MEMOIRS
OF THE
AMERICAN MATHEMATICAL SOCIETY

Number 52

GALOIS THEORY AND COHOMOLOGY OF COMMUTATIVE RINGS

by
S. U. CHASE
D. K. HARRISON
ALEX ROSENBERG

Published by the
American Mathematical Society
Providence, Rhode Island
1965

Standard Book Number 8218-1252-1
Library of Congress Catalog Number 52-42839

First Printing 1965
Second Printing with corrections 1968
Fourth Printing 1978

Printed in the United States of America

CONTENTS

GALOIS THEORY AND GALOIS COHOMOLOGY OF COMMUTATIVE RINGS

by

S. U. Chase, D. K. Harrison, and Alex Rosenberg[1,2]

In [2], M. Auslander and O. Goldman introduced the notion of a Galois extension of a commutative ring, and used it to generalize to arbitrary commutative rings the theory of crossed products and Galois cohomology for fields. However, they obtained no corresponding generalization of the Fundamental Theorem of Galois Theory. In this paper we exhibit such a generalization; in addition, we derive a certain exact sequence of seven terms which extends the Galois cohomology results of [2]. In particular, it includes Theorems A.9 and A.15 of that paper, and its existence was first suggested to us by a careful study of the proofs of these theorems. If the commutative rings involved are taken to be fields, then the above-mentioned exact sequence reduces to the two classical theorems of Galois cohomology of fields: Hilbert's Theorem 90 and the isomorphism of the Brauer group of the field with a second cohomology group.

The base rings in our Galois theory are arbitrary commutative rings. However, the extensions are always separable commutative algebras; i.e., if R is the base ring the extensions are commutative R-algebras S with S a projective $S \otimes_R S$-module. A simplification occurs for rings in which 0 and 1 are the only idempotents. Since the usual Galois theory for fields is not assumed, we have, as a by-product, an alternative approach to this theory. Our methods are quite elementary; all that is needed for the Fundamental Theorem is a knowledge of the notions of tensor product and projective module, together with their easier properties.

In 1. we give six equivalent conditions which characterize Galois extensions. One of these is the definition of [2]. In 2. our generalization of the Fundamental Theorem of Galois theory appears. Section 3 is devoted to

Received by the editors August 5, 1963.

[1]Presented to the society June 28, 1963 under the title "Galois-theory of commutative rings" (Abstract 63T-322, Notices Amer. Math. Soc. vol. 10 (1963) p. 515).

[2]This paper was written with the support of N.S.F. grant G-23454 for D. K. Harrison and G-23834 for S. U. Chase and Alex Rosenberg.

the study of homomorphisms of Galois extensions and includes our generalization of the theorem that the Galois group of a field consists of all automorphisms that are the identity on the fixed field. In 4. we study the normal basis theorem in our context. Finally, 5. is devoted to deducing the seven term exact sequence, already mentioned, from [7]. Section 4. requires a slight knowledge of localization and the theory of the radical, while 5. needs Amitsur cohomology and the main result of [7].

Our Galois theory has been used by one of us in [10].

After having obtained our results we learned that Grothendieck has developed a Galois theory for schemes [9, p. 18] which presumably includes ours in the affine case. This theory, however, seems not to have been published yet in any readily available source.

We should like to express our warmest thanks to P. Cartier for many helpful comments which enabled us to improve greatly the exposition of our results. We also thank S. A. Amitsur, O. Villamayor, and D. Zelinsky for many useful suggestions.

In all that follows all rings have identities, modules are unitary, and for R a commutative ring the unadorned $\otimes$ means tensor product over R.

After this paper was accepted for publication, we learned that T. Kanzaki, in a paper received by the Osaka Mathematical Journal on May 6, 1964, has proved the Fundamental Theorem of Galois Theory for the special case of commutative integral domains.

1. GALOIS EXTENSIONS.

The most interesting rings for the following theory are commutative rings with no idempotents other than 0 and 1. These include local rings (not necessarily Noetherian) and integral domains. We prefer to state some of the results in a form valid for arbitrary commutative rings, and for this reason introduce the following

DEFINITION 1.1. Let $f,g\colon S \to T$ be homomorphisms of commutative rings. f and g are called strongly distinct if, for every non-zero idempotent e of T, there is an s in S such that $f(s)e \neq g(s)e$.

