GALOIS THEORY IN SEPARABLE ALGEBRAS OVER COMMUTATIVE RINGS

BY

F. R. DeMeyer[1]

Introduction

In [1], M. Auslander and O. Goldman introduced the notion of a Galois extension of a commutative ring. The study of these Galois extensions was continued by S. Chase, D. K. Harrison and A. Rosenberg in [3] and by Harrison in [8]. Further work by Harrison [9] indicates that the notion of a Galois extension will have significant applications in the general theory of rings.

Throughout, K will denote a commutative ring (with 1) and S (with 1) a faithful K-algebra. Let G be a finite group of algebra automorphisms of S.

We call S a Galois extension of K with group G in case

1. $K = S^G$;
2. there exists $x_1, \cdots, x_n; y_1, \cdots, y_n \in S$ such that for all $a \in G$,

$$\begin{aligned} \textstyle\sum_i x_i\, a(y_i) &= 1 \quad \text{if} \quad a = e \\ &= 0 \quad \text{if} \quad a \neq e \end{aligned}$$

where if H is a subgroup of G, S^H denotes

$$\{x \in S \mid a(x) = x \quad \text{for all} \quad a \in H\}$$

This paper has as its purpose the study of not necessarily commutative Galois extensions of a commutative ring K. We show that if S is a Galois extension of K with no central idempotents except 0 and 1 then the center of S is left fixed by a normal subgroup of the Galois group. This reduces the study of Galois K-algebras S to the situation where S is either commutative or S is central over K. We concentrate here on the study of central Galois K-algebras whose Galois group is represented by inner automorphisms. The Galois group will always be represented by inner automorphisms in case K is a principal ideal domain, local ring, or field. We show that any central Galois K-algebra S whose Galois group G is represented by inner automorphisms is a separable projective group algebra. In case K has no idempotents but 0 and 1 we employ this result to find all the central Galois K-algebras with an Abelian Galois group of inner automorphisms. We conclude with an application to the commutative theory by giving a Kummer type theorem for Abelian extensions when appropriate roots of unity are present.

This paper forms a part of the author's Doctoral Dissertation at the Uni-

Received January 26, 1965.

[1] This work was done while the author held a National Science Foundation Fellowship.

versity of Oregon written under the guidance of Professor D. K. Harrison. The author extends his heartfelt thanks to Professor Harrison for his advice and encouragement, and he also wishes to thank fellow students of the University of Oregon, especially G. J. Janusz, for many stimulating and helpful conversations.[2]

Section 1

Let S be a Galois K-algebra with Galois group G and let C be the center of S. Let

$$H = \{a \in G \mid a(x) = x \quad \text{for all} \quad x \in C\};$$

then we have

THEOREM 1. *If S has no central idempotents but* 0 *and* 1, *then H is a normal subgroup of G and $C = S^H$. Moreover C is Galois over K with group G/H and S is Galois over C with group H.*

Proof. Let G/H be defined as a group of automorphisms on S^H by $aH(x) = a(x)$. Via restriction G/H may also be viewed as a group of distinct automorphisms on C.

Since S is a Galois extension of K, there exists $x_1, \cdots, x_n; y_1, \cdots, y_n$ in S so that $\sum_i x_i\, a(y_i) = \delta_{a,e}$ (δ is Kroneckers delta). Let

$$\operatorname{tr}(-x) \in \operatorname{Hom}_K(S, K)$$

be defined by

$$\operatorname{tr}(-x)(y) = \operatorname{tr}(xy) = \textstyle\sum_{a\in G} a(xy).$$

$\{\operatorname{tr}(-x_i), y_i\}$ form a dual basis for S as a K module so S is finitely generated projective as a K module (Prop. 4.4 of [2]).

Let $\varepsilon \in S \otimes_K S^0$ (S^0 the opposite algebra of S) be given by $\varepsilon = \sum_i x_i \otimes y_i$. For all $x \in S$,

$$(x \otimes 1)\varepsilon = \textstyle\sum_{ij} x_j \operatorname{tr}(y_j x x_i) \otimes y_i = (1 \otimes x)\varepsilon$$

so by Proposition 7.7 of [2] S is separable over K. By Theorem 2.3 of [1], C is then separable over K and since C has no idempotents but 0 and 1 by Theorem 1.3 of [3], C is a Galois extension of K with group G/H. One can show that S^H is a Galois extension of K with group G/H by employing the definition or by a straightforward generalization of Lemma 2.2 of [3]. Let $i : C \rightarrow S^H$ be the inclusion map; i commutes with the automorphisms in G/H so by the appropriate generalization of Theorem 3.4 of [3] or by a computation using the definition i is onto. This proves the theorem.

