\{1, \dots, m\}$, and $e \geqq ef_u > 0$. Hence $e = ef_u$. Let $f_u \neq \sigma(f_u)$ for some $\sigma \in G$. Then $\sigma(ef_u)f_u = \sigma(e)\sigma(f_u)f_u = 0$. Since $(ef_u)f_u \neq 0$, we have $ef_u \neq \sigma(ef_u)$. Hence, it follows that

$$m = m_{O(\mathfrak{B}(B);\,G)} \geqq |G\{e\}| = |G\{ef_u\}| \geqq m.$$

Thus we obtain $|G\{e\}| = m$, completing the proof.

Lemma 2. *Let A be a connected ring and B/A a G-extension. Then, there exists a primitive idempotent e in B, and $G\{e\}$ coincides with the set of all the primitive idempotents in B. Moreover, $|\mathfrak{B}(B)| = 2^m$ for $m = |G\{e\}|$.*

Proof. By Lemma 1, B contains a primitive idempotent e. Set $m = |G\{e\}|$ and $G\{e\} = \{\sigma_1(e), \dots, \sigma_m(e)\}$. Then the elements $\sigma_i(e)$'s are orthogonal to each other and $\sum_{i=1}^m \sigma_i(e) = 1$. Now, let f be an arbitrary element of $\mathfrak{B}(B)$. If $f\sigma_u(e) \neq 0$ $(1 \leqq u \leqq m)$ then $0 < f\sigma_u(e) \leqq \sigma_u(e)$ and so $f\sigma_u(e) = \sigma_u(e)$. Hence $f = \sum_{i=1}^m f\sigma_i(e)$, which is the sum of the $\sigma_u(e)$'s with $f\sigma_u(e) \neq 0$. In particular, any primitive idempotent of B is contained in $\{\sigma_1(e), \dots, \sigma_m(e)\}$. From this, the rest of our assertions follows immediately.

Lemma 3. *Let B/A be a G-extension. Let e be a primitive idempotent of B and set $G\{e\} = \{\sigma_1(e), \dots, \sigma_m(e)\}$ where $m = |G\{e\}|$. Then $\sum_{i=1}^m \sigma_i(e)$ is a primitive idempotent of A.*

Proof. We set $f = \sum_{i=1}^m \sigma_i(e)$. Then, one will easily see that $f \in A$. Moreover, each $\sigma_i(e)$ $(1 \leqq i \leqq m)$ is a primitive idempotent of B. Since $\sigma_i(e) \neq \sigma_j(e)$ for each pair $i \neq j$ $(1 \leqq i, j \leqq m)$, the $\sigma_i(e)$ are orthogonal to each other. Hence we have $f \in \mathfrak{B}(A)$. We assume that f is not primitive in $\mathfrak{B}(A)$. Then, there are non-zero elements f_1 and f_2 in $\mathfrak{B}(A)$ such that $f = f_1 + f_2$ and $f_1 f_2 = 0$. It is obvious that $f_1 = f_1 f = \sum_{i=1}^m f_1 \sigma_i(e) = \sum_{i=1}^m \sigma_i(f_1 e)$. Hence $f_1 e \neq 0$. Since e is primitive in $\mathfrak{B}(B)$ and $e \geqq f_1 e > 0$, we obtain $e = f_1 e$. Therefore, it follows that $f_1 = \sum_{i=1}^m \sigma_i(e) = f$, which is a contradiction. Thus, f is primitive in $\mathfrak{B}(A)$.

Lemma 4. *Let B/A be a G-extension. Let f be a primitive idempotent of A. Then, there exists a primitive idempotent e of B such that $f = \sum_{i=1}^m \sigma_i(e)$ for $G\{e\} = \{\sigma_1(e), \dots, \sigma_m(e)\}$ where $m = |G\{e\}|$.*

Proof. Obviously, Af is a connected ring with an identity f. Since $Bf^G = Af$, Bf/Af is a $(G|Bf)$-extension. Hence by Lemma 2, there exists a primitive idempotent e in Bf. Then, one will easily see that e is also a primitive idempotent in B. We set $m = |G\{e\}|$, $G\{e\} = \{\sigma_1(e), \dots, \sigma_m(e)\}$ and $f' = \sum_{i=1}^m \sigma_i(e)$. Since $\sigma(e) \in Bf$ for every $\sigma \in G$, we have $f' \in Bf$. Hence by Lemma 3, f' is a non-zero idempotent of $A \cap Bf = Af$. Since Af is connected, it follows that $f' = f$, completing the proof.

Combining Lemma 3 with Lemma 4, we obtain the following

Theorem 5. *Let B/A be a G-extension. Let $\mathfrak{B}(B)'$ (resp. $\mathfrak{B}(A)'$) be the set of non-zero primitive idempotents in $\mathfrak{B}(B)$ (resp. $\mathfrak{B}(A)$). Then*

(i) $|\mathfrak{B}(A)'| \leqq |\mathfrak{B}(B)'| \leqq |\mathfrak{B}(A)'|\,|G|$.

(ii) $|\mathfrak{B}(A)| \leqq |\mathfrak{B}(B)| \leqq 2^{|\mathfrak{B}(A)||G|}$ *if either* $|\mathfrak{B}(A)| < \infty$ *or* $|\mathfrak{B}(B)| < \infty$.

In virtue of Theorem 5, we obtain the following

Corollary 6. *Let B/A be a G-extension. Then, B has a primitive idempotent if and only if A has a primitive idempotent.*

Corollary 7. *Let B/A be a G-extension. Then, B is semi-connected if and only if A is semi-connected.*

2. On G-extension of rings. Throughout the rest of this note, B will mean a ring which is not necessarily commutative.

Firstly, in virtue of Corollary 7, we shall prove the following

Theorem 8. *Let B/A be a G-extension. If A is semi-connected then so is B.*

Proof. Since $\sigma(C_B) = C_B$ for all $\sigma \in G$, C_B/C_B^G is a $(G\,|\,C_B)$-extension. Moreover, we have $C_B^G = C_B \cap A \subset C_A$, and so, $\mathfrak{B}(C_B^G) \subset \mathfrak{B}(C_A)$. Hence, if C_A is semi-connected then so is C_B^G, and whence C_B is semi-connected by Corollary 7.

