

IMBEDDINGS OF SOME SEPARABLE EXTENSIONS IN GALOIS EXTENSIONS

TAKASI NAGAHARA

Throughout this paper, all rings will be assumed commutative with identity element, R will mean a ring, and all ring extensions of R will be assumed with identity element 1, the identity element of R . A ring extension T/R is called strongly separable if T is a separable R -algebra which is projective as an R -module (and so, T is a finitely generated R -module). Given a set $\mathfrak{G}$ of automorphisms in a ring A and a subset T of A , we shall use the following conventions: $\mathfrak{F}(T, \mathfrak{G})$ = the subset of elements in $\mathfrak{G}$ which leave the elements of T fixed; $J(\mathfrak{G}, A)$ = the fixring of $\mathfrak{G}$ in A ; $\mathfrak{G}|T$ = the restriction of $\mathfrak{G}$ to T . Now, in [1], M. Auslander and O. Goldman proved that if T/R is a strongly separable extension such that T is a free R -module then T/R is imbedded in a Galois extension of R . In [5], G. J. Janusz proved that if T/R is a strongly separable extension such that T has no proper idempotents then T/R is imbedded in a $\mathfrak{G}$ -Galois extension A/R such that A has no proper idempotents (cf. [4], [8]). In this case, there holds that $J(\mathfrak{F}(T, \mathfrak{G}), A) = T$, and moreover, A/T and T/R have ranks in the sense of [2, Def. 2.5.2]. If, in general, A/R is a $\mathfrak{G}$ -Galois extension and T is an intermediate ring of A/R with $J(\mathfrak{F}(T, \mathfrak{G}), A) = T$ then A/T and T/R are strongly separable extensions with ranks (cf. [3, Th. 1.3, Th. 2.2, Lemma 4.1], and [2, Th. 2.5.1, Prop. 2.5.5]). In [7], the present author proved that every strongly separable extension $R[a]/R$ with rank can be imbedded in a $\mathfrak{G}$ -Galois extension A/R such that $J(\mathfrak{F}(R[a], \mathfrak{G}), A) = R[a]$.

In this paper, we shall prove the following imbedding theorems which are analogous to some of the results on Galois extensions of fields.

Theorem 1. *Let $R[a]/R$ be a strongly separable extension with rank, and $T/R[a]$ an $\mathfrak{H}$ -Galois extension. Then, the ring extension T/R can be imbedded in a $\mathfrak{G}$ -Galois extension A/R such that $J(\mathfrak{F}(T, \mathfrak{G}), A) = T$ and $\mathfrak{F}(R[a], \mathfrak{G})|T = \mathfrak{H}$.*

Theorem 2. *Let $E = R[a_1, \dots, a_s]$, and set $E_i = R[a_1, \dots, a_i]$, $i = 1, \dots, s$, and $E_0 = R$. Assume that for every $0 \leq i < s$, E_{i+1}/E_i is a strongly separable extension with rank. Then, the ring extension E/R can be*

imbedded in a $\mathfrak{G}$ -Galois extension A/R such that $A = R[a_1, \dots, a_s, a_{s+1}, \dots, a_m]$ and $J(\mathfrak{F}(R[a_1, \dots, a_t], \mathfrak{G}), A) = R[a_1, \dots, a_t]$, $t = 1, \dots, m$.

Throughout the rest of this note, let $R[a]/R$ be a strongly separable extension with rank, and $T/R[a]$ an $\mathfrak{G}$ -Galois extension. Then, by [7, Th. 1.1], there exists a separable polynomial $f(X)$ in $R[X]$ such that $R[X]/(f(X)) \cong R[a]$ ($g(X) + (f(X)) \longrightarrow g(a)$). By [6, Th. 1.1], $f(X)$ has a free splitting ring $S = R[x_1, \dots, x_n]$ where $f(X) = (X - x_1) \cdots (X - x_n)$. By [6, Th. 2.1], S is a Galois extension of R with Galois group $\mathfrak{F}$ where $\mathfrak{F}$ is isomorphic to the group of permutations of the set $\{x_1, \dots, x_n\}$ under the mapping

$$\sigma \longrightarrow \begin{pmatrix} x_1 & \cdots & x_n \\ \sigma(x_1) & \cdots & \sigma(x_n) \end{pmatrix}$$

