A THEOREM OF HARRISON, KUMMER THEORY, AND GALOIS ALGEBRAS

S. U. CHASE and ALEX ROSENBERG[1)]

To the memory of TADASI NAKAYAMA

1. Introduction. Let R be a field and S a separable algebraic closure of R with galois group $\mathfrak{G}_R$. In [8] Harrison succeeded in describing $\mathfrak{G}_R/\mathfrak{G}'_R$ in terms of R only. More precisely, he constructed a certain complex $\mathfrak{H}(R, Q/Z)$ and proved $\mathrm{Hom}_c(\mathfrak{G}_R, Q/Z) \cong H^2(R, Q/Z)$, where Hom_c denotes continuous homomorphisms and H^2 stands for the second cohomology group of the complex $\mathfrak{H}$. In this paper, which is mainly expository in nature, we reexamine Harrison's proof and show how [8] connects with Kummer theory and the theory of galois algebras [16]. We emphasize that most of the ideas on which this paper is based originate in [8].

In 2. the complex $\mathfrak{H}(R, J)$ is introduced for any commutative ring R and abelian group J. If J is a finite abelian group of exponent e and R a field of characteristic prime to e, we show that $\mathfrak{H}(R, J)$ is isomorphic to a complex arising in ordinary group cohomology. This enables us to compute $H^n(R, J)$ in case R is a field of characteristic prime to e and containing the e^{th}-roots of unity. In 3. we consider a field R and a galois extension field S with galois group $\mathfrak{G}$. We give two proofs, one using spectral sequences, of the existence of an exact sequence

$$0 \to \mathrm{Hom}_c(\mathfrak{G}, J) \to H^2(R, J) \to H^2(S, J).$$

From this we can already deduce Harrison's result in case R has characteristic 0 and also obtain the main exact sequence of Kummer theory. Section 4 is devoted to a new exposition of the foundation of the theory of galois algebras [16] over a commutative ring. It turns out that the dual concept, that of galois coalgebra, is much more amenable to treatment and we accordingly

Received August 26, 1965.
1) Written with the partial support of N.S.F. grant GP-3665.

treat matters in this way. The connection of this theory with the complex $\mathfrak{H}$ is also given. In the last section we show that galois algebras with cyclic galois groups are necessarily commutative and complete the proof of Harrison's theorem in the general case. The main result of 5. for algebras over fields has recently been generalized in [10].

A treatment of this material from the viewpoint of category theory will be published by S. U. Chase in the Proceedings of the Conference on Categorical algebra held at LaJolla, California, in June 1965.

All commutative rings occuring in this paper have identities.

2. Harrison cohomology and group cohomology. Let R be a commutative ring and J an abelian group. In [8] Harrison defined a cochain complex $\mathfrak{H}(R, A)$ as follows. Let U denote the functor which assigns the multiplicative group of units to any R-algebra, J^n the direct product of J with itself n times, $R(J^n)$ the group algebra of J^n over R, and let $R(J^0) = R$. We shall often identify $R(J^n)$ with $R(J) \otimes \cdots \otimes R(J)$ [2] via the usual natural isomorphism. Then $\mathfrak{H}^n(R, J)$, the n^{th}-cochain group is $U(R(J^n))$, $n = 0, 1, 2, \ldots$. Let $\Delta : R(J) \to R(J^2)$ denote the usual diagonal map and let $\Delta_i : R(J^n) \to R(J^{n+1})$, $i = 1, 2, \ldots, n$, denote the "diagonal map applied at the i^{th}-place". Explicitly, Δ_i is defined by linearity and $\Delta_i(a_1 \otimes \cdots \otimes a_n) = a_1 \otimes \cdots a_{i-1} \otimes a_i \otimes a_i \otimes \cdots \otimes a_n$, for a_n in J. Furthermore, let Δ_0, $\Delta_{n+1} : R(J^n) \to R(J^{n+1})$ be defined by $\Delta_0(a) = 1 \otimes a$, $\Delta_{n+1}(a) = a \otimes 1$. Then the coboundary operator δ_H of $\mathfrak{H}(R, J)$ is defined by

$$\delta_H(x) = \prod_0^{n+1} \Delta_i(x)^{(-1)^i}, \quad n = 0, 1, \ldots \tag{2.1}$$

for x in $U(R(J^n))$. Note that for x in $U(R) = U(R(J^0))$, $\delta_H(x) = 1$. The cohomology groups of $\mathfrak{H}(R, J)$ will be denoted by $H^n(R, J)$, $n = 0, 1, 2, \ldots$.