Examples show that the hypothesis that S contain no proper central idempotents is necessary. However by a generalization of the techniques developed in Theorem 7 of [8], if K has no idempotents but 0 and 1, one can

[2] The author wishes to thank the referee for many helpful suggestions.

write S as a direct sum of Galois extensions of K which contain no central idempotents. In the course of the proof of Theorem 1 we showed that any Galois K-algebra S is separable finitely generated and projective over K, this fact will be employed in the sequel. We will now characterize the central Galois extensions S of a commutative ring K with a Galois group G represented by inner automorphisms on S.

$U(K)$ will always denote the multiplicative group of units of K. We recall that $f : G \times G \to U(K)$ is called a 2-cocycle of G in case

$$f(ab, c)f(a, b) = f(a, bc)f(b, c)$$

for all a, b, c in G. A 2-coboundary $q : G \times G \to U(K)$ is a 2-cocycle with the property that there is a map $p : G \to U(K)$ so that

$$q(a, b) = p(a)(b)p(ab)^{-1}.$$

The group $Z^2(G, K)$ of 2-cocycles of G modulo the subgroup $B^2(G, K)$ of 2-coboundaries is the second cohomology group of G, $H^2(G, K)$. If f is a 2-cocycle in G we denote its projection in $H^2(G, K)$ by $|f|$ and if f' is another 2-cocycle so that $|f'| = |f|$ we say f is cohomologous to f'.

A projective group algebra KG_f is a free K-module with K basis $\{U_a \mid a \in G\}$ and multiplication given by $\alpha_a U_a \alpha_b U_b = \alpha_a \alpha_b U_{ab} f(a, b)$ where $\alpha_a, \alpha_b \in K$, a, $b \in G$ and $f \in Z^2(G, K)$. f and g are cohomologous cocycles if and only if KG_f is isomorphic to KG_g under a map carrying basis elements to basis elements. We associate in this way the projective group algebras KG_f and the elements of $H^2(G, K)$.

Remark. It has been shown in [13] that if each element in the class group of K has order relatively prime to the order of G and if S is a central Galois extension of K with group G, then every element in G is inner on S.

THEOREM 2. *Let S be a central Galois extension of K with group G and assume all the automorphisms in G are inner on S; then S is a projective group algebra KG_f.*

Proof. We need the following lemma which appears to be well known; a proof in this generality appears in [6].

LEMMA 1. *Let KG_f be a projective group algebra and let $(G{:}1)$ denote the number of elements in G. KG_f is a separable K algebra if and only if $(G{:}1)$ is a unit in K.*

Now let S be a K-algebra satisfying the hypothesis of the theorem. For each $a \in G$ there exists $x_1, \cdots, x_n, y_1, \cdots, y_n$ in S so that $\sum_i x_i b(y_i) = \delta_{a,b}$ for all $b \in G$. Pick $U_a \in S$, one for each $a \in G$, so that $a(x) = U_a x U_a^{-1}$. Assume $\sum_b \alpha_b U_b = 0$ with $\alpha_b \in K$. Then for each $a \in G$,

$$0 = \sum_i x_i(\sum_b \alpha_b U_b) y_i = \alpha_a U_a .$$

Thus the U_a are linearly independent over K. Define

$$f : G \times G \to U(K)$$

by $f(a, b) = U_a U_b U_{ab}^{-1}$. By the associative law in S, f is a 2-cocycle of G and $\sum_{a \in G} KU_a = KG_f$ is a subalgebra of S.

