A COHOMOLOGICAL DESCRIPTION OF ABELIAN GALOIS EXTENSIONS

BY
MORRIS ORZECH[1]

Let J be a finite abelian group, and let R be a commutative ring. Let $E_R(J)$ denote the set of equivalence classes of Galois extensions of R with group J, and let $A_R(J)$ denote the subset of $E_R(J)$ consisting of those extensions which have a normal basis.

In [8], Chase and Rosenberg obtained a bijection of pointed sets, $A_R(J) \cong H^2(R, J)$, where $H^2(R, J)$ is the cohomology group that Harrison denoted by $H^2(R(J), R(H))$ [11].

We show that this bijection is an isomorphism of abelian groups, and that it is natural in R and J (§§1 and 2). Let S be a faithfully flat commutative R-algebra. Using techniques similar to those employed in [7], a double complex is defined, depending on S and J, whose two coboundary maps are those of Harrison [11] and Amitsur [1]. The first cohomology group of this double complex is shown to be isomorphic to a subgroup of $E_R(J)$ (§3). By passing to the direct limit over those faithfully flat R-algebras which arise from partitions of unity in R, we obtain an isomorphism between $E_R(J)$ and a cohomology group H^1 depending only on R and J. We then have that the inclusion of $A_R(J)$ in $E_R(J)$ is given as the composite $A_R(J) \cong H^2(R, J) \to H^1 \cong E_R(J)$, where the middle map α is an edge homomorphism. Under certain assumptions α is an isomorphism, and then every Galois extension of R with group J has a normal basis (§4).

This paper constitutes a portion of the author's doctoral dissertation at Cornell University. The author wishes to thank S. U. Chase for his helpful advice and encouragement.

1. **Groups of Galois extensions.** In this section we will establish some properties of (not necessarily commutative) Galois extensions, and of certain sets of such extensions. In what follows, R will always denote a commutative ring, and unadorned tensor products will be over R.

For S a ring and G a group, $S(G)$ will denote the group ring of G over S. We define a category ${}_G\mathscr{A}_R$ as follows: the objects of ${}_G\mathscr{A}_R$ are R-algebras which are also left $R(G)$-modules, the elements of G acting as R-algebra automorphisms; the

Presented to the Society, December 9, 1965 under the title *A cohomology theory of Harrison for connected rings*; received by the editors May 22, 1967 and, in revised form, March 18, 1968.

[1] This work was done while the author was a National Science Foundation Graduate Fellow.

morphisms in ${}_G\mathscr{A}_R$ are R-algebra homomorphisms which are also $R(G)$-module maps.

Let G be a finite group, and let A be any ring. Define $e_G(A)=\{$Set functions $v\colon G\to A\}$. Then $e_G(A)$ is a ring under pointwise operations, and is an R-algebra if A is an R-algebra. Now suppose A is an object of ${}_G\mathscr{A}_R$. We let $A^G=\{a \text{ in } A \mid x(a)=a$ for all x in $G\}$. Define $h\colon A\otimes A\to e_G(A)$ to be the homomorphism such that $h(a\otimes b)(x)=ax(b)$ for a, b in A and x in G. We say that *A is a Galois extension of R with group G* if h is a bijection and $A^G=R$.

Let $\phi\colon G\to H$ be a homomorphism of finite groups. Define a covariant functor $\phi\colon {}_G\mathscr{A}_R\to {}_H\mathscr{A}_R$ by

$$\phi(A)=\{\text{Set maps } v\colon H\to A \mid v(\phi(x)y)=xv(y) \text{ for } x \text{ in } G,\ y \text{ in } H\};$$

for $f\colon A\to B$ a morphism in ${}_G\mathscr{A}_R$, $\phi(f)(v)=fv$. Let $\iota\colon {}_H\mathscr{A}_R\to {}_G\mathscr{A}_R$ be the functor obtained by viewing an object in ${}_H\mathscr{A}_R$ as an object in ${}_G\mathscr{A}_R$, via ϕ. The functor ϕ is a right adjoint to ι. H acts on $\phi(A)$ via $(yv)(z)=v(zy)$.

Suppose now that $\phi'\colon G\to K$, $\phi''\colon K\to H$ are homomorphisms of finite groups. Let $\phi=\phi''\phi'$, and let ι, ι', ι'' be the functors which are the left adjoints of ϕ, ϕ', ϕ'' respectively. It is easy to see that there is a natural equivalence of functors, $\iota'\iota''\sim\iota$. By uniqueness of adjoints up to equivalence, we conclude that the following lemma holds.

LEMMA 1.1. *Let ϕ', ϕ'' and ϕ be as described above, and let*

$$\phi'\colon {}_G\mathscr{A}_R\to {}_K\mathscr{A}_R,\qquad \phi''\colon {}_K\mathscr{A}_A\to {}_H\mathscr{A}_R,\qquad \phi\colon {}_G\mathscr{A}_R\to {}_H\mathscr{A}_R$$

be the corresponding functors. Then there exists a natural equivalence of functors, $\phi''\phi'\sim\phi$.

THEOREM 1.2. *Let $\phi\colon G\to H$ be a homomorphism of finite groups, and let A be a Galois extension of R with group G. Then $\phi(A)$ is a Galois extension of R with group H.*

Proof. We first remark that for an object A of ${}_G\mathscr{A}_R$ to be a Galois extension of R with group G, it is necessary and sufficient that there exist elements $a_1,\dots,a_n$, $b_1,\dots,b_n$ in A such that $\sum_i a_ix(b_i)=\delta_{1,x}$ for x in G, and that $A^G=R$. This is proved in [6] for A commutative; with trivial modifications, the arguments used [6, Theorem 1.3, (b) $\Leftrightarrow$ (c) $\Leftrightarrow$ (d) $\Leftrightarrow$ (e)] are valid even when A is not commutative.

First assume that ϕ is one-one, and identify G with $\phi(G)$. Then $\phi(A)=\{v\colon H\to A \mid v(xy)=xv(y)$ for x in G, y in $H\}$. Choose $a_1,\dots,a_n$, $b_1,\dots,b_n$ in A such that $\sum_i a_ix(b_i)=\delta_{1,x}$.

Let $1=z_1,\dots,z_m$ be a set of coset representatives of G; thus $H=\bigcup H(i)$, where $H(i)=Gz_i$ for $i=1,\dots,m$. Define a map $|\ \ |\colon H\to G$ by $|xz_i|=x$ for x in G. Clearly $|\ \ |$ satisfies the conditions: (i) $|1|=1$ and (ii) $|xy|=x|y|$ for x in G and y in H. Now for $i\leqq n$, $j\leqq m$ define $v_{i,j}\colon H\to A$, $w_{i,j}\colon H\to A$ by $v_{i,j}(z)=|z|(a_i)\delta_{H(i),Gz}$,

$w_{i,j}(z)=|z|(b_i)\delta_{H(j),Gz}$ for z in H. By (ii), $v_{i,j}$ and $w_{i,j}$ are in $\phi(A)$ for $i\leqq n, j\leqq m$. Now for each z in H we have that

$$\Big(\sum_{i,j} v_{i,j}w_{i,j}\Big)(z) = \sum_{i,j} v_{i,j}(z)w_{i,j}(z) = \sum_i |z|(a_ib_i) = 1.$$

If $y\neq 1$ is in H, we get:

$$\Big(\sum_{i,j} v_{i,j}y(w_{i,j})\Big)(z) = \sum_{i,j} |z|(a_i)|zy|(b_i)\delta_{H(j),Gz}\delta_{H(j),Gzy}.$$

Case 1. $Gz\neq Gzy$. Then $(\sum_{i,j} v_{i,j}y(w_{i,j}))(z)=0$.

Case 2. $Gz=Gzy$. Then $u=zyz^{-1}$ is in G, and $uz=zy$. Thus $|zy|=u|z|$ by (ii) and $|zy|=|z|t$ where $t=|z|^{-1}u|z|\neq 1$ is in G. Thus

$$\Big(\sum_{i,j} v_{i,j}y(w_{i,j})\Big)(z) = \sum_i |z|(a_i)|z|t(b_i) = |z|\Big(\sum_i a_it(b_i)\Big) = 0.$$

It is easy to see that $\phi(A)^H=R$, and thus $\phi(A)$ is a Galois extension of R with group H.

Now suppose $\phi: G\to H$ is onto. Let $K=$kernel (ϕ). Define maps $j: A^K\to\phi(A)$, $j': \phi(A)\to A^K$ by $j(a)(\phi(x))=x(a), j'(v)=v(1)$ for a in A^K, x in G, v in $\phi(A)$. It is easy to verify that j, j' are morphisms in ${}_H\mathscr{A}_R$, and that $jj'=1, j'j=1$. (The action of H on A^K is given by $\phi(x)(a)=x(a)$ for x in G.) That A^K is a Galois extension of R with group H is proved in [14, Proposition 1].

For ϕ arbitrary, write $\phi=\phi''\phi'$, where ϕ' is onto and ϕ'' is one-one. Using (1.1) and the special cases above, we conclude that the theorem holds.