In this section we show that if J is a finite abelian group and R a field of characteristic prime to the exponent of J, then the complex $\mathfrak{H}(R, J)$ is isomorphic to a more familiar one arising in group cohomology. The latter arises as follows. Let G be a group, M a left G-module, and $\mathfrak{G}$ a group operating on both G and M as group automorphisms such that

$$\omega(\sigma m) = \omega(\sigma)\,\omega(m)$$

[2] The unadorned $\otimes$ always means tensor over R.

for all ω in $\mathfrak{G}$, σ in G, and m in M. An equivariant n-cochain of G to M is a function $f: G^n \to M$, such that for all ω in $\mathfrak{G}$ and $\sigma_1, \ldots, \sigma_n$ in G

$$\omega(f(\sigma_1, \ldots, \sigma_n)) = f(\omega(\sigma_1), \ldots, \omega(\sigma_n)).$$

Under pointwise addition these form a group which is denoted by $C^n_{\mathfrak{G}}(G, M)$. Note that if $C^n(G, M)$ is the ordinary n-cochain group, $\mathfrak{G}$ acts on it via

$$(\omega f)(\sigma_1, \ldots, \sigma_n) = \omega(f(\omega^{-1}(\sigma_1), \ldots, \omega^{-1}(\sigma_n))),$$

and that $C^n_{\mathfrak{G}}(G, M) = (C^n(G, M))^{\mathfrak{G}}$. The usual coboundary operator, δ, of group cohomology [11, (5.8) p. 116] sends $C^n_{\mathfrak{G}}(G, M)$ to $C^{n+1}_{\mathfrak{G}}(G, M)$ and we thus obtain a complex $C_{\mathfrak{G}}(G, M)$ whose cohomology groups are denoted by $H^n_{\mathfrak{G}}(G, M)$, $n = 0, 1, 2, \ldots$. If $\mathfrak{G} = 1$ we clearly obtain the usual cohomology groups $\mathfrak{H}^n(G, M)$ [11, p. 115].

Returning now to $\mathfrak{H}(R, J)$, let $S \supset R$ be a commutative ring and $\mathfrak{G}$ a group of R-automorphisms of S. By $\hat{J}(S)$ we shall mean the group of characters of J to S. It is clear that $\mathfrak{G}$ operates on $\hat{J}(S)$, and so viewing S as a trivial $\hat{J}(S)$-module, $C^1_{\mathfrak{G}}(\hat{J}(S), S)$ is defined and indeed is an R-algebra under pointwise operations. We define

$$T: R(J) \to C^1_{\mathfrak{G}}(\hat{J}(S), S)$$

by $T(\sum r_a a)(\chi) = \sum r_a \chi(a)$ for a in J, χ in $\hat{J}(S)$, r_a in R.

LEMMA 2.1. *T is a homomorphism of R-algebras. If J is a finite abelian group of exponent e, R a field of characteristic prime to e, S the field obtained by adjoining the e^{th}-roots of unity to R, and $\mathfrak{G}$ the galois group of S over R, then T is an isomorphism.*

Proof. The first statement is clear. Under the further hypotheses, it is well known that $\hat{J}(S)$ is the full character group of J and that the square matrix $[\chi(a)]$, χ in $\hat{J}(S)$, a in J, is nonsingular [15, § 126, p. 181]. Therefore it follows that for any function $f: \hat{J}(S) \to S$, the equations

$$f(\chi) = \sum x_a \chi(a) \quad \chi \text{ in } \hat{J}(S) \tag{2.2}$$

have *unique* solutions s_a in S. Hence, if $T(\sum r_a a) = 0$, we have $r_a = 0$ and so T is injective. Now for an f in $C^1_{\mathfrak{G}}(\hat{J}(S), S)$,

$$\omega(f(\chi)) = \sum \omega(s_a)(\omega\chi)(a) = f(\omega\chi) = \sum s_a(\omega\chi)(a)$$

for all ω in $\mathfrak{G}$. Since $\omega\chi$ runs through $\hat{J}(S)$ as χ does, this means that $\{\omega(s_a)\}$ is another set of solutions of (2.2). Thus $\omega(s_a) = s_a$ for all ω in $\mathfrak{G}$ so that $s_a = r_a$ lies in R. Hence T is surjective, proving Lemma 2.1.

