GALOIS EXTENSIONS AS MODULES OVER THE GROUP RING

GERALD GARFINKEL AND MORRIS ORZECH

1. Introduction. Suppose that R is a commutative ring and G is a finite abelian group. In § 2 we review the definition of $E(R, G)$ $(T(R, G))$, the group of all (commutative) Galois extensions S of R with Galois group G. We discuss the properties of these groups as functors of G and give an example which exhibits some of the pathological properties of the functor $E(R, -)$. In § 3 we display a homomorphism from $E(R, G)$ to $\mathrm{Pic}(R(G))$; we use this homomorphism to prove that if S is commutative, G has exponent m, and $R(G)$ has Serre dimension 0 or 1, then a direct sum of m copies of S is isomorphic as a G-module to a direct sum of m copies of $R(G)$. (This result is related to [**5**, Theorem 4.2], where it is shown that if S is a free R-module and G is any finite group with n elements, then S^n is isomorphic to $R(G)^n$ as G-modules.) We also give some examples of Galois extensions without normal bases.

2. The groups $E(R, G)$ **and** $T(R, G)$**.** Let R be a commutative ring, let G be a finite group, and suppose that S is an R-algebra on which G acts as a group of R-algebra automorphisms. S is said to be a Galois extension of R with group G if (i) $S^G = R$, where $S^G = \{s \text{ in } S \mid xs = s \text{ for all } x \text{ in } G\}$; and (ii) there exist $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ such that $a_1xb_1 + \ldots + a_nxb_n = \delta_{1,x}$ for all x in G. We will use [**5**] and [**9**] as references for facts about Galois extensions.

Let $\mathscr{E}(R, G)$ denote the category whose objects are Galois extensions of R with group G; a morphism is a map which is an R-algebra homomorphism and an RG-module homomorphism. In [**5**, Theorem 3.4] it is shown that a morphism between commutative Galois extensions is an isomorphism. The argument in [**5**] actually proves the stronger result below.

Proposition 1. *Let S_1 and S_2 be R-algebras on which G acts as a group of R-algebra automorphisms. Suppose that ${S_2}^G = R$ and suppose that S_1 is a Galois extension of R with group G. Let $j: S_1 \to S_2$ be a map which is an R-algebra homomorphism and an RG-module homomorphism. Then j is an isomorphism.*

Let G be a finite *abelian* group, and define an equivalence relation on the objects of $\mathscr{E}(R, G)$ by writing $S_1 \sim S_2$ if S_1 and S_2 are isomorphic. The set $E(R, G) = \mathscr{E}(R, G)/\sim$ may be given the structure of an abelian group [**7**, § 1]: Writing (S) for the class of S in $E(R, G)$, the multiplication is defined by $(S_1)(S_2) = ((S_1 \otimes_R S_2)^{\delta G})$; here $\delta G = \{(x, x^{-1}) \text{ in } G \times G\}$ and $G \times G$ acts

Received November 22, 1968. This research was partially supported by research grant NSF GP-5926.

on $S_1 \otimes_R S_2$ by $(x, y)(s_1 \otimes s_2) = xs_1 \otimes ys_2$. G acts on $(S_1)(S_2)$ by $x(s_1 \otimes s_2) = xs_1 \otimes s_2$. $(S)^{-1}$ is given by $(S)^{-1} = (S^{-1})$, where

$$S^{-1} = \{\text{Set maps } v\colon G \to S \mid v(x^{-1}y) = xv(y) \text{ for all } x \text{ and } y \text{ in } G\}.$$

The multiplication on S^{-1} is pointwise, and the G-action is $(xv)(y) = v(yx)$. The identity element of $E(R, G)$ is $(e_G(R))$, where $e_G(R) = \{\text{Set maps } v\colon G \to R\}$; the action of G on $e_G(R)$ is given by $(xv)(y) = v(yx)$. That these operations give $E(R, G)$ a well-defined group structure is shown in [**7**, § 1]. It is easy to verify that S^{-1} is isomorphic in $\mathscr{E}(R, G)$ to the R-algebra having S for its underlying set, but with "inverse" G-action.

If $\mathscr{T}(R, G)$ denotes the full subcategory of $\mathscr{E}(R, G)$ whose objects are *commutative* R-algebras, then $\sim$ defines an equivalence relation on $\mathscr{T}(R, G)$, and $T(R, G) = \mathscr{T}(R, G)/\sim$ is a subgroup of $E(R, G)$; Harrison dealt with this group in [**6**].