Lemma 9. *Let B/A be a G-extension. Let e be an arbitrary element of $O(\mathfrak{B}(C_B); G)$. Then, for any $\tau \in G$, $B\tau(e)/A\tau(e)$ is a $(\tau G_e \tau^{-1}|\,B\tau(e))$-extension, $G_{\tau(e)} = \tau G_e \tau^{-1}$, and $A\tau(e) \cong A(\sum_{i=1}^{m} \sigma_i(e))$ for $G = \sigma_1 G_e \cup \cdots \cup \sigma_m G_e$ (disjoint).*

Proof. Firstly, by making use of the same methods as in the proof of [6, Lemma 2.14], we shall prove that Be/Ae is a $(G_e|\,Be)$-extension. For $G = \sigma_1 G_e \cup \cdots \cup \sigma_m G_e$ (disjoint), we have $G|e| = \{\sigma_1(e), \ldots, \sigma_m(e)\}$ and $m = |G|e||$. We may assume that $\sigma_1 = 1$. Set here $f = \sum_{i=1}^{m} \sigma_i(e)$. Then $f \in \mathfrak{B}(C_A)$ since $\sigma(f) = f$ for all $\sigma \in G$. Noting $B = Bf \oplus B(1-f)$ (direct sum), one will easily see that $Bf^G = A \cap Bf = Af$. Now, clearly we have

$Ae \subset Be^{G_e}$. For any $a_1 \in Be^{G_e}$, we set

$$a_i = \sigma_i(a_1)\ (i = 1, \dots, m), \quad \text{and} \quad a = a_1 + \cdots + a_m.$$

Then $a \in Bf$. Let τ be an arbitrary element of G. Since

$$\bigcup_{i=1}^m \sigma_i G_e \,(\text{disjoint}) = G = \tau G = \bigcup_{i=1}^m \tau\sigma_i G_e \,(\text{disjoint}),$$

there exist elements $\tau_1, \dots, \tau_m$ in G_e such that

$$\{\tau\sigma_1, \dots, \tau\sigma_m\} = \{\sigma_1\tau_1, \dots, \sigma_m\tau_m\},$$

and then $\tau(a) = \sum_{i=1}^m \tau\sigma_i(a_1) = \sum_{i=1}^m \sigma_i\tau_i(a_1) = \sum_{i=1}^m \sigma_i(a_1) = a$. Hence we obtain that $a \in Bf^G = Af$, and so $a_1 = ae \in Afe = Ae$. Therefore, it follows that $Be^{G_e} = Ae$, that is, Be/Ae is a $(G_e|Be)$-extension (cf. [4, Lemma 1.1] and [7, Lemma 10]). Now, it is obvious that $G_{\tau(e)} \supset \tau G_e \tau^{-1}$. For any $\sigma \in G_{\tau(e)}$, we have $\sigma\tau(e) = \tau(e)$, which implies $\tau^{-1}\sigma\tau \in G_e$, and so $\sigma \in \tau G_e \tau^{-1}$. Hence we obtain $G_{\tau(e)} = \tau G_e \tau^{-1}$. Noting $\tau(e) \in O(\mathfrak{B}(C_B); G)$, we see that $B\tau(e)/A\tau(e)$ is a $(\tau G\tau^{-1}|B\tau(e))$-extension. If $ae = 0$ for $a \in A$ then

$$0 = \sum_{i=1}^m \sigma_i(ae) = a\sum_{i=1}^m \sigma_i(e) = af.$$

This implies that $Af \cong Ae$, and so $Af \cong A\tau(e)$.

Lemma 10. *Let B/A be a G-extension. Let e be an arbitrary element of $O(\mathfrak{B}(C_B); G)$, and $G = \sigma_1 G_e \cup \cdots \cup \sigma_m G_e$ (disjoint). If $\sum_{i=1}^m \sigma_i(e) = 1$ then B is a direct sum of $(\sigma_i G_e \sigma_i^{-1}|B\sigma_i(e))$-extensions $B\sigma_i(e)/A\sigma_i(e)$ with $A\sigma_i(e) \cong A$ $(a\sigma_i(e) \leftrightarrow a)$, $1 \leqq i \leqq m$.*

Proof. One will easily see that $G\{e\} = \{\sigma_1(e), \dots, \sigma_m(e)\}$, $m = |G\{e\}|$, and so, $\sigma_i(e) \neq \sigma_j(e)$ for each $i \neq j$. If $\sum_{i=1}^m \sigma_i(e) = 1$ then

$$B = B\sigma_1(e) \oplus \cdots \oplus B\sigma_m(e)$$

and for each i $(1 \leqq i \leqq m)$, $B\sigma_i(e)/A\sigma_i(e)$ is a $(\sigma_i G_e \sigma_i^{-1}|B\sigma_i(e))$-extension with $A\sigma_i(e) \cong A$ by Lemma 9.

Now, in virtue of Lemma 2 and Lemma 10, we shall prove the following

Theorem 11. *Let A be a connected ring, and B/A a G-extension. Then, there is a primitive idempotent e in C_B, and for*

$$G = \sigma_1 G_e \cup \cdots \cup \sigma_m G_e \quad (\textit{disjoint}),$$

there holds that

(i) $|\mathfrak{B}(C_B)| = 2^m$, $m = |G\{e\}|$, $G\{e\}$ *coincides with the set of all the primitive idempotents of* C_B, *and*

(ii) B *is a direct sum of connected* $(\sigma_i G_e \sigma_i^{-1} | B\sigma_i(e))$*-extensions* $B\sigma_i(e)/A\sigma_i(e)$ *with* $A\sigma_i(e) \cong A$ $(1 \leqq i \leqq m)$.