For G a finite group, define $E_R(G)$ to be the set of equivalence classes of Galois extensions of R with group G, two such extensions being equivalent if they are isomorphic in ${}_G\mathscr{A}_R$.

We define a *Galois* (R, G)-*algebra* to be a Galois extension A of R with group G such that $A\cong R(G)$ as $R(G)$-modules. Equivalently, there exists a in A such that $\{x(a) \mid x \text{ in } G\}$ is an R-basis for A; this basis is called a *normal basis* and is said to be generated by a.

We define $A_R(G)$ to be the set of equivalence classes of Galois (R, G)-algebras, equivalent algebras being those isomorphic in ${}_G\mathscr{A}_R$. Clearly, $A_R(G)$ is a subset of $E_R(G)$. We shall write (A) for the class of A in either $E_R(G)$ or $A_R(G)$.

THEOREM 1.3. *Let $\phi: G\to H$ be a homomorphism of finite groups. If A is a Galois (R, G)-algebra, then $\phi(A)$ is a Galois (R, H)-algebra.*

Proof. It is clear that there is an $R(H)$-module isomorphism $\phi(A)\cong \mathrm{Hom}_{R(G)}(R(H), A)$, where $R(H)$ is viewed as an $(R(G), R(H))$-bimodule via ϕ. We must show that $\mathrm{Hom}_{R(G)}(R(H), R(G))\cong R(H)$ as left $R(H)$-modules.

For X a finite group, $\mathrm{Hom}_R(R(X), R)\cong R(X)$ as left $R(X)$-modules, the isomorphism being given by $f(\alpha)=\sum_{x\in X}\alpha(x)x^{-1}$ for α in $\mathrm{Hom}_R(R(X), R)$. Now using this fact and an adjointness relation between Hom and $\otimes$, we obtain $R(H)$-isomorphisms

$$\operatorname{Hom}_{R(G)}(R(H), R(G)) \cong \operatorname{Hom}_{R(G)}(R(H), \operatorname{Hom}_R(R(G), R))$$
$$\cong \operatorname{Hom}_R(R(G) \otimes_{R(G)} R(H), R) \cong \operatorname{Hom}_R(R(H), R) \cong R(H).$$

Let S be a commutative R-algebra. Define a functor from ${}_G\mathscr{A}_R$ to ${}_G\mathscr{A}_S$ by $A \to S \otimes A$, where $x(s \otimes a) = s \otimes x(a)$ for s in S, a in A and x in G; for $\alpha: A \to G$ a map in ${}_G\mathscr{A}_R$, we send α to $1 \otimes \alpha$.

LEMMA 1.4. *Let S be an R-algebra, and let G and H be finite groups. Then*

(a) *There exists an isomorphism $j: e_H(S) \to S \otimes e_H(R)$ which is simultaneously an R-algebra and an $S(H)$-module map.*

(b) *If S is an object of ${}_G\mathscr{A}_R$ then j is also a $G \times H$-module map; $G \times H$ acts on $S \otimes e_H(R)$ and on $e_H(S)$ by $(x, y)(s \otimes v) = x(s) \otimes y(v)$, $((x, y)w)(z) = x(v(zy))$ for s in S, v in $e_H(R)$, w in $e_H(S)$, y, z in H and x in G.*

Proof. Let v_x in $e_H(S)$ be defined by $v_x(y) = \delta_{x,y}$ for x in H. The set $\{v_x \mid x \text{ in } H\}$ is an S-basis of $e_H(S)$, and $e_H(R)$ has a corresponding R-basis $\{w_x \mid x \text{ in } H\}$. Let $j(\sum_{x\in H} s_x v_x) = \sum s_x \otimes w_x$. An inverse to j is defined by $j'(s \otimes v) = sv$, and conditions (a) and (b) are easily verified.

LEMMA 1.5. *Let A be an object in ${}_G\mathscr{A}_R$, where G is a finite group. Let S be a commutative R-algebra. Then*

(a) *If A is a Galois extension of R with group G (respectively a Galois (R, G)-algebra) then $S \otimes A$ is a Galois extension of S with group G (respectively a Galois (S, G)-algebra).*

(b) *If S is a faithfully flat R-module* [3, p. 46] *and $S \otimes A$ is a Galois extension of S with group G, then A is a Galois extension of R with group G.*

Proof. (a) The proof of [6, Lemma 1.7] for A commutative holds here.

(b) Let $h: A \otimes A \to e_G(A)$ be defined as at the beginning of this section. We have isomorphisms $(S \otimes A) \otimes_S (S \otimes A) \cong S \otimes A \otimes A$ and

$$S \otimes e_G(A) \cong S \otimes A \otimes e_G(R) \cong e_G(S \otimes A),$$

defined respectively by $(s \otimes a) \otimes_S (s' \otimes a') \to ss' \otimes a \otimes a'$, and as in (1.4). Let $h': (S \otimes A) \otimes_S (S \otimes A) \to e_G(S \otimes A)$ be defined analogously to h. Then the diagram below is commutative:

$$\begin{tikzcd}
S \otimes A \otimes A \arrow[r, "1 \otimes h"] \arrow[d, "\cong"'] & S \otimes e_G(A) \arrow[d, "\cong"] \\
(S \otimes A) \otimes_S (S \otimes A) \arrow[r, "h'"'] & e_G(S \otimes A)
\end{tikzcd}$$

By assumption, h' is an isomorphism; thus h is an isomorphism since S is faithfully flat [3, Proposition 1]. If a is in A^G then $1 \otimes a$ is in $(S \otimes A)^G = S$. Thus $1 \otimes a = s \otimes 1$ for some s in S. Then $1 \otimes s \otimes 1 = s \otimes 1 \otimes 1 = 1 \otimes 1 \otimes a$, so that $1 \otimes s = s \otimes 1$. By [7, Lemma 3.8] we conclude that s is in R, so that a is in R.

The following theorem is proved in [6, Theorem 3.4] for A, B commutative. The same proof holds in the noncommutative case.

THEOREM 1.6. *Let A, B be Galois extensions of R with group G. Suppose $f: A \to B$ is an R-algebra homomorphism and an $R(G)$-module homomorphism. Then f is an isomorphism.*

Let $\mathscr{G}$ denote the category of *finite* groups and group homomorphisms; let $\mathscr{S}$ denote the category of sets and set maps; let $\mathscr{R}$ denote the category of *commutative* rings and ring homomorphisms.

PROPOSITION 1.7. (a) *The following definitions yield a functor $E_R: \mathscr{G} \to \mathscr{S}$. $E_R(G)$ is defined as following* (1.2). *For $\phi: G \to H$ a homomorphism of finite groups, define $E_R(\phi): E_R(G) \to E_R(H)$ by $E_R(\phi)(A) = (\phi(A))$.*

(b) *The following definitions yield a functor $E_{(\ )}(G): \mathscr{R} \to \mathscr{S}$. $E_{(\ )}(G)(R) = E_R(G)$. For $\theta: R \to S$ a homomorphism of commutative rings, define $E_\theta: E_R(G) \to E_S(G)$ by $E_\theta(G)(A) = (S \otimes A)$.*

(c) *E becomes a bifunctor from $\mathscr{R} \times \mathscr{G}$ to $\mathscr{S}$ under the definitions in* (a) *and* (b); *specifically, $E_\theta(H)E_R(\phi) = E_S(\phi)E_\theta(G)$, where ϕ, θ are as in* (a) *and* (b).

Proof. (a) First we note that $E_R(\phi)$ is a well-defined map. $\phi(A)$ is a Galois extension of R with group H by (1.2); if $A \simeq B$ in ${}_G\mathscr{A}_R$ and $j: A \to B$ is a morphism in ${}_G\mathscr{A}_R$, define $j_1: \phi(A) \to \phi(B)$ by $j_1(v) = jv$ for v in $\phi(A)$. j_1 is easily seen to be a morphism in ${}_H\mathscr{A}_R$, and is thus an isomorphism by (1.6).

Now let $1: G \to G$ be the identity map. Then $1(A) = \{\text{Set maps } v: G \to A \mid v(xy) = xv(y) \text{ for } x, y \text{ in } G\}$. Define $f: 1(A) \to A$ by $f(v) = v(1)$. By (1.6) we conclude that $(1(A)) = (A)$ and $E_R(1)$ is thus the identity map.

If $\phi': G \to K$, $\phi'': K \to H$ are homomorphisms of finite groups, we conclude from (1.1) that $E_R(\phi''\phi') = E_R(\phi'')E_R(\phi')$.

(b) If A is a Galois extension of R with group G, $S \otimes A$ is a Galois extension of S with group G by (1.5). Clearly, $E_\theta(G)$ is well defined. The functorial properties of $E_{(\ )}(G)$ are straightforward results of associativity relations for tensor products, and of (1.4).

(c) Define a map $f: S \otimes \phi(A) \to \phi(S \otimes A)$ by $f(s \otimes v)(y) = s \otimes v(y)$ for s in S, y in H and v in $\phi(A)$. By (1.6) we conclude that (c) holds.