and there holds that $J(\mathfrak{F}(R[x_i], \mathfrak{F}), S) = R[x_i]$, $i = 1, \dots, n$. Moreover, by [6, Cor. 1.1], $R[x_i]$ and $R[a]$ are R -algebra isomorphic under the mapping $g(x_i) \longrightarrow g(a)$. We shall identify $R[x_i]$ (resp. $g(x_i)$) with $R[a]$ (resp. $g(a)$). Then T is an $\mathfrak{G}$ -Galois extension of $R[x_i]$, and for each i , T is an $R[x_i]$ -algebra by virtue of the R -algebra isomorphism $R[x_i] \longrightarrow R[x_1]$ ($x_i \longrightarrow x_1$).

Now, we set $[i] = R[x_i]$, $i = 1, \dots, n$, and for any permutation

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ p_1 & p_2 & \cdots & p_n \end{pmatrix}$$

of the set $\{1, \dots, n\}$ and for any integer $m \leq n$, we consider the tensor product

$$(\cdots ((S \otimes_{[p_1]} T) \otimes_{[p_2]} T) \otimes \cdots) \otimes_{[p_m]} T$$

where $S = S_{[p_1], [p_2], \dots, [p_m]}$. Then this is an S -algebra, and which will be denoted by $S(p_1, \dots, p_m)$. Moreover, elements

$$(\cdots ((a \otimes b_1) \otimes b_2) \otimes \cdots) \otimes b_m \in S(p_1, \dots, p_m)$$

will be denoted by $a \otimes b_1 \otimes b_2 \otimes \cdots \otimes b_m$. Under this situation, we prove first the following

Lemma 1. *Let*

$$\begin{pmatrix} 1 & 2 & \cdots & m \\ p_1 & p_2 & \cdots & p_m \end{pmatrix}$$

be any permutation of the set $\{1, \dots, m\}$ ($m \leq n$). Then $S(1, \dots, m)$ is S -algebra isomorphic to $S(p_1, \dots, p_m)$ under the mapping

$$a \otimes b_1 \otimes b_2 \otimes \dots \otimes b_m \longrightarrow a \otimes b_{p_1} \otimes b_{p_2} \otimes \dots \otimes b_{p_m}.$$

Proof. For any $i < m$, we have canonical S -isomorphisms

$$\begin{aligned} S(p_1, \dots, p_{i-1}, p_i, p_{i+1}) \\ &= (S(p_1, \dots, p_{i-1}) \otimes_{[p_i]} T) \otimes_{[p_{i+1}]} T \\ &\cong T \otimes_{[p_{i+1}]} (S(p_1, \dots, p_{i-1}) \otimes_{[p_i]} T) \\ &\cong (T \otimes_{[p_{i+1}]} S(p_1, \dots, p_{i-1})) \otimes_{[p_i]} T \\ &\cong (S(p_1, \dots, p_{i-1}) \otimes_{[p_{i+1}]} T) \otimes_{[p_i]} T \\ &= S(p_1, \dots, p_{i-1}, p_{i+1}, p_i). \end{aligned}$$

Hence we obtain

$$S(p_1, \dots, p_m) \cong S(p_1, \dots, p_{i-1}, p_{i+1}, p_i, p_{i+2}, \dots, p_m).$$

Repeating such transpositions, it follows that

$$S(p_1, \dots, p_m) \cong S(1, \dots, m),$$

completing the proof.

Now we set

$$\begin{aligned} A &= S(1, \dots, n) \\ S_* &= \{a \otimes 1 \otimes 1 \otimes \dots \otimes 1 \in A; a \in S\}, \\ T_i &= \{1 \otimes b_1 \otimes \dots \otimes b_n \in A; b_j = 1 \text{ for all } j \neq i\} \end{aligned}$$

where $i = 1, \dots, n$. Then we can prove the following

Lemma 2. $S \cong S_*$, $T \cong T_i$ ($i = 1, \dots, n$) under the canonical mappings.

Proof. Since $R[x_1]$ is a direct summand of T (as $R[x_1]$ -module), the canonical mappings

$$S \longrightarrow S(1), S(1, \dots, i) \longrightarrow S(1, \dots, i+1) \quad (i = 1, \dots, n-1)$$

are injective. Hence $S \cong S_*$ under the canonical mapping. Moreover, for each $i \leq n$, the canonical mapping

$$S(i) \longrightarrow S(i, 1, \dots, i-1, i+1, \dots, n)$$

is injective. Since $R[x_i]$ is a direct summand of S (as $R[x_i]$ -module),

the canonical mapping $T \longrightarrow S(i)$ is injective. Then, by Lemma 1, it follows that $T \cong T_i$ under the canonical mapping.

