ABELIAN GALOIS EXTENSIONS OF RINGS CONTAINING ROOTS OF UNITY

BY

L. N. CHILDS[1]

Let R be a commutative ring and A a Galois extension of R with abelian group G of exponent n. Then A is a rank one projective $R[G]$-module and is a free $R[G]$-module iff A has a normal basis. If R is connected, and contains $1/n$ and a primitive n-th root of unity, then $R[G]$ decomposes into the direct sum $\oplus R_i$ of copies of R (as rings), so that as $R[G]$-module, $A = \oplus A_j$, a direct sum of rank one projective R-modules. In this paper we first show (Theorem 1) that in this situation this decomposition makes A into a kind of generalized group ring with nicely described G-structure, so that if all the A_i are isomorphic to R, i.e., A has a normal basis, then A is a projective group algebra.

We then give two applications of Theorem 1. In Section 2 we investigate for central Galois extensions the relationship between Theorem 1 and a similar result of Kanzaki, to obtain a description of central abelian extensions with normal basis.

The set of isomorphism classes of all Galois extensions of R with abelian group G which are R-algebras forms an abelian group, with a subgroup consisting of classes of extensions which have normal basis. In Section 3 we use Theorem 1 and a result of G. Garfinkel and M. Orzech to compute the group of Galois extensions modulo those with normal basis when R and G satisfy the hypotheses cited above.

I wish to thank M. Orzech for suggesting some useful improvements.

0. Definitions and notation

All rings have units. A commutative ring R will be called connected if it has no idempotents but 0 and 1.

Let A be a ring, G a finite group of automorphisms, and $R = A^G$, the fixed ring of G. Assume R is contained in the center of A. Then A is a Galois extension of R with group G if there exist $x_1 \cdots x_n$, $y_1 \cdots y_n$ in A so that $\sum_i x_i \sigma(y_i) = \delta_{1,\sigma}$ for all σ in G. This particular choice of definition of Galois extension is equivalent to several other standard conditions (since [CHR 1.3(b) $\Leftrightarrow$ (c) $\Leftrightarrow$ (d) (e) $\Rightarrow$ (a)] remains valid). In particular, A is a separable R-algebra [D1, Theorem 1].

If A, A' are Galois extensions of R with group G, we say A and A' are isomorphic as Galois extensions if there is an R-algebra isomorphism of A onto A' which is at the same time a G-module homomorphism.

Received November 22, 1968.

[1] Research partially supported by a National Science Foundation grant at Northwestern University.

If G is abelian (resp. R is the center of A) we say A is an abelian (resp. central) Galois extension.

Let $\hat{G} = \text{Hom}(G, U(R))$ where $U(R)$ denotes the units of R. We will denote elements of G by σ, τ, ρ, and elements of $\hat{G}$ by χ, Ψ.

1. The structure theorem

THEOREM 1. *Let R be a connected commutative ring, G a finite abelian group of exponent n and order m and assume that R contains $1/n$ and a primitive n-th root of unity. Let A be a Galois extension of R with group G. Then $A = \otimes_{\chi\in\hat{G}} I_\chi$ where for each χ,*

$$I_\chi = \{a \in A \mid \sigma(a) = \chi(\sigma)a \text{ for all } \sigma \text{ in } G\}$$

is a rank one projective R-module, and for χ, ψ in $\hat{G}$, $I_\chi \cdot I_\psi = I_{\chi\psi}$.

Proof. We first note that since R is connected, there exist at most n n-th roots of unity ([J]), so that $\hat{G} \cong G$ and $R[G]$ decomposes as $R[G] = \oplus_{\chi\in\hat{G}} Rv_\chi$ where

$$v_\chi = \textstyle\sum_{\sigma\in G} \chi^{-1}(\sigma)u_\sigma/m$$

satisfy $v_\chi v_\psi = \delta_{\chi\psi} v_\chi$.