Not only are $E(R, G)$ and $T(R, G)$ abelian groups, but $E(R, -)$ and $T(R, -)$ are functors from the category of finite abelian groups to the category of abelian groups. Harrison showed this for $T(R, -)$ [**6**, p. 3], and a proof applicable to our situation is given in [**7**, Theorems 1.2 and 1.9]. The definition of the functoriality of $E(R, -)$ and $T(R, -)$ is sketched here for convenience.

Let $\phi\colon G \to H$ be a homomorphism of finite abelian groups. Let S be a Galois extension of R with group G. Define

$$\phi(S) = \{\text{Set maps } v\colon H \to S \mid v(\phi(x)y) = xv(y) \text{ for } x \text{ in } G \text{ and } y \text{ in } H\}.$$

Define a pointwise multiplication on $\phi(S)$, and an H-action given by $(yv)(z) = v(zy)$ for y and z in H. Now $E(R, \phi)((S)) = (\phi(S))$ determines a homomorphism from $E(R, G)$ to $E(R, H)$. It also induces a homomorphism from $T(R, G)$ to $T(R, H)$. We note that $(S)^{-1} = E(R, t)((S))$, where $t\colon G \to G$ is given by $t(x) = x^{-1}$.

The following two facts about Galois extensions should also be explicitly noted.

(1) Let S_1 and S_2 be Galois extensions of R with respective groups G and H. Then $S_1 \otimes_R S_2$ is a Galois extension of R with group $G \times H$, the action being given by $(x, y)(s_1 \otimes s_2) = xs_1 \otimes ys_2$.

(2) Let H be a subgroup of G and let S be a Galois extension of R with group G. Let $S^H = \{s \text{ in } S \mid xs = s \text{ for all } x \text{ in } H\}$. G/H acts on S^H via $(xH)s = xs$, and S^H is a Galois extension of R with group G/H. If $\phi\colon G \to G/H$ is the canonical projection, then $E(R, \phi)((S)) = (S^H)$ in $E(R, H)$.

The two facts just listed are proved in [**9**, Proposition 1 and Theorem 1].

Let i_1 and i_2 be the homomorphisms from G to $G \times G$ given by $i_1(x) = (x, 1)$ and $i_2(x) = (1, x)$, respectively. The maps $E(R, i_1)$ and $E(R, i_2)$ from $E(R, G)$ to $E(R, G \times G)$ induce a map $\mu\colon E(R, G) \times E(R, G) \to E(R, G \times G)$, which may be shown to be given by $\mu((S_1), (S_2)) = (S_1 \otimes_R S_2)$ [**6**, p. 3]. Moreover, μ induces a map $\nu\colon T(R, G) \times T(R, G) \to T(R, G \times G)$. The projections p_1

and p_2 from $G \times G$ to G, onto the first and second factors, respectively, induce homomorphisms χ: $E(R, G \times G) \to E(R, G) \times E(R, G)$ and

$$\theta: T(R, G \times G) \to T(R, G) \times T(R, G).$$

Using Proposition 1, it is not difficult to see that $\chi((D)) = ((D^{1\times G}), (D^{G\times 1}))$, and θ is defined by the same formula when D is commutative. In [**6**], Harrison showed that θ and ν are isomorphisms inverse to each other. Thus $T(R, -)$ is an additive functor.

PROPOSITION 2. *$\chi\mu$ is the identity map on $E(R,G) \times E(R,G)$, so that $E(R, G) \times E(R, G)$ is a direct summand of $E(R, G \times G)$.*

Proof. Let S_1 and S_2 be Galois extensions with group G. We wish to show that $S_1 \sim (S_1 \otimes_R S_2)^{1\times G}$. Define j: $S_1 \to (S_1 \otimes_R S_2)^{1\times G}$ by $j(s) = s \otimes 1$. Using fact (2) above and Proposition 1, we can conclude that j is an isomorphism. We remark that the present proposition follows from the fact that $E(R, -)$ is a functor which sends the 0-object to the 0-object.

The following example is referred to in [**4**, p. 684].

Example I. χ need not be an isomorphism. Let R be any integral domain containing 1/2. Let D be the ring of 2×2 matrices over R. Let G be the cyclic group of order 2, with x as its generator. Let $G \times G$ act on D as follows:

$$(x, 1)\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}; \qquad (1, x)\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & c \\ b & a \end{pmatrix};$$
$$(x, x)\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}.$$