Clearly, if T has no idempotents other than 0 and 1, then f and g are strongly distinct if and only if they are distinct.

Following Auslander-Goldman [2] we call a commutative R-algebra S separable if S is a projective $S \otimes S$-module. For the case in which R and S are fields, this condition is equivalent to the condition that S be a finite separable extension of R in the usual sense [13, Th. 1; 6, IX, 7.10; 12, VII, 5.6]. Commutative separable algebras over Noetherian rings have been studied in [1].

LEMMA 1.2. Let S be a commutative separable R-algebra, and $f: S \to R$ be an R-algebra homomorphism. Then there exists a unique idempotent e in S such that $f(e) = 1$ and $se = f(s)e$ for all s in S. Furthermore, if $f_1, \ldots, f_n$ are pairwise strongly distinct R-algebra homomorphisms from S to R, then the corresponding idempotents $e_1, \ldots, e_n$ are pairwise orthogonal and $f_i(e_j) = \delta_{ij}$, the latter denoting the Kronecker delta.

Proof. By an easy argument, cf. [6, IX, 7.7; 12, VII, 5.1], the separability of S is equivalent to the existence of elements x_i, y_i of S ($i = 1, \ldots, m$) such that (a) $\Sigma_{i=1}^{m} x_i y_i = 1$, and (b) $\Sigma_{i=1}^{m} s x_i \otimes y_i = \Sigma_{i=1}^{m} x_i \otimes y_i s$ in $S \otimes S$ for any s in S. Now let $e = \Sigma_{i=1}^{m} f(x_i) y_i$. (a) then guarantees that $f(e) = 1$, whereas applying $f \otimes 1$ to (b) yields $f(s)e = se$ for s in S. Setting $s = e$ in the latter equation shows that $e^2 = e$. If e' is another idempotent of S satisfying the same pair of conditions, then $e' = f(e)e' = e'e = f(e')e = e$, so that the first statement of the lemma is proved.

As for the second statement, note that $f_i(e_j)$ is an idempotent of R, and $f_i(s)f_i(e_j) = f_i(se_j) = f_i(f_j(s)e_j) = f_j(s)f_i(e_j)$ for any s in S. Since f_i and f_j are strongly distinct for $i \neq j$, it follows that $f_i(e_j) = \delta_{ij}$. Finally, $e_i e_j = f_j(e_i)e_j = \delta_{ij} e_j$, so that $e_1, \ldots, e_n$ are indeed pairwise orthogonal. This completes the proof.

In the body of this paper we shall be primarily concerned with the following situation: S is a commutative ring, G is a finite group of ring automorphisms of S, and $R = S^G$, the subring of S consisting of all elements of S left fixed by every element of G. Auslander and Goldman have called S a Galois extension of R if a certain condition is satisfied [2, p. 396]. We shall show that this definition admits many equivalent forms. In order to do this we first introduce two auxiliary R-algebras.

Let $D = D(S,G)$ denote the trivial crossed product of S with G. This means that D is a free S-module with generators u_σ (σ in G), with R-algebra structure defined by the formula

$$(su_\sigma)(tu_\tau) = s\sigma(t)u_{\sigma\tau} \quad (s,t \text{ in } S;\ \sigma,\tau \text{ in } G).$$

The identity of D is u_1, and we shall denote it by the symbol 1. There is an R-algebra homomorphism $j: D \to \mathrm{Hom}_R(S,S)$ defined by $j(su_\sigma)(x) = s\sigma(x)$ for s,x in S and σ in G. j is also a left S-module homomorphism, where the S-module structure on $\mathrm{Hom}_R(S,S)$ arises from the S-module structure of the covariant argument.

Let E be the S-algebra of all functions from G to S under pointwise addition and multiplication. If v_σ is the function defined by $v_\sigma(\tau) = \delta_{\sigma\tau}$, it is clear that $E = \Sigma_{\sigma \text{ in } G} \oplus Sv_\sigma$ and that the v_σ are pairwise orthogonal idempotents of E whose sum is 1. Regarding $S \otimes S$ as an S-algebra via the first factor, we have an S-algebra homomorphism $h: S \otimes S \to E$ defined by $h(s \otimes t)(\sigma) = s\sigma(t)$.

In the following results we place brackets around those hypotheses which may be omitted if 0 and 1 are the only idempotents of S.