Set

$$I_\chi = v_\chi(A) = \left\{\sum_{\sigma\in G} \frac{\chi^{-1}(\sigma)\sigma(a) \mid a\in A}{m}\right\}.$$

Clearly if $b = \sum_\sigma \chi^{-1}(\sigma)\sigma(a)/m$ then $\chi(\alpha)b = \sigma(b)$ for all σ in G. Conversely, if b is in A and $\chi(\sigma)b = \sigma(b)$ for all σ in G, then

$$b = (1/m)\textstyle\sum_\sigma \sigma(b)/\chi(\sigma)$$

so b is in $v_\chi(A)$.

Since A is a rank 1 projective $R[G]$-module, each I_χ is a rank 1 projective R-module.

It is easy to show that $I_\chi \cdot I_\psi \subseteq I_{\chi\psi}$. Conversely, if a is in $I_{\chi\psi}$, then

$$a = \textstyle\sum_\sigma \chi^{-1}\psi^{-1}(\sigma)\sigma(a)/m.$$

Let x_i, y_i, $i = 1, \cdots, n$, be in A so that $\sum_i x_i\sigma(y_i) = \delta_{1,\sigma}$. Then

$$a = \textstyle\sum_{i,\tau} x_i\tau(y_i)\tau(a)\psi^{-1}(\tau),$$

so

$$a = \frac{1}{m}\sum_{\sigma,\tau,i} \chi^{-1}(\sigma)\psi^{-1}(\sigma)\sigma(x_i)\sigma\tau(y_i)\sigma\tau(a)\psi^{-1}(\tau)$$

$$= \sum_i \left[\sum_\sigma \frac{\chi^{-1}(\sigma)\sigma(x_i)}{m}\right]\left[\sum_\rho \frac{\psi^{-1}(\rho)\rho(y_i\,am)}{m}\right]$$

is in $I_\chi \cdot I_\psi$, completing the proof.

In case A is a Galois extension of R with normal basis, we have the following corollary.

COROLLARY 2. *With G, R, A as in Theorem* 1, *the following conditions are equivalent*:

(i) *For each χ in $\hat{G}$ there exists u_χ in I_χ so that $I_\chi = Ru_\chi$.*

(ii) *A has normal basis.*

(iii) *A is a projective group algebra, i.e., $A = \oplus_{\chi \in \hat{G}} Ru_\chi$ with multiplication $ru_\chi \cdot su_\chi = rsa(\chi, \psi)u_{\chi\psi}$, $a(\chi, \psi)$ in $U(R)$, with G acting on A via*

$$\sigma(u_\chi) = \chi(\sigma)u_\chi.$$

Proof. (i) $\Rightarrow$ (iii) is immediate from Theorem 1.

(i) $\Leftrightarrow$ (ii). Having a normal basis is equivalent to being free as an $R[G]$-module. But A is a free $R[G] = \oplus_\chi Rv_\chi$-module iff $A \oplus_{R[G]} Rv_\chi = v_\chi(A) = I_\chi$ is free over $Rv_\chi \cong R$ for each χ.

(iii) $\Rightarrow$ (i). If $A = \oplus_{\chi\in\hat{G}} Ru_\chi$ with σ in G acting on u_χ by $\sigma(u_\chi) = \chi(\sigma)u_\chi$, then clearly $Ru_\chi \subseteq I_\chi$ for all χ in $\hat{G}$, so (i) follows.

Remarks 3. The R-algebra isomorphism classes of projective group algebras with group G are in 1-1 correspondence with elements of $H^2(G, U(R))$. The verification that in fact with R as above there is an isomorphism between the group of isomorphism classes of Galois extensions with group G, having normal basis, and elements of $H^2(G, U(R))$, is a slight extension of results in [*W*], or can be obtained as a special case of the more general cohomological classification of abelian Galois extensions with normal basis in [CR] and [O].

4. With R, G as in Theorem 1, suppose S is a commutative Galois extension with group G. Then the decomposition of S as in Theorem 1 yields a collection of rank 1 projective R-modules I_χ split by S, whose isomorphism classes form a subgroup of

$$\text{Pic }(S/R) = \ker\{\text{Pic }(R) \to \text{Pic }(S)\}.$$

In terms of the well-known cohomological description

$$\text{Pic }(S/R) \cong H^1(G, U(S))$$

(e.g. [CHR, Corollary 5.5]) it is very easy to describe the subgroup consisting of the I_χ. For the map $H^1(G, U(S)) \to \text{Pic }(R)$ is induced by sending a cocycle $h : G \to U(S)$ to

$$I_h = \{s \in S \mid \sigma(s) = h(\sigma)s \text{ for all } \sigma \in G\}$$

Thus the subgroup of $H^1(G, U(S))$ corresponding to the I_χ is the image of $\text{Hom }(G, U(R)) = \hat{G}$ under the obvious map from $\text{Hom }(G, U(R))$ to $H^1(G, U(S))$.