Next, let maps $\theta_i : C^n_{\mathfrak{G}}(G, M) \to C^{n+1}_{\mathfrak{G}}(G, M)$, $i = 0, 1, 2, \ldots, n+1$, be defined by

$$(\theta_0 f)(\sigma_1, \ldots, \sigma_{n+1}) = f(\sigma_2, \ldots, \sigma_{n+1})$$
$$(\theta_i f)(\sigma_1, \ldots, \sigma_{n+1}) = f(\sigma_1, \ldots, \sigma_{i-1}, \sigma_i\sigma_{i+1}, \sigma_{i+2}, \ldots, \sigma_{n+1}),\ i = 1, 2, \ldots, n$$
$$(\theta_{n+1} f)(\sigma_1, \ldots, \sigma_{n+1}) = f(\sigma_1, \ldots, \sigma_n).$$

As usual we identify $(\hat{J}(S))^n$ with $\hat{J}^n(S)$ by setting

$$(\chi_1 \otimes \cdots \otimes \chi_n)(a_1 \otimes \cdots \otimes a_n) = \prod_1^n \chi_i(a_i).$$

Let $T^n : R(J^n) \to C^1_{\mathfrak{G}}((\hat{J}(S))^n, S)$ denote the R-algebra homomorphism defined just before Lemma 2.1. Then it is easily verified that all the diagrams

$$\begin{array}{ccc} R(J^n) & \xrightarrow{T^n} & C^1_{\mathfrak{G}}((\hat{J}(S))^n, S) \\ \downarrow \Delta_i & & \downarrow \theta_i \\ R(J^{n+1}) & \xrightarrow{T^{n+1}} & C^1_{\mathfrak{G}}((\hat{J}(S))^{n+1}, S) \end{array}$$

$i = 0, 1, \ldots, n+1$, are commutative. Furthermore, $U(C^1_{\mathfrak{G}}((\hat{J}(S))^n, S)) = C^1_{\mathfrak{G}}((\hat{J}(S))^n, U(S))$ with $U(S)$ viewed as a trivial $\hat{J}(S)$-module. Since the coboundary operator of $C_{\mathfrak{G}}(\hat{J}(S), U(S))$ is $\prod_1^{n+1} \theta_i^{(-1)^i}$, the above commutativity shows that the mappings T^n induce a complex homomorphism $\mathfrak{H}(R, J) \to C_{\mathfrak{G}}(\hat{J}(S), U(S))$. Since the exponent of J^n is that of J, Lemma 2.1 then yields

THEOREM 2.2. *Let J be a finite abelian group of exponent e, R a field of characteristic prime to e, S the field obtained by adjoining the e^{th}-roots of unity to R, and $\mathfrak{G}$ the galois group of S over R. The map defined by linearity and $a_1 \otimes \cdots \otimes a_n \to f$ with $f(\chi_1, \ldots, \chi_n) = \prod_1^n \chi_i(a_i)$ (a_i in J, χ_i in $\hat{J}(S)$) induces an isomorphism of complexes $\mathfrak{H}(R, J) \cong C_{\mathfrak{G}}(\hat{J}(S), U(S))$, with $U(S)$ being viewed as trivial $J(S)$-module. Hence $H^n(R, J) \cong H^n_{\mathfrak{G}}(\hat{J}(S), U(S))$, $n = 0, 1, 2, \ldots$.*

COROLLARY 2.3. *Let J be a cyclic group of order n, and R be a field of characteristic prime to n containing the n^{th}-roots of unity. Then*

$$H^{2k}(R, J) \cong U(R)/(U(R))^n, \quad k = 1, 2, \ldots$$
$$H^{2k+1}(R, J) \cong J \qquad\qquad k = 0, 1, \ldots,$$

Proof. Theorem 2.1 with $R=S$ and $\mathfrak{G}=1$ is applicable. Since $\hat{J}(R)\cong J$ [15, p. 180] is cyclic, the groups $H^n(\hat{J}(R), U(R))$ are well known [11, p. 122] and the result follows upon noting that, since $\hat{J}(R)$ acts trivially, the norm is just raising to n^{th}-powers and the elements annihilated by the norm are precisely the n^{th}-roots of unity in R, a group isomorphic to J.