Proof. As in the proof of Theorem 4, C_B/C_B^G is a $(G | C_B)$-extension. Since $C_B^G = C_B \cap A \subset C_A$, C_B^G is a connected ring. Hence by Lemma 2, there is a primitive idempotent e in C_B, for which (i) holds. Now, since $\sum_{i=1}^m \sigma_i(e) = 1$ and the $\sigma_i(e)$ are orthogonal to each other, we have $C_{B\sigma_i(e)} = C_B\sigma_i(e)$ $(1 \leqq i \leqq m)$. Obviously, each $C_B\sigma_i(e)$ is a connected ring with an identity $\sigma_i(e)$. Hence the rings $B\sigma_i(e)$ are connected. The other assertions follow immediately from Lemma 10.

Corollary 12. *Let* A *be a connected ring, and* B/A *a* G*-extension with* $|G| = n$.

(i) *The following conditions are equivalent.*

(a) B *is ring isomorphic to* $A^{(n)}$, *a direct sum of* n*-copies of* A.

(b) *There exists a primitive idempotent* e *in* C_B *with* $|G\{e\}| = n$.

(c) C_B *contains* C_A, C_B *is ring isomorphic to* $C_A^{(n)}$ *and* $B \cong C_B \otimes_{C_A} A$.

Moreover, if this is the case, $G\{e\}$ *is a* G*-normal bases for* B/A, *and* G *is an outer group.*

(ii) *If* n *is prime, then the following conditions are equivalent.*

(a′) B *is ring isomorphic to* $A^{(n)}$.

(b′) B *is disconnected.*

Proof. Let S be the set of primitive idempotents of C_B. Then S is non-empty by Theorem 11. Let e be an arbitrary element of S. Then, we have $S = G\{e\}$ by Theorem 11.

(a) $\Rightarrow$ (b): Since $B \cong A^{(n)}$, we have $|S| \geqq n$, and so $|G\{e\}| \geqq n$. On the other hand, it is obvious that $|G\{e\}| \leqq |G| = n$. Hence $|G\{e\}| = n$.

(b) $\Rightarrow$ (a): Since $|G\{e\}| = n$, we have $G_e = \{1\}$. Hence, by Theorem 11, we obtain $B = \sum_{\tau \in G} \oplus A\tau(e)$ and $A\tau(e) \cong A$. Moreover, $G\{e\}$ is a G-normal bases for B/A.

(a) $\Leftrightarrow$ (c): This will be easily seen, and by (c), G is an outer group. Clearly $|G\{e\}|$ is a divisor of $|G|$. Noting this fact, one will easily see the assertion (ii).

Next, we shall make some remarks on G-Galois extensions of rings.

Lemma 9′. *Let B/A be a G-Galois extension. Let e be an arbitrary element of $O(\mathfrak{B}(C_B); G)$. Then, for any $\tau \in G$, $B\tau(e)/A\tau(e)$ is a $(\tau G_e \tau^{-1} | B\tau(e))$-Galois extension with $\tau G_e \tau^{-1} | B\tau(e) \cong \tau G_e \tau^{-1}$.*

Proof. Since B/A is G-Galois, there is a G-Galois coordinate system $\{u_i, v_i; i = 1, \dots, r\}$ in B such that $\sum_i u_i\sigma(v_i) = \delta_{1,\sigma}$ $(\sigma \in G)$. Let τ be an element of G_e. Then we have

$$\sum_i eu_i\tau(ev_i) = e\sum_i u_i\tau(v_i) = e\delta_{1,\tau}.$$

If $\tau | Be = 1$ then

$$e = e\sum_i u_i v_i = \sum_i eu_iev_i = \sum_i eu_i\tau(ev_i) = e\delta_{1,\tau}$$

and whence $\tau = 1$. This implies that $G_e \cong G_e | Be$. Moreover, $\{eu_i, ev_i; i = 1, \dots, r\}$ is a $(G_e | Be)$-Galois coordinate system for Be/Be^{G_e}. Since $Be^{G_e} = Ae$ (Lemma 9), Be/Ae is a $(G_e | Be)$-Galois extension. Now, for any $\tau \in G$, since $\tau(e) \in O(\mathfrak{B}(C_B); G)$ and $G_{\tau(e)} = \tau G_e \tau^{-1}$, we obtain our assertion by the above remark.

By Lemma 9′, Lemma 10 and Theorem 11, we obtain the following

Lemma 10′. *Let B/A be a G-Galois extension. Let e be an arbitrary element of $O(\mathfrak{B}(C_B); G)$, and $G = \sigma_1 G_e \cup \cdots \cup \sigma_m G_e$ (disjoint). If $\sum_{i=1}^m \sigma_i(e) = 1$ then B is a direct sum of $(\sigma_i G_e \sigma_i^{-1} | B\sigma_i(e))$-Galois extensions $B\sigma_i(e)/A\sigma_i(e)$ with $A\sigma_i(e) \cong A$ and $\sigma_i G_e \sigma_i^{-1} | B\sigma_i(e) \cong \sigma_i G_e \sigma_i^{-1}$ $(1 \leqq i \leqq m)$.*

Theorem 11′. *Let A be a connected ring, and B/A a G-Galois extension. Then, there is a primitive idempotent e in C_B, and for $G = \sigma_1 G_e \cup \cdots \cup \sigma_m G_e$ (disjoint), B is a direct sum of connected $(\sigma_i G_e \sigma_i^{-1} | B\sigma_i(e))$-Galois extensions $B\sigma_i(e)/A\sigma_i(e)$ with $A\sigma_i(e) \cong A$ and $\sigma_i G_e \sigma_i^{-1} | B\sigma_i(e) \cong \sigma_i G_e \sigma_i^{-1}$ $(1 \leqq i \leqq m)$.*

3. A Galois theory of strong G-extensions of semi-connected rings. In [8], O. E. Villamayor and D. Zelinsky presented a Galois theory for a G-extension S/R such that R is a semi-connected commutative ring and S is a projective and separable commutative R-algebra. In this section, we shall present a partial generalization of this theory to non-commutative rings (Theorem 13).