Now let A and B be Galois extensions of R with groups G and H respectively. $G \times H$ acts on $A \otimes B$ via $(x, y)(a \otimes b) = x(a) \otimes y(b)$ for x in G, y in H, a in A and b in B. In [14, Proposition 1] it is shown that $A \otimes B$ is a Galois extension of R with group $G \times H$; the equivalence of our definition of Galois extension with other definitions is discussed in the proof of (1.2).

LEMMA 1.8. (a) *Let $e: G \to H$ be the trivial homomorphism between the finite groups G and H. Let A be a Galois extension of R with group G. Then $e_H(R) \cong e(A)$ in ${}_H\mathscr{A}_R$.*

(b) *Let $\phi: G \to H$ and $\phi': G' \to H'$ be homomorphisms of finite groups. Let A and A' be Galois extensions of R with groups G and G' respectively. Then $(\phi \times \phi')(A \otimes A') \cong \phi(A) \otimes \phi'(A')$ in ${}_{H \times H'}\mathscr{A}_R$.*

Proof. (a) We first observe that if $e_H: \{1\} \to H$ is the trivial map, the two interpretations of $e_H(A)$, given near the beginning of this section, coincide. Take $e': G \to \{1\}$, so that $e = e_H e'$. Now $e'(A) \cong R$ since R is the only Galois extension of R with group $\{1\}$. By (1.1), $e(A) \cong e_H(e'(A)) \cong e_H(R)$.

(b) From the definitions, we have that

$$B_1 = (\phi \times \phi')(A \otimes A') = \{w: H \times H' \to A \otimes A' \mid w(\phi(x)y, \phi'(x')y') = (x, x')w(y, y') \text{ for } x \text{ in } G,\ x' \text{ in } G',\ y \text{ in } H \text{ and } y' \text{ in } H'\};$$

$$B_2 = \phi(A) \otimes \phi'(A') = \{v: H \to A \mid v(\phi(x)y) = xv(y)\} \otimes \{v': H' \to A' \mid v'(\phi'(x')y') = x'v'(y')\}.$$

Define $f: B_2 \to B_1$ by linearity and $f(v \otimes v')(y \otimes y') = v(y) \otimes v'(y')$. It is easy to verify that f maps B_2 to B_1 and that f is an R-algebra and an $R(H \times H')$-module map. By (1.6) and the remarks preceding this lemma, f is an isomorphism.

Restrict G to be a finite *abelian* group, and let $m: G \times G \to G$ be the multiplication map, a homomorphism since G is abelian. Let $t: G \to G$ be the homomorphism defined by $t(x) = x^{-1}$. Define a binary and a unary operation on $E_R(G)$ by the respective formulas: $(A) \cdot (B) = (m(A \otimes B))$, $(A)^{-1} = (t(A))$ for (A), (B) in $E_R(G)$. It is not difficult to verify that if A and B are Galois (R, G)-algebras, then $A \otimes B$ is a Galois $(R, G \times G)$-algebra. Combining this with (1.2), we see that the formulas above define operations on $A_R(G)$ as well as on $E_R(G)$. Let $\mathscr{G}^{\mathrm{ab}}$ denote the category of *finite abelian groups.*

THEOREM 1.9. (a) *Let G be a finite abelian group. With the operations defined as above, $E_R(G)$ and $A_R(G)$ are abelian groups. The identity element of these groups is $(e_G(R))$.*

(b) *The bifunctor E of* (1.7) *is a bifunctor from $\mathscr{R} \times \mathscr{G}^{\mathrm{ab}}$ to $\mathscr{Ab}$, the category of abelian groups.*

(c) *$A_R(G)$ is functorial in R and G, and $A: \mathscr{R} \times \mathscr{G}^{\mathrm{ab}} \to \mathscr{Ab}$ is a sub-bifunctor of E.*

Proof. (a) Clearly $(A) \cdot (B) = (B) \cdot (A)$. Functoriality of E_R yields $E_R(m(m \times 1)) = E_R(m)E_R(m \times 1) = E_R(m(1 \times m))$, and (1.8) implies that $(m \times 1)(A \otimes B \otimes C) \cong m(A \otimes B) \otimes C$ in ${}_G\mathscr{A}_R$. From these remarks it follows that the binary operation on $E_R(G)$ is associative.

Now $(e_G(R))$ is the identity element of $E_R(G)$, since we have

$$A \otimes e_G(R) \cong (1 \times e_G)(A \otimes R)$$

by (1.8), with $e_G\colon\{1\}\to G$ (we are using the observation made in the proof of (1.8)(a)). But using the identifications $A\otimes R\cong A$, $G\times\{1\}\cong G$ we have that $(1\times e_G)(A\otimes R)\cong i(A)$, where $i\colon G\to G\times G$ is given by $i(x)=(x,1)$. Since $mi=1_G$, $m(A\otimes e_G(R))\cong 1_G(A)\cong A$ in ${}_G\mathscr{A}_R$.

It follows from (1.8) that $(1\times t)(A\otimes A)\cong A\otimes t(A)$ in ${}_{G\times G}\mathscr{A}_R$; by (a) of the same result, $E_R(e)(A\otimes A)\cong e_G(R)$ in ${}_G\mathscr{A}_R$, where $e\colon G\times G\to G$ is the trivial homomorphism. But $e=m(1\times t)$. Applying E_R to this relation, we obtain $(A)\cdot(A)^{-1}=(e_G(R))$.

The proofs for $A_R(G)$ are precisely the same as those for $E_R(G)$.

(b) Let $\phi\colon G\to H$ be a homomorphism of finite abelian groups. Let $m_G\colon G\times G\to G$, $t_G\colon G\to G$ denote the group operations here, and let m_H, t_H be the corresponding homomorphisms for H. By (1.8) and functoriality of E_R, we get the following chain of isomorphisms in ${}_H\mathscr{A}_R$:

$$m_H(\phi(A)\otimes\phi(B))\cong m_H((\phi\times\phi)(A\otimes B))\cong(m_H(\phi\times\phi))(A\otimes B)\cong(\phi m_G)(A\otimes B).$$

Thus $E_R(\phi)$ is a group homomorphism.

Let $\theta\colon R\to S$ be a homomorphism of commutative rings. As in the proof of (1.7)(c), we can show that $S\otimes m(A\otimes B)\cong m(S\otimes A\otimes B)$ in ${}_G\mathscr{A}_S$. But $S\otimes A\otimes B\cong S\otimes A\otimes_S S\otimes B$ in ${}_{G\times G}\mathscr{A}_S$. It follows that $E_\theta(G)$ is a group homomorphism, and (b) is proved.

(c) One can verify that A is a bifunctor precisely as one verified functoriality of E. The proofs above also hold for $A_R(G)$.

Remark. In [12] Harrison introduced $T(G,R)$, the subset of $E_R(G)$ consisting of classes of commutative Galois extensions. It is shown in [12] that $T(G,R)$ is functorial in G and R, and that $T(G,R)$ defines a bifunctor $T\colon\mathscr{G}^{\mathrm{ab}}\times\mathscr{R}\to\mathscr{Ab}$. Using the lemma below, which we state here for later reference, it is not difficult to show that the group structure defined on $T(G,R)$ in [12] agrees with that induced on $T(G,R)$ from the group structure of $E_R(G)$.

Lemma 1.10. *Let $\phi\colon G\to H$ be a map of finite abelian groups. Let $K=\{(x,\phi(x)^{-1})$ in $G\times H\}$. Then for A a Galois extension of R with group G, we have $\phi(A)\cong(A\otimes e_H(R))^K$ in ${}_H\mathscr{A}_R$. If ϕ is the identity map from G to G and $m\colon G\times G\to G$ is the multiplication map, then $m(A\otimes B)\cong(A\otimes B)^K$ in ${}_G\mathscr{A}_R$.*

Proof. Define $\phi'\colon G\times H\to H$ by $\phi'(x,y)=\phi(x)y$ for x in G, y in H; thus $K=\text{kernel}(\phi')$. Let $j\colon e_H(A)\to A\otimes e_H(R)$ be defined as in (1.4). Using the explicit definition of j, the definition of $\phi(A)$ as a subalgebra of $e_H(A)$, and the fact that H is abelian, we see that j restricts to a map $j_1\colon\phi(A)\to(A\otimes e_H(R))^K$. From (1.4) we know that j is an R-algebra and an $R(G\times H)$-module homomorphism, and thus j_1 is an R-algebra and an $R(H)$-module homomorphism. But $(A\otimes e_H(R))^K$ is a Galois extension of R with group H (we refer the reader to the remark directly preceding (1.8), and to [14, Proposition 1]). By (1.6), j_1 is an isomorphism. Using (1.6) it is easy to show that $m(A\otimes B)\cong(A\otimes B)^K$ when ϕ is the identity map on G.

2. **A cohomological description of $A_R(J)$.** In this section we introduce a cohomology theory patterned after one introduced by Harrison in [11], and used in [5] to classify $A_R(J)$.