Remark. The isomorphism $H^2(R, J)\cong H^2(\hat{J}(R), U(R))$ in case R is a field of characteristic prime to e and contains the e^{th}-roots of unity has already been noted in a slightly different form in [16, p. 82].

3. An exact sequence and Kummer theory.

LEMMA 3.1. (cf. [8, Lemma, p. 233]) *Let R be a commutative ring containing no idempotent but 0 and 1. Then $H^1(R, J)\cong J$.*

Proof. Let $x=\sum r_a a$ in $U(R(J))$ be a 1-cocycle. Applying (2.1), we have $\Delta_0(x)\,\Delta_2(x)=\Delta_1(x)$ or

$$\sum_{a,b} r_a r_b(a\otimes b)=\sum_a r_a(a\otimes a).$$

Since $\{(a\otimes b)\mid a, b \text{ in } J\}$ is a basis of $R(J^2)$ over R, the r_a are a system of orthogonal idempotents. Hence $x=a$ is in J. Since $\delta_H : U(R)\to U(R(J))$ is the trivial map, 1 is the only 1-coboundary and the lemma is proved.

Now let R be a field and S a galois extension field with galois group $\mathfrak{G}$. We allow $\mathfrak{G}$ to be infinite and then view it as a pro-finite group, i.e. as a compact totally disconnected topological group [14]. For any abelian group J, the action of $\mathfrak{G}$ on S turns $U(S(J^q))$ into a $\mathfrak{G}$-module. Moreover, $\mathfrak{G}$ operates continuously on the discrete space $U(S(J^q))$, since it is clear that if $\{S_i\}$ is the family of finite galois extensions of R contained in S, then $U(S(J^q))$ is the union of the $U(S_i(J^q))$. If M is any discrete $\mathfrak{G}$-module on which $\mathfrak{G}$ operates continuously, we denote the complex of continuous cochains of $\mathfrak{G}$ in M by $C(\mathfrak{G}, M)$, and the cohomology groups of this complex by $H^p(\mathfrak{G}, M)$, $p=0, 1, 2\cdots$ [14, 1-9].

Now consider, for any abelian group J, the bigraded group

$$E_0=\sum E_0^{p,q},\ p, q=0, 1, 2, \ldots, \text{ where } E_0^{p,q}=C^p(\mathfrak{G}, U(S(J^{q+1})))$$

There are two derivations on E_0,

$$\delta : E_0^{p,q}\to E_0^{p+1,q}$$

being the usual one of group cohomology [11, p. 116] and,

$$\delta_H : E_0^{p,q} \to E_0^{p,q+1}$$

defined by $(\delta_H f)(\sigma_1, \ldots, \sigma_p) = \delta_H(f(\sigma_1, \ldots, \sigma_p))$, with δ_H as in (2.1). It is easily verified that $\delta_H \delta = \delta_H \delta$ and, making an obvious change in sign, we obtain a bicomplex $(E_0, \delta, \pm \delta_H)$ [11, p. 340] whose associated total complex $\{\sum_{p+q=n} E_0^{p,q}, \delta \pm \delta_H\}$ we denote by Tot. As usual there are two spectral sequences, both converging to $H(\mathrm{Tot})$. Letting H_δ and H_{δ_H} stand for cohomology with respect to δ and δ_H respectively, their E_2-terms are given by $H_\delta H_{\delta_H} E_0$ and $H_{\delta_H} H_\delta E_0$ [4, p. 331].

PROPOSITION 3.2. *There is a spectral sequence*

$$H^p(\mathfrak{G}, H^{q+1}(S, J)) \underset{p}{\Longrightarrow} H^n(\mathrm{Tot}).$$

Proof. It is readily seen that $C^p(\mathfrak{G}, \ )$ is an exact functor on the category of discrete $\mathfrak{G}$-modules on which $\mathfrak{G}$ operates continuously. Hence by [4, Thm. 7.2, p. 68], $\mathrm{H}_{\delta_H} E_0^{p,q} \cong C^p(\mathfrak{G}, H^{q+1}(S, J))$. For the first of the above spectral sequences, therefore

$$E_2^{p,q} \cong H^p(\mathfrak{G}, H^{q+1}(S, J)),$$

which proves the proposition.

