Math. J. Okayama Univ. 35(1993), 147-154

ON GALOIS EXTENSIONS OF POLYNOMIAL TYPE OF RINGS

Dedicated to Professor Kazuo Kishimoto on his 60th birthday

TAKASI NAGAHARA

In this note, we shall present some Galois theory for a special type of Galois extensions of rings which is contributive by means of that the discussions are simple and useful, where rings mean associative rings which are not necessarily commutative. In fact, the ring extensions in [5]–[9] are Galois extensions of our type. Some parts of discussions in their papers is simplified by applications of our results (cf. [7, Theorem 4, Lemma 13 and Theorem 14], [8, Theorem 1.2], [9, Theorem 1.2], and etc.). As is well known, in [1] and [4] we can see elegant deliverances of Galois theory of fields. On the other hand, restricting the proofs of our results to field extensions, we obtain an alternatively simple proof of the fundamental theorem in Galois theory of fields (cf. [1, Theorem 14, Corollary 1, Corollary 2 and Theorem 16], [4, p. 16, Theorem 10 and Theorem 11] and Remark 2).

Throughout this paper, let A be a ring with identity element 1, and G a finite group of ring automorphisms of A. Moreover, for a subset S of A and a subset H of G, we shall use the following conventions:

$A(H) = \{a \in A;\ \sigma(a) = a \text{ for all } \sigma \in H\}$.
$G(S) = \{\sigma \in G;\ \sigma(a) = a \text{ for all } a \in S\}$.
$H|S$ =the restriction of H to S.
$|H|$ =the cardinality of H.
$U(S)$ =the set of inversible elements in S when S is a subring with 1.
$[G : H]$ =the index of H in G when H is a subgroup.

For $B = A(G)$, the ring extension A/B will be called a *Galois extension of polynomial type with respect to* (G, F) if there exists a subset F of A such that $F \ni 0$, $A = B[F]$, $\alpha\sigma(\alpha) = \sigma(\alpha)\alpha$ for all σ in G, and $\{\alpha - \sigma(\alpha);\ \sigma \in G\} \subset U(A) \cup \{0\}$ for each $\alpha \in F$, where F is not necessarily finite.

Our purpose of this note is to prove the following

Theorem. *Let A/B be a Galois extension of polynomial type with respect to (G, F). Then, there holds the following*

(i) *For any subset S of F, $A(G(B[S])) = B[S]$.*

(ii) *For any subgroup H of G, $G(A(H)) = H$.*

(iii) *A is a finite left (and right) free B-module of rank $|G|$.*

Now, we shall start at the following lemma which plays an essential rôle in our study.

Lemma 1. *Let $B = A(G)$, and α a non-zero element of A such that*

$$\alpha\sigma(\alpha) = \sigma(\alpha)\alpha \text{ for all } \sigma \text{ in } G, \text{ and}$$
$$\{\alpha - \sigma(\alpha);\ \sigma \in G\} \subset U(A) \cup \{0\}.$$

Let $m = [G:\ G(B[\alpha])]$. Then

(i) *$A(G(B[\alpha])) = B[\alpha]$.*

(ii) *$B[\alpha] = B + B\alpha + \cdots + B\alpha^{m-1} = B + \alpha B + \cdots + \alpha^{m-1}B$, and $1,\ \alpha,\ \alpha^2, \cdots,\ \alpha^{m-1}$ are linearly left (and right) independent over B.*

(iii) *If G_0 is a subgroup of G such that $A(G_0) = B$ then*

$$[G_0:\ G_0(B[\alpha])] = m.$$

(iv) *There are elements $y_1,\ y_2, \cdots,\ y_m$ in $B[\alpha]$ such that*

$$\sum_{i=1}^{m} \alpha^{m-i}\sigma(y_i) = \delta_{1,\ \sigma|B[\alpha]} \text{ for all } \sigma \text{ in } G,$$

where $\delta_{1,\ \sigma|B[\alpha]} = 0$ (resp. $= 1$) if $\sigma|B[\alpha] \neq 1$ (resp. $= 1$ (identity map)).