Throughout this section, B will mean a semi-connected ring with $P = \{e_1, \dots, e_n\}$, the set of all central primitive idempotents of B, and B/A will mean a G-extension (where G is a finite group of automorphisms of B). Moreover, for any subset S (resp. H) of B (resp. G), we shall use the notations $S(H)$ and $H(S)$ instead of S^H and H_S respectively.

Now, we set

$$S_i = Be_i \quad \text{and} \quad H_i = G(\{e_i\})|Be_i$$

where $i = 1, \dots, n$. Obviously, there holds that the e_i are orthogonal, $\sum_{i=1}^n e_i = 1$ and $\sum_{i=1}^n \oplus S_i = B$. As is seen in [8], by G^*, we denote the set of automorphisms σ of B such that for each i ($1 \leqq i \leqq n$), $\sigma|S_i = g_i|S_i$ for some g_i in G. Then, one will easily see that G^* is a group and $G \subset G^* = (G^*)^*$ ($= G^{**}$ as an abbreviation). If $G = G^*$ then G will be called to be a *fat group*. Moreover, if for each i ($1 \leqq i \leqq n$), $H_i(S_i(N)) = N$ for every subgroup N of H_i then B/A will called to be a *strong G-extension.*

First, we consider a G-extension B/A such that

(I) *G is transitive on the set P.*

Let f be a non-zero idempotent of $C_B \cap A$. Then, there exists an element e in P such that $fe \neq 0$. Since e is a primitive idempotent of C_B, we have $fe = e$. Hence $f\sigma(e) = \sigma(e)$ for all $\sigma \in G$. This implies $f = 1$. Moreover, if $a \in A$ and $ae = 0$ for some $e \in P$ then $a\sigma(e) = 0$ for all $\sigma \in G$ and so $a = 0$, which implies $A \cong Ae$ (cf. Theorem 11). Thus we obtain the following

(I, i) *$C_B \cap A$ is connected, and $A \cong Ae$ ($a \leftrightarrow ae$) for every $e \in P$.*

We set

$$\mathfrak{R}(G) = H_1 \times \cdots \times H_n \quad \text{(direct product)}.$$

Since G is transitive on P, there is a subset $\{\sigma_1, \dots, \sigma_n\}$ in G such that $\sigma_1 = 1$ and $\sigma_i(e_1) = e_i$ ($i = 1, \dots, n$). Then for $E_1 = G(\{e_1\})$,

$$G(\{e_i\}) = \sigma_i E_1 \sigma_i^{-1} \ (1 \leqq i \leqq n) \text{ and } G = \sigma_1 E_1 \cup \cdots \cup \sigma_n E_1 \text{ (disjoint)}.$$

Let $\mathfrak{S}(G)$ be the symmetric group of permutations on the set $\{1, \dots, n\}$.

Now, we define compositions

$$\mathfrak{R}(G) \times B \to B \quad \text{and} \quad \mathfrak{S}(G) \times B \to B$$

by

$$(\tau_1, \dots, \tau_n)(b_1+\cdots+b_n) = \tau_1(b_1)+\cdots+\tau_n(b_n)$$

and

$$\begin{aligned}((u, v)\cdots(r, s)(i, j))(b_1+\cdots+b_n) \\ &= (u, v)(\cdots(r, s)((i, j)(b_1+\cdots+b_n))\cdots) \\ &= (u, v)(\cdots(r, s)(b_1+\cdots+b_{i-1}+\sigma_i\sigma_j^{-1}(b_j)+b_{i+1}+\cdots+b_{j-1} \\ &\qquad +\sigma_j\sigma_i^{-1}(b_i)+b_{j+1}+\cdots+b_n)\cdots)\end{aligned}$$

respectively, where $b_i \in S_i$, $\tau_i \in H_i$ for $i = 1, \dots, n$, and the (i, j)'s are transpositions in $\mathfrak{S}(G)$.

Under the above situations, we shall prove that

(I, ii) $\mathfrak{R}(G) \cap \mathfrak{S}(G) = \{1\}$, $\mathfrak{R}(G)\mathfrak{S}(G) = \mathfrak{S}(G)\mathfrak{R}(G)$ *and* $\mathfrak{R}(G)$ *is a normal subgroup of* $\mathfrak{R}(G)\mathfrak{S}(G)$.

Proof. It is obvious that $\mathfrak{R}(G) \cap \mathfrak{S}(G) = \{1\}$. Now, let $(i, j) \in \mathfrak{S}(G)$, $\tau = (\tau_1, \dots, \tau_m) \in \mathfrak{R}(G)$, and set

$$\begin{aligned}\tau^* = (\tau_1, \dots, \tau_{i-1}, \sigma_i\sigma_j^{-1}\tau_j\sigma_j\sigma_i^{-1}, \tau_{i+1}, \dots, \\ \tau_{j-1}, \sigma_j\sigma_i^{-1}\tau_i\sigma_i\sigma_j^{-1}, \tau_{j+1}, \dots, \tau_n).\end{aligned}$$

Then, for $b_1+\cdots+b_n \in B$ ($b_i \in S_i$, $i = 1, \dots, n$), we have

$$\begin{aligned}&(i, j)\tau(b_i) = (i, j)\tau_i(b_i) = \sigma_j\sigma_i^{-1}\tau_i(b_i), \\ &(i, j)\tau(b_j) = (i, j)\tau_j(b_j) = \sigma_i\sigma_j^{-1}\tau_j(b_j), \quad \text{and} \\ &(i, j)\tau(b_k) = \tau_k(b_k) \text{ for } k \neq i, j.\end{aligned}$$

Hence

$$\begin{aligned}\tau^*(i, j)(b_i) &= \tau^*\sigma_j\sigma_i^{-1}(b_i) = \sigma_j\sigma_i^{-1}\tau_i\sigma_i\sigma_j^{-1}\sigma_j\sigma_i^{-1}(b_i) \\ &= \sigma_j\sigma_i^{-1}\tau_i(b_i) = (i, j)\tau(b_i), \\ \tau^*(i, j)(b_j) &= \tau^*\sigma_i\sigma_j^{-1}(b_j) = \sigma_i\sigma_j^{-1}\tau_j\sigma_j\sigma_i^{-1}\sigma_i\sigma_j^{-1}(b_j) \\ &= \sigma_i\sigma_j^{-1}\tau_j(b_j) = (i, j)\tau(b_j), \quad \text{and} \\ \tau^*(i, j)(b_k) &= \tau^*(b_k) = \tau_k(b_k) = (i, j)\tau(b_k) \quad \text{for } k \neq i, j.\end{aligned}$$

Thus, we obtain $\tau^*(i, j) = (i, j)\tau$. Therefore, it follows that $p\mathfrak{R}(G) = \mathfrak{R}(G)p$ for all $p \in \mathfrak{S}(G)$, completing the proof.