Before dealing with the second spectral sequence we note the following generalization of Hilbert's theorem 90:

LEMMA 3.3. *If J is a torsion group, then $H^1(\mathfrak{G}, U(S(J^{q+1}))) = 0$, $q = 0, 1, 2, \ldots$.*

Proof. Let $\{S_i\}$ be the family of finite galois extensions of R contained in S with galois groups $\mathfrak{G}_i$. Then ([14, Prop. 8, p. I-9]) $H^1(\mathfrak{G}, U(S(J^{q+1}))) = \varinjlim H^1(\mathfrak{G}_i, U(S_i(J^{q+1})))$. Since J is torsion, $J \cong \varinjlim J_j$ where the J_j's are finite abelian groups. Once more by [14, Prop. 8, p. I-9], $H^1(\mathfrak{G}_i, U(S_i(J^{q+1}))) \cong \varinjlim H^1(\mathfrak{G}_i, U(S_i(J_j^{q+1})))$. It therefore suffices to prove Lemma 3.3 assuming that both $\mathfrak{G}$ and J are finite. In this form the lemma is a special case of [13, Exc. 2, p. 160] or also follows from [5]. Indeed, by [5, Lemma 1.7], $S(J^{q+1}) \cong S \otimes R(J^{q+1})$ is a galois extension of $R(J^{q+1})$ with galois group $\mathfrak{G}$. Hence by Corollary 5.5 of [5], $H^1(\mathfrak{G}, U(S(J^{q+1})))$ is a subgroup of $P(R(J^{q+1}))$, the group of finitely generated projective $R(J^{q+1})$-modules of rank one. But the latter

is 0, since $R(J^{q+1})$ is a finite-dimensional algebra over a field and thus is a semilocal ring [3, Prop. 5, p. 143].

PROPOSITION 3.4. *If J is a torsion group there is a spectral sequence*

$$E_2^{p,q} \underset{q}{\Longrightarrow} H^n(\mathrm{Tot})$$

with $E_2^{0,q} \cong H^{q+1}(R, J)$ and $E_2^{1,q} = 0$, $q = 0, 1, 2, \ldots$.

Proof. Clearly $H_\delta E_0^{p,q} \cong H^p(\mathfrak{G}, U(S(J^{q+1})))$. Hence $H_\delta E_0^{0,q} \cong U(S(J^{q+1}))^{\mathfrak{G}} = U(R(J^{q+1}))$ and so for the second of the above spectral sequences, $E_2^{0,q} \cong H^{q+1}(R, J)$. By Lemma 3.3, $H_\delta E_0^{1,q} = 0$ and so $E_2^{1,q} = 0$ for this spectral sequence.

COROLLARY 3.5. *If R is a field, S a galois extension field with galois group $\mathfrak{G}$, and J an abelian torsion group viewed as trivial $\mathfrak{G}$-module there is an exact sequence*

$$0 \to H^1(\mathfrak{G}, J) \to H^2(R, J) \to H^2(S, J)^{\mathfrak{G}}$$

Proof. The five term exact sequence of low degree terms [7, Thm. 4.5.1, p. 82] of the spectral sequence in Lemma 3.4 yields an exact sequence

$$0 \to E_2^{0,1} \to H^1(\mathrm{Tot}) \to E_2^{1,0}$$

In view of Lemma 3.4, this shows that the edge homomorphism $H^2(R, J) \to H^1(\mathrm{Tot})$ is an isomorphism. Applying the same exact sequence in the case of the spectral sequence of Proposition 3.2 and keeping Lemma 3.1 in mind, then yields the exactness of

$$0 \to H^1(\mathfrak{G}, J) \to H^2(R, J) \to H^2(S, J)^{\mathfrak{G}}.$$

Remark. It should be noted that since $\mathfrak{G}$ operates trivially on J, $H^1(\mathfrak{G}, J)$ is simply the group of continuous homomorphisms of $\mathfrak{G}$ to J, denoted by $\mathrm{Hom}_c(\mathfrak{G}, J)$ in [8].