Proof. We set $H = G(B[\alpha])$, and $G = \sigma_1 H \cup \cdots \cup \sigma_m H$ (disjoint) where $\sigma_1 = 1$. Then $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ for all pair $i \neq j$. Moreover, we set

$$\begin{aligned}\{\sigma(\alpha);\ \sigma \in G\} &= \{\alpha_1 = \sigma_1(\alpha) = \alpha,\ \alpha_2 = \sigma_2(\alpha), \cdots,\ \alpha_m = \sigma_m(\alpha)\},\\ f(X) &= (X - \alpha_1)\cdots(X - \alpha_m)\\ &= X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0, \text{ and}\\ g(X) &= (X - \alpha_2)\cdots(X - \alpha_m)\\ &= X^{m-1} + b_{m-2}X^{m-2} + \cdots + b_1X + b_0.\end{aligned}$$

By E, we denote the commutative subring of A generated by $1,\ \alpha_1, \cdots,\ \alpha_m$. Then, since the a_i are the elementary symmetric polynomials of $\alpha_1, \cdots,\ \alpha_m$, we have that $a_i \in A(G) \cap E = B \cap E$ $(i = 0,\ 1, \cdots,\ m-1)$.

Noting $f(X) \in (B \cap E)[X]$ and $f(\alpha_1) = 0$, it is easily seen that $f(X) = (X - \alpha_1)h(X)$ in the polynomial ring $((B \cap E)[\alpha_1])[X]$. Since $g(X)$, $h(X) \in E[X]$ and $X - \alpha_1$ is not a zero divisor in $E[X]$, we have $g(X) = h(X)$, that is, $b_i \in (B \cap E)[\alpha_1]$ $(i = 0, 1, \cdots, m-2)$. Now, we set

$$\delta = g(\alpha_1) = \alpha_1^{m-1} + b_{m-2}\alpha_1^{m-2} + \cdots + b_1\alpha_1 + b_0, \text{ and}$$
$$B_0 = A(H) \ (\supset B[\alpha_1]).$$

Then $\delta \in B[\alpha_1] \cap U(A) \subset B_0 \cap U(A) = U(B_0)$ and so $\delta^{-1} \in B_0$. Hence

$$\alpha_1^{m-1}\delta^{-1} + \alpha_1^{m-2}(b_{m-2}\delta^{-1}) + \cdots + \alpha_1(b_1\delta^{-1}) + b_0\delta^{-1} = 1, \text{ and}$$
$$b_i\delta^{-1} \in B_0 \ (i = 0, 1, \cdots, m-2).$$

We put here

$$x_1 = \alpha_1^{m-1}, \ x_2 = \alpha_1^{m-2}, \ \cdots, \ x_{m-1} = \alpha_1, \ x_m = 1, \text{ and}$$
$$y_1 = \delta^{-1}, \ y_2 = b_{m-2}\delta^{-1}, \cdots, \ y_{m-1} = b_1\delta^{-1}, \ y_m = b_0\delta^{-1}.$$

Then $\Sigma_{i=1}^m x_i y_i = 1$ $(x_i \in B[\alpha_1], \ y_i \in B_0)$. Let σ be an element of G such that $\sigma|B[\alpha_1] \neq 1$ (identity map). Since $G = \sigma_1 H \cup \cdots \cup \sigma_m H$ (disjoint), it follows that $\alpha_1 \in \{\sigma(\alpha_2), \cdots, \sigma(\alpha_m)\}$ and so

$$\textstyle\sum_{i=1}^m x_i\sigma(y_i) = (\alpha_1 - \sigma(\alpha_2)) \cdots (\alpha_1 - \sigma(\alpha_m))\sigma(\delta^{-1}) = 0.$$

Therefore, we obtain

$$\textstyle\sum_{i=1}^m x_i\sigma(y_i) = \delta_{1,\,\sigma|B[\alpha_1]} \text{ for each } \sigma \text{ in } G.$$

where $\delta_{1,\,\sigma|B[\alpha_1]} = 0$ (resp.=1) if $\sigma|B[\alpha_1] \neq 1$ (resp.=1). Let t be the map of B_0 into A defined by setting

$$t(a) = \sigma_1(a) + \cdots + \sigma_m(a) \ (a \in B_0).$$

Then, for any a in B_0, we have

$$\begin{aligned}\textstyle\sum_{i=1}^m x_i t(y_i a) &= \textstyle\sum_{j=1}^m (\sum_{i=1}^m x_i\sigma_j(y_i a)) \\ &= \textstyle\sum_{j=1}^m (\sum_{i=1}^m x_i\sigma_j(y_i))\sigma_j(a) = a.\end{aligned}$$