THEOREM 1.3. Let S be a commutative ring, G a finite group of automorphisms of S, and $R = S^G$. Then the following statements are equivalent:

(a) S is a separable R-algebra [and the elements of G are pairwise strongly distinct].

(b) There exist elements $x_1,\ldots,x_n;\ y_1,\ldots,y_n$ of S such that $\Sigma_{i=1}^n x_i\sigma(y_i) = \delta_{1,\sigma}$ for all σ in G.

(c) S is a finitely generated projective R-module and j is an isomorphism.

(d) Let M be a left D-module, which we may also view as a left G-module with $\sigma(m) = u_\sigma(m)$. Then the mapping $\omega: S \otimes M^G \to M$ defined by $\omega(s \otimes m) = sm$ is an S-module isomorphism.

(e) $h: S \otimes S \to E$ is an S-algebra isomorphism.

(f) Given $\sigma \neq 1$ in G and a maximal ideal p of S, there exists $s = s(p,\sigma)$ in S with $s - \sigma(s)$ not in p.

Proof. (a) => (b): Since S is a separable R-algebra, $S \otimes S$ is a separable $S \otimes 1$-algebra [12, VII, 5.3] (or an easy direct argument). Define $f_\sigma: S \otimes S \to S$ for σ in G by $f_\sigma(s \otimes t) = s\sigma(t)$. The f_σ are S-algebra homomorphisms, and are strongly distinct because the elements of G are. By Lemma 1.2 there is an idempotent e in $S \otimes S$ with $f_\sigma(e) = \delta_{\sigma,1}$ for all σ. If $e = \Sigma_{i=1}^n x_i \otimes y_i$, then $x_1,\ldots,x_n,y_1,\ldots,y_n$ are the desired elements of S.

(b) => (c): As usual, we define the trace of an element s of S by the formula $tr(s) = \Sigma_{\sigma \text{ in } G}\, \sigma(s)$. Then tr(s) is in $S^G = R$. Hence the functions $\varphi_1,\ldots,\varphi_n$ on S defined by $\varphi_i(s) = tr(sy_i)$ lie in $Hom_R(S,R)$. But then it follows easily from (b) that

$$(1.4) \qquad s = \Sigma_{i=1}^n \varphi_i(s)x_i$$

for all s in S, and hence we may apply [6, VII, 3.1] to obtain that S is a finitely generated projective R-module. Now let u be in $Hom_R(S,S)$. Then a routine computation using (1.4) shows that $j(\Sigma_\sigma \Sigma_{i=1}^n u(x_i)\sigma(y_i)u_\sigma) = u$, and so j is onto. Furthermore, if $v = \Sigma_\tau s_\tau u_\tau$ in D, then $\Sigma_\sigma \Sigma_{i=1}^n \{j(v)(x_i)\}\sigma(y_i)u_\sigma = \Sigma_{\sigma,\tau,i}\, s_\tau \tau(x_i)\sigma(y_i)u_\sigma = v$, since by (b) $\Sigma_{i=1}^n \tau(x_i)\sigma(y_i) = \delta_{\sigma,\tau}$. Hence j is a monomorphism, and (c) holds.

(c) => (d): Since S is a finitely generated projective R-module, it again follows from [6, VII, 3.1] that there are elements x_i in S, φ_i in $Hom_R(S,R)$ $(i = 1,\ldots,n)$ such that (1.4) holds for all s in S. Since j is an isomorphism there are elements $d_1,\ldots,d_n$ in D with $j(d_i) = \varphi_i$. Also, since $j(\Sigma_{i=1}^n x_i d_i)(s) = \Sigma_{i=1}^n x_i\varphi_i(s) = s$ for s in S, (c) again shows that $\Sigma_{i=1}^n x_i d_i = u_1 = 1$ in D. Moreover, $j(u_\sigma d_i)(s) = \sigma(\varphi_i(s)) = \varphi_i(s) = j(d_i)(s)$, and so (c) implies that $u_\sigma d_i = d_i$. Thus $d_i m$ is in M^G for all m in M. Since $S \subseteq D$ we may view M as an S-module, and another computation then shows that $d(sm_o) = \{j(d)(s)\}m_o$ for s in S, d in D, and m_o in M^G. Now define a map $\gamma: M \to S \otimes M^G$ by $\gamma(m) = \Sigma_{i=1}^n x_i \otimes d_i m$; then $\omega\gamma$ is the identity map of M. On the other hand, if s and m_o are in S and M^G, respectively, then $\gamma\omega(s \otimes m_o) = \Sigma_{i=1}^n x_i \otimes d_i(sm_o) = \Sigma_{i=1}^n x_i \otimes \varphi_i(s)m_o = \Sigma_{i=1}^n x_i\varphi_i(s) \otimes m_o = s \otimes m_o$; hence $\gamma\omega$ is the identity map of $S \otimes M^G$. We may then conclude that ω is an isomorphism.

