IMBEDDINGS OF SOME SEPARABLE EXTENSIONS IN GALOIS EXTENSIONS II

Dedicated to Professor Kiiti Morita on his 60th birthday

TAKASI NAGAHARA

This note is a supplement to the previous paper [10]. In [12], O. E. Villamayor proved an imbedding theorem which is as follows:

Let R_1/R be a strongly separable extension with $\mathrm{rank}_R R_1 = n$. Then the extension R_1/R can be imbedded in an $\mathfrak{F}$-Galois extension S/R such that $J(\mathfrak{I}(R_1, \mathfrak{F}), S) = R_1$ and $\mathfrak{F}$ is isomorphic to the symmetric group S_n (the group of permutations of $\{a_1, \cdots, a_n\}$) where $\mathfrak{I}(R_1, \mathfrak{F})$ is imbedded into $\mathfrak{S}_n$ as the subgroup leaving fixed the element a_1.

Recently, he kindly advised me of that the theorem is useful for the study of imbeddings of separable algebras into Galois extensions. Indeed, this contains the results of [1, Th. A. 7], [6, Cor. 2. 3], a partial result of [4, Th. 1. 1] (cf. [5]), and some partial results of our theorems [8, Th. 1. 1] and [10, Ths. 1 and 2].

In this note, we shall prove that every strongly separable extension can be imbedded in a Galois extension with Galois group isomorphic to some symmetric group (Th. 1). Moreover, by using its result, we shall verify some generalizations of the results [10, Ths. 1 and 2] (Ths. 2, 3 and 4). In their proofs, the Villamayor's theorem plays an important rôle. As to notations and terminologies used here, we follow our previous paper [10].

Now, if B/R is a strongly separable extension then the $\mathrm{rank}_{R_\mathfrak{p}}(S\otimes_R R_\mathfrak{p})$ ($\mathfrak{p} \in \mathrm{Spec}\ R$) have the least common multiple, which will be denoted by $l(B/R)$ (where $R_\mathfrak{p}$ denotes the localization of R with respect to $\mathfrak{p}$). First, we shall prove the following

Theorem 1. *Let B/R be a strongly separable extension with $l(B/R) = m$. Then, the extension B/R can be imbedded in a Galois extension with Galois group isomorphic to the symmetric group $\mathfrak{S}_m$ (in the sense of CHR-Galois extension defined in [3]).*

Proof. By [2, Th. 2. 5. 1], there exists a finite set of orthogonal non-zero idempotents $\{e_1, \cdots, e_s\}$ in R such that $\sum_{i=1}^{s} e_i = 1$ and the each extension Be_i/Re_i is a strongly separable extension with $\mathrm{rank}_{Re_i} Be_i = m_i$

$(i=1, \cdots, s)$. Then $B=Be_1+\cdots+Be_s$ (direct sum), $R=Re_1+\cdots+Re_s$, and m is the least common multiple of the m_i. We set here $q_i=m/m_i$ $(i=1, \cdots, s)$, and consider the following rings:

$$B_i^*=Be_i\oplus\cdots\oplus Be_i \quad (q_i \text{ copies}),$$
$$B_i'=\{(b_i, \cdots, b_i)\in B_i^* ;\ b_i\in Be_i\},$$
$$R_i'=\{(r_i, \cdots, r_i)\in B_i^* ;\ r_i\in Re_i\}$$

(where the direct sum $\oplus$ is that of rings). Clearly the extension Be_i/Re_i is isomorphic to the extension B_i'/R_i' by the canonical map, and hence B_i'/R_i' is a strongly separable extension with rank m_i. Moreover, by [9, Lemma 1.1], the extension B_i^*/B_i' is a strongly separable extension with rank q_i. Thus the extension B_i^*/R_i' is a strongly separable extension with rank m. Next we consider the following rings:

$$B^* = B_1^* \oplus \cdots \oplus B_s^*$$
$$B' = B_1' \oplus \cdots \oplus B_s' \subset B^*$$
$$R' = R_1' \oplus \cdots \oplus R_s' \subset B'.$$

Then the extension B^*/R' is a strongly separable extension with rank m. Hence, by Villamayor's imbedding theorem, this extension can be imbedded in a Galois extension with Galois group isomorphic to the symmetric group $\mathfrak{S}_m$. Moreover, the extension B'/R' is isomorphic to the extension B/R by the canonical map, which is our desired one. This completes the proof.