Since $G(B_0) = H$, we have $\sigma(t(a)) = t(a)$ for all $\sigma \in G$ and $a \in B_0$. This implies that $t(a) \in B$ for each $a \in B_0$. Particularly $y_i a \in B_0$ and $t(y_i a) \in B$ for each $a \in B_0$. Since $x_i = \alpha_1^{m-i}$, it follows that

$$B_0 \subset \textstyle\sum_{i=1}^m x_i B = \sum_{i=0}^{m-1} \alpha_1^i B \subset B[\alpha_1] \subset B_0 = A(H).$$

This proves (i). Next, we shall prove that $1, \alpha_1, \cdots, \alpha_1^{m-1}$ are linearly right independent over B. We assume $\sum_{i=0}^{m-1} \alpha_1^i a_i = 0$ $(a_i \in B)$. Then

$$\sum_{i=0}^{m-1} \sigma_j(\alpha_1)^i a_i = 0 \text{ for } j = 1, \cdots, m.$$

Since the $m \times m$ matrix $(\sigma_j(\alpha_i)^i)$ is non-singular, we obtain $a_i = 0$ for $i = 0, 1, \cdots, m-1$. Symmetrically, it is seen that $B[\alpha_1] = \sum_{i=0}^{m-1} B\alpha_1^i$ and $1, \alpha_1, \cdots, \alpha_1^{m-1}$ are linearly left independent over B. Thus, we obtain (ii). To see (iii), we set $E_0 = B \cap E$. Then by (ii), we have

$$E_0[\alpha_1] = E_0 + \alpha_1 E_0 + \cdots + \alpha_1^{m-1} E_0,$$

and $1, \alpha_1, \cdots, \alpha_1^{m-1}$ are linearly right independent over E_0. Next, for G_0 given in our lemma, we set $n = [G_0 : G_0(B[\alpha_1])]$ $(\alpha_1 = \alpha)$. Then by (ii), we also have

$$E_0[\alpha_1] = E_0 + \alpha_1 E_0 + \cdots + \alpha_1^{n-1} E_0,$$

and $1, \alpha_1, \cdots, \alpha_1^{n-1}$ are linearly independent over E_0. Since $E_0[\alpha_1]$ is a commutative ring, the lengths of free E_0-bases of $E_0[\alpha_1]$ are uniquely determined. Hence it follows that $m = n$ and so $[G_0 : G_0(B[\alpha_1])] = m$.

Lemma 2. *Let $B = A(G)$, and F a finite subset of A such that $F \not\ni 0$,*

$$\beta\sigma(\beta) = \sigma(\beta)\beta \text{ for all } \sigma \in G, \text{ and}$$
$$\{\beta - \sigma(\beta);\ \sigma \in G\} \subset U(A) \cup \{0\}$$

for each β in F. Then

(i) $A(G(B[F])) = B[F]$. *If $G(B[F]) = \{1\}$ then $B[F] = A$.*

(ii) *If G_0 is a subgroup of G containing $G(B[F])$ then $G(A(G_0)) = G_0$, and in case $A(G_0) = B$, G_0 coincides with G.*

(iii) *Let $F = \{\beta_1, \cdots, \beta_r\}$, $m_1 = [G : G(B[\beta_1])]$, and*
$$m_i = [G(B[\beta_1, \cdots, \beta_{i-1}]) : G(B[\beta_1, \cdots, \beta_i])]$$
for $i = 2, \cdots, r$. Then $B[F]$ has a right (resp. left) free B-basis

$$\{\beta_r^{s_r} \cdots \beta_1^{s_1};\ 0 \leqq s_i \leqq m_i - 1,\ 1 \leqq i \leqq r\}$$
$$(\text{resp. } \{\beta_1^{s_1} \cdots \beta_r^{s_r};\ 0 \leqq s_i \leqq m_i - 1,\ 1 \leqq i \leqq r\}).$$

which consists of $[G : G(B[F])]$ elements.