2. On central abelian Galois extensions

For R connected, in order to have central Galois extensions of R with abelian group G of exponent n it is necessary that $1/n$ and a primitive n-th root of 1 be in R. Over local rings R this follows by results in [D1] and [D2]; the general statement follows by localizing. Thus the description of Theorem 1 applies in particular to all central abelian Galois extensions.

In [K3], T. Kanzaki obtained a description similar to that of Theorem 1 for central Galois extensions with not necessarily abelian Galois group G. In order to state his result we recall a definition:

Let A be a central separable (= Azumaya) R-algebra. Let σ be an R-algebra automorphism of A and let

$$J_\sigma = \{a \text{ in } A \mid \sigma(x)a = ax \text{ for all } x \text{ in } A\}.$$

Then J_σ is a rank one projective R-module and is free if and only if σ is an inner automorphism. If σ, τ are in $\operatorname{Aut}_R(A)$ then $J_\sigma \cdot J_\tau = J_{\sigma\tau}$ (see [RZ]).

Kanzaki's description is the following:

PROPOSITION 5 [K3, Corollary 2]. *If A is a central Galois extension of R with group G, then $A = \oplus_{\sigma\epsilon G} J_\sigma$.*

Assume now that A is a central abelian extension of R with group G. Our Theorem 1 showed that $A = \oplus_{\sigma\epsilon\hat{G}} I_\chi$, where

$$I_\chi = \{a \text{ in } A \mid \tau(a) = \chi(\tau)a \text{ for all } \tau \text{ in } G\}.$$

But in fact,

PROPOSITION 6. *There exists a map $\bar{\theta} : G \rightarrow \hat{G}$ such that $I_{\bar{\theta}(\sigma)} = J_\sigma$.*

Proof. Write a in I_χ as $a = \sum a_\sigma$, a_σ in J_σ. Since τ in G leaves J_σ stable one has easily that each a_σ is then in I_χ. Thus $I_\chi = \oplus_\sigma (I_\chi \cap J_\sigma)$ But by a rank argument only one of those summands can be non-zero. Let $\bar{\beta} : \hat{G} \rightarrow G$ be defined by setting $\bar{\beta}(\chi)$ to be that σ in G such that $I_\chi \cap J_\sigma \neq 0$. Then it follows easily that $\bar{\beta}$ is onto, hence bijective, and $I_\chi = J_{\bar{\beta}(\chi)}$ for all χ. That $\bar{\beta}$ is a homomorphism follows from the multiplicative properties of the I_χ and J_σ. Setting $\bar{\theta} = \bar{\beta}^{-1}$ completes the proof.

There is a bijection between the set of isomorphisms of G and $\hat{G}$ and the set of pairings, or bimultiplicative maps $G \times G \rightarrow U(R)$ which are non-singular ($\theta(\sigma, G) = 1 \Rightarrow \sigma = 1$), as follows: $\bar{\theta} : G \rightarrow \hat{G}$ an isomorphism yields $\theta : G \times G \rightarrow U(R)$ by $\theta(\sigma, \tau) = \bar{\theta}(\sigma)(\tau)$; $\eta : G \times G \rightarrow U(R)$ a non-singular pairing, yields $\bar{\eta} : G \rightarrow \hat{G}$ by $\bar{\eta}(\sigma)(\tau) = \eta(\sigma, \tau)$.

