A NOTE ON GALOIS THEORY OF COMMUTATIVE RINGS

TAKASI NAGAHARA[1]

In [4], S. U. Chase, D. K. Harrison, and Alex Rosenberg succeeded in constructing a finite Galois theory of commutative rings.

This paper is about an infinite Galois extension of commutative rings, for which we shall present a corresponding generalization of the Fundamental Theorem of Galois theory. The main results of this paper have been announced in Notices Amer. Math. Soc. **11** (1964), 569. Recently, from Dr. G. J. Janusz we heard that he has obtained many important results for separable algebras over commutative rings, and so in our study we shall refer to his paper [5] to appear, too.

Throughout the present paper, S will be a ring with the identity element 1, and R a subring of S containing the identity element 1 of S. As to notations and terminologies used in this paper we follow [2] and [4].

Recently, O. Villamayor has proved the following theorem which is useful in our study, and he kindly permitted me to cite the proof here.

VILLAMAYOR'S THEOREM. *Let S be a separable R-algebra and a projective R-module, then S is a finitely generated R-module.*

PROOF. Let $\{p_i\} \subset S$, : $\{\pi_i\} \subset \mathrm{Hom}_R(S, R)$ be a projective coordinate system for S over R. Then π_i extends naturally to $\pi_i^* \in \mathrm{Hom}_{1\otimes S}(S\otimes S, S)$ and $\{p_i\otimes 1\}$, $\{\pi_i^*\}$ form a projective coordinate system for $S\otimes S$ over $1\otimes S$. For every $v \in S\otimes S$, $v = \sum_{\text{finite}}(p_i\otimes 1)\pi_i^*(v)$. If ϵ: $S\otimes S \to S$ is the contraction, then

$$\epsilon(v) = \sum_{p_i} \pi_i^*(v).$$

Now, let $1 \to u \in S\otimes S$ under the splitting map $S \to S\otimes S$, so $ux = xu$ for every $x \in S$ and $\epsilon(ux) = \epsilon(u)x = x$. But

$$\begin{aligned}\{i;\ \pi_i^*(xu) \neq 0\} &= \{i;\ \pi_i^*(ux) \neq 0\} \\ &= \{i;\ \pi_i^*(u)x \neq 0\} \\ &\subset \{i;\ \pi_i^*(u) \neq 0\},\end{aligned}$$

Presented to the Society, July 2, 1964; received by the editors July 22, 1965.

[1] This work was supported in part by the NSF Grant GP 1649.

which is a fixed finite set I. Hence

$$x = \epsilon(xu) = \sum_I p_i\pi_i^*(xu) = \sum_I \sum_{j=1}^n p_i\pi_i(xa_j)b_j$$

where $u = \sum_j a_j \otimes b_j$. Since R is the center of S, $\{p_ib_j\}$ generates S over R. This completes the proof.

First, we shall prove the following theorem whose proof is partially similar to that of [4, Theorem 3.5 and Theorem 1.3].

THEOREM 1. *Let S be a commutative ring with no idempotents other than 0 or 1. If R' is a finitely generated separable R-subalgebra of S such that $R \subset S^G \subset R'$ for a group of automorphisms of S and if we set $R'' = S^G$ (where S^G means fixed ring of G in S) then:*

(i) *The number $\#(G|R')$ of restrictions $G|R'$ of G to R' is finite.*

(ii) *R' is a projective R''-algebra.*

(iii) *$S^H = R'$ for $H = \{\sigma \in G;\ \sigma|R' = 1\}$.*

(iv) *If $G|R' = \{\sigma_1', \cdots, \sigma_n'\}$ $(n = (G:H))$, set $M = \sum_1^n \sigma_i' S$ (direct sum) where $r'\sigma_i' = \sigma_i' \cdot \sigma_i'(r')$ for every $r' \in R'$. Then, M is R'-S-isomorphic to $\mathrm{Hom}_{R''}(R', S)$ under the mapping $r'\sigma_i' s (r' \in R',\ s \in S) \to (r'\sigma_i' s)(x) = (\sigma_i'(xr'))s$ $(x \in R')$.*

(v) *If G^* is the set of R''-(algebra) automorphisms of S, then $G^*|R' = G|R'$.*