Proof. (i). For a subset S of F, we set $H = G(B[S])$, and assume $A(H) = B[S]$, which holds for the case $S = \emptyset$ (empty). Since $H \subset G$, it follows from Lemma 1(i) that

$$A(G(B[S, \beta])) = A(G(B[S][\beta])) = A(H(B[S][\beta])) = B[S][\beta] = B[S, \beta].$$

for any $\beta \in F$. Hence by induction methods, we obtain $A(G(B[F])) = B[F]$. (ii). We set $B = B_0$ and $B_i = B[\beta_1, \cdots, \beta_i]$ $(1 \leqq i \leqq r)$. Then $B_i = B_{i-1}[\beta_i]$ $(1 \leqq i \leqq r)$. Now, for G_0 given in our Lemma, we assume that $A(G_0) = B$ and

$$G_0(B_t) = G(B_t) \text{ for some } t \leqq r,$$

which holds for the case $t = r$ by our assumption. By (i), we have

$$A(G_0(B_{t-1})) = B_{t-1} = A(G(B_{t-1})), \text{ and } G_0(B_{t-1}) \subset G(B_{t-1}).$$

Hence by Lemma 1(iii), we have

$$[G_0(B_{t-1}) : G_0(B_t)] = [G(B_{t-1}) : G(B_t)].$$

Therefore, it follows that $G_0(B_{t-1}) = G(B_{t-1})$. Hence by induction methods, we obtain $G_0 = G_0(B) = G(B) = G$. From this, (i) and Lemma 1(ii), the other assertions will be easily seen.

Now, we are at the position to prove our theorem.

The Proof of Theorem. Let S be an arbitrary subset of F. Since G is a finite group, there is a finite subset S_0 in S such that $G(B[S_0]) = G(B[S])$. Then by Lemma 2, we have

$$B[S_0] = A(G(B[S_0])) = A(G(B[S])) \supset B[S] \supset B[S_0].$$

Hence we obtain $B[S_0] = A(G(B[S])) = B[S]$. In particular, $A = B[F] = B[F_0]$ for some finite subset F_0 of F. The other assertions follow from Lemma 2 immediately.

Corollary 3. *Let A/B be a Galois extension of polynomial type with respect to (G, F). Then, the extension A/B has a G-Galois coordinate system, that is, there are elements $a_1, \cdots, a_s$; $b_1, \cdots, b_s$ in A such that $\sum_{i=1}^{s} a_i \sigma(b_i) = \delta_{1,\sigma}$ for all σ in G. Hence A/B is a G-Galois extension which is separable in the sense of* [10].

Proof. As in the proof of Theorem, we have $A = B[F_0]$ for some finite subset F_0 of F. We set $F_0 = \{\beta_1, \cdots, \beta_r\}$, $B_0 = B$, and $B_j = B[\beta_1, \cdots, \beta_j]$ $(1 \leqq j \leqq r)$. Applying Lemma 1(iv) and Lemma 2(i) to the extensions A/B_{j-1} and B_j/B_{j-1}, we see that there is a finite subset $\{x_i^{(j)}, y_i^{(j)}; i = 1, \cdots, m_j\}$ in B_j such that

$$\sum_{i=1}^{m_j} x_i^{(j)} \sigma(y_i^{(j)}) = \delta_{1, \sigma|B_j} \quad \text{for all} \quad \sigma \in G(B_{j-1}).$$

We set here

$$a(i_r, \cdots, i_1) = x_{i_r}^{(r)} \cdots x_{i_1}^{(1)}, \text{ and } b(i_1, \cdots, i_r) = y_{i_1}^{(1)} \cdots y_{i_r}^{(r)}$$

where $1 \leqq i_j \leqq m_j$ and $j = 1, \cdots, r$. Then, it is easily seen that

$$\sum_{i_j} a(i_r, \cdots, i_1)\sigma(b(i_1, \cdots, i_r)) = \delta_{1, \sigma} \quad \text{for all} \quad \sigma \in G.$$

where i_j (resp. j) runs over all the $1 \leqq i_j \leqq m_j$ (resp. $1 \leqq j \leqq r$). Hence A/B is a G-Galois extension (cf. [10, p. 116]). Since B is a direct summand of B-module A, A/B is a separable extension (cf. [3, Proposition. 3.4]).