Let J be an abelian group. For each integer $n \geqq 0$ we define maps $\Delta_{n,i}\colon J^n \to J^{n+1}$ as follows (where we use multiplicative notation for J):

$$\begin{aligned}\Delta_{n,i}((x_1,\dots,x_n)) &= (1, x_1,\dots,x_n) &&\text{for } i = 0,\\ &= (x_1,\dots,x_i,x_i,x_{i+1},\dots,x_n) &&\text{for } 0 < i < n+1,\\ &= (x_1,\dots,x_n,1) &&\text{for } i = n+1.\end{aligned}$$

We will henceforth suppress the subscript n on $\Delta_{n,i}$ and we shall use Δ_i to designate the corresponding map $\Delta_i\colon G^n \to G^{n+1}$, where G is any other abelian group. One may easily verify the relations

$$\Delta_{j+1}\Delta_i = \Delta_i\Delta_j \quad \text{for } 0 \leqq i \leqq j \leqq n+1. \tag{2.1}$$

Now suppose $F\colon \mathscr{G}^{\mathrm{ab}} \to \mathscr{A}\ell$ is a (covariant, not necessarily additive) functor from the category of finite abelian groups to the category of abelian groups. We define a complex $CF(J)$ by setting $C^nF(J)=0$ for $n<0$, $C^nF(J)=F(J^n)$ for $n\geqq 0$; $\delta^n_F(J)\colon F(J^n)\to F(J^{n+1})$ is given by $\delta^n_F(J)=\prod_{i=0}^{n+1}(F(\Delta_i))^{(-1)^i}$ for $n\geqq 0$, where $F(J)$ is denoted multiplicatively. That $\delta^{n+1}\delta^n=0$ follows from (2.1) and from functoriality of F (see, e.g. [1, Theorem 5.1]). The nth cohomology group of this complex, $\operatorname{Ker}(\delta^n)/\operatorname{Im}(\delta^{n-1})$, will be denoted by $H^nF(J)$.

We define a functor $U_R\colon \mathscr{G}^{\mathrm{ab}} \to \mathscr{A}\ell$ by setting $U_R(J)=U(R(J))$, the (multiplicative) abelian group of units of the group ring $R(J)$. In the discussion below we shall use multiplicative notation for J as well as for $U_R(J)$. The cochain complex $CU_R(J)$ is given by

$$\cdots \longrightarrow \{1\} \to U(R) \xrightarrow{\delta^0} U(R(J)) \xrightarrow{\delta^1} U(R(J^2)) \longrightarrow \cdots.$$

In [11] Harrison introduced this complex for the case of R a field.

If u is a cocycle in $U(R(J^n))$, $\mathrm{cl}(u)$ will denote the cohomology class of u in $H^nU_R(J)$. We note that δ^0 is the trivial map.

THEOREM 2.2. *There exists an isomorphism of abelian groups $\beta\colon H^2U_R(J)\to A_R(J)$. The map β determines a natural equivalence of the bifunctors H^2U and A.*

Proof. The existence of a bijection of sets $\beta\colon H^2U_R(J)\to A_R(J)$ is proved in [8, Corollary 4.8] and in [5, Corollary 2.16]. The abelian group structure on $A_R(J)$ is that defined in §1. That H^2U is a bifunctor from $\mathscr{R}\times\mathscr{G}^{\mathrm{ab}}$ to $\mathscr{A}\ell$ can be verified in a straightforward manner. ($\mathscr{R}$ is the category of commutative rings.) We will give the construction of β and β^{-1}, and some pertinent facts, for later reference.

Let $\mathrm{cl}(u)$ be in $H^2U_R(J)$, $u=\sum_{x,y\in J} a_{x,y}(x,y)$ being in $U(R(J^2))$. Define an operation $\circ$ on the $R(J)$-module $R(J)$ by R-linearity and $x\circ y=\sum_{z\in J} a_{x^{-1}z,y^{-1}z}\, z$ for x, y in J. The fact that $\circ$ gives an associative operation follows from the fact that u is a cocycle; moreover $\circ$ makes $R(J)$ into a Galois extension of R with group J.

We write $R(J)^u$ for the algebra thus arising, and we note that by its definition, $R(J)^u$ has a normal basis. We set $\beta(\mathrm{cl}\,(u))=(R(J)^u)$ in $A_R(J)$.

Conversely, suppose (A) is in $A_R(J)$. There exists an isomorphism $f\colon R(J)\to A$ of $R(J)$-modules. We obtain a new multiplication on $R(J)$, which we denote by $\circ'$, rendering f into an R-algebra isomorphism. Then $x^{-1}\circ' y^{-1}=\sum_{z\in J} a_{x,y}(z)z$ where $a_{x,y}(z)$ is in R for x, y, z in J. Setting $u_A=\sum_{x,y} a_{x,y}(1)(x, y)$ defines a cocycle in $U(R(J^2))$. We define $\beta^{-1}((A))=\mathrm{cl}\,(u_A)$.

It follows that β and β^{-1} are well-defined set maps. Moreover, if $A=R(J)^u$ and $f\colon R(J)\to R(J)^u$ is taken to be the identity map, the operation $\circ'$ on $R(J)$ agrees with the operation $\circ$ on $R(J)$. Also, if A and f are as above, and if we endow $R(J)$ with the algebra structure defined by u_A, then f becomes an R-algebra isomorphism. From these remarks its follows that β and β^{-1} are bijections that are inverse to each other.

We now show that β is a homomorphism of abelian groups. It is easy to verify that $R(J)^u\cong e_J(R)$ in ${}_J\mathscr{A}_R$ iff u is a coboundary i.e. iff $\mathrm{cl}\,(u)=1$. Now let $u=\sum a_{x,y}(x, y)$ and $v=\sum b_{x,y}(x, y)$ be cocycles in $U(R(J^2))$. Let $K=\{(x, x^{-1}) \text{ in } J\times J\}$. Define a map $j\colon R(J)^{u\cdot v}\to (R(J)^u\otimes R(J)^v)^K$ by R-linearity and by the formula $j(x)=\sum_{y\in J} xy\otimes y^{-1}$. It is easy to see that j is a well-defined map. Using the formulas for u and v and for the multiplication in $R(J)^u$ and $R(J)^v$, it is straightforward to show that j is an R-algebra and $R(J)$-module homomorphism. By (1.6), j is an isomorphism, and we conclude from (1.10) that $(R(J)^u)\cdot(R(J)^v)=(R(J)^{u\cdot v})$. Thus β is a homomorphism.

That β defines a natural equivalence of bifunctors may be shown using a direct, though computationally involved, approach. Scrutiny of [8] and [5] also reveals that β is natural, since it is defined there in a more canonical manner.

REMARK 2.3. Let u and v be cocycles in $U(R(J^2))$, and let $f\colon R(J)^u\to R(J)^v$ be an isomorphism of Galois extension i.e. an isomorphism in ${}_J\mathscr{A}_R$. Then f defines an $R(J)$-module automorphism of $R(J)$, so there exists a unique w in $U(R(J))$ such that $f(x)=wx$ for x in $R(J)^u$. From the definitions of the multiplication in $R(J)^u$ and $R(J)^v$, it is easy to see that $u=v\delta^1(w)$. Conversely, if w is in $U(R(J))$ and $u=\delta^1(w)v$, defining a map $f\colon R(J)^u\to R(J)^v$ by $f(x)=wx$, we obtain an isomorphism of Galois extensions.

3. **A cohomological description of $E_R(J)$.** Before introducing the Amitsur-Harrison bicomplex, we review the definition of Amitsur cohomology for ease of future reference.

Let S be a commutative R-algebra, and let S^n denote the n-fold tensor product of S over R. For $n\geqq 0$ and $0\leqq i\leqq n+1$, define $\varepsilon_i^{(n)}\colon S^{n+1}\to S^{n+2}$ by

$$\varepsilon_i^{(n)}(s_0\otimes\cdots\otimes s_n) = s_0\otimes\cdots\otimes s_{i-1}\otimes 1\otimes s_i\otimes\cdots\otimes s_n.$$

Let F be a covariant functor from the category of commutative R-algebras to $\mathscr{A}b$. We define a cochain complex $C(S/R, F)$ by setting $C^n(S/R, F)=F(S^{n+1})$, the coboundary $d^n\colon C^n(S/R, F)\to C^{n+1}(S/R, F)$ being given by $d^n=\prod_{i=0}^{n+1}(F(\varepsilon_i))^{(-1)^i}$

(here, as henceforth, we write ε_i for $\varepsilon_i^{(n)}$; we consider $F(S^i)$ as a multiplicative abelian group). The nth cohomology group of $C(S/R, F)$ is denoted by $H^n(S/R, F)$. That $d^{n+1}d^n=0$ follows from the relations (3.1), as shown in [1, Lemma 5.1],

$$\varepsilon_i\varepsilon_j = \varepsilon_{j+1}\varepsilon_i \qquad \text{for } i \leqq j. \tag{3.1}$$

Abusing notation, we will write cl (v) for the cohomology class in $H^n(S/R, F)$ of a cocycle v in $F(S^{n+1})$.