PROOF. Let $k: R' \otimes_R R' \to R'$ denote the contraction mapping defined by $k(x \otimes y) = xy$, and let $J = \ker(k)$. Since R' is R-separable, $R' \otimes_R R' = (R' \otimes R')e + J$ (direct sum), where $e^2 = e = \sum_1^r x_i \otimes y_i$, $eJ = 0$, and $(R' \otimes R')e$ is $R' \otimes R'$-isomorphic to R' $(e \to 1)$. Moreover, from $(R' \otimes_R R') \otimes_{R'} S = R' \otimes_R S$, we have that $R' \otimes_R S = (R' \otimes_R S)e + (R' \otimes_R S)(1-e)$ (direct sum) and $(R' \otimes_R S)e$ is $R' \otimes_R S$-isomorphic to S. By k^* we denote the mapping $R' \otimes_R S \to S$. Since S has no nontrivial idempotents, it follows that e is a minimal idempotent in $R' \otimes_R S$. Now, let $\sigma \in G$. Then $(1 \otimes \sigma)(e) = \sum_1^r x_i \otimes \sigma(y_i)$ is a minimal idempotent in $R' \otimes_R S$. If $(1 \otimes \sigma)(e) = e$ then, for any $x \in R'$, $x = xk^*(e) = xk^*[(1 \otimes \sigma)(e)] = k^*[(1 \otimes \sigma)(xe)] = k^*[(1 \otimes \sigma)(ex)] = k^*[(1 \otimes \sigma)(e)]\sigma(x) = k^*(e)\sigma(x) = \sigma(x)$ and so $\sigma|R' = 1$. Hence, for $\tau \in G$, $(1 \otimes \sigma)(e) \neq (1 \otimes \tau)(e)$ if and only if $\sigma|R' \neq \tau|R'$, and then $(1 \otimes \sigma)(e)$ and $(1 \otimes \tau)(e)$ are orthogonal. If $(1 \otimes \sigma)(e) \neq e$ then $(1 \otimes \sigma)(e)$ lies in $(R' \otimes_R S)(1-e) = \ker(k^*)$; and so, $\sum_1^r x_i\sigma(y_i) = k^*[(1 \otimes \sigma)(e)] = 0$. Moreover $(R' \otimes_R S)[(1 \otimes \sigma)(e)]$ is isomorphic to S as R-algebra, and for distinct elements $\sigma_1|R', \cdots, \sigma_n|R'$ of $G|R'$,

$$\sum_1^n (R' \otimes_R S)[(1 \otimes \sigma_i)(e)] \quad (\subset R' \otimes_R S)$$

is a direct sum, and this is a direct summand of $R' \otimes_R S$. Hence, it follows that $\#(G|R') < \infty$ (cf. [3, Corollaire 2, p. 132 and Remarque, p. 141]), and

$$\sum_1^r x_i\sigma(y_i) = 1 \quad \text{if} \quad \sigma|R' = 1,$$
$$= 0 \quad \text{if} \quad \sigma|R' \neq 1.$$

If $G|R' = \{\sigma_1|R', \cdots, \sigma_n|R'\}$ $(n = (G:H)$, where $H = \{\sigma \in G; \sigma|R' = 1\})$, we set $t(x) = \sum_j \sigma_j(x)$ for all $x \in R'$. Then it is clear that $\sigma(t(x)) = t(x)$ for any $\sigma \in G$, and so $t(x) \in R''$ $(= S^G)$ (note that $G = \bigcup_j \sigma_j H$ (disjoint)). Now we may define R''-homomorphisms f_i: $R' \to R''$ by $f_i(x) = t(xy_i)$ $(i \leqq r, x \in R')$. Then, for all $x \in R'$,

$$\sum_i f_i(x)x_i = \sum_{i,j} \sigma_j(xy_i)x_i = \sum_{i,j} \sigma_j(x)\sigma_j(y_i)x_i$$
$$= \sum_j \sigma_j(x)\left(\sum_i \sigma_j(y_i)x_i\right) = x.$$

Hence, $x_1, \cdots, x_r$ in R' and $f_1, \cdots, f_r$ in $\mathrm{Hom}_{R''}(R', R'')$ form a projective coordinate system for R' as R''-module. Therefore R' is a projective R''-algebra.