Remark 1. The result of Theorem (ii) follows from [10, Proposition 2.2] and Corollary 3. If A is commutative and A/B is a Galois extension of polynomial type with respect to (G, F) then, by Corollary 3 and [2, pp. 22–23, Theorem 2.2], there exists a 1-1 dual corespondence between the set of G-strong separable B-subalgebras of A and the set of subgroup of G in the usual sense of Galois theory.

Remark 2. Let K be a (commutative) field, and G a finite group of automorphisms of K. Then, since $K = K(G)[U(K)]$, $K/K(G)$ is a Galois extension of polynomial type with respect to $(G, U(K))$. Hence, it follows from Theorem that $K(G(B_0)) = B_0 (= K(G)[U(B_0)])$ for any intermediate field B_0 of $K/K(G)$. Therefore, the result of Theorem directly contains the fundamental theorem in Galois theory of fields. Moreover, from the proof of Lemma 1, it is easily seen that there are elements $\beta_1, \cdots, \beta_s \in K$ and a polynomial $h(X) \in K(G)[X]$ such that $\beta_i \neq \beta_j$ for each $i \neq j$, $K = K(G)[\beta_1, \cdots, \beta_s]$ and $h(X) = (X - \beta_1) \cdots (X - \beta_s)$.

Next, we shall present an example. Let B be a field, and X an indeterminate. For $f(X) \in B[X]$, $f(X)$ will be called to be *separable* if $f(X)B[X] + f'(X)B[X] = B[X]$, where $f'(X)$ is the derivative of $f(X)$. As

is easily seen, the above $h(X)$ is separable over $K(G)$. To see the converse, let $f(X)$ be a separable plynomial in $B[X]$, and $K = B[\alpha_1, \cdots, \alpha_n]$ a splitting field of $f(X)$, that is, K is a field and $f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$. Now, by making use of our theorem, we shall prove that the extension K/B is Galois. Let $X_1, \cdots, X_n$ be indeterminates and consider the homomorphism

$$\varphi : B[X_1, \cdots, X_n] \to B[\alpha_1, \cdots, \alpha_n] \ (X_i \to \alpha_i, \ 1 \leqq i \leqq n).$$

We set $M = \ker\varphi$ and $f(X) = X^n + a_1 X^{n-1} \cdots + a_{n-1} X + a_n$. Moreover, let $s_1, \cdots, s_n$ be the elementary symmetric polynomials of $X_1, \cdots, X_n$ where $\deg s_i = i$, $1 \leqq i \leqq n$. Then $s_i - a_i \in M$ for $i = 1, \cdots, n$. Let S_n be the group of B-automorphisms of $B[X_1, \cdots, X_n]$ induced by permutations of $X_1, \cdots, X_n$, and $\{\sigma(M);\ \sigma \in S_n\} = \{M_1 = M, M_2, \cdots, M_m\}$ where $M_i \neq M_j$ for each $i \neq j$. We set here $I = M_1 \cap \cdots \cap M_m$, $A = B[X_1, \cdots, X_n]/I$ (the ring of residue classes modulo I), and $\beta_i = X_i + I$ for $i = 1, \cdots, n$. Then $I \cap B = \{0\}$, $s_i - a_i \in I$ for $i = 1, \cdots, n$, and $f = (X - \beta_1) \cdots (X - \beta_n)$. Since $f(X)$ is separable, we have $f'(\beta_i) B[\beta_i] = B[\beta_i] \subset A$ for $i = 1, \cdots, n$, and $\beta_i - \beta_j \in U(A)$ for each $i \neq j$. Hence the group G of automorphisms of A induced by S_n is of order $n!$, and $A/A(G)$ is a Galois extension of polynomial type with respect to $(G, \{\beta_1, \cdots, \beta_n\})$, where $n! = n(n-1) \cdots 2 \cdot 1$. Applying our theorem to this extension, we obtain $[A : B] = |G|[A(G) : B] = n![A(G) : B]$. On the other hand, we have