It is easy to see that $G \times G$ acts as a group of R-algebra automorphisms of D, and that $D^G = R$. Let e_{ij} denote the element of D with 1 in the ith row and jth column, and zeros elsewhere. Let $a_1 = e_{11}$, $a_2 = e_{22}$, $a_3 = e_{12}$, $a_4 = e_{21}$, $b_1 = \frac{1}{2}e_{11}$, $b_2 = \frac{1}{2}e_{22}$, $b_3 = \frac{1}{2}e_{21}$, $b_4 = \frac{1}{2}e_{12}$. Then $a_1yb_1 + \ldots + a_4yb_4 = \delta_{1,y}$ so that D is a Galois extension of R with group $G \times G$. Now $D^{1\times G}$ and $D^{G\times 1}$ are Galois extensions of R with cyclic group G, and it is easily verified that they are commutative; $D^{G\times 1}$ is the set of diagonal matrices. It is trivial to verify that $D^{G\times 1}$ is the trivial Galois extension of R with group G. Moreover, $D^{1\times G}$ is the set of matrices of the form $\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)$. An isomorphism from $D^{1\times G}$ to

$$e_G(R) = \{\text{Set maps } v: G \to R\}$$

is given by

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \to v, \quad \text{where } v(1) = a + b \text{ and } v(x) = a - b.$$

Thus D is in the kernel of χ, but not being commutative, it is not the trivial extension. The element $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ gives rise to a normal basis for D. Letting R be the complex numbers, for example, provides us with an example of a nontrivial Galois extension of an algebraically closed field. No such commutative extensions exist.

3. Galois extensions as rank 1 projectives. The following result is proved in [**7**, Theorem 3.6].

THEOREM 1. *Let G be a finite abelian group, and let S be a Galois extension of R with group G. Then S is a finitely generated projective RG-module of rank* 1.

LEMMA 1. *Let S be a Galois extension of R with (not necessarily abelian) group G. Let H be a subgroup of G. Define a map $\mathrm{tr}_H\colon S \to S^H$ by $\mathrm{tr}_H(s) = \sum_{x\in H} xs$. Then tr_H maps S onto S^H.*

Proof. Choose e in S such that $\sum_{x\in G} xe = 1$; that such an element exists is shown in [**5**, Lemma 1.6]. Let $Hy_1, \ldots, Hy_m$ be a complete set of cosets of H in G, and let $e' = \sum_{i=1}^{m} y_i e$. Then $\mathrm{tr}_H(e') = \mathrm{tr}_G(e) = 1$. Now tr_H is a (right and left) S^H-linear map, and hence it is onto S^H.

We may consider the abelian group $\mathrm{Pic}(RG)$ [**2**, *chapitre* 2, § 5, no. 4] of isomorphism classes of projective RG-modules of rank 1; we are here assuming that G is a finite abelian group. For $\langle P\rangle$, $\langle Q\rangle$ classes in $\mathrm{Pic}(RG)$, $\langle P\rangle\langle Q\rangle$ is defined to be $\langle P \otimes_{RG} Q\rangle$. The inverse element $\langle P\rangle^{-1}$ is $\langle \mathrm{Hom}_{RG}(P, RG)\rangle$.

THEOREM 2. *Let S_1 and S_2 be Galois extensions of R with abelian group G. Then $S_1 \otimes_{RG} S_2$ may be given the structure of a Galois extension of R with group G, and as such, it is isomorphic to $(S_1 \otimes_R S_2)^{\delta G}$. In particular, the natural map from $E(R, G)$ to $\mathrm{Pic}(RG)$, which sends (S) to $\langle S\rangle$, is a homomorphism of abelian groups.*

Proof. To condense notation, we adopt several definitions. An unadorned tensor product will be over R. If P and Q are RG-modules, then $P \otimes_{RG} Q$ will be written as $P \bigotimes Q$; for p in P and q in Q we shall write $p \bigotimes q$ for the element $p \otimes q$ of $P \otimes_{RG} Q$. We have a canonical epimorphism $\rho\colon P \otimes Q \to P \bigotimes Q$. Now let S be a Galois extension of R with group G. The trace map $\mathrm{tr}\colon S \to R$ is defined by the formula $\mathrm{tr}(a) = \sum_{x\in G} xa$. By [**5**, Lemma 1.6], there is an element e of trace 1 in S. For S_1 and S_2, Galois extensions of R with group G, define $\kappa\colon S_1 \otimes S_2 \to S_1 \otimes S_2$ by

$$\kappa(a \otimes b) = \sum_{x\in G} xa \otimes x^{-1}b.$$

We note that κ is a map into $(S_1 \otimes S_2)^{\delta G}$, and in fact it is a map onto the latter set by Lemma 1. (Recall that $\delta G = \{(x, x^{-1})\}$ in $G \times G$, and $(S_1 \otimes S_2)^{\delta G}$ denotes the set of elements of $S_1 \otimes S_2$ which are fixed by δG.)