One can show that S has K rank equal to $(G:1)$ exactly as in Theorem 4.1 of [3]; so if K were a field, then by a dimension argument S would equal KG_f. If A is a commutative K-algebra, then as in [3] or by employing the definition, one can see that $A \otimes_K S$ is a Galois extension of A with group G. Thus for every maximal ideal $\mathfrak{A}$ of K, $K/\mathfrak{A} \otimes_K S$ is a central Galois extension of the field $K/\mathfrak{A}$ with group G. Since $K/\mathfrak{A} \otimes_K S$ is a central Galois extension of the field K/A, by Lemma 1, $(G:1)$ belongs to no maximal ideal of K so $(G:1) \in U(K)$. Since $S^G = K$, KG_f is central over K and we have shown then that KG_f is a central separable K-algebra. By Theorem 3.3 of [1], $S = KG_f \otimes_K S'$ where S' is a central separable subalgebra of S and each element in S' commutes with every element in KG_f. But if $x \in S$ and $U_a x = xU_a$ for all $a \in G$ then $x \in S^G = K$ so $S' = K$ and $S = KG_f$.

We can prove a converse to Theorem 2.

THEOREM 3. *Let G be a finite group and KG_f a projective group algebra which is central separable over K; then KG_f is a Galois extension of K with group G, where if $a \in G$ and U_a is the basis element of KG_f corresponding* to a, *then* $a(x) = U_a x U_a^{-1}$ *for all $x \in KG_f$.*

Proof. Since KG_f is central, $K \cdot e = K$ is exactly the fixed subring of KG_f under action by the elements in G. We show that the set

$$\{(G:1)^{-1}U_a^{-1}, U_a \mid a \in G\}$$

satisfy the condition of the definition. To do this let $\mathrm{tr} \in \mathrm{Hom}_K(KG_f, K)$ be given by

$$\mathrm{tr}\,(x) = \textstyle\sum_{a \in G} a(x) = \sum_{a \in G} U_a x U_a^{-1}.$$

For any $b \in G$,

$$\textstyle\sum_{a \in G} U_a^{-1}(G:1)^{-1} b(U_a) = \sum_{a \in G} a(U_b) U_b^{-1} (G:1)^{-1}.$$

$$\textstyle\sum_{a \in G} a(U_b) = \mathrm{tr}\,(U_b) \in Ke.$$

On the other hand, $a(U_b) = U_{aba^{-1}}\,\alpha$ where $\alpha \in U(K)$ and $aba^{-1} = e$ if and only if $b = \mathrm{e}$. Thus $\mathrm{tr}\,(U_b) = 0$ unless $b = e$ and

$$\textstyle\sum_{a \in G} U_a^{-1}(G:1)^{-1} b(U_a) = \mathrm{tr}\,(U_b) U_b^{-1} (G:1)^{-1} = \delta_{e,b}.$$

This completes the proof.

Section 2

If S and S' are Galois extensions of K with group G we say S is G-isomorphic to S' in case there is an algebra isomorphism F mapping S onto S' so that for any $a \in G$, $x \in S$; $aF(x) = F(ax)$. If KG_f and KG_g are central Galois extensions of K, then KG_f is G isomorphic to KG_g if and only if f is cohomologous to g. The study of the G-isomorphism classes of central Galois extensions with inner Galois group is reduced by Theorem 2 and Theorem 3 to the study of the subset of $H^2(G, K)$ which yields the central projective group algebras.

In what follows let G be an abelian group. A pairing of G with itself to K is a biadditive mapping ψ of $G \times G$ into $U(K)$. ψ is called skew if $\psi(a, a) = 1$ for all $a \in G$. Let $P_{\mathrm{sk}}(G, K)$ denote the set of skew pairings of G to K. If $|f| \in H^2(G, K)$, we call $|f|$ symmetric in case $f(a, b) = f(b, a)$ for all $a, b \in G$. (If f' is another 2-cocycle so that $|f'| = |f|$ then $f'(a, b) = f'(b, a)$.) We denote the subgroup of $H^2(G, K)$ whose representing cocycles are symmetric by $H^2_{\mathrm{sym}}(G, K)$.

PROPOSITION 1. *Let K be a commutative ring, G a finite abelian group, and assume K has no more than m distinct m^{th} roots of 1 where m is the exponent of G; then the map*

$$F : H^2(G, K) \to P_{\mathrm{sk}}(G, K)$$

given by $F(|f|)(a, b) = f(a, b)f(b, a)^{-1}$ yields the split exact sequence

$$0 \to H^2_{\mathrm{sym}}(G, K) \to H^2(G, K) \to P_{\mathrm{sk}}(G, K) \to 0.$$

This proposition was proved by the author in case G has odd order but the proposition for all finite abelian groups is an immediate consequence of Theorem 2 and Corollary 3 of [14].