In terms of the map $\bar{\theta}$ and its associated pairing θ we have the following immediate results on the structure of A:

COROLLARY 7. (i) *For a in $J_\sigma = I_{\bar{\theta}(\sigma)}$, $\tau(a) = \bar{\theta}(\sigma)(\tau)a = \theta(\sigma, \tau)a$.*
(ii) *For a_σ in J_σ, b_τ in J_τ, $a_\sigma b_\tau = \theta(\tau, \sigma) b_\tau a_\sigma$.*

In the special case where we have an extension of the form

$$A = \oplus Ru_\sigma = \oplus Ru_{\bar{\theta}(\sigma)},$$

then

$$u_\sigma u_\tau = a(\sigma, \tau)u_{\sigma\tau}$$

for some factor set $a(\sigma, \tau)$, so

$$\theta(\sigma, \tau) = a(\tau, \sigma)a(\sigma, \tau)^{-1}$$

and the map $\bar{\theta}$ of Proposition 6 arises from the factor set $a(\sigma, \tau)$. This fact, together with Corollaries 2 and 7, yields

THEOREM 8. *Let R be connected and let A be a central abelian Galois extension with normal basis. Then $A = \oplus Ru_\sigma$ is a projective group algebra with elements τ of G acting on A via conjugation by u_τ.*

This is a converse to Theorem 13 of [D2].

3. On Galois extensions without normal basis

In this section we apply Theorem 1 to describe (with R, G as in Theorem 1) the group of Galois extensions modulo those with normal basis.

Let R be a commutative ring, and denote by Gal (R, G) the set of isomorphism classes (as Galois extensions) of Galois extensions of R with abelian group G. Denote by NGal (R, G), Comm (R, G) and NComm (R, G) the subsets of Gal (R, G) consisting of those isomorphism classes of Galois extensions which have normal basis, which are commutative, and which are commutative with normal basis, respectively. An abelian group structure can be put on Gal (R, G) which makes the subsets NGal (R, G), etc., subgroups. This group structure was first described by Harrison ([H], see also [O]), and is obtained by setting the product $(A)\cdot(B)$ of two Galois extensions A, B of R with group G, as the fixed ring of $A \otimes_R B$, an element of Gal $(R, G \times G)$, with respect to the subgroup of $G \times G$ consisting of the kernel of the multiplication map $G \times G \to G$.

For any commutative ring R let Pic (R) denote the group of isomorphism classes of rank one projective R-modules, with multiplication induced by tensor product (over R) [BAC 2].

G. S. Garfinkel and M. Orzech [GO, Theorem 2] showed that the map Gal (R, G) to Pic $(R[G])$ induced by viewing a Galois extension as a rank one projective $R[G]$ module via the obvious action, is a homomorphism of abelian groups, whose kernel, clearly, is the subgroup NGal (R, G).

Under the assumptions on R and G made in Theorem 1, we can describe the image of that map. (All tensor products are taken over R.)

THEOREM 9. *Let G be a finite abelian group which is the direct product of cyclic groups, $G = \times_{i=1}^{k} G_1$ of orders $e_1, \cdots, e_k$. Let n be the exponent of G, and let R be a connected commutative ring containing $1/n$ and a primitive n-th root of unity (i.e., R and G are as in Theorem 1). Denote by* Pic $(R)(e)$ *the elements of* Pic (R) *annihilated by e (where e is a positive integer). Then we have*

$$\text{Gal}(R, G)/\text{NGal}(R, G) \cong \text{Comm}(R, G)/\text{NComm}(R, G) \cong \times_{i=1}^{k} \text{Pic}(R)(e_i).$$

Proof. Let G be as in the theorem, and fix χ_i, a generator of $\hat{G}_i$, for each i. Then, by Theorem 1, any Galois extension is, as $R(G)$-module, of the form

$$A = \oplus_\chi I_\chi = \otimes_{i=1}^k \oplus_j (I_{\chi_i})^j \qquad (j = 1, \cdots, e_i)$$

since for any χ, ψ *in* $\hat{G}$

$$I_\chi \otimes I_\psi = I_\chi \cdot I_\psi = I_{\chi\psi}.$$

So as $R[G]$-module, A is completely determined by the set $\{I_{\chi_i}, \cdots, I_{\chi_k}\}$. We map A into the class of $(I_{\chi_i}, \cdots, I_{\chi_k})$ in $\times_{i=1}^k \operatorname{Pic}(R)$. By the multiplicative properties of the I_χ's it is clear that the image of A under this map is in $\times_{i=1}^k \operatorname{Pic}(R)(e_i)$. Since this map is the composition of the map