Now, if $\mathfrak{H}_1, \cdots, \mathfrak{H}_n$ are groups then $\mathfrak{H}_1\times\cdots\times\mathfrak{H}_n$ will mean the direct product of the groups $\mathfrak{H}_i$, and in case $\mathfrak{H}_1=\cdots=\mathfrak{H}_n=\mathfrak{H}$, this product will be denoted by $(\times\mathfrak{H})^n$. Moreover, if $\mathfrak{S}_n$ is the symmetric group of permutations of $\{1, \cdots, n\}$ and $\mathfrak{H}$ is a group then $\mathfrak{S}_n \tilde{\times} (\times\mathfrak{H})^n$ will mean the semi-direct product of $\mathfrak{S}_n$ and $(\times\mathfrak{H})^n$ such that given any $\sigma=\{i\rightarrow p_i ;\ i=1, \cdots, n\}\in\mathfrak{S}_n$, $(\tau_1, \cdots, \tau_n)\sigma=\sigma(\tau_{p_1}, \cdots, \tau_{p_n})$ for all $(\tau_1, \cdots, \tau_n)\in(\times\mathfrak{H})^n$. If $\mathfrak{S}_n\times(\times\mathfrak{H})^n=\{(\sigma, (\tau_1, \cdots, \tau_n)) ;\ \sigma\in\mathfrak{S}_n$ and $\tau_i\in\mathfrak{H}$ $(i=1, \cdots, n)\}$ then the subgroup $\{(\sigma, (\tau_1, \cdots, \tau_n))\in\mathfrak{S}_n\tilde{\times}(\times\mathfrak{H})^n ;\ \sigma(1)=1\}$ $(\cong(\mathfrak{S}_{n-1}\tilde{\times}(\times\mathfrak{H})^{n-1})\times\mathfrak{H})$ will be denoted by $[(\mathfrak{S}_{n-1}\tilde{\times}(\times\mathfrak{H})^{n-1})\times\mathfrak{H}]'$, and moreover, the subgroup $\{(\sigma, (1, \tau_2, \cdots, \tau_n))\in\mathfrak{S}_n\tilde{\times}(\times\mathfrak{H})^n ;\ \sigma(1)=1\}$ $(\cong\mathfrak{S}_{n-1}\tilde{\times}(\times\mathfrak{H})^{n-1})$ will be denoted by $[\mathfrak{S}_{n-1}\tilde{\times}(\times\mathfrak{H})^{n-1}]'$. Under this situation, we shall prove the following

Theorem 2. *Let R_1/R be a strongly separable extension with* $\mathrm{rank}_R R_1$ $=n$ *and T/R_1 an $\mathfrak{H}$-Galois extension. Then the ring extension T/R can be imbedded in a $\mathfrak{G}$-Galois extension A/R such that* $\mathfrak{J}(R_1, \mathfrak{G})|T=\mathfrak{H}$,

$J(\mathfrak{J}(T, \mathfrak{G}), A) = T$, and $\mathfrak{G} \cong \mathfrak{S}_n \tilde{\times} (\times \mathfrak{H})^n$ where the subgroups $\mathfrak{J}(R_1, \mathfrak{G}) \supset \mathfrak{J}(T, \mathfrak{G})$ are imbedded into $\mathfrak{S}_n \tilde{\times} (\times \mathfrak{H})^n$ as the subgroups $[(\mathfrak{S}_{n-1} \tilde{\times} (\times \mathfrak{H})^{n-1}) \times \mathfrak{H}]' \supset [\mathfrak{S}_{n-1} \tilde{\times} (\times \mathfrak{H})^{n-1}]'$.

Proof. By Villamayor's imbedding theorem, the extension R_1/R can be imbedded in a $\mathfrak{F}$-Galois extension S/R such that $\mathfrak{F} \cong \mathfrak{S}_n$ $(\sigma \rightarrow \sigma')$ and $\mathfrak{J}(R_1, \mathfrak{F}) \cong \mathfrak{S}_{n-1}$ $(\sigma \rightarrow \sigma')$ where $\mathfrak{S}_n$ is the group of permutations of $\{a_1, \cdots, a_n\}$ and $\mathfrak{S}_{n-1} = \{\sigma' \in \mathfrak{S}_n ;\ \sigma'(a_1) = a_1\}$. By Galois theory, the cardinal number of $\mathfrak{F}|R_1$ (the restriction of $\mathfrak{F}$ to R_1) is n. We write here

$$\mathfrak{F}|R_1 = \{\sigma_1|R_1 = 1, \cdots, \sigma_n|R_1\}.$$

Then, we have that $\{\sigma_1'(a_1), \cdots, \sigma_n'(a_1)\} = \{a_1, \cdots, a_n\}$, and hence, for $\sigma \in \mathfrak{F}$, we may write $\sigma' = \{\sigma_i'(a_1) \rightarrow \sigma'\sigma_i'(a_1) ;\ i = 1, \cdots, n\}$. We consider the group homomorphism of $\mathfrak{F}$ into the group of permutations of $\mathfrak{F}|R_1$ which is defined by the following

$$\phi : \sigma \longrightarrow \{\sigma_i|R_1 \rightarrow \sigma\sigma_i|R_1 ;\ i = 1, \cdots, n\}.$$