(I, iii) $G^* = \mathfrak{R}(G)\mathfrak{S}(G) \supset G$, $B(G^*) = A$ *and* $\mathfrak{R}(G^*) = \mathfrak{R}(G)$.

Proof. It is easily seen that $G^* \supset \mathfrak{R}(G)$, $\mathfrak{S}(G)$ and $\mathfrak{R}(G)\mathfrak{S}(G)$.

Let σ be an arbitrary element of $G*$. Then, for each i $(1 \leqq i \leqq n)$, we have $\sigma | S_i = g_i | S_i$ for some $g_i \in G$. Moreover, since $\sigma(e) \in P$ for all $e \in P$, there exists an element p in $\mathfrak{S}(G)$ such that $\sigma(e_i) = p(e_i)$ for $i = 1, \ldots, n$. Then

$$p^{-1}\sigma | S_i = p^{-1}g_i | S_i = p^{-1}g_i | Be \quad \text{and} \quad p^{-1}\sigma(e_i) = e_i$$

where $i = 1, \ldots, n$. One will easily see that for each $j = 1, \ldots, n$, $p^{-1} | S_j = h_j | S_j$ for some $h_j \in G$. Hence $p^{-1}g_i | S_i = \tau_i$ for some $\tau_i \in H_i$ $(i = 1, \ldots, n)$. Therefore, it follows that $p^{-1}\sigma \in \mathfrak{N}(G)$ and $\sigma \in p\mathfrak{N}(G) \subset \mathfrak{S}(G)\mathfrak{N}(G)$. Thus, we obtain $G* = \mathfrak{S}(G)\mathfrak{N}(G)$. The other assertions will be easily seen.

(I, iv) *If K is a subgroup of G which is transitive on P then $G* = \mathfrak{N}(G)\mathfrak{S}(K)$.*

Proof. As is easily seen, we have $\mathfrak{S}(K)\mathfrak{N}(G) \subset G*$. Now, let $p \in \mathfrak{S}(G)$. Then, there is an element q in $\mathfrak{S}(K)$ such that $q(e_i) = p(e_i)$, that is, $q^{-1}p(e_i) = e_i$ for $i = 1, \ldots, n$. This implies that $q^{-1}p \in \mathfrak{N}(G*) = \mathfrak{N}(G)$ (by (I, iii)) and so $p \in q\mathfrak{N}(G) \subset \mathfrak{S}(K)\mathfrak{N}(G)$. Hence we obtain $\mathfrak{S}(G) \subset \mathfrak{S}(K)\mathfrak{N}(G)$. Therefore, it follows that

$$G* = \mathfrak{S}(G)\mathfrak{N}(G) \subset \mathfrak{S}(K)\mathfrak{N}(G)\mathfrak{N}(G) = \mathfrak{S}(K)\mathfrak{N}(G)$$

and whence $G* = \mathfrak{S}(K)\mathfrak{N}(G) = \mathfrak{N}(G)\mathfrak{S}(K)$.

Moreover, we have

(I, v) *Let B/A be a strong G-extension. If K is a subgroup of $G*$ such that $B(K) = A$ then $K* = G*$.*

Proof. By (I, i), $C_B \cap A$ is connected. Since $B(K) = A$, it is easily seen that K is transitive on P. Hence, by (I, iii) and (I, iv), we have

$$G* = (G*)* = \mathfrak{N}(G*)\mathfrak{S}(K) = \mathfrak{N}(G)\mathfrak{S}(K).$$

Moreover, since $B(G) = A = B(K)$, by Theorem 11, we have

$$S_i(\mathfrak{N}(G) | S_i) = Ae_i = S_i(\mathfrak{N}(K) | S_i) \quad \text{for } i = 1, \ldots, n.$$

Since $\mathfrak{N}(G) = \mathfrak{N}(G*) \supset \mathfrak{N}(K)$ and B/A is a strong G-extension, we obtain

$$\mathfrak{N}(G) | S_i = \mathfrak{N}(K) | S_i \quad \text{for } i = 1, \ldots, n.$$

Hence $\mathfrak{N}(G) = \mathfrak{N}(K)$. Therefore, it follows that $G^* = \mathfrak{N}(K)\mathfrak{S}(K) = K^*$.

Next, we consider a G-extension B/A such that

(II) *G is not necessarily transitive on P.*

As is easily seen, we have a decomposition of P into G-orbits such that

$$P = P_1 \cup \cdots \cup P_r \quad \text{(disjoint)}$$

where $GP_i = P_i$ and G is transitive on P_i for each i $(1 \leqq i \leqq r)$. We set $f_i = \sum_{e \in P_i} e$, $i = 1, \ldots, r$. Then

$$B = Bf_1 \oplus \cdots \oplus Bf_r \quad \text{and}$$
$$A = Af_1 \oplus \cdots \oplus Af_r.$$

Moreover, we set $G_i = G \mid Bf_i$, $i = 1, \ldots, r$. Then

$$G \subset G_1 \times \cdots \times G_r,\ G^* = G_1^* \times \cdots \times G_r^* \quad \text{and}$$
$$\begin{aligned} B(G^*) &= Bf_1(G_1^*) + \cdots + Bf_r(G_r^*) \\ &= Bf_1(G_1) + \cdots + Bf_r(G_r) \\ &= Af_1 + \cdots + Af_r = A. \end{aligned}$$