It is clear that a domain can have no more than m distinct m^{th} roots of 1. In [10], G. J. Janusz has developed a theory of separable polynomials with coefficients in a commutative ring. One of the results there is the following:

PROPOSITION 2. *Let K be a commutative ring without idempotents except 0 and 1 and assume m is a unit in K; then there are at most m distinct m^{th} roots of 1 in K.*

A pairing ψ of G to K is called nonsingular in case $\psi(a, G) = 1$ implies $a = e$ for all $a \in G$. Let I be the subset of $P_{\mathrm{sk}}(G, K)$ consisting of the non-singular skew pairings of G to K. If $(G{:}1) \notin U(K)$ then as we saw in the proof of Theorem 2 there are no central Galois extensions of K with group G. On the other hand

THEOREM 4. *Let K be a commutative ring without idempotents but 0 and 1 and assume $(G{:}1)$ is a unit in K; then the G-isomorphism classes of central Galois K-algebras with Galois group represented by inner automorphisms is in one to one correspondence with $I \times H^2_{\mathrm{sym}}(G, K)$.*

Proof. The central Galois K-algebras with Galois group represented by inner automorphisms is in one to one correspondence with the G-isomorphism classes of central projective group algebras KG_f with the action of G on KG_f given by $a(U_b) = U_a U_b U_a^{-1}$ for $a, b \in G$ and U_a, U_b the basis elements in KG_f

corresponding to a and b. Let KG_f be a central projective group algebra. By a simple computation, for all $a, b \in G$, $a(U_b) = U_b f(a, b)f(b, a)^{-1}$. Define the skew pairing ψ on G to K by $\psi(a, b) = f(a, b)f(b, a)^{-1}$. Since $K \cdot e$ is the fixed subring of KG_f under action by the elements in G, ψ is non-singular. The correspondence of Proposition 1 then yields the result.

We could have replaced the hypothesis that K have no idempotents but 0 and 1 in Theorem 4 by the weaker hypothesis that K contain no more than m distinct m^{th} roots of 1 where m is the exponent of G.

To complete the classification theory we have begun it remains to examine the conditions a non-singular skew pairing of an Abelian group G to a commutative ring K impose on the structure of G and K, to give a description of all such pairings, and to apply this information to study the algebra structure of the corresponding Galois algebras. First, it is easy to see that the existence of a non-singular pairing of G to K is equivalent to the existence of a primitive m^{th} root of 1 in K where m is the exponent of G. We now describe the conditions imposed on an Abelian group G by the existence of a non-singular skew pairing of G to K in the situation where K contains no more than m distinct m^{th} roots of 1.

PROPOSITION 3. *Let K be a commutative ring, G a finite Abelian group of exponent m, and assume K contains no more than m distinct m^{th} roots of* 1. *Let ψ be a skew non-singular pairing of G to K; then $G \cong H_1 \oplus H_2$ and there is an isomorphism $\alpha : H_1 \to H_2$ and a non-singular pairing β of H_2 to K so that*

1. $\psi(h_i, h_i) = 1$ *for all* $h_i \in H_i$
2. $\psi(h_1, h_2) = \psi(h_2, h_1)^{-1} = \beta(\alpha(h_1), h_2)$ *for all* $h_i \in H_i$.

The non-singular pairings on H to K correspond to the isomorphisms from H to Hom $(H, U(K))$. *Conversely, any ψ so defined is a skew non-singular pairing of G to K.*

Proof. Write $G \cong H_1 \oplus \cdots \oplus H_n$, the H_i Sylow p-subgroups of G. One easily checks that $\psi(H_i, H_j) = 1$ if $i \neq j$, and that ψ restricted to H_i is a non-singular skew pairing of G to K. Let C be a cyclic direct summand of $H = H_1$ of largest possible order, and let c generate C. $(C:1) = p^n$ for a prime p. By the non-singularity of ψ on H and the hypothesis on K the map $b \to \psi(b, -)$ of H to $H^\# =$ Hom $(H, U(K))$ is an isomorphism. The element $\psi(c, -)$ has order p^n in $H^\#$ so there then must exist an element $d \in H$ so that $\psi(c, d)$ has order p^n in $U(K)$. By maximality of the order of C, d must also have order p^n. Let D be the cyclic subgroup of H generated by d, then we contend that $D \cap C = \{e\}$. Let $D \cap C$ be generated by the element m in H. Since $m \in D$ and ψ is non-singular, $\psi(m, d) = 1$. Since $m \in C$, $m = c^r$ with $r \leq p^n$.