$$\operatorname{Gal}(R, G) \to \operatorname{Pic}(R[G]) \cong \times_{\chi \in \hat{G}} \operatorname{Pic}(R)_\chi$$

followed by projection onto the factors of $\times_{\chi\in\hat{G}} \operatorname{Pic}(R)_\chi$ corresponding to the generators χ_i, the map is a homomorphism. By Corollary 2 this map yields a monomorphism of $\operatorname{Gal}(R, G)/\operatorname{NGal}(R, G)$ into $\times \operatorname{Pic}(R)(e_i)$.

In order to finish the proof it is enough to show that the map $\operatorname{Comm}(R, G)$ to $\times \operatorname{Pic}(R)(e_i)$ is onto. Now it suffices to show this latter fact in case G is cyclic. For suppose we have shown the cyclic case. Then, given $G = \times G_i$, χ_i, e_i as above, for each i let P_i be a representative of a class in $\operatorname{Pic}(R)(e_i)$, and let S_i be a Galois extension of R with group G_i such that

$$S_i = \oplus_{j=1}^{e_i} (I_{\chi i})^j$$

and $I_{\chi i} \cong P_i$. Then $S = \otimes_{i=1}^k S_i$ is a commutative Galois extension with group G, and as $R[G]$-module,

$$S = \otimes_{i=1}^k \oplus_{j=1}^{e_i} (I_{\chi i})^j,$$

so S goes under the map we have defined to the class of $(I_{\chi_1}, \cdots, I_{\chi_k})$, which is the same as the class of $(P_1, \cdots, P_k)$, in $\times \operatorname{Pic}(R)(e_i)$.

The cyclic case in an immediate consequence of part (b) of the following independently interesting result, suggested to the author by R. T. Hoobler and G. S. Garfinkel.

PROPOSITION 10. *Let R be a commutative ring. Let P represent a class in* $\operatorname{Pic}(R)(e)$. *Denoting $P \otimes P \otimes \cdots \otimes P$ (r times) by $P^{(r)}$, let $P^{(e)} = Ru$ for some u in $P^{(e)}$. Let $R(P)$ denote the ring $T(P)/(u - 1)$, where $T(P)$ is the tensor algebra over R of P (and 1 is in $P^{(0)}$). Then*

(a) *$R(P)$ is a commutative ring, and is a separable R-algebra iff e is a unit in R.*

(b) *If R is connected and contains $1/e$ and a primitive e-th root of 1, then if χ is a given generator of $\hat{Z}_e$, $R(P)$ is a Galois extension of R with cyclic group Z_e, in such a way that*

$$P = P^{(1)} = \{a \in R(P) \mid \sigma(a) = \chi(\sigma)a \text{ for all } \sigma \text{ in } G\}$$

Proof. (a) That $R(P)$ is commutative follows from Proposition 3 of [G] (or by localizing); the separability is Proposition 4 of [G] (or can be obtained by localizing and using results in [J, Section 2]).

(b) First note that if ζ, ζ' are *e-th* roots of unity in R, then $\zeta - \zeta'$ is a unit of R (by [J, Propositions 2.1 and 2.4], since e is a unit in R).

Since $R(P) \cong R \oplus P \oplus \cdots \oplus P^{(e-1)}$ as R-modules, we shall abusively identify the two sides.

Let σ and χ be generators of $G = Z_e$ and $\hat{G}$, respectively, and define an action of G on $R(P)$ via $\sigma(p) = \chi(\sigma)p$ for p in $P = P^{(1)}$, extending by linearity and by diagonal action on tensor products. Then

$$P^{(r)} = \{a \text{ in } R(P) \mid \tau(a) = \chi^r(\tau)a \text{ for all } \tau \text{ in } G\}$$

for all $r = 0, \cdots, e-1$. In particular, $R(P)^G = R = P^{(0)}$. To show that $R(P)$ is a Galois extension of R with group G, since $R(P)$ is separable over R, it suffices by Theorem 1.3a of [CHR] to show that the elements of G are pairwise strongly distinct on $R(P)$ (in the terminology of [CHR]). That is, if u is a non-zero idempotent of $R(P)$ and $\sigma^i, \sigma^j, i \neq j$, are any two distinct elements of G, then there exists an x in $R(P)$ such that