Next, we shall prove the following

Lemma 3. Let $\sigma \in \mathfrak{F}$ so that $\sigma(x_i) = x_{p_i}$, $\sigma^{-1}(x_i) = x_{q_i}$ ($i = 1, \dots, n$) and τ an element in the Galois group $\mathfrak{G}$ of $T/R[x_1]$. Then

(1) there exists an R -algebra automorphism σ^* of A such that $\sigma^*(a \otimes b_1 \otimes b_2 \otimes \dots \otimes b_n) = \sigma(a) \otimes b_{q_1} \otimes b_{q_2} \otimes \dots \otimes b_{q_n}$.

(2) For each $i \leq n$, there exists an R -algebra automorphism $\tau^{(i)}$ of A such that

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

(3) $\sigma^* \tau^{(i)} = \tau^{(p_i)} \sigma^*$ and $\tau^{(i)} \rho^{(j)} = \rho^{(j)} \tau^{(i)}$ for every $\rho \in \mathfrak{G}$ where $i, j = 1, \dots, n$ and $i \neq j$.

(4) If $\tau_1, \dots, \tau_n \in \mathfrak{G}$ and $\sigma^* \tau_1^{(1)} \dots \tau_n^{(n)} = 1$ then $\sigma^* = \tau^{(1)} = \dots = \tau^{(n)} = 1$.

Proof. As is easily seen, we have an R -algebra isomorphism

$$A = S(1, \dots, n) \longrightarrow S(p_1, \dots, p_n)$$

such that

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

Then by Lemma 1, we obtain an automorphism of A such that

$$a \otimes b_1 \otimes \dots \otimes b_n \longrightarrow \sigma(a) \otimes b_{q_1} \otimes \dots \otimes b_{q_n}.$$

Thus we obtain (1). The assertion (2) is easily seen. To see (3), let $a \otimes b_1 \otimes \dots \otimes b_n$ be an arbitrary element of A , and $1 \leq i$ an integer $\leq n$. If we set $j = p_i$ then

$$\begin{aligned} \sigma^* \tau^{(i)}(a \otimes b_1 \otimes \dots \otimes b_n) &= \sigma^*(a \otimes b_1 \otimes \dots \otimes b_{i-1} \otimes \tau(b_i) \otimes b_{i+1} \otimes \dots \otimes b_n) \\ &= \sigma(a) \otimes b_{q_1} \otimes \dots \otimes b_{q_{j-1}} \otimes \tau(b_j) \otimes b_{q_{j+1}} \otimes \dots \otimes b_{q_n} \\ &= \tau^{(j)}(\sigma(a) \otimes b_{q_1} \otimes \dots \otimes b_{q_{j-1}} \otimes b_j \otimes b_{q_{j+1}} \otimes \dots \otimes b_{q_n}) \\ &= \tau^{(j)} \sigma^*(a \otimes b_1 \otimes \dots \otimes b_n). \end{aligned}$$

Thus $\sigma^* \tau^{(i)} = \tau^{(p_i)} \sigma^*$. The other half of (3) is obvious. The assertion (4) will be easily seen by using of the result of Lemma 2.

Now, for $\sigma \in \mathfrak{F}$, and for $\tau \in \mathfrak{G}$, we denote by σ^* , $\tau^{(i)}$ ($i = 1, \dots, n$) automorphisms of A as in the preceding lemma, and write

$$\begin{aligned}\mathfrak{F}^* &= \{\sigma^*; \sigma \in \mathfrak{F}\}, \quad \mathfrak{F}_1^* = \{\sigma^* \in \mathfrak{F}^*; \sigma(x_1) = x_1\}, \\ \mathfrak{G}^{(i)} &= \{\tau^{(i)}; \tau \in \mathfrak{G}\} \quad (i = 1, \dots, n), \\ \mathfrak{G} &= \text{the group generated by } \mathfrak{F}^* \cup \mathfrak{G}^{(1)} \cup \dots \cup \mathfrak{G}^{(n)}, \\ \mathfrak{G}_1 &= \text{the group generated by } \mathfrak{F}_1^* \cup \mathfrak{G}^{(2)} \cup \dots \cup \mathfrak{G}^{(n)}.\end{aligned}$$