Remark 3.2. Pic (S) will denote the set of isomorphism classes of finitely generated projective S-modules of rank 1 [3, p. 141]. For P such a module, we will write $\langle P\rangle$ for the class of P in Pic (S). As shown in [3], Pic (S) is an abelian group with identity $\langle S\rangle$, the operation being $\langle P\rangle\cdot\langle Q\rangle=\langle P\otimes_S Q\rangle$. If $f\colon S\to T$ is a homomorphism of commutative rings, $\operatorname{Pic}(f)\colon \operatorname{Pic}(S)\to\operatorname{Pic}(T)$ defined by $\operatorname{Pic}(f)(\langle P\rangle)=\langle T\otimes_S P\rangle$ is a group homomorphism [3].

The following theorem of Grothendieck is to be found in [7, Corollary 4.6] and is given here, along with parts of its proof, for future reference.

Theorem 3.3. *Let T be a faithfully flat commutative R-algebra* [3, p. 46] *and let $i\colon R\to T$ be the inclusion map. Then there is a natural isomorphism $\alpha\colon H^1(T/R, U)\to$* Ker (Pic (i)), *where U denotes the "units" functor.*

Proof. We sketch the construction of α and α^{-1}. For proofs, we refer the reader to [7, §4].

Given a cocycle v in $U(T^2)=C^1(T/R, U)$, we let $P(v)=\{x \text{ in } T \mid v\varepsilon_0(x)=\varepsilon_1(x)\}$. The sequence

$$0\to T\otimes P(v)\to T^2\to T^3$$

is exact, where the map from T^2 to T^3 is $1\otimes v\varepsilon_0-1\otimes v\varepsilon_1$ [7, Lemma 3.8]. Thus $T\otimes P(v)$ may be identified with its image in T^2. Then $j\colon T\to T^2$ defined by $j(x)=v^{-1}\varepsilon_1(x)$ may be shown to define a T-isomorphism $j\colon T\to T\otimes P(v)$, with inverse j_1 given by $j_1(t\otimes x)=tx$ [7, Theorem 4.2]. It now follows that setting $\alpha(\mathrm{cl}(v))=\langle P(v)\rangle$ gives a well-defined homomorphism $\alpha\colon H^1(T/R, U)\to$ Ker (Pic (i)).

Conversely, if $\langle P\rangle$ is in Pic (R) and $f\colon T\to T\otimes P$ is a T-isomorphism, we get a T^2-module isomorphism $\bar f\colon T^2\to T^2$ given as the composite

$$T^2\xrightarrow{1\otimes f}T^2\otimes P\xrightarrow{\sigma\otimes 1}T^2\otimes P\xrightarrow{1\otimes f^{-1}}T^2\xrightarrow{\sigma^2}T^2 \tag{3.4}$$

where $\sigma(t_1\otimes t_2)=t_2\otimes t_1$. $\bar f$ must be defined by left multiplication by some element v_P in $U(T^2)$, since it is a T^2-module isomorphism. α^{-1} is now defined by $\alpha^{-1}(\langle P\rangle)=\mathrm{cl}(v_P)$.

Remark 3.5. If T is a faithfully flat R-algebra, and J is an abelian group, then $T(J)$ is a faithfully flat $R(J)$-algebra [3, Chapter I, §3, Proposition 4].

Theorem 3.6. *Let J be a finite abelian group, and let A be a Galois extension of R with group J. Then A is a finitely generated projective $R(J)$-module of rank* 1.

Proof. We recall the observations made in the proof of (1.2) that A satisfies conditions (b)–(e) of [6, Theorem 1.3], even if A is not commutative. In particular, let $D(A, J)$ be the free left A-module on the symbols u_x, x in J. A multiplication is defined by linearity and by the formula $(au_x)(bu_y)=ax(b)u_{xy}$ for x, y in J, a and b in A. Then the homomorphism $j\colon D(A, J) \to \mathrm{End}_R(A)$ defined by $j(au_x)(b)=ax(b)$ is a ring isomorphism. A computation shows that the image of $R(J)$ under j is $\mathrm{End}_{R(J)}(A)$. Thus $R(J)\cong \mathrm{End}_{R(J)}(A)$. Thus, if A were a finitely generated projective $R(J)$-module, A would have rank 1 by [3, p. 181, exercise 20]. That A is $R(J)$-projective when it is commutative is proved in [6, Lemma 1.6 and Theorem 4.2]. The same proofs are valid for A not commutative.

Let F be a functor from the category of commutative R-algebras to the category of abelian groups. Define a new functor FJ by $FJ(S)=F(S(J))$. The isomorphisms $S(J)\cong S \otimes R(J)$, $S \otimes_T T\cong S$ give rise to natural isomorphisms

$$C(T(J)/R(J), F) \cong C(T/R, FJ), \qquad H^n(T(J)/R(J), F) \cong H^n(T/R, FJ),$$

and we shall treat these as identifications. We shall also identify $T(J) \otimes_{R(J)} A$ with $T \otimes A$ when A is an $R(J)$-module.

For T a commutative R-algebra, we introduce a cochain bicomplex $C(J, T/R)$ by setting:

$$\begin{aligned} C^{n,m}(J, T/R) &= 0 \quad \text{if } n < 0 \text{ or } m < 0,\\ &= U(T^{n+1}(J^{m+1})) \quad \text{for } n, m \geqq 0. \end{aligned}$$

The coboundaries are defined by using the Harrison and Amitsur coboundaries, i.e. those introduced following (2.1), and preceding (3.1) respectively; a change of sign is needed to assure that the axioms for a bicomplex are satisfied [4, p. 60]:

$$\delta^{n,m}\colon U(T^{n+1}(J^{m+1})) \to U(T^{n+1}(J^{m+2}))$$

is given by $\delta^{n,m}=(\delta^{m+1})^{(-1)^n}$. The map

$$d^{n,m}\colon U(T^{n+1}(J^{m+1})) \to U(T^{n+2}(J^{m+1}))$$

is defined by $d^{n,m}=d^n$, the latter being the coboundary in $C(T(J^{m+1})/R(J^{m+1}), U)$.

The double complex $C(J, T/R)$ gives rise to a total complex [4], which we also denote by $C(J, T/R)$, and to cohomology groups $H^n(J, T/R)$. We note that the group operation on $U(T^n(J^m))$ is multiplicative. The low degree terms of the total complex are:

$$U(T(J)) \to U(T(J^2)) \oplus U(T^2(J)) \to U(T(J^3)) \oplus U(T^2(J^2)) \oplus U(T^3(J)),$$

and the two maps here shown, call them D^0 and D^1, are given by $D^0(u)=(\delta^1(u), d^0(u))$ for u in $U(T(J))$, and $D^1((u, v))=(\delta^2(u), d^0(u)\delta^1(v^{-1}), d^1(v))$ for u in $U(T(J^2))$ and v in $U(T^2(J))$.

THEOREM 3.7. *Let $i\colon R \to T$ be a ring homomorphism such that T is a faithfully flat commutative R-algebra. Let J be a finite abelian group.*

Then there exists a natural isomorphism $\varphi\colon H^1(J, T/R) \to K(J, T/R)$ *where* $K(J, T/R)$ *is the inverse image of* $A_T(J)$ *under the map* $E_i(J)\colon E_R(J) \to E_T(J)$.

Proof. We first construct $\varphi_1\colon K(J, T/R) \to H^1(J, T/R)$. Let (A) be in $K(J, T/R)$, i.e. A is a Galois extension of R with group J, and there exists a $T(J)$-isomorphism $f\colon T(J) \to T \otimes A = A'$. Then, as in the proof of (2.2), we have a unique $u = u_{A'}$ in $U(T(J^2))$ such that $\delta^2(u) = 1$, and such that $f\colon T(J)^u \to A'$ is an isomorphism of Galois extensions. Now consider the composite mapping $\bar{f}$ defined by the diagram below, where $e(i) = \varepsilon_i(u)$ for $i = 0, 1$:

$$(3.8)\qquad \begin{gathered} T^2(J)^{e(0)} \xrightarrow{1 \otimes f} T^2 \otimes A \xrightarrow{\sigma \otimes 1} \\ T^2 \otimes A \xrightarrow{1 \otimes f^{-1}} T^2(J)^{e(0)} \xrightarrow{\sigma} T^2(J)^{e(1)} \end{gathered}$$

By a slight variant of the discussion surrounding (3.4) (and using (3.6) to justify the argument), there exists an element $v = v_A$ in $U(T^2(J))$ such that $d^1(v) = 1$ and such that $\bar{f}(x) = vx$ for x in $T^2(J)$; but since each map in (3.8) is a ring isomorphism, as well as a $T^2(J)$-module isomorphism, $\bar{f}$ is an isomorphism of Galois extensions of T^2 with group J. By (2.2) we conclude that $\varepsilon_0(u) = \varepsilon_1(u)\delta^1(v)$; so $d^0(u) = \delta^1(v)$ and (u, v) is a cocycle in the total complex. We set $\varphi_1((A)) = \text{class } (u, v) = \text{class } (u_{A'}, v_A)$.