$$f(X) = (X - \beta_1) \cdots (X - \beta_s) f_s(X) \in B[\beta_1, \cdots, \beta_s][X], \text{ and } f_s(\beta_{s+1}) = 0$$

where $s = 1, \cdots, n-1$. Since $A = B[\beta_1, \cdots, \beta_n]$, one will easily see that $[A : B] \leqq n!$. Therefore, it follows that $[A : B] = n!$ and $[A(G) : B] = 1$, that is, $A(G) = B$. Now, since the ideals M_i in $B[X_1, \cdots, X_n]$ are maximal, by the chinease remainder theorem, we have

$$A \cong B[X_1, \cdots, X_n]/M_1 \oplus \cdots \oplus B[X_1, \cdots, X_n]/M_m$$

Hence $A = Ae_1 \oplus \cdots \oplus Ae_m$ where $\{e_1, \cdots, e_m\}$ is the set of primitive idempotents of A and the Ae_i/Be_i are field extensions. We set $\{\sigma(e_1);\ \sigma \in G\} = \{\sigma_1(e_1) = e_1, \sigma_2(e_1), \cdots, \sigma_t(e_1)\}$ $(\subset \{e_1, \cdots, e_m\})$ and $e = \sigma_1(e_1) + \cdots + \sigma_t(e_1)$, where $\sigma_1 = 1$ (identity map) and $\sigma_i(e_1) \neq \sigma_j(e_1)$ if $i \neq j$. Then $\sigma(e) = e$ for all $\sigma \in G$ and so $e \in B$ which implies $e = 1$ and $t = m$. We set $G(\{e_1\}) = G_1$, and $b = \sigma_1(a_1) + \cdots + \sigma_m(a_1)$ for an arbitrary element

$a_1 \in Ae_1(G_1|Ae_1)$. Then, noting $G = \sigma_1 G_1 \cup \cdots \cup \sigma_m G_1$ (disjoint), We have $\sigma(b) = b$ for all $\sigma \in G$, whence $b \in B$ and so $a_1 = be_1 \in Be_1$. Hence $Ae_1(G_1|Ae_1) = Be_1$, and Ae_1/Be_1 is a Galois extension. Now, we consider the B-algebra homomorphism

$$\psi : A = B[\beta_1, \cdots, \beta_n] \to K = B[\alpha_1, \cdots, \alpha_n] \ (\beta_i \to \alpha_i, \ 1 \leqq i \leqq n).$$

Then $B[\alpha_1, \cdots, \alpha_n] \cong A/\ker\psi \cong Ae_i$ (as B-algebras) for some i ($1 \leqq i \leqq n$). Since $\sigma_i^{-1}(Ae_i) = Ae_1$, it follows that K/B is a Galois extension.

REFERENCES

[1] E. ARTIN: Galois Theory, Notre Dame Math. Lec. No. 2(1959), Notre Dame Univ. Press.

[2] 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.

[3] K. HIRATA and K. SUGANO: On semisimple extensions and separable extensions over non-commutative rings, J. Math. Soc. Japan **18**(1966), 360–373.

[4] I. KAPLANSKY: Fields and Rings, Chicago Lec. in Math. (1970), The Univ. of Chicago Press.

[5] I. KIKUMASA and T. NAGAHARA: Primitive elements of Galois extensions of finite fields, Proc. Amer. Math. Soc. **115**(1992), 593–600.

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

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

[8] T. NAGAHARA and A. NAKAJIMA: On cyclic extensions of commutative rings, Math. J. Okayama Univ. **15**(1971), 81–90.

[9] T. NAGAHARA and A. NAKAJIMA: On strongly cyclic extensions of commutative rings, Math. J. Okayama Univ. **15**(1971), 91–100.

[10] Y. MIYASHITA: Finite outer Galois theory of non-commutative rings, J. Fac. Sci. Hokkaido Univ., Ser I, **19**(1966), 114–134.

DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE, OKAYAMA UNIVERSITY
OKAYAMA 700, JAPAN

(Received November 5, 1991)