(d) => (e): As usual, we let G act on E by setting $(\sigma v)(\tau) = \sigma(v(\sigma^{-1}\tau))$ for σ,τ in G and v in E. Then $\sigma(sv) = \sigma(s)\sigma(v)$ for s in S, and so E may be viewed as a D-module via the formula $(su_\sigma)(v) = s\sigma(v)$. Now, E^G is easily seen to be the G-homomorphisms of G to S and thus the map $\theta: S \to E^G$ defined by $\theta(s)(\sigma) = \sigma(s)$ is an R-module isomorphism, and hence by (d) the composition $\omega(1 \otimes \theta): S \otimes S \to E$ is an S-module isomorphism which is simply h.

(e) => (a): The E-module $Ev_1 = Sv_1$ is E-projective. Viewing E as an $S \otimes S$-module via the isomorphism $h: S \otimes S \to E$, we then have that Sv_1 is $S \otimes S$-projective. Moreover, the equation $h(s \otimes 1)v_1 = h(1 \otimes s)v_1$ shows that $Sv_1 \approx S$ as $S \otimes S$-modules, and so we may conclude that S is $S \otimes S$-projective and therefore a separable R-algebra. Setting $h^{-1}(v_1) = \Sigma_{i=1}^{n} x_i \otimes y_i$, we have that $x_1, \ldots, x_n, y_1, \ldots, y_n$ satisfy (b). Now suppose e is an idempotent of S such that $\sigma(s)e = \tau(s)e$ for some distinct σ, τ in G and all s in S; then $e = \Sigma_{i=1}^{n} x_i y_i e = \Sigma_{i=1}^{n} x_i \tau^{-1}\sigma(y_i)e = 0$. Hence the elements of G are pairwise strongly distinct, and (a) holds.

(b) => (f): If, for some $\sigma \neq 1$ in G and some maximal ideal p of S, $(1-\sigma)S \subseteq p$, then we would have from (b) that $1 = \Sigma_{i=1}^{n} x_i(y_i - \sigma(y_i))$ is in p, a contradiction.

(f) => (b): Let $\sigma \neq 1$ be an element of G. By hypothesis the ideal of S generated by the elements $s - \sigma(s)$ is not contained in any maximal ideal of S, and is thus S itself. Hence there are elements $a_1, \ldots, a_r$, $b_1, \ldots, b_r$ in S (depending upon σ) such that $\Sigma_{j=1}^{r} a_j(b_j - \sigma(b_j)) = 1$. Let $a_{r+1} = -\Sigma_{j=1}^{r} a_j\sigma(b_j)$ and $b_{r+1} = 1$; then $\Sigma_{j=1}^{r+1} a_j b_j = 1$ but $\Sigma_{j=1}^{r+1} a_j\sigma(b_j) = 0$. To obtain the desired elements x_i, y_i of (b), it is then necessary only to multiply together the a_j and b_j constructed above for each non-trivial element of G. This establishes (b) and completes the proof of the theorem.

DEFINITION 1.4. If G is a finite group of automorphisms of a commutative ring S and $R = S^G$, then S will be called a Galois extension of R with Galois group G if any (and hence all) of the conditions of Theorem 1.3 hold.

REMARKS 1.5. (a) If S is a field, then condition (f) of Theorem 1.3 clearly holds, and so in this case our definition coincides with the usual one. Moreover, (a) and (c) then show that a Galois field extension is a finite separable extension of its fixed field of dimension equal to the order of the Galois group.

(b) In [2, p. 396], condition (c) is used as the definition of a Galois extension. That (c) implies (e) and the first statement of (a) is proved there, but by methods other than ours.

(c) Conditions (b) and (c) express the fact that the rings D and R, to-