Hence by (I, ii) and (I, iii), we obtain

(II, i) $B(G^*) = B(G) = A$. *If B/A is a strong G-extension then this is also a strong G^*-extension, and for any subgroup K of G^*, $B/B(K)$ is a strong K-extension.*

Next, we shall prove the following

(II, ii) *Let B/A be a strong G-extension. If K is a subgroup of G^* then $G^*(B(K)) = K^*$.*

Proof. Case 1: $B(K) = A$. We set $K_i = K \mid Bf_i$, $i = 1, \ldots, r$. Then

$$K_i \subset G_i^* \quad \text{and} \quad Bf_i(K_i) = Af_i \quad (i = 1, \ldots, r).$$

Since each Bf_i/Af_i is a strong G_i-extension, it follows from (I, v) that $K_i^* = G_i^*$ for $i = 1, \ldots, r$. Hence we obtain

$$K^* = K_1^* \times \cdots \times K_r^* = G^* = G^*(A) = G^*(B(K)).$$

Case 2: $B(K) \supsetneqq A$. We set $T = B(K)$. Then $B(G^*(T)) = T$ and

B/T is a strong $G^*(T)$-extension by (II, i). Since $K \subset G^*(T)$, it follows from Case 1 that $K^* = G^*(T)^*$. Moreover, we have $B(G^*(T)^*) = B(G^*(T)) = T$ by (II, i). Since $G^*(T)^* \subset G^{**} = G^*$, we see that $G^*(T)^* \subset G^*(T)$ and so $G^*(T)^* = G^*(T) = G^*(B(K)) = K^*$.

An intermediate ring T of B/A is said to be G^*-*subfixed* if *for every* $e \in P$, $Be(G^*(Te)) = Te$, *and* $\sum_{e' \in G^*(T)\{e\}} e' \in T$. Clearly $G^*(Te) \mid Be \subset G^{**}(T) \mid Be$. By this and Lemma 3, our condition is equivalent to that

(α) *for every* $e \in P$, $Be(G^*(T \cup \{e\})) = Te$, *and*

(β) *for every primitive idempotent* g *of* $C_B \cap T$, $G^*(T)$ *is transitive on the set* $\{e \in P;\ eg \neq 0\}$.

Now, we shall prove the following

(II, iii) *Let* B/A *be a* G-*extension. If* K *is a subgroup of* G^* *then* $B(K)$ *is* G^*-*subfixed.*

Proof. Let e be an arbitrary element of P. Then, we have $e \in O(\mathfrak{B}(C_B);\ G)$. Hence, it follows from Lemma 9 that

$$\begin{aligned} B(K)e &= Be(K(\{e\})) \\ &= Be(K(B(K) \cup \{e\})) \supset Be(G^*(B(K) \cup \{e\})) \supset B(K)e. \end{aligned}$$

This implies that $B/B(K)$ satisfies the condition (α). Now, we have a decomposition of P into K-orbits such that

$$P = P_1 \cup \cdots \cup P_s \quad \text{(disjoint)}$$

where $KP_i = P_i$ and K is transitive on P_i for each i ($1 \leqq i \leqq s$). We set $g_i = \sum_{e \in P_i} e$, $i = 1, \ldots, s$. Then $\sum_{i=1}^{s} g_i = 1$. Hence, it follows from Lemma 3 that $\{g_i;\ i = 1, \ldots, s\}$ coincides with the set of primitive idempotents of $C_B \cap B(K)$, and $\{e \in P;\ eg_i \neq 0\} = P_i$ ($1 \leqq i \leqq s$) on which $G^*(B(K))$ is transitive. Thus, we see that $B(K)$ is G^*-subfixed.

(II, iv) *Let* B/A *be a* G-*extension. If* T *is an intermediate ring of* B/A *which is* G^*-*subfixed then* $B(G^*(T)) = T$.

Proof. Let $\{g_1, \ldots, g_s\}$ be the set of primitive idempotents of $C_B \cap T$. Then

$$B = Bg_1 \oplus \cdots \oplus Bg_s \quad \text{and} \quad T = Tg_1 \oplus \cdots \oplus Tg_s.$$

We set $K = G^*(T)$ and $\{e \in P;\ g_1 e \neq 0\} = \{e_{11}, \ldots, e_{1s_1}\}$. Then

$$g_1 = e_{11} + \cdots + e_{1s_1} \quad \text{and} \quad \sigma(e_{1j}) \in \{e_{11}, \dots, e_{1s_1}\}$$

for all $\sigma \in K$ and $j = 1, \dots, s_1$. Hence by the condition (α), we have

$$\begin{aligned} Bg_1(K) &\subset \bigcap_{i=1}^{s_1} (Be_{11} \oplus \cdots \oplus Be_{1(i-1)} \oplus Te_{1i} \oplus Be_{1(i+1)} \oplus \cdots \oplus Be_{1s_1}) \\ &= Te_{11} \oplus \cdots \oplus Te_{1s_1}. \end{aligned}$$

Moreover, by the condition (β), there exist elements $\sigma_2, \dots, \sigma_{s_1}$ in K such that $\sigma_i(e_{11}) = e_{1i}$, $i = 2, \dots, s_1$. Let $c = t_1e_{11} + t_2e_{12} + \cdots + t_{s_1}e_{1s_1}$ ($t_i \in T$) be an arbitrary element of $Bg_1(K)$. Then

$$c = \sigma_2(c) = t_1e_{12} + t_2\sigma_2(e_{12}) + \cdots + t_{s_1}\sigma_2(e_{1s_1}).$$

Hence $t_2e_{12} = t_1e_{12}$. By a similar way, we have

$$c = t_1(e_{11} + e_{12} + \cdots + e_{1s_1}) = t_1g_1 \in Tg_1.$$

Hence we obtain $Bg_1(K) = Tg_1$. Moreover, by a similar way, it follows that

$$Bg_i(K) = Tg_i \quad \text{for } i = 1, \dots, s.$$

This shows that $B(K) = Tg_1 + \cdots + Tg_s = T$, completing the proof.