Then, as an easy consequence of Lemmas 2 and 3, we obtain the following

- Lemma 4.** (1) $\mathfrak{F} \cong \mathfrak{F}^* (\sigma \longrightarrow \sigma^*), \mathfrak{G} \cong \mathfrak{G}^{(i)} (\tau \longrightarrow \tau^{(i)}) (i = 1, \dots, n).$
 (2) $\Pi_i \mathfrak{G}^{(i)} = \mathfrak{G}^{(1)} \times \dots \times \mathfrak{G}^{(i)} \text{ (direct product).}$
 (3) $\mathfrak{G} = \mathfrak{F}^*(\Pi_i \mathfrak{G}^{(i)}) = (\Pi_i \mathfrak{G}^{(i)}) \mathfrak{F}^* \text{ (semi-direct product), in which } \Pi_i \mathfrak{G}^{(i)} \text{ is normal.}$
 (4) $\mathfrak{G}_1 = \mathfrak{F}_1^*(\Pi_{i=2}^n \mathfrak{G}^{(i)}) = (\Pi_{i=2}^n \mathfrak{G}^{(i)}) \mathfrak{F}_1^* \text{ (semi-direct product), in which } \Pi_{i=2}^n \mathfrak{G}^{(i)} \text{ is normal.}$
 (5) $\mathfrak{G}_1 \mathfrak{G}^{(1)} = \mathfrak{G}_1 \times \mathfrak{G}^{(1)} \text{ (direct product).}$

Now, for any subset B of S , we denote by B_* the image of B under the canonical isomorphism $S \longrightarrow S_*$, and for any subset C of T , we denote by C_i the image of C under the canonical isomorphism $T \longrightarrow T_i$, where $i = 1, \dots, n$ (cf. Lemma 2). It is obvious that $R[x_1]_* = R[x_1]_1$. We write $R[x_1] = R[x_1]_*$ and $R = R_*$. Under this situation, we shall prove the following

- Lemma 5.** (1) *If C is an $R[x_1]$ -subalgebra of T and $J(\mathfrak{F}(C, \mathfrak{G}), T) = C$ then $J(\mathfrak{F}(S_* T_1 \dots T_{i-1} C_i, \mathfrak{G}), A) = S_* T_1 \dots T_{i-1} C_i, i = n, n-1, \dots, 2$. In particular, $J(\mathfrak{F}(S_* T_1, \mathfrak{G}), A) = S_* T_1$.*
 (2) *If B is an $R[x_1]$ -subalgebra of S and $J(\mathfrak{F}(B, \mathfrak{F}), S) = B$ then $J(\mathfrak{F}(B_* T_1, \mathfrak{G}), A) = B_* T_1$. In particular, $J(\mathfrak{F}(T_1, \mathfrak{G}), A) = T_1$.*
 (3) *A is a Galois extension of R with Galois group $\mathfrak{G}$.*
 (4) *T_1 is a Galois extension of $R[x_1]$ with Galois group $\mathfrak{F}(R[x_1], \mathfrak{G})|T_1$ which is isomorphic to T as Galois extension of $R[x_1]$ under the canonical mapping.*

Proof. By Lemma 4, we have the normal series

$$\begin{aligned}\mathfrak{G}^{(n)} \subset \mathfrak{G}^{(n-1)} \mathfrak{G}^{(n)} \subset \dots \subset \Pi \mathfrak{G}^{(i)} \subset \mathfrak{F}^*(\Pi \mathfrak{G}^{(i)}) = \mathfrak{G}, \text{ and} \\ \Pi_{i=2}^n \mathfrak{G}^{(i)} \subset \mathfrak{F}_1^*(\Pi_{i=2}^n \mathfrak{G}^{(i)}) = \mathfrak{G}_1.\end{aligned}$$

Then, by [3, Th. 1.3] and [4, Cor. 1.3], we obtain

$$\begin{aligned}S_* T_1 \dots T_{j-1} &= J(\mathfrak{G}^{(j)} \dots \mathfrak{G}^{(n)}, A) \quad (j = n, n-1, \dots, 2), \\ S_* &= J(\Pi \mathfrak{G}^{(i)}, A), \quad R = J(\mathfrak{G}, A), \text{ and} \\ S_* T_1 &= J(\Pi_{i=2}^n \mathfrak{G}^{(i)}, A) \supset J(\mathfrak{G}_1, A) = T_1.\end{aligned}$$