$$\sigma^i(x)u \neq \sigma^j(x)u.$$

Let u be an idempotent of $R(P)$ such that for all x in $P^{(1)}$

$$\sigma^i(x)u = \sigma^j(x)u.$$

Then, since $\sigma(x) = \zeta x$ for ζ some primitive *e-th* root of unity, we have $(\xi^i - \zeta^j)xu = 0$. But if $i \neq j$, $\zeta^i - \zeta^j$ is a unit of R so $xu = 0$ for all x in $P^{(1)}$. The elements of $P^{(1)}$ generate $R(P)$, so u must therefore be 0.

Thus the elements of G are pairwise strongly distinct on $R(P)$, proving (b), Proposition 10, and Theorem 9.

Remark 11. Theorem 9 shows that

$$\text{Gal }(R, G)/\text{NGal }(R, G) \cong H^1(G, \text{Pic }(R))$$

when R, G satisfy the hypotheses of Theorem 1. Since group cohomology and Harrison cohomology coincide in this case [CR], Theorem 9 shows that Gal (R, G)/NGal (R, G) is isomorphic to the "primitive" elements of Pic $(R[G])$, those classes (P) in Pic $(R[G])$ such that

$$\text{Pic }(\epsilon_1)(P)\ \text{Pic }(\epsilon_2)(P) = \text{Pic }(\Delta)(P)$$

where $\varepsilon_1, \varepsilon_2, \Delta : R[G] \to R[G] \otimes_R R[G]$ are defined by R-linearity and $\varepsilon_1(\sigma) = 1 \otimes \sigma$, $\epsilon_2(\sigma) = \sigma \otimes 1$ and $\Delta(\sigma) = \sigma \otimes \sigma$, resp. This interpretation of Theorem 9 was pointed out by W. C. Waterhouse, who has raised the open question whether the assumptions on R can be relaxed.

References

BAC2. N. Bourbaki, *Algebre commutative*, Chapter 2, Eleménts de Mathématique, Livre XXVIII, Hermann, Paris, 1961.

CHR. S. CHASE, D. HARRISON, A. ROSENBERG, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc., no. 52, 1965. pp. 15–33.

CR2. S. CHASE AND A. ROSENBERG, *A theorem of Harrison, Kummer theory and Galois algebras*, Nagoya Math. J., vol. 27 (1966), pp. 663–685.

D1. F. R. DE MEYER, *Galois theory in separable algebras over commutative rings*, Illinois J. Math., vol. 10 (1966), pp. 287–295.

D2. ——— , *Some notes on the general Galois theory of rings*, Osaka J. Math., vol. 2 (1965), pp. 117–127.

GO. G. S. GARFINKEL AND M. ORZECH, *Galois extensions as modules over the group ring*, Canad. J. Math., vol. 22 (1970), pp. 242–248.

G. G. S. GARFINKEL, *Generic splitting algebras for Pic*, Pacific J. Math., vol. 35 (1970), pp. 369–380.

H. D. K. HARRISON, *Abelian extensions of commutative rings*, Mem. Amer. Math. Soc., no. 52, 1965, pp. 1–14.

J. G. J. JANUSZ, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc., vol. 122 (1966), pp. 461–479.

K2. T. KANZAKI, *On Galois extension of rings*, Nagoya Math. J. vol. 27 (1966), pp. 43–49.

K3. ——— , *On Galois algebra over a commutative ring*, Osaka J. Math., vol. 2 (1965), pp. 309–317.

O. M ORZECH, *A cohomological description of abelian Galois extensions*. Trans. Amer. Math. Soc., vol. 137 (1969), pp. 481–499.

RZ. A. ROSENBERG AND D. ZELINSKY, *Automorphisms of separable algebras*, Pacific J. Math., vol. 11 (1961), pp. 1109–1118.

W. P. WOLF, *Algebraische Theorie der Galoisschen Algebren*, Deutscher Verlag, Berlin, 1956.

STATE UNIVERSITY OF NEW YORK
ALBANY, NEW YORK