Now, combining (II, ii) with (II, iii) and (II, iv), we obtain the following theorem which is one of our main results.

Theorem 13. *Let B/A be a strong G-extension. Then, there exists a $1-1$ dual correspondence between the set of intermediate G^*-subfixed subrings T of B/A and the set of fat subgroups K of G^* in the usual sense of Galois theory: $T \leftrightarrow K$ with $G^*(T) = K$ and $B(K) = T$.*

Corollary 14. *Let B_i ($i = 1, \dots, t$) be semi-connected rings, and each B_i a G_i-Galois extension of a subring A_i. Let*

$$B = B_1 \oplus \cdots \oplus B_t, \; A = A_1 \oplus \cdots \oplus A_t, \quad \text{and} \quad G = G_1 \times \cdots \times G_t$$

which is an automorphism group of B by the composition:

$$(\sigma_1, \dots, \sigma_t)(b_1 + \cdots + b_t) = \sigma_1(b_1) + \cdots + \sigma_t(b_t)$$

where $\sigma_i \in G_i$ and $b_i \in B_i$ ($i = 1, \dots, t$). Then B/A is a strong G-extension to which Theorem 13 applies.

Proof. It is obvious that $B(G) = A$ and $G | B_i \cong G_i$ ($i = 1, \dots, t$).

Hence it suffices to prove that our assertion holds for $t = 1$. We set $B = B_1$ and $G = G_1$. Let e be an arbitrary primitive idempotent of C_B. Then we have $e \in O(\mathfrak{B}(C_B) ; G)$. Hence by Lemma 9', Be is a Galois extension of Ae with a Galois group $H = G(\{e\})|Be$. Therefore, it follows from [5, Proposition 2.2] that $H(Be(N)) = N$ for any subgroup N of H. Thus B/A is a strong G-extension.

In [8], O. E. Villamayor and D. Zelinsky proved the following theorem, which can be also proved by making use of Theorem 13.

Theorem 15 (O. E. Villamayor and D. Zelinsky). *Let S be a commutative ring with identity element 1 which is a G-extension of a semi-connected ring R such that S is projective and separable over R. Let H be the group of all R-algebra automorphisms of S. Then, S is semi-connected, $G^* = H$ and there exists a $1-1$ dual correspondence between the set of separable R-subalgebras of S and the set of fat subgroups of H in the usual sense of Galois theory.*

Proof. By Corollary 7, S is semi-connected. Hence, by Theorem 13, it suffices to prove that

(1) S/R is a strong G-extension, $G^* = H$, and

(2) for an intermediate ring T of S/R, T is separable over R if and only if T is H-subfixed.

Let $P = \{e_1, \dots, e_n\}$ be the set of primitive idempotents of S, and $\{f_1, \dots, f_r\}$ the set of primitive idempotents of R. Then

$$S = Sf_1 \oplus \cdots \oplus Sf_r, \quad Sf_i(G|Sf_i) = Rf_i \quad (i = 1, \dots, r)$$

and each Sf_i is projective and separable over Rf_i. Hence, it suffices to prove that our assertion holds for $r = 1$, and so, let R be connected. Then G is transitive on P. By (I, i), $R \cong Re$ ($a \leftrightarrow ae$) for each $e \in P$ and Se is projective and separable over Re. By Lemma 9, Se/Re is a $(G(\{e\})|Se)$-extension. Since Se is connected, we see that Se/Re is $(G(\{e\})|Se)$-Galois by CHR Galois theory [1]. Hence S/R is a strong G-extension. Moreover, we have $G(\{e\})|Se = H(\{e\})|Se$. Noting $HP = P$ and $\sum_{e' \in P} e' = 1$, one will easily see that H is a finite group and so S/R is a strong H-extension. Since $S(G) = R = S(H)$, it follows from (I, v) that $G^* = H^* = H$. To see (2), let T be an intermediate ring of S/R with $\{g_1, \dots, g_s\}$, the set of primitive idempotents of T, and set $P_i = \{e \in P : eg_i \neq 0\}$ for $i = 1, \dots, s$. Then

$$S = Sg_1 \oplus \cdots \oplus Sg_s \quad \text{and} \quad T = Tg_1 \oplus \cdots \oplus Tg_s.$$

Now, we assume that T is H-subfixed. Then $S(H(T)) = T$ by Theorem 13. Hence, it follows from Lemma 9 that for each $e \in P_i$ $(1 \leqq i \leqq s)$,

$$Se(H(T)(\{e\})) = Te = Se(H(Te)) \quad \text{and} \quad Te = Tg_ie \cong Tg_i$$

since $H(T)\{e\} = P_i$ and $\sum_{e' \in P_i} e' = g_i$. Since Se is connected and Se/Re is Galois, we see that Te is separable over $Re \cong R$ and so Tg_i is separable over $Rg_i \cong R$ $(1 \leqq i \leqq s)$. Thus T is separable over R. To see the converse, we assume that T is separable over R. Let e be an element in P. Then, as is noted in the above, Se/Re is a $H(\{e\})|Se$-Galois extension. Moreover Te/Re is separable. Hence $Se(H(Te)|Se) = Te$ by CHR Galois theory. Since

$$T \subset Te \oplus T(1-e) \subset Se \oplus S(1-e) = S,$$

any automorphism in $H(Te)|Se$ can be extended in a T-algebra automorphism of S. This implies that $Se(H(T \cup \{e\})) = Te$. Next, let e_1 and e_2 be any elements of P_i $(1 \leqq i \leqq s)$. Then, it follows from [2, Proposition 1.5 and Lemma 1.6] that

$$Te_1 = Tg_ie_1 \cong Tg_i \cong Tg_ie_2 = Te_2$$

which is defined by $ae_1 \to ag_i \to ae_2$ $(a \in T)$. This isomorphism $Te_1 \to Te_2$ can be extended to an isomorphism φ: $Se_1 \to Se_2$ by an extension theorem in CHR Galois theory for connected rings (cf. [1, Lemma 4.1] and [2, Lemma 1.3 and Corollary 1.8]). Since

$$\begin{aligned} S &= Se_1 \oplus Se_2 \oplus S(g_i - e_1 - e_2) \oplus S(1-g_i) \\ &\supset Te_1 \oplus Te_2 \oplus T(g_i - e_1 - e_2) \oplus T(1-g_i) \\ &\supset T(e_1 + e_2 + (g_i - e_1 - e_2) + (1-g_i)) = T, \end{aligned}$$

φ can be extended to a T-automorphism φ' of S such that $\varphi'(e_1) = e_2$ and $\varphi'(e_2) = e_1$. This implies that $H(T)$ is transitive on P_i for $i = 1, \ldots, s$. Thus T is H-subfixed.