Let σ be in the kernel of ϕ. Then, for each $1 \leqq i \leqq n$, there exists an element ε_i in $\mathfrak{J}(R_1, \mathfrak{F})$ such that $\sigma\sigma_i = \sigma_i\varepsilon_i$. Hence $\sigma'\sigma_i' = \sigma_i'\varepsilon_i'$, and so, $\sigma'\sigma_i'(a_1) = \sigma_i'\varepsilon_i'(a_1) = \sigma_i'(a_1)$. This implies $\sigma' = 1$ (identity), that is, $\sigma = 1$. Thus ϕ is an isomorphism (whence, by the results of [7, Lemma 3.1] and [3, Th. 2.2], S is generated by the subrings $\sigma_i(R_1)$, $1 \leqq i \leqq n$). Now, we set $[i] = \sigma_i(R_1)$ $(i = 1, \cdots, n)$. For each i, the isomorphism $\sigma_i^{-1}|[i]$ $([i] \rightarrow [1] = R_1)$ makes T into an $[i]$-algebra. We consider the tensor product of $S_{[1], \cdots, [n]}$ and the ${}_{[i]}T$:

$$A = (\cdots((S \otimes {}_{[1]}T) \otimes {}_{[2]}T) \otimes \cdots) \otimes {}_{[n]}T,$$

and we denote $(\cdots((a \otimes b_1) \otimes b_2) \otimes \cdots) \otimes b_n \in A$ as $a \otimes b_1 \otimes b_2 \otimes \cdots \otimes b_n$ omitting all parentheses. Then, A is an R-algebra, and the canonical map

$$\psi : b \longrightarrow 1 \otimes b \otimes 1 \otimes \cdots \otimes 1 \quad (b \in T)$$

is an R-algebra monomorphism of T into A (cf. [10, Lemma 2]). As in [10], if $\tau \in \mathfrak{H}$ then, for each $1 \leqq i \leqq n$, there exists an R-algebra automorphism $\tau^{(i)}$ of A such that

$$\tau^{(i)}(a \otimes b_1 \otimes \cdots \otimes b_n) = a \otimes b_1 \otimes \cdots \otimes b_{i-1} \otimes \tau(b_i) \otimes b_{i+1} \otimes \cdots \otimes b_n.$$

Given such automorphisms $\tau^{(i)}$ and $\nu^{(j)}$ $(\tau, \nu \in \mathfrak{H})$, it is obvious that $\tau^{(i)}\nu^{(j)} = \nu^{(j)}\tau^{(i)}$ for $i \neq j$. Next let $\sigma \in \mathfrak{F}$ so that $\sigma\sigma_i | R_1 = \sigma_{p_i} | R_1$ and $\sigma^{-1}\sigma_i | R_1 = \sigma_{q_i} | R_1$. Then we have an R-algebra isomorphism

$$A \longrightarrow (\cdots((S \otimes_{[p_1]} T) \otimes_{[p_2]} T) \otimes \cdots) \otimes_{[p_n]} T$$

which is defined by the following

$$a \otimes b_1 \otimes \cdots \otimes b_n \longrightarrow \sigma(a) \otimes b_1 \otimes \cdots \otimes b_n .$$

Hence there exists an R-algebra automorphism σ^* of A such that

$$\sigma^*(a \otimes b_1 \otimes b_2 \otimes \cdots \otimes b_n) = \sigma(a) \otimes b_{q_1} \otimes b_{q_2} \otimes \cdots \otimes b_{q_n} .$$