Define an operation $\circ$ on $S_1 \bigotimes S_2$ by setting $\rho(a) \circ \rho(b) = \rho(\kappa(a)b) = \rho(a\kappa(b))$, i.e. for s_i and s_i' in S_i, we have

$$(s_1 \bigotimes s_2) \circ (s_1' \bigotimes s_2') = \sum_{x\in G} x(s_1)s_1' \bigotimes x^{-1}(s_2)s_2'.$$

It is easy to verify that this operation is well-defined, and that it endows

$S_1 \otimes S_2$ with the structure of an associative ring. Letting e_i, $i = 1, 2$, be the element of trace 1 in S_i, we see that $e_1 \otimes 1 = 1 \otimes e_2$ is a unity element of $S_1 \otimes S_2$; the latter is also an R-algebra, where r in R is identified with $e_1 \otimes r$. Moreover, $S_1 \otimes S_2$ has a G-module structure with

$$x(s_1 \otimes s_2) = xs_1 \otimes s_2 = s_1 \otimes xs_2$$

for s_i in S_i and x in G, $i = 1, 2$. With this action, the elements of G act as R-algebra automorphisms of $S_1 \otimes S_2$.

We remark that for r in R and s in S_2, we have that $r \otimes s$ is in R. For, $r \otimes s = 1 \otimes rs = \mathrm{tr}(e_1) \otimes rs = e_1 \otimes \mathrm{tr}(rs)$.

The trace map tr: $S_1 \otimes S_2 \to S_1 \otimes S_2$, given by $\mathrm{tr}(a) = \sum_{x \in G} xa$, thus maps $S_1 \otimes S_2$ to R; it is R-linear and maps $e_1 \otimes e_2$ to the identity element $e_1 \otimes 1$, so that tr: $S_1 \otimes S_2 \to R$ is an epimorphism. Since the trace map is $(S_1 \otimes S_2)^G$-linear, it follows that $(S_1 \otimes S_2)^G = R$.

Now define j: $(S_1 \otimes S_2)^{\delta G} \to S_1 \otimes S_2$ by $j(u) = \rho(u(e_1 \otimes 1))$. From the definition of the multiplication in $S_1 \otimes S_2$ and from the fact that κ is $(S_1 \otimes S_2)^{\delta G}$-linear, it follows that j is a multiplicative map. It can be easily verified that j is an R-algebra and RG-module homomorphism, and is thus an isomorphism by Proposition 1. This completes the proof of the theorem.

Remarks. (a) The inverse of j may be verified to be given by the formula $j^{-1}(\rho(a)) = \kappa(a)$.

(b) A less computational proof, using homological machinery, can be given for the existence of a homomorphism $T(R, G) \to \mathrm{Pic}(RG)$, given by $(S) \to \langle S \rangle$. Let A be a faithfully-flat commutative R-algebra. Then

$$H^1(A/R, U(-G)) \cong \mathrm{Ker}(\mathrm{Pic}(RG) \to \mathrm{Pic}(AG)),$$

where $U(AG)$ denotes the group of units of AG, H^1 is the first Amitsur cohomology group, and the map $\mathrm{Pic}(RG) \to \mathrm{Pic}(AG)$ is given by $\langle P \rangle \to \langle AG \otimes_{RG} P \rangle$ [**3**, Corollary 4.6]. Let

$$V(AG) = \left\{ \sum_{x \in G} a_x x \text{ in } AG \,\middle|\, a_x a_y = \delta_{x,y} a_x \text{ and } \sum_{x \in G} a_x = 1 \right\}.$$

Then

$$H^1(A/R, V(-G)) \cong \mathrm{Ker}(T(R, G) \to T(A, G)),$$

where the map $T(R, G) \to T(A, G)$ is given by $(S) \to (A \otimes_R S)$ for (S) in $T(R, G)$; this follows from [**7**, Theorem 3.9] and from the observation that if $A \otimes_R S$ is commutative, then S is commutative. Now $V(AG) \subset U(AG)$, and hence there is a natural map $H^1(A/R, V(-G)) \to H^1(A/R, U(-G))$, which when composed with the isomorphisms just given yields a homomorphism τ from $\mathrm{Ker}(T(R, G) \to T(A, G))$ to $\mathrm{Ker}(\mathrm{Pic}(RG) \to \mathrm{Pic}(AG))$. By scrutinizing the construction of the isomorphisms mentioned above, it can be seen that $\tau((S)) = \langle S \rangle$. By using the naturality in A of the maps involved, and the fact that (S) is in the kernel of $T(R, G) \to T(S, G)$, we obtain a homomorphism $(S) \to \langle S \rangle$ from $T(R, G)$ to $\mathrm{Pic}(RG)$.