Remark. Let S be a commutative separable algebra over a finite field $\mathrm{GF}(p)$ consisting of p elements where p is a positive integer. Let H be the group of all automorphisms of S. Then S is finitely generated over $\mathrm{GF}(p)$ and H is of finite order. By $\mu(S)$, we denote the cardinality of the set of (ring-) isomorphism classes of maximal ideals of S. Then S is projective and separable over $S(H)$,

$$S(H) \cong \mathrm{GF}(p)^{(r)} \quad \text{(a direct sum of } r\text{-copies of GF}(p))$$

where $r = \mu(S)$ and, there exists a $1-1$ dual correspondence between the set of intermediate rings of $S/S(H)$ and the set of fat subgroups of H in the usual sense of Galois theory.

The proof is as follows: Since S is projective and separable over $\mathrm{GF}(p)$, S is a direct sum of a finite number of finite fields which are of characteristic p. Let P be the set of primitive idempotents of S, and φ a map of P into the set of integers defined by $\varphi(e) = \mathrm{Dim}_{\mathrm{GF}(p)} Se$ $(e \in P)$. Then, one will easily see that $|\text{image } \varphi| = \mu(S)$. We set here

$$\text{image } \varphi = \{n_1, \cdots, n_r\} \ (n_1 < n_2 < \cdots < n_r, \ r = \mu(S))$$
$$P_i = \{e \in P;\ \varphi(e) = n_i\},\ f_i = \textstyle\sum_{e \in P_i} e \quad (1 \leqq i \leqq r), \text{ and}$$
$$R = \mathrm{GF}(p)f_1 + \cdots + \mathrm{GF}(p)f_r.$$

Then, by [4, Remark 1.1], it will be easily seen that $S(H) = R \cong \mathrm{GF}(p)^{(r)}$. Now, let T be an intermediate ring S/R. Since there are no nilpotent elements in S, T is a semi-simple ring which is a direct sum of finite fields. Therefore, T is separable over $\mathrm{GF}(p)$, and in particular, R is separable over $\mathrm{GF}(p)$. Hence S and T are projective and separable over R (cf. [2, Proposition 1.5]). Applying Theorem 15 to the H-extension S/R, we obtain our assertion.

Next, we consider a direct sum S^* of a finite number of finite fields. As is easily seen, S^* is a direct sum of some separable $\mathrm{GF}(p_i)$-subalgebras S_i, $i = 1, \ldots, m$, where $0 < p_1 < p_2 < \cdots < p_m$ and the p_i are prime integers. Let H^* be the group of all automorphisms of S^*. Then, for each $a \in S_i$, we have $\sigma(a) \in S_i$ for all $\sigma \in H^*$ $(i = 1, \ldots, m)$. We set here

$$H_i = H^*(S_1 + \cdots + S_{i-1} + S_{i+1} + \cdots + S_m)$$

for $i = 1, \ldots, m$. Then, since $S^* = S_1 \oplus \cdots \oplus S_m$, each restriction $H_i | S_i$ coincides with the group of all automorphisms of S_i $(i = 1, \ldots, m)$. Moreover, we have

$$H^* = H_1 \times \cdots \times H_m \quad \text{(direct product), and}$$
$$S^*(H^*) = S_1(H_1) + \cdots + S_m(H_m).$$

Further, for any intermediate ring T of $S^*/S^*(H^*)$, we have

$$S_i(H_i) \subset T \cap S_i \subset S_i \quad (i = 1, \ldots, m), \text{ and}$$

$$T = (T \cap S_1) + \cdots + (T \cap S_m).$$

Hence, from the preceeding remarks, one will easily see that

$$S^*(H^*) \cong \mathrm{GF}(p_1)^{(r_1)} \oplus \cdots \oplus \mathrm{GF}(p_m)^{(r_m)} \text{ where } r_i = \mu(S_i)\ (i = 1, \ldots, m)$$

and, there exists a $1-1$ dual correspondence between the set of intermediate rings of $S^*/S^*(H^*)$ and the set of fat subgroups of H^* in the usual sense of Galois theory.

REFERENCES

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

[2] M. FERRERO and K. KISHIMOTO : On connectedness of p-Galois extensions of rings, Math. J. Okayama Univ. 25 (1983), 103−121.

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

[4] I. KIKUMASA, T. NAGAHARA and K. KISHIMOTO : On primitive elements of Galois extensions of commutative semi-local rings, Math. J. Okayama Univ. 31 (1989), 31−55.

[5] Y. MIYASHITA : Finite outer Galois theory of non-commutative rings, J. Fac. Sci. Hokkaido Univ. 19 (1966), 114−134.

[6] S. MONTGOMERY : Fixed Rings of Finite Automorphism Groups of Associative Rings, Lecture Notes in Math. 818 (1980), Springer-Verlag.

[7] T. NAGAHARA : On splitting rings of separable skew polynomials, Math. J. Okayama Univ. 26 (1984), 71−85.

[8] O. E. VILLAMAYOR and D. ZELINSKY : Galois theory of rings with finitely many idempotents, Nagoya Math. J. 27 (1966), 721−731.

DEPARTMENT OF MATHEMATICS
SHINSHU UNIVERSITY
MATSUMOTO, JAPAN 390

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY
TSUSHIMA-NAKA, OKAYAMA-SHI, JAPAN 700

(*Received January 11, 1989*)