From these facts, one will easily see (1) and (2). Now, since S is $\mathfrak{F}$ -Galois over R and T is $\mathfrak{G}$ -Galois over $R[x_1]$, by [3, Th. 1.3], there exist elements $a_1, \dots, a_r, b_1, \dots, b_r$ in S and $u_1, \dots, u_s, v_1, \dots, v_s$ in T such that

$$\sum_j a_j \sigma(b_j) = \delta_{1,\sigma} \text{ (Kronecker's delta) for all } \sigma \in \mathfrak{F} \text{ and} \\ \sum_k u_k \tau(v_k) = \delta_{1,\tau} \text{ for all } \tau \in \mathfrak{G}.$$

Then we have

$$\sum_{j, k_1, \dots, k_n} (a_j)_* (u_{k_1})_1 \cdots (u_{k_n})_n \rho((v_{k_n})_n \cdots (v_{k_1})_1 (b_j)_*) = \delta_{1,\rho}$$

for all $\rho \in \mathfrak{F}^*(\Pi \mathfrak{G}^{(1)}) = \mathfrak{G}$ where $(a_j)_*, (b_j)_* \in S_*$, $j = 1, \dots, r$, $(u_{k_i})_i \in T_i$, $k_i = 1, \dots, s$ ($1 \leq i \leq n$). Hence by [3, Th. 1.3], A is $\mathfrak{G}$ -Galois over R . Thus we obtain (3). The last assertion (4) follows immediately from the fact $T_1 = J(\mathfrak{G}_1, A) \supset J(\mathfrak{G}_1 \mathfrak{G}^{(1)}, A) = R[x_1]$ and the product $\mathfrak{G}_1 \mathfrak{G}^{(1)}$ is direct (Lemma 4).

Now we are at the position to prove our theorems.

Proofs of Theorems 1 and 2. The first theorem is a easy consequence of Lemma 5 (2, 3, 4). Hence we shall prove the second theorem. Since the ring extension E/E_s is Galois, we assume that for an integer $0 < i \leq s$, the ring extension E/E_i can be imbedded in a $\mathfrak{G}_i$ -Galois extension A_i of E_i such that

$$A_i = E_i[a_{i+1}, \dots, a_s, a_{s+1}, \dots, a_{m_i}], \text{ and} \\ J(\mathfrak{G}(E_i[a_{i+1}, \dots, a_t], \mathfrak{G}_i), A_i) = E_i[a_{i+1}, \dots, a_t]$$

where $t = i + 1, \dots, m_i$. Then by Lemma 5, the ring extension A_i/E_{i-1} can be imbedded in a $\mathfrak{G}_{i-1}$ -Galois extension A_{i-1} of E_{i-1} such that

$$A_{i-1} = E_{i-1}[a_i, \dots, a_s, a_{s+1}, \dots, a_{m_i}, \dots, a_{m_{i-1}}], \text{ and} \\ J(\mathfrak{G}(E_{i-1}[a_i, \dots, a_t], \mathfrak{G}_{i-1}), A_{i-1}) = E_{i-1}[a_i, \dots, a_t]$$

where $t = i, \dots, m_{i-1}$. This argument enables us to obtain the theorem.

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, Herman, 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] F. DEMEYER: Separable algebras over commutative rings, Lecture notes in Math., No. 181, Springer, Berlin, 1971.

- [5] G. J. JANUSZ : Separable algebras over commutative rings, Trans. Amer. Math. Soc., **122** (1966), 461—479.
- [6] T. NAGAHARA : On separable polynomials over a commutative rings II, Math. J. Okayama Univ., **15** (1972), 149—162.
- [7] T. NAGAHARA : On separable polynomials over a commutative rings III, Math. J. Okayama Univ., **16** (1974), 189—197.
- [8] T. NAGAHARA : An imbedding theorem for separable algebras, Proc. Amer. Math. Soc., **41** (1973), 399—402.

DEPARTMENT OF MATHEMATICS,
OKAYAMA UNIVERSITY

(Received August 17, 1973)