Set $R^* = S^H$, and set $t^*(x) = \sum_j \sigma_j(x)$, $f_i^*(x) = t^*(xy_i)$ for $i \leqq r$ and all $x \in R^*$. Then f_i^* is a R''-homomorphism of R^* into R'' and $\sum_i f_i^*(x)x_i = x$ $(x \in R^*)$. Hence we have $R^* = R'$.

If $\tau \in \{\sigma_1, \cdots, \sigma_n\}$ and $t = \sum_j \sigma_j$ $(\in M)$, then

$$\sum_i y_i t \cdot \tau(x_i) = \sum_i \left(\sum_j \sigma_j \cdot \sigma_j(y_i)\tau(x_i)\right)$$
$$= \sum_{i,j} \sigma_j \cdot (\sigma_j(y_i)\tau(x_i))$$
$$= \sum_{i,j} \sigma_j \cdot \tau(\tau^{-1}\sigma_j(y_i)x_i)$$
$$= \sum_j \sigma_j \cdot \tau\left(\sum_i \tau^{-1}\sigma_j(y_i)x_i\right) = \tau$$

and

$$\sum_i y_i t \cdot (\tau + \tau')(x_i) = \tau + \tau' \qquad (\tau' \in \{\sigma_i\})$$

and, for all $x \in S$,

$$\sum_i y_i t \cdot (\tau x)(x_i) = \sum_i y_i t \cdot \tau(x_i)x = \tau x.$$

Hence, we have $u=\sum_i y_i t\cdot u(x_i)$ for any u in M. If $u(R')=0$, then $u=0$, and so $M\to \mathrm{Hom}_{R'}(R', S)$ is a monomorphism. On the other hand, if h is in $\mathrm{Hom}_{R'}(R', S)$, set $u=\sum_i y_i t\cdot h(x_i)$ $(\in M)$. We then have for all $x\in R'$ that

$$u(x) = \sum_i t(xy_i)h(x_i) = \sum_i f_i(x)h(x_i)$$

$$= h\left(\sum_i f_i(x)x_i\right) = h(x).$$

Hence $M\to \mathrm{Hom}_{R'}(R', S)$ is an isomorphism.

Finally we shall prove our last assertion (v). We set $G^*|R' = \{\sigma_1^*, \cdots, \sigma_m^*\}$ $(m=(G^*: H^*)$, where $H^*=\{\sigma\in G^*;\ \sigma|R'=1\})$. Then $\{\sigma_1', \cdots, \sigma_n'\}\subset\{\sigma_1^*, \cdots, \sigma_m^*\}$ $(n\leqq m)$. Moreover, by (iv), we have $\sum_1^n \sigma_i' S$ (direct sum)$\cong \mathrm{Hom}_{R'}(R', S)\cong \sum_1^m \sigma_i^* S$ (direct sum). Hence $\{\sigma_1', \cdots, \sigma_n'\}=\{\sigma_1^*, \cdots, \sigma_m^*\}$, and so $G^*|R'=G|R'$.

Now, by Villamayor's Theorem and Theorem 1 (ii), we obtain the following

COROLLARY. *Let S be a commutative ring with no idempotents other than 0 or 1, and let $R=S^G$ for some automorphism group G of S. Then, for a R-subalgebra R' of S, the following conditions are equivalent.*

(a) *R' is a separable R-algebra and a finitely generated R-module.*

(b) *R' is a separable R-algebra and a projective R-module.*

REMARK 1. Let A be a commutative separable R-algebra which is a finitely generated projective R-module, and let B be an R-subalgebra of A. Then, as a slight variation of [1, Proposition 4.8], there holds the following: B is separable over R if and only if A is B-projective. If one of these conditions holds, then B is a finitely generated projective R-module and is a B-direct summand of A. This result is a direct consequence of [5, Proposition 1.5], too.

REMARK 2. By making use of Theorem 1, we shall present a simple proof of the Fundamental Theorem of finite Galois theory (cf. [4, Theorem 2.3]) for a Galois extension with no idempotents other than 0 or 1. Let S be a commutative ring and a finitely generated separable R-algebra with no idempotents other than 0 or 1, and let $R=S^G$ for some automorphism group G of S. Then

(i) For any R-subalgebra R' of S which is separable over R, the R'-automorphism group H of S is contained in G and $R'=S^H$.

(ii) For any subgroup H of G, S^H is separable over R and the S^H-automorphism group of S coincides with H.