We must show that φ_1 is well defined. Let $j\colon A_1 \to A_2$ be an isomorphism of Galois extensions of R with group J. Let $f_i\colon T(J) \to A_i'$ be $T(J)$-module isomorphisms, for $i = 1, 2$. Write v_i, u_i for v_{A_i}, $u_{A_i'}$, $i = 1, 2$. The composite map

$$f = f_2^{-1}(1 \otimes j)f_1\colon T(J)^{u_1} \to T(J)^{u_2}$$

defines a unique isomorphism f of Galois extensions such that $f_2 f = (1 \otimes j)f_1$. By (2.3) there is a unique w in $U(T(J))$ such that $f(x) = wx$ and $u_1 = u_2\delta^1(w)$. Moreover, each square of the diagram below commutes (we write $e(i, j) = \varepsilon_i(u_j)$ for $i = 0, 1, j = 1, 2$).

$$\begin{array}{ccccccccc}
T^2(J)^{e(0,1)} & \xrightarrow{1 \otimes f_1} & T^2 \otimes A_1 & \xrightarrow{\sigma \otimes 1} & T^2 \otimes A_1 & \xrightarrow{1 \otimes f_1^{-1}} & T^2(J)^{e(0,1)} & \xrightarrow{\sigma} & T^2(J)^{e(1,1)} \\
\downarrow{\scriptstyle \varepsilon_0(f)} & & \downarrow{\scriptstyle 1 \otimes 1 \otimes j} & & \downarrow{\scriptstyle 1 \otimes 1 \otimes j} & & \downarrow{\scriptstyle \varepsilon_0(f)} & & \downarrow{\scriptstyle \varepsilon_1(f)} \\
T^2(J)^{e(0,2)} & \xrightarrow[1 \otimes f_2]{} & T^2 \otimes A_2 & \xrightarrow[\sigma \otimes 1]{} & T^2 \otimes A_2 & \xrightarrow[1 \otimes f_2^{-1}]{} & T^2(J)^{e(0,2)} & \xrightarrow[\sigma]{} & T^2(J)^{e(1,2)}
\end{array}$$

Now from the definition of v_i and w we obtain that $\varepsilon_0(w)v_2 = v_1\varepsilon_1(w)$, or $v_1 = v_2 d^0(w)$. Thus $(u_1, v_1) = (u_2, v_2)D^0(w)$, showing φ_1 to be well defined.

We now define $\varphi\colon H^1(J, T/R) \to K(J, T/R)$. Let (u, v) in $U(T(J^2)) \oplus U(T^2(J))$ be a 1-cocycle of the total complex. Define $A(u, v) = \{x \text{ in } T(J)^u \mid v\varepsilon_0(x) = \varepsilon_1(x)\}$. Letting $e(i) = \varepsilon_1(u)$, we have the map $\varepsilon_0\colon T(J)^u \to T^2(J)^{e(0)}$ is a ring homomorphism, as is the similar map ε_1. The map $l(v)\colon T^2(J)^{e(0)} \to T^2(J)^{e(1)}$, given by left multiplication by v, is a ring homomorphism by (2.3) and by the fact that $\varepsilon_0(u) = \varepsilon_1(u)\delta^1(v)$. Thus

$A(u, v)$, being the set on which ε_1 and $l(v)\varepsilon_0$ agree, is a subring of $T(J)^u$. By (3.3) and the relation $d^1(v)=1$, we have that $A(u, v)$ is a projective $R(J)$-module of rank 1, and J acts as a group of R-algebra automorphisms of $A(u, v)$, since J acts as a group of T-algebra automorphisms of $T(J)^u$. Now the map $j_1: T \otimes A(u, v) \to T(J)^u$ defined as in (3.3) by $j_1(t \otimes x)=tx$, is a $T(J)$-module isomorphism, and is clearly a T-algebra isomorphism as well. Thus by (b) of (1.5), $A(u, v)$ is a Galois extension of R with group J. Set $\varphi(\text{class } (u, v))=(A(u, v))$.

We wish to show that $(A(u, v))$ is independent of the choice of representative for class (u, v). Let w be in $U(T(J))$ and suppose $(u', v')=(u, v)D^0(w)=(u\delta^1(w), vd^0(w))$. By (2.3), the map $j: T(J)^{u'} \to T(J)^u$, defined by multiplication by w, is an isomorphism of Galois extensions. Now the diagrams below are easily seen to commute

$$\begin{array}{ccccc}
T(J)^{u'} & \xrightarrow{\varepsilon_0} & T^2(J)^{e'(0)} & \xrightarrow{l(v')} & T^2(J)^{e'(1)} \\
{\scriptstyle j}\downarrow & & \downarrow{\scriptstyle \varepsilon_0(j)} & & \downarrow{\scriptstyle \varepsilon_1(j)} \\
T(J)^u & \xrightarrow[\varepsilon_0]{} & T^2(J)^{e(0)} & \xrightarrow[l(v)]{} & T^2(J)^{e(1)}
\end{array}$$

$$\begin{array}{ccc}
T(J)^{u'} & \xrightarrow{\varepsilon_1} & T^2(J)^{e'(1)} \\
{\scriptstyle j}\downarrow & & \downarrow{\scriptstyle \varepsilon_1(j)} \\
T(J)^u & \xrightarrow[\varepsilon_1]{} & T^2(J)^{e(1)}
\end{array}$$

where $e'(i)=\varepsilon_i(u')$ for $i=0, 1$. It follows trivially that $A(u, v)\cong A(u', v')$ as Galois extensions, and φ_1 is well defined.

φ and φ_1 are inverse maps. Let (u, v) be a cocycle giving rise to $T(J)^u$ and to $A=A(u, v)$. As in the proof of (3.3), there is an isomorphism

$$=j_1^{-1}: T(J)^u \to T \otimes A$$

of Galois extensions, where $T \otimes A$ is considered as a subset of $T^2(J)$, and j is defined by $j(x)=v^{-1}\varepsilon_1(x)$. In particular, the cocycle $u_{A'}$ can be taken to be u itself. Now v_A is defined by a composite map $\bar{j}$ given as in (3.8), i.e. for y in $T^2(J)$,

$$v_A y = \bar{j}(y) = (\sigma(1 \otimes j^{-1})(\sigma \otimes 1)(1 \otimes j))(y).$$

Now for x in A, it is easy to see that the relation $j(x)=v^{-1}\varepsilon_1(x)=\varepsilon_0(x)$ implies the relation $\bar{j}(\varepsilon_0(x))=\varepsilon_1(x)$. Thus $v_A\varepsilon_0(x)=v\varepsilon_0(x)$ for x in A. But since j is an isomorphism, $\varepsilon_0(A)$ generates $T^2(J)$ as a $T^2(J)$-module. Since multiplication by v_A and by v are each $T^2(J)$-module maps, we have that $v=v_A$, and $\varphi_1\varphi$ is the identity map.

Conversely, let (A) be in $K(J, T/R)$, and let $f: T(J) \to A'=T \otimes A$ be a $T(J)$-isomorphism. Let $u=u_{A'}$, $v=v_A$. Then $f: T(J)^u \to T \otimes A$ is an isomorphism of Galois extensions. The diagrams below commute, where v_1 is defined by letting v

act on $T^2 \otimes A$, the latter being considered as a $T^2(J)$-module:

$$\begin{tikzcd}
T(J)^u \arrow[r, "\varepsilon_0"] \arrow[d, "f"'] & T^2(J)^{e(0)} \arrow[r, "l(v)"] \arrow[d, "\varepsilon_0(f)"] & T^2(J)^{e(1)} \arrow[d, "\varepsilon_1(f)"] \\
T \otimes A \arrow[r, "\varepsilon_0 \otimes 1"'] & T^2 \otimes A \arrow[r, "l(v_1)"'] & T^2 \otimes A
\end{tikzcd}$$

$$\begin{tikzcd}
T(J)^u \arrow[r, "\varepsilon_1"] \arrow[d, "f"'] & T^2(J)^{e(1)} \arrow[d, "\varepsilon_1(f)"] \\
T \otimes A \arrow[r, "\varepsilon_1 \otimes 1"'] & T^2 \otimes A
\end{tikzcd}$$

By an easy computation, and by [7, Lemma 3.8] we conclude that

$$A = \{x \text{ in } T \otimes A \mid v(\varepsilon_0 \otimes 1)(x) = (\varepsilon_1 \otimes 1)(x)\}.$$

It follows that $A \cong A(u, v)$ as Galois extensions. Thus $\varphi\varphi_1$ is the identity map.

We now show that φ_1 is a group homomorphism. Let (A_1), (A_2) be in $K(J, T/R)$, and let $A=(A_1 \otimes A_2)^H$, where $H=\{(\alpha, \alpha^{-1}) \text{ in } J \times J\}$. By definition, and by (1.10), $(A)=(A_1)\cdot(A_2)$ in $E_R(J)$. Write u_i for $u_{A_i'}$, u for $u_{A'}$, etc., and let $(u', v')=(u_1u_2, v_1v_2)$.