Then we have $\psi(c, d)^r = \psi(c^r, d) = \psi(m, d) = 1$ with $r \leq p^n$ which by choice of c and d implies $r = p^n$ and $m = 1$. Let $N = C + D$ and let

$$N' = \{h \in H \mid \psi(h, N) = 1\}.$$

$N \cap N' = \{e\}$ and N' is a subgroup of H. Let $N^{\#} = \mathrm{Hom}\,(N, U(K))$, then

$$N^{\#} = \{\psi(h, \text{-}) \in \mathrm{Hom}\,(N, K) \mid h \in H\}$$

and $H \cong H^{\#}$, $N \cong N^{\#}$ by the hypothesis on K. Define a biadditive map

$$\gamma : N \times H \rightarrow U(K)$$

by $\gamma(b, h) = \psi(b, h)$ for $b \in N$, $h \in H$. $\gamma(b, h) = 1$ for all $b \in N$ if and only if $h \in N'$ so we have the exact sequence

$$0 \rightarrow H_1/N' \rightarrow N^{\#}.$$

Thus $(N:1)(N':1) = (H:1)$ and $N \oplus N' = H$. ψ restricted to either N or N' is a non-singular skew inner product on N or N' so inductively we need only verify the proposition for N. $N \cong C \oplus D$ with $C \cong D$ by $\alpha(c) = d$. Define a non-singular pairing of C to K by $\beta(c^i, c^j) = \psi(c^i, d^j)$. α and β satisfy the conditions of the proposition. The proofs of the remaining statements are straightforward and so we omit them.

In the course of the proof of Proposition 3 we have shown that if ψ is a non-singular skew pairing of a finite Abelian group G of exponent m and a commutative ring K with no more than m distinct m^{th} roots of 1, then

$$G \cong N_1 \oplus \cdots \oplus N_k$$

with $\psi(N_i, N_j) = 1$ $(i \neq j)$, ψ restricted to N_i non-singular, and with N_i the direct sum of two cyclic groups of order $p_i^{n_i}$ for some prime p_i and integer n_i. This yields a corresponding decomposition for central Galois extensions in the following way: if S is a central inner extension of K with group G and associated pairing ψ, and if $G \cong N_1 \oplus N_2$ with $\psi(N_1, N_2) = 1$, then $S \cong S^{N_1} \otimes_K S^{N_2}$ and S^{N_i} is a central Galois extension of K with group N_j $(i \neq j)$. Those facts follow with some work from the representation of S afforded by Theorem 2.

This completes our description of the central extensions in case G is Abelian. One can ask why can be said in case the Galois group G is not necessarily Abelian. We saw in the proof of Theorem 2 that if S is a central Galois extension of K with group G, and if $\mathfrak{A}$ is a maximal ideal of K, then $K/\mathfrak{A} \otimes_K S$ is a central separable $K/\mathfrak{A}$-algebra of dimension $(G:1)$ over $K/\mathfrak{A}$. Thus any Galois group of a central extension must have order a perfect square. By elementary number theoretic considerations we can rule out, for example, the symmetric groups S_n and alternating groups A_n from consideration as candidates for groups of central extensions. If we let K be the complex numbers, then the existence of a central Galois extension of K with Galois group G is equivalent to the existence of a faithful irreducible projective representation of G in some central simple algebra over K. This problem has received some study in [12], but little is known about groups admitting such representations.

We now apply these ideas to obtain an elementary Kummer Theorem for commutative rings without idempotents but 0 and 1.