PROPOSITION 3. *Let S be a commutative Galois extension of R with abelian group G. Suppose that G has exponent n. Then $S \otimes_{RG} \ldots \otimes_{RG} S$ (n times) is isomorphic to RG as an RG-module. Indeed, $S \otimes_{RG} \ldots \otimes_{RG} S$ is the trivial Galois extension of R with group G.*

Proof. Letting (S), as usual, denote the class of S in $T(R, G)$, we have from [**6**, Theorem 4] that $(S)^n = 1$ in $T(R, G)$. From Theorem 2 we conclude that $\langle S\rangle^n = 1$, i.e. that $S \otimes_{RG} \ldots \otimes_{RG} S \cong RG$ as RG-modules.

4. Normal bases. Let R be a commutative ring of Serre dimension 1, i.e. any finitely generated projective R-module P may be decomposed as $P = F \oplus P_0$, where F is free and P_0 is of rank 1. It is known [**2**, *chapitre* 2, § 5, *exercise* 21 (c)] that if the n-fold tensor product of P with itself (over R) is isomorphic to R, and if P is a finitely generated projective R-module of rank 1, then the n-fold direct sum of P with itself is isomorphic to R^n. This follows readily by writing $P^n \cong R^{n-1} \oplus P_0$ and then taking the nth exterior product of both sides. Using Proposition 3, we obtain the following analogue of [**5**, Theorem 4.2] for G abelian.

THEOREM 3. *Let S be a commutative Galois extension of R with abelian group G. Suppose that G has exponent n. Let RG have Serre dimension at most* 1. *Then a direct sum of n copies of S is RG-isomorphic to a direct sum of n copies of RG.*

The ring RG has Serre dimension at most 1, for example, if R is a semi-local ring, or if R is a finite-dimensional algebra over a Dedekind domain [**1**, Proposition 10.1].

Example II. We conclude with an example of a Galois extension S of a ring R which does not have a normal basis. Such examples exist in the case where R and S are rings of integers of number fields; e.g. let $K = Q(\sqrt{(-5)})$, $L = K(i)$ [L. R. McCulloh, private communication]. The example here is topological in character.

Let X denote the real n-sphere, for $n \geqq 1$. Let τ be the map of X to itself obtained by reflecting each point through the centre, i.e. τ sends a point to its antipode. Then $\{1, \tau\} = G$ is a group acting on X without fixed points; let Y be the identification space X/G, i.e. projective n-space. Let $C(X)$ and $C(Y)$ denote the rings of continuous functions of X and Y to the real numbers. By [**5**, p. 21, example (e)], $C(X)$ is a Galois extension of $C(Y)$ with group G. However, $C(X)$ does not have a normal basis. For suppose α in $C(X)$ gives rise to a normal basis, i.e. α and $\tau\alpha$ freely generate $C(X)$ over $C(Y)$. By the Borsuk-Ulam Theorem [**8**, Theorem 9, p. 266], there exists a pair of antipodal points, call them p and p', such that $\alpha(p) = \alpha(p')$. But then, every element of $C(X)$ would have the same value on p and p'. This is patently false.

REFERENCES

1. H. Bass, *K-theory and stable algebras,* Inst. Hautes Etudes Sci. Publ. Math. No. 22 (1964), 5–60.

2. N. Bourbaki, *Eléments de mathématique*, Fasc. XXVII, *Algèbre commutative*, Chapitre 1: *Modules plats*, Chapitre 2: *Localization*, Actualités Sci. Indust., No. 1290 (Hermann, Paris, 1961).
3. S. U. Chase and Alex Rosenberg, *Amitsur cohomology and the Brauer group*, Mem. Amer. Math. Soc. No. 52 (1965), 34–79.
4. ——— *A theorem of Harrison, Kummer theory, and Galois algebras*, Nagoya Math. J. *27* (1966), 663–685.
5. S. U. Chase, D. K. Harrison, and Alex Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965), 15–33.
6. D. K. Harrison, *Abelian extensions of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965), 1–14.
7. M. Orzech, *A cohomological description of abelian Galois extensions*, Trans. Amer. Math. Soc. *137* (1969), 481–499.
8. E. H. Spanier, *Algebraic topology* (McGraw-Hill, New York, 1966).
9. Y. Takeuchi, *On Galois extensions over commutative rings*, Osaka J. Math. *2* (1965), 137–145.

University of Illinois,
Urbana, Illinois;

University of Illinois, *and* *Queen's University,*
Urbana, Illinois *Kingston, Ontario*

https://doi.org/10.4153/CJM-1970-031-6 Published online by Cambridge University Press