Moreover, there holds that for any $\tau \in \mathfrak{H}$, $\sigma^*\tau^{(i)} = \tau^{(p_i)}\sigma^*$ ($i = 1, \cdots, n$). Therefore, if $(\tau_1, \cdots, \tau_n) \in (\times \mathfrak{H})^n$ then

$$\sigma^*(\tau_1^{(1)} \cdots \tau_n^{(n)}) = (\tau_1^{(p_1)} \cdots \tau_n^{(p_n)})\sigma^* = (\tau_{q_1}^{(1)} \cdots \tau_{q_n}^{(n)})\sigma^*$$

so that

$$(\tau_1^{(1)} \cdots \tau_n^{(n)})(\sigma^{-1})^* = (\sigma^{-1})^*(\tau_{q_1}^{(1)} \cdots \tau_{q_n}^{(n)})$$

and similarly

$$(\tau_1^{(1)} \cdots \tau_n^{(n)})\sigma^* = \sigma^*(\tau_{p_1}^{(1)} \cdots \tau_{p_n}^{(n)})$$

(cf. [10 , Lemma 3]). We set

$$\mathfrak{F}^* = \{\sigma^* ; \sigma \in \mathfrak{F}\},\ \mathfrak{F}_1^* = \{\sigma^* ; \sigma \in \mathfrak{J}(R_1, \mathfrak{F})\},$$

$$\mathfrak{H}^{(i)} = \{\tau^{(i)} ; \tau \in \mathfrak{H}\}\ (i = 1, \cdots, n), \text{ and } \mathfrak{G} = \mathfrak{F}^*(\Pi_i \mathfrak{H}^{(i)}).$$

Then $\mathfrak{F} \cong \mathfrak{F}^*$, $\mathfrak{J}(R_1, \mathfrak{F}) \cong \mathfrak{F}_1^*$, $\mathfrak{H} \cong \mathfrak{H}^{(i)}$ ($i = 1, \cdots, n$), $\mathfrak{F}^* \cap \Pi_i \mathfrak{H}^{(i)} = \{1\}$, and the product $\Pi_i \mathfrak{H}^{(i)}$ is direct. Moreover, since $\mathfrak{F}^*(\Pi_i \mathfrak{H}^{(i)}) = (\Pi_i \mathfrak{H}^{(i)})\mathfrak{F}^*$, this makes $\mathfrak{G}$ into a group. If $\sigma \in \mathfrak{F}$ and $\sigma\sigma_i \mid R_1 = \sigma_{p_i} \mid R_1$ ($i = 1, \cdots, n$) then we write $\sigma'' = \{i \rightarrow p_i ; i = 1, \cdots, n\}$. Since the above mentioned ϕ is an isomorphism, the map $\sigma \rightarrow \sigma''$ ($\sigma \in \mathfrak{F}$) is an isomorphism of $\mathfrak{F}$ into the symmetric group of permutations of $\{1, \cdots, n\}$. Hence, there exists a canonical isomorphism of $\mathfrak{G}$ into $\mathfrak{S}_n \widetilde{\times} (\times \mathfrak{H})^n$ which is defined by the following

$$\pi : (\sigma^*(\tau_1^{(1)} \cdots \tau_n^{(n)})) \longrightarrow (\sigma'', (\tau_1, \cdots, \tau_n))$$

(cf. [10, Lemma 4]). Now we write

$$T_1 = \{1 \otimes b \otimes 1 \otimes \cdots \otimes 1 ; b \in T\},$$

$$R_{11} = \{1 \otimes r_1 \otimes 1 \otimes \cdots \otimes 1 ; r_1 \in R_1\},$$

$$R_* = \{1 \otimes r \otimes 1 \otimes \cdots \otimes 1 ; r \in R\}.$$

Then A/R_* is a $\mathfrak{G}$-Galois extension, $J(\mathfrak{J}(R_{11}, \mathfrak{G}), A) = R_{11}$, $J(\mathfrak{J}(T_1, \mathfrak{G}), A) = T_1$, $\mathfrak{J}(R_{11}, \mathfrak{G}) = \mathfrak{F}_1^*(\Pi_i \mathfrak{H}^{(i)})$, $\pi(\mathfrak{J}(R_{11}, \mathfrak{G})) = [(\mathfrak{S}_{n-1} \widetilde{\times} (\times \mathfrak{H})^{n-1}) \times \mathfrak{H}]'$, $\mathfrak{J}(T_1, \mathfrak{G}) = \mathfrak{F}_1^*(\Pi_{i=2}^n \mathfrak{H}^{(i)})$, $\pi(\mathfrak{J}(T_1, \mathfrak{G})) = [\mathfrak{S}_{n-1} \widetilde{\times} (\times \mathfrak{H})^{n-1}]'$, and T_1/R_{11} is a Galois extension with Galois group $\mathfrak{J}(R_{11}, \mathfrak{G}) \mid T_1$ ($\cong \mathfrak{H}$). Moreover, for the above mentioned ψ, we see that $\psi(R)=R_*$, $\psi(R_1)=R_{11}$, and ψ is an isomorphism of the $\mathfrak{H}$-Galois extension T/R_1 into the $(\mathfrak{J}(R_{11}, \mathfrak{G})|T_1)$-Galois extension T_1/R_{11} (cf. [10, Lemma 5]). Therefore, the extension A/R_* is a desired one. This completes the proof.