THEOREM 5. *Let S be a commutative faithful K-algebra and assume that the class group $P(K)$ of K is trivial and that S has no idempotents but* 0 *and* 1. *Assume also that S is a Galois extension of K with cyclic group H, that $(H:1) = n$ is a unit in K and that there is a primitive n^{th} root of* 1 *in K; then $S = K(\alpha)$ with α a unit in S and $\alpha^n \in K$.*

Proof. Let b generate the cyclic group H. Define $f : H \to U(S)$ by $f(b^i) = \gamma^i$ where γ is a primitive n^{th} root of 1 in K. Since $f(bc) = f(b)b(f(c))$ where $b, c \in H$ we apply Hilbert's Theorem 90 (Corollary 5.5 of [3]) to infer that there is an $\alpha \in U(S)$ so that $f(b^i) = \alpha \cdot b(\alpha)^{-1} = \gamma^i$. We conclude that $b(\alpha) = \gamma\alpha$, $b^i(\alpha) = \gamma^i\beta$, and the elements $\gamma^i\alpha$ are distinct. Also, $\alpha^n \in K$ since $b(\alpha^n) = \alpha^n$ so α satisfies the polynomial $p(x) = x^n - k$ for some $k \in U(K)$. Let A be the K-algebra $K(\alpha)$. A is a K-subalgebra of S on which H acts faithfully as a group of algebra automorphisms and $A^H = K$. By Theorem 1.3 and Theorem 3.4 of [3] the proof will be complete when we show A is separable as a K-algebra.

Let $A' = KH_f$ where KH_f is a projective group algebra with f defined by

$$\begin{aligned} f(b^i, b^j) &= 1 \qquad \text{if} \quad i + j < n \\ &= k \qquad \text{if} \quad i + j \geq n. \end{aligned}$$

By Lemma 1, A' is a separable K-algebra. There is an obvious algebra homomorphism of A' onto A and since the homomorphic image of a separable algebra is separable, A is separable and this proves the result.

COROLLARY. *Let S be a faithful commutative K-algebra without idempotents but* 0 *and* 1, *assume $P(K)$ is trivial, and assume S is a Galois extension of K with Abelian group G of exponent m. If m is a unit in K and there is a primitive m^{th} root of* 1 *in K then S is G-isomorphic to $S_1 \otimes_K \cdots \otimes_K S_n$ with the S_i Galois extensions of K with cyclic group H_i.*

BIBLIOGRAPHY

1. M. AUSLANDER AND O. GOLDMAN, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc., vol. 97 (1960), pp. 367–409.
2. H. CARTAN AND S. EILENBERG, *Homological algebra*, Princeton, Princeton University Press, 1956.
3. S. CHASE, D. HARRISON, AND A. ROSENBERG, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc., no. 52 (1965).
4. C. W. CURTIS AND I. REINER, *Representation theory of finite groups and associative algebras*, New York, Interscience, 1962.
5. F. R. DEMEYER, *Some notes on the general Galois theory of rings*, Osaka Math. J., vol.2(1965),pp.117–127.
6. M. HARADA, *Some criteria for hereditarity of crossed products*, Osaka Math. J., vol. 1 (1964), pp. 69–80.
7. D. K. HARRISON, *Abelian extensions of arbitrary fields*, Trans. Amer. Math. Soc., vol. 106 (1963), pp. 230–235.
8. ———, *Abelian extensions of commutative rings*, Mem. Amer. Math. Soc., no. 52 (1965), pp. 1–14.

9. ———, *Finite and infinite primes for rings and fields*, Trans. Amer. Math. Soc.,
10. G. J. JANUSZ, Ph.D. Thesis, University of Oregon, 1965.
11. T. KANZAKI, *On commutator rings and Galois theory of separable algebras*, Osaka Math. J., vol. 1 (1964), pp. 103–115.
12. R. KOCHENDÖRFFER, *Uber Treue irreducible Darstellugen endlicher Gruppen*, Math. Nachr., vol. 1 (1948), pp. 25–39.
13. A. ROSENBERG AND D. ZELINSKY, *Automorphisms of separable algebras*, Pacific J. Math., vol. 11 (1957), pp. 1109–1118.
14. K. YAMAZAKI, *On projective representations and ring extensions of finite groups*, J. Fac. Sci. Univ. Tokyo, vol. 10 (1964), pp. 147–195.

UNIVERSITY OF OREGON
EUGENE, OREGON