Define $j\colon T(J)^{u'} \to (T(J)^{u_1} \otimes T(J)^{u_2})^H$ by $j(\alpha)=\sum_{\beta\in J} \beta\alpha \otimes \alpha^{-1}$ for α in J. Let $f_i\colon T(J)^{u_i} \to T \otimes A_i$ be isomorphisms of Galois extensions for $i=1, 2$; and let

$$h\colon ((T \otimes A_1) \otimes (T \otimes A_2))^H \to T \otimes (A_1 \otimes A_2)^H$$

be the natural map (which is an isomorphism by (1.6)). The relations $u=u'$, $v=v'$ follow respectively from the proof of (2.2), and via a computation, from commutativity of the diagram below, in which the notation is as indicated:

$$T^2(J)^{\varepsilon_0(u_i)} = M_i \quad \text{for } i = 1, 2;\ T^2(J)^{\varepsilon_0(u)} = M.$$
$$T^2(J)^{\varepsilon_1(u_i)} = N_i \quad \text{for } i = 1, 2;\ T^2(J)^{\varepsilon_1(u)} = N.$$

$$\begin{tikzcd}
M \arrow[r, "\varepsilon_0(j)"] \arrow[d, "1 \otimes f"'] & M_1 \otimes_{T^2} M_2 \arrow[d, "\varepsilon_0(f_1) \otimes \varepsilon_0(f_2)"] \\
T^2 \otimes A \arrow[r, "\varepsilon_0(h^{-1})"] \arrow[d, "\sigma \otimes 1"'] & (T^2 \otimes A_1) \otimes_{T^2} (T^2 \otimes A_2) \arrow[d, "\sigma \otimes 1 \otimes \sigma \otimes 1"] \\
T^2 \otimes A \arrow[r, "\varepsilon_0(h^{-1})"] \arrow[d, "1 \otimes f^{-1}"'] & (T^2 \otimes A_1) \otimes_{T^2} (T^2 \otimes A_2) \arrow[d] \\
M \arrow[r, "\varepsilon_0(j)"] \arrow[d, "\sigma"'] & M_1 \otimes M_2 \arrow[d] \\
N \arrow[r, "\varepsilon_1(j)"'] & N_1 \otimes N_2
\end{tikzcd}$$

This completes the proof of the theorem, as naturality is easily verified.

THEOREM 3.9. *Let R, i, T be as in* (3.7). *Then there exists a natural isomorphism* $H^1(T/R, H^1U_{(\ )}(J)) \cong \operatorname{Ker}(E_i(J): E_R(J) \to E_T(J))$.

Proof. $H^1U_{(S)}(J)$, as defined preceding (2.2), is the kernel of

$$\delta^1: U(S(J)) \to U(S(J^2)),$$

since δ^0 is the trivial map. (It is easy to see that $H^1U_{(S)}(J) = \{\sum_{\alpha\in J} s_\alpha\alpha \text{ in } S(J) \mid s_\alpha s_\beta = \delta_{\alpha,\beta}s_\alpha, \text{ and } \sum_\alpha s_\alpha = 1\}$.) We have a chain map:

$$\begin{array}{ccc} H^1U_T(J) \to & H^1U_{T^2}(J) \to \cdots & \\ \downarrow & \downarrow & \\ U(T(J)) \to & U(T(J^2)) \oplus U(T^2(J)) \to \cdots & \end{array}$$

where the vertical maps are the inclusions. This chain map induces a map on cohomology $h: H^1(T/R, H^1U_{(\ )}(J)) \to H^1(J, T/R)$ which is given by $h(\mathrm{cl}\,(v)) = \text{class}\,(1, v)$. h is easily seen to be one-one. Using the fact that $T(J)^1 = e_J(T)$, and the constructions employed in the proof of (3.7), it is not difficult to verify that the image of φh consists of $\{(A) \mid T \otimes A \cong e_J(T)$ as Galois extensions$\}$. This completes the proof.

PROPOSITION 3.10. *Let $f: T \to T'$ be a homomorphism of R-algebras. Then f induces a homomorphism of bicomplexes $C(J,f): C(J, T/R) \to C(J, T'/R)$. If $g: T \to T'$ is another R-algebra map, then $C(J,f)$ and $C(J,g)$ are chain homotopic, and thus induce the same map $H(J,f): H(J, T/R) \to H(J, T'/R)$.*

Proof. f induces $f^n: T^n \to T'^n$ and also $f^{n,m}: U(T^{n+1}(J^{m+1})) \to U(T'^{n+1}(J^{m+1}))$. $\{f^{n,m}\}$ is easily seen to be a cochain map. Define $\bar{\psi}_i^n: T^{n+1} \to T'^n$ by

$$\bar{\psi}_i^n(t_1 \otimes \cdots \otimes t_{n+1}) = f(t_1) \otimes \cdots \otimes f(t_{i-1})g(t_i) \otimes g(t_{i+1}) \otimes \cdots \otimes g(t_{n+1})$$

for $1 \leqq i \leqq n$.

Let

$$\bar{\psi}_i^{n,m}: U(T^{n+1}(J^{m+1})) \to U(T'^{n+1}(J^{m+1}))$$

be induced by $\bar{\psi}_i^n$. Now define

$$s_1^{n,m}: U(T^{n+1}(J^{m+1})) \to U(T'^{n+1}(J^{m+1}))$$

by $s_1^{n,m} = \sum_{i=1}^n (-1)^i \psi_i^{n,m}$. Let

$$s_2^{n,m}: U(T^{n+1}(J^{m+1})) \to U(T'^{n+1}(J^m))$$

be the zero map.

From [2, Theorem 2.7] we know that $ds_1 + s_1d = f - g$, d being the Amitsur coboundary. Thus $ds_1 + s_1d + \delta s_2 + s_2\delta = f - g$, δ being the Harrison coboundary. By definition, $s_2d + ds_2 = 0$, and it is easily verified that $s_1\delta + \delta s_1 = 0$. By [4, p. 60], $(s_\cdot, s_2)$ defines a chain homotopy.

We define $\mathscr{U}$ to be the set of partitions of unity in R, i.e. the set of subsets $\{x_1, \dots, x_n\}$ of R for which $x_1 + \cdots + x_n = 1$. For x in R, R_x will denote the localization of R at $\{1, x, x^2, \dots\}$. If $V = \{x_1, \dots, x_n\}$, we will write $R_V = \sum_{i=1}^n \oplus R_{x_i}$. If V is in $\mathscr{U}$, R_V is a faithfully flat R-algebra [3, p. 88, Théorème 1], [3, p. 44, Proposition 1(d)].

For V, W in $\mathscr{U}$, write $R_V \leqq R_W$ if there exists an R-algebra homomorphism $R_V \to R_W$. Write $R_V \sim R_W$ if $R_V \leqq R_W$ and $R_W \leqq R_V$. Let $\mathscr{U}^*$ denote the set of equivalence classes of $\mathscr{U}$ relative to $\sim$, and for V in $\mathscr{U}$, write $(R_V)^*$ for the class of R_V in $\mathscr{U}^*$. If $V = \{x_1, \dots, x_n\}$ and $W = \{y_1, \dots, y_m\}$ are in $\mathscr{U}$, write

$$VW = \{z_{i,j} \mid i = 1, \dots, n; j = 1, \dots, m; z_{i,j} = x_i y_j\}.$$

Clearly VW is in $\mathscr{U}$, and the relation $\leqq$ defines a partial order on $\mathscr{U}^*$ under which the latter is a directed set, e.g. $(R_V)^* \leqq (R_{VW})^*$.

Definition 3.11. Let $n \geqq 0$. For R_V in $\mathscr{U}^*$, define an abelian group X_V by $X_V = H^n(J, R_V/R)$; X_V is well defined by (3.10). If $(R_V)^* \leqq (R_W)^*$, define $\alpha_V^W \colon X_V \to X_W$ by $\alpha_V^W = H^n(J, f)$ with $f \colon R_V \to R_W$. It is easy to see that we thus obtain a directed system of abelian groups $\{X_V, \{\alpha_V^W\}\}$. We define $H^n(J, R) =$ dir lim $H^n(J, R_V/R)$, where the direct limit is taken over $(R_V)^*$ in $\mathscr{U}^*$.

Theorem 3.12. (a) *There is a natural isomorphism* $H^1(J, R) \cong E_R(J)$.

(b) *There is a natural isomorphism*

$$\operatorname{dir\,lim} H^1(T/R, H^1U_{(\ \ )}(J)) \cong \{(A) \text{ in } E_R(J) \mid A_M \cong e_J(R_M) \text{ as Galois extensions for every maximal ideal } M \text{ of } R\},$$

where the direct limit is taken over the elements of $\mathscr{U}^*$.

Proof. Because of (3.7), it suffices to show that $E_R(J) = \bigcup_{T \in \mathscr{U}} K(J, T/R)$. Let A be a Galois extension of R with group J. For M a maximal ideal of R, we have from (1.4) and from [6, Theorem 4.2(c)] that

$$R_M \otimes A \cong R_M \otimes R_M(J) \cong R_M \otimes e_J(R)$$

as $R_M(J)$-modules (the proof of [6, Theorem 4.2(c)], and the results used in that proof, hold when A is not necessarily commutative; we also refer the reader to the comments at the beginning of the proof of (1.2)). Now [7, Lemma 5.1 and Theorem 5.2] may be applied to obtain a partition of 1, call it V, such that

$$R_V \otimes A \cong R_V \otimes e_J(R) \cong e_J(R_V)$$

as $R_V(J)$-modules; we remark that the results of [7] hold under somewhat weaker hypotheses than stated, and that the proof of [7, Lemma 5.1] can be easily corrected. Thus (a) is proved.