By virtue of Ths. 1 and 2, we shall prove the following

Theorem 3. *Let R_1/R be a strongly separable extension with* $\text{rank}_R R_1 = n$ *and B/R_1 a strongly separable extension with $l(B/R_1)=m$. Then the extension B/R can be imbedded in a $\mathfrak{G}$-Galois extension A/R such that $J(\mathfrak{J}(R_1, \mathfrak{G}), A)=R_1$, and $\mathfrak{G}\cong\mathfrak{S}_n \tilde{\times} (\times\mathfrak{S}_m)^n$ where the subgroup $\mathfrak{J}(R_1, \mathfrak{G})$ is imbedded into $\mathfrak{S}_n \tilde{\times} (\times\mathfrak{S}_m)^n$ as the subgroup $[(\mathfrak{S}_{n-1} \tilde{\times} (\times\mathfrak{S}_m)^{n-1})\times\mathfrak{S}_m]'$.*

Proof. By Th. 1, the extension B/R_1 can be imbedded in Galois extension T/R_1 with Galois group isomorphic to the symmetric group $\mathfrak{S}_m$. Hence, by Th. 2, we obtain our desired $\mathfrak{G}$-Galois extension A/R.

Finally, we have the following theorem which will be easily seen by using the results of Ths. 2 and 3.

Theorem 4. *Let $R=R_0\subset R_1\subset\cdots\subset R_s\subset B$ a chain of subrings of B, and assume that for each $0\leqq i<s$, the extension R_{i+1}/R_i is a strongly separable extension with rank and the extension B/R_s is a strongly separable extension. Then, the extension B/R can be imbedded in a $\mathfrak{G}$-Galois extension A/R such that $J(\mathfrak{J}(R_i, \mathfrak{G}), A)=R_i$ $(i=0, 1, \cdots, s)$.*

REFERENCES

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

[2] N. BOURBAKI: Algèbre commutative, Chapitres I—II, Actualités Sci. Indust., No. 1290, Hermann, Paris, 1961.

[3] 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.

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

[5] A. MAGID: The separable Galois theory of commutative rings, Marcel Dekker, Inc., New York, 1974.

[6] A. MAGID: Principal homogeneous spaces and Galois extensions, Pacific J. Math. **53** (1974), 501—513.

[7] T. NAGAHARA: On separable polynomials over a commutative ring II, Math. J. Okayama Univ. **15** (1972), 149—162.

[8] T. NAGAHARA: On separble polynomials over a commutative ring III, Math. J. Okayama Univ. **16** (1974), 189—197.

[9] T. NAGAHARA and A. NAKAJIMA: On separable polynomials over a commutative ring IV,

Math. J. Okayama Univ. **17**(1974), 49—58.
[10] T. NAGAHARA : Imbeddings of some separable extensions in Galois extensions, Math. J. Okayama Univ. **17** (1974), 59—65.
[11] O. E. VILLAMAYOR and D. ZELINSKY : Galois theory with infinitely many idempotens, Nagoya Math. J. **35** (1969), 83—93.
[12] O. E. VILLAMAYOR : Separable algebras and Galois extensions, Osaka J. Math. **4** (1967), 161—171.

DEPARTMENT OF MATHEMATICS,
OKAYAMA UNIVERSITY

(Received January 27, 1976)

Added in proof: From the proof of Th. 1, one will easily see that the result of Th. 1 can be sharpened as follows

Theorem 1′. *Let B/R be a strongly separable extension with $l(B/R)=m$. Then, the extension B/R can be imbedded in a $\mathfrak{H}$-Galois extension T/R such that $\mathfrak{H}$ is isomorphic to the symmetric group $\mathfrak{S}_m$ (the group of permutations of $\{a_1, \cdots, a_m\}$) where $\mathfrak{J}(B, \mathfrak{H})$ is imbedded into $\mathfrak{S}_m$ as the subgroup leaving fixed the element a_1.*

In Th. 1′, we have $\mathrm{rank}_R J(\mathfrak{J}(B, \mathfrak{H}), T)=m$, and hence, if B has the rank over R then $\mathrm{rank}_R B=m$ and $J(\mathfrak{J}(B, \mathfrak{H}), T)=B$, which is the result of the Villamayor's theorem.