(iii) A subgroup H of G is normal in G if and only if S^H is mapped

onto itself by every element of G, in which case S^H is a Galois extension of R with Galois group G/H.

PROOF. By Theorem 1(v), the R-automorphism group of S coincides with G. Moreover, by the Corollary of Theorem 1, S is a finitely generated projective separable R-algebra. (i): By Remark 1, R' is a finitely generated separable R-algebra. Therefore we have $R'=S^H$ by Theorem 1(iii). (ii): By Theorem 1(ii), S is a projective S^H-module. Hence, by Remark 1, S^H is separable over R. Moreover, by Theorem 1(v), the S^H-automorphism group of S coincides with H. By similar methods, we obtain (iii).

Now, for convenience we shall introduce some definitions about R-algebras.

DEFINITION. An R-algebra R' will be called f.g. separable if R' is finitely generated and separable over R. Moreover, an R-algebra S will be called locally f.g. separable if for each finite subset F of S there exists an f.g. separable R-subalgebra R' of S containing F.

As in [5], an R-algebra B will be called strongly separable if B is f.g. separable and projective over R. Moreover, an R-algebra A will be called locally strongly separable if for each finite subset F of A there exists a strongly separable R-subalgebra B of A containing F. If R is a commutative ring with no idempotents other than 0 or 1 then, by [5, Proposition 1.11], there is a locally strongly separable commutative R-algebra, Ω, such that Ω has no idempotents other than 0 or 1 and if Γ is a strongly separable commutative Ω-algebra with no idempotents other than 0 or 1 then $\Gamma=\Omega$. Such a commutative R-algebra will be called a separable closure of R. Moreover, by [5, Proposition 1.14], the separable closure of R is unique up to isomorphism. If S is a commutative ring and a locally f.g. separable R-algebra, and $R=S^G$ for some automorphism group G of S then, by the corollary of Theorem 1, S is a locally strongly separable R-algebra. Now we shall prove the following theorem.

THEOREM 2. *Let S be a commutative ring and a locally f.g. separable R-algebra with no idempotents other than* 0 *or* 1, *and let $R=S^G$ for some automorphism group G of S. Then*

(i) $\sum_{\sigma\in G}\sigma S$ (*direct sum*) *is isomorphic to a dense subring of* $\mathrm{Hom}_R(S, S)$ (*in the finite topology*).

(ii) *If R' is an f.g. separable R-subalgebra of S, then $R'=S^H$ for $H=\{\sigma\in G;\ \sigma|R'=1\}$ and $(G:H)<\infty$. Conversely, if H is a subgroup of G such that $(G:H)<\infty$, then S^H is an f.g. separable R-subalgebra of S.*

(iii) *For each finite subset F of S, there exists an f.g. separable R-subalgebra R' of S containing F which is a Galois extension of R with Galois group $G|R'$.*

(iv) *The R-automorphism group G^* of S is compact and the closure $\overline{G}$ of G coincides with G^*.*

PROOF. (i). For any f.g. separable R-subalgebra R' of S, we have $\sum_{i=1}^{n}(\sigma_i|R')S$ (direct sum, $\sigma_i\in G$) $=\mathrm{Hom}_R(R', S)$ by Theorem 1(iv). Since $\mathrm{Hom}_R(R', S)\supset\mathrm{Hom}_R(S, S)|R'\supset(\sum_{i=1}^{n}\sigma_i S)|R'=\sum_{i=1}^{n}(\sigma_i|R')S$, it follows that $\sum_{i=1}^{n}(\sigma_i|R')S=\mathrm{Hom}_R(S, S)|R'$. This proves our assertion. (ii). First assertion is a direct consequence of Theorem1 (i, iii). For the second assertion, we set $R^*=S^H$. Then, for any f.g. separable R-subalgebra R' of S, we have $R'\cap R^*=S^{H'H}$, where $H'=\{\sigma\in G;\ \sigma|R'=1\}$ and $H'H$ is the composite group of H' and H. Hence, by Theorem 1(ii), R' is a projective $(R'\cap R^*)$-module, and so, by Remark 1, $R'\cap R^*$ is an f.g. separable R-subalgebra of R^*. Therefore R^* is a locally f.g. separable R-algebra. For any f.g. separable R-subalgebra R', R'' such that $R^*\supset R''\supset R'\supset R$, we obtain

$$\sum_{i=1}^{n}(\sigma_i|R')S \quad (\text{direct sum, } \sigma_i\in G)=\mathrm{Hom}_R(R', S),$$

and

$$\sum_{i=1}^{m}(\tau_i|R'')S \quad (\text{direct sum, } \tau_i\in G)=\mathrm{Hom}_R(R'', S).$$