(b) Suppose $T = \sum_{i=1}^n \oplus R_{x_i}$ is such that $T \otimes A \cong e_J(T)$ as Galois extensions of T, where $\sum x_i = 1$. Tensoring with each direct summand of T, and using the fact that $S \otimes e_J(T) \cong e_J(S \otimes T)$ as Galois extensions, we get that $R_{x_i} \otimes A \cong e_J(R_{x_i})$ as

Galois extensions for $i \leqq n$. Let M be a maximal ideal of R. Choose j such that x_j is in R-M. We have a homomorphism of R-algebras, $S = R_{x_j} \to R_M$. Thus we obtain isomorphisms $R_M \otimes A \cong R_M \otimes (S \otimes A) \cong R_M \otimes_S e_J(S) \cong e_J(R_M)$. Thus the direct limit of (3.12)(b) is a subset of the indicated subset of $E_R(J)$.

We now prove the reverse inclusion. To begin with, we make the following observation: Let A be a Galois extension of R with group J, and let M be a maximal ideal of R such that $A_M \cong e_J(R_M)$ as Galois extensions of R_M; then there exists d in R-M such that $A_d \cong e_J(R_d)$ as Galois extensions of R_d. For let $\{r_\alpha/b$ in $A_M \mid r_\alpha$ is in A, b is in R-M, α is in $J\}$ be a set in A_M such that $r_\alpha r_\beta/b^2 = (\delta_{\alpha,\beta})r_\alpha/b$, $(\sum_\alpha r_\alpha)/b = 1$, and $\beta(r_\alpha)/b = r_{\alpha\beta}/b$ in A_M. It is easily seen that there exists an element c in R-M such that $c(br_\alpha r_\beta - b^2\delta_{\alpha,\beta}r_\alpha) = 0$, $c(\sum_\alpha r_\alpha - b) = 0$, and $bc(r_{\alpha\beta} - \beta(r_\alpha)) = 0$ in A. Let $d = bc$. We can compute that $\{r_\alpha/d \mid \alpha \text{ in } J\}$ is a set of mutually orthogonal idempotents in A_d, whose sum is 1, and which are a normal basis for A_d over R_d. Thus $A_d \cong e_J(R_d)$ as Galois extensions of R_d.

Now suppose $A_M \cong e_J(R_M)$ as Galois extensions for all maximal ideals M of R. Let I be the ideal in R generated by $\{x \text{ in } R \mid A_x \cong e_J(R_x)$ as Galois extensions$\}$. By the observation above, we conclude that $I = R$. Thus there exist $z_1, \ldots, z_n$ in R and $y_1, \ldots, y_n$ in I such that $z_1y_1 + \cdots + z_ny_n = 1$. Lct $x_i = z_iy_i$. Letting $T = \sum_{i=1}^n \oplus R_{x_i}$, we see that $T \otimes A \cong e_J(T)$ as Galois extensions of T. This completes the proof.

4. **A spectral sequence and the semilocal case.** We begin by proving a normal basis theorem.

THEOREM 4.1. *Let R be of characteristic p, and let J be a finite abelian group of exponent p. Then*

(a) *If T is a faithfully flat R-algebra, we have that $H^n(J, T/R) \cong H^{n+1}U_R(J)$ for $n \geqq 0$.*

(b) *$A_R(J) = E_R(J)$, i.e. every Galois extension of R with group J is a Galois (R, J)-algebra.*

Proof. By [13, Theorem 3.4], the maps $\alpha_n: T(J^n) \to T$ defined by $\alpha_n(\sum t_x x) = \sum t_x$ induce isomorphisms $\beta_n: H^n(T(J^n)/R(J^n), U) \cong H^n(T/R, U)$ for $n > 0$; (note that the definition of $H^0(T/R, U)$ in [13] differs from ours). Then

$$H^p(T/R, U) \cong {}'H^{p,q} = \operatorname{Ker}(d^{p,q})/\operatorname{Im}(d^{p-1,q})$$

under the isomorphism β_{q+1}; it is not difficult to see that the composite

$$\beta_{q+1}\delta^{p,q}\beta_{q+1}^{-1}: H^p(T/R, U) \to {}'H^{p,q} \to {}'H^{p,q+1} \to H^p(T/R, U)$$

is either the zero map or the identity map, depending on whether q is odd or even respectively; this follows by noting that $\delta^n: U(R(J^n)) \to U(R(J^{n+1}))$, when restricted to $U(R)$, is the zero map or the identity map depending on whether n is even or odd respectively. Thus, the homology of the double complex taken with respect to first d, and then δ, is 0 for $q > 0$ and by [10, p. 89, Théorème 4.8.1] we see that the injection of Ker $(U(T(J^n)) \to U(T^2(J^n)))$ into the bicomplex induces an isomorphism of cohomology. But if T is faithfully flat over R, the kernel in question is $U(R(J^n))$. Thus we have isomorphisms $H^{n+1}U_R \cong H^n(J, T/R)$. Now (b) follows from (2.2), from (3.12), and from the fact that the isomorphism obtained in (a) is induced by inclusion maps.

THEOREM 4.2. *Suppose that R is a semilocal ring, and that T is a faithfully flat R-algebra. Then $H^1(J, T/R) \cong H^2U_R(J)$.*

Proof. The exact sequence associated with the first spectral sequence of our bicomplex [4, chapter XV, §6] yields

$$0 \to E^2_{0,1} \to H^1(J, T/R) \to E^2_{1,0},$$

where $E^2_{p,q}$ is the homology of the double complex taken with respect to d and δ in that order. The faithful flatness of T implies that $E^2_{0,1} = H^2U_R(J)$. Now

$$E^2_{1,0} = \operatorname{Ker}(H^1(T(J)/R(J), U) \to H^1(T(J^2)/R(J^2), U)),$$

a subset of $H^1(T(J)/R(J), U)$; the last set may be considered as a subgroup of Pic $(R(J))$ by (3.3) and (3.5). If S is semilocal, Pic $(S) = 0$ by [3, p. 143, Proposition 5]. If we show Pic $(R(J)) = 0$ we will be done. For M a maximal ideal of R, only finitely many maximal ideals of $R(J)$ contain M. For if $K = R/M$, there is a one-one correspondence between the maximal ideals of $R(J)$ containing M and the maximal ideals of $R(J)/MR(J) = K(J)$. But K is a field, so that $K(J)$ has the descending chain conditions on ideals, and is thus semilocal by a Nakayama's lemma argument. Thus only finitely many maximal ideals of $R(J)$ contain M. Now $R(J)$ is an integral extension of R [15, p. 254] since it is a finitely generated R-module. Thus every maximal ideal of $R(J)$ lies over some maximal ideal of R [15, p. 259]. This completes the proof.

Using (4.2), (3.12) and the fact that every Galois extension over a semilocal ring has a normal basis, we can recover the isomorphism between $H^2U_R(J)$ and $A_R(J)$ described in (2.2).

REFERENCES

1. S. A. Amitsur, *Simple algebras and cohomology groups of arbitrary fields*, Trans. Amer. Math. Soc. **90** (1959), 73–112.

2. ———, *Homology groups and double complexes for arbitrary fields*, J. Math. Soc. Japan **14** (1962), 1–25.

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

4. H. Cartan and S. Eilenberg, *Homological algebra*, Princeton Univ. Press, Princeton, N. J., 1956.

5. S. U. Chase, *Abelian extensions and a cohomology theory of Harrison*, Proc. La Jolla Conference on Categorical Algebra, 1965.

6. S. U. Chase, D. K. Harrison and Alex Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965), pp. 15–33.

7. S. U. Chase and Alex Rosenberg, *Amitsur cohomology and the Brauer group*, Mem. Amer. Math. Soc. No. 52 (1965), 34–77.

8. ———, *A theorem of Harrison, Kummer theory, and Galois algebras*, Nagoya Math. J. **27–2** (1966), 663–685.

9. F. R. DeMeyer, *Some notes on the general Galois theory of rings*, Osaka J. Math. **2** (1965), 117–127.

10. R. Godement, *Théorie des faisceaux*, Actualités Sci. Ind., No. 1252, Hermann, Paris, 1958.

11. D. K. Harrison, *Abelian extensions of arbitrary fields*, Trans. Amer. Math. Soc. **106** (1963), 230–235.

12. ———, *Abelian extensions of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965), 1–14.

13. Alex Rosenberg and D. Zelinsky, *Amitsur's complex for inseparable fields*, Osaka J. Math. **14** (1962), 219–240.

14. Y. Takeuchi, *On Galois extension over commutative rings*, Osaka J. Math. **2** (1965), 137–145.

15. O. Zariski and P. Samuel, *Commutative algebra*, Vol. I, Van Nostrand, Princeton, N. J., 1958.

Cornell University,
Ithaca, New York