By Remark 1, R' is a direct summand of R'' as R'-module. Hence, if $R''\supsetneq R'$ then $m>n$. Since $m\leqq(G: H)<\infty$, it follows that R^* is an f.g. separable R-subalgebra of S. (iii). For a finite subset F of S, we set $R^*=S[F^*]$ for $F^*=\{\sigma(x);\ \sigma\in G,\ x\in F\}$, and $H^*=\{\sigma\in G;\ \sigma|R^*=1\}$. Then H^* is a normal subgroup of G. Since F^* is a finite set (Theorem 1(i)), we have $(G: H^*)<\infty$. Hence, by (ii), S^{H^*} is an f.g. separable R-subalgebra of S, and so, S^{H^*} is a Galois extension of R containing F with Galois group $G|S^{H^*}$. (iv). By (iii), G^* is an inverse limit of finite groups. Hence G^* is compact. For any f.g. separable R-subalgebra R', we have $G|R'=G^*|R'$ by Theorem 1(v); whence G^* is the closure of G.

THEOREM 3. *Let S be a commutative ring and a locally f.g. separable R-algebra with no idempotents other than* 0 *or* 1, *and let $R=S^G$ for some automorphism group of S. Then*

(i) *There exists an* 1-1 *dual correspondence between locally f.g. separable R-subalgebras of S and closed subgroups of the R-automorphism group G^* of S, in the usual sense of Galois theory.*

(ii) *A subgroup H of G is normal in G if and only if S^H is mapped onto itself by every element of G, in which case S^H is a locally f.g. separable R-algebra with a R-automorphism group G/H such that $(S^H)^{G/H}=R$.*

PROOF. Let H be a closed subgroup of G^*. Then, by making use of the same method as in the proof of Theorem 2(ii), we can see that S^H is a locally f.g. separable R-algebra. We set $H^* = \{\sigma \in G^*; \sigma | S^H = 1\}$. Then H^* is a closed subgroup of G^*. Let F be an arbitrary finite subset of S. Then, by Theorem 2(iii), we can find an f.g. separable R-subalgebra R' of S containing F which is a Galois extension of R with Galois group $G|R'$. Then, we have $G^*|R' = G|R'$ by Theorem 1(v), and so $H^*|R' = H|R'$ by finite Galois theory. Hence $H^*|F = H|F$. Therefore H is dense in H^*. Since H is closed, it follows that $H^* = H$.

Let R^* be a locally f.g. separable R-subalgebra of S ($R^* \subsetneqq S$), and x an arbitrary element of the complement of R^* in S. Consider the following

$$U = \{\sigma \in G^*; \sigma(x) = x\},$$

$$X = \{R_i; i \in I\} \text{ (the set of all f.g. separable } R\text{-subalgebras } R_i \text{ of } R^*),$$

$$Y = \{H_i; i \in I\}, \text{ where } H_i = \{\sigma \in G^*; \sigma | R_i = 1\}.$$

Then $H_i \backslash U$ (the complement of $H_i \cap U$ in H_i) is a closed subset of G^*, and by Theorem 1(iii), $\{H_i \backslash U; i \in I\}$ has the finite intersection property. Hence $\bigcap_{i \in I} H_i \backslash U$ is nonempty, (note that G^* is compact). Therefore, there exists a R^*-automorphism σ of S such that $\sigma(x) \neq x$. This implies that $S^H = R^*$ for $H = \{\sigma \in G^*; \sigma | R^* = 1\}$. The remainder of the proof is obvious.

REFERENCES

1. M. Auslander and D. Buchsbaum, *On the ramification theory in noetherian rings*, Amer. J. Math. **81** (1959), 749–765.

2. M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367–409.

3. N. Bourbaki, *Algèbre commutative*, Chapitre I–II, Actualités Sci. Ind. No. 1290, Hermann, Paris, 1962.

4. S. U. Chase, D. K. Harrison and Alex Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965), 77 pp.

5. G. J. Janusz, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc. **125** (1966), 290–297.

NORTHWESTERN UNIVERSITY