We proceed to compute the above map $H^1(\mathfrak{G}, J) \to H^2(R, J)$ explicitly in order to see that it is the same as the map Δ of [8, p. 232], and at the same time sketch a proof of Corollary 3.5 that does not use spectral sequences.

The two edge homomorphisms $E_2^{1,0} \to H^1(\mathrm{Tot})$ and $E_2^{0,1} \to H^1(\mathrm{Tot})$ in the two spectral sequences arise from injecting the δ_H-cycles on the x-axis and the δ-cycles on the y-axis into Tot [7, p. 89].

An arbitrary element of degree 1 in Tot has the form (u, v) with u in

$C^1(\mathfrak{G}, U(S(J)))$ and v in $C^0(\mathfrak{G}, U(S(J^2))) = U(S(J^2))$. Hence the isomorphism $H^2(R, J) \to H^1(\mathrm{Tot})$ arises from mapping a 2-cocycle v in $U(R(J^2))$, the δ-cocycles of $U(S(J^2))$, to $(1, v)$, and the mapping $H^1(\mathfrak{G}, J) \to H^1(\mathrm{Tot})$ is given by sending a continuous homomorphism $f : \mathfrak{G} \to J$, to $(f, 1)$. Hence, for a given f in $H^1(\mathfrak{G}, J)$, there is a unit v in $R(J^2)$ and a unit w in $S(J)$ such that

$$(f, 1) = (\delta w, \delta_H w)(1, v).$$

Thus, for all σ in $\mathfrak{G}$ we have $f(\sigma) = \dfrac{\sigma(w)}{w}$ and $\delta_H(w) = v$. The mapping $H^1(\mathfrak{G}, J) \to H^2(R, J)$ then sends the class of f to that of v in $U(R(J^2))$, which is precisely the mapping Δ of [8, p. 232]. Furthermore, this immediately suggests the following alternate proof of Corollary 3.5. The residue class of w modulo $U(R(J))$ is clearly a 1-cocycle in $\mathfrak{H}(S, J)/\mathfrak{H}(R, J)$, a complex which we denote by V. The exact sequence of complexes

$$1 \to \mathfrak{H}(R, J) \to \mathfrak{H}(S, J) \to V \to 1$$

yields the exact cohomology sequence

$$H^1(R, J) \to H^1(S, J) \to H^1(V) \to H^2(R, J) \to H^2(S, J).$$

In view of Lemma 3.1, this becomes the exact sequence

$$0 \to H^1(V) \to H^2(R, J) \to H^2(S, J).$$

To prove $H^1(\mathfrak{G}, J) \cong H^1(V)$ we proceed as follows: given a 1-cocycle of V, let w be a representative in $U(S(J))$ and define $f : \mathfrak{G} \to U(S(J))$ by $f(\sigma) = \dfrac{\sigma(w)}{w}$. Since $\delta_H(w)$ is in $U(R(J^2))$, it is readily verified that $f(\sigma)$ is a 1-cocycle in $\mathfrak{H}(S, J)$ and thus, by Lemma 3.1, lies in J. Hence f is in $H^1(\mathfrak{G}, J)$. Conversely, given f in $H^1(\mathfrak{G}, J)$, it may be viewed as a 1-cocycle of $\mathfrak{G}$ in $U(S(J))$. By Lemma 3.3, there is a unit w in $S(J)$ with $f(\sigma) = \dfrac{\sigma(w)}{w}$ for all σ in $\mathfrak{G}$. Since $f(\sigma)$ is in J it follows readily that the class of w modulo $U(R(J))$ is a 1-cocycle in V. It is then straightforward to verify that the correspondence $f \leftrightarrow w$ induces an isomorphism $H^1(\mathfrak{G}, J) \cong H^1(V)$. Except for the use of Lemma 3.3, this is the essential idea of Harrison's proof that "the map is one-one".

COROLLARY 3.6. *Let R be a field, S a separable algebraic closure of R with galois group $\mathfrak{G}_R$. Then in order to prove Harrison's theorem,* $\mathrm{Hom}_c(\mathfrak{G}_R, Q/Z) = H^1(\mathfrak{G}_R, Q/Z) \cong H^2(R, Q/Z)$, *it is sufficient to show $H^2(S, J) = 0$ for all finite cyclic groups J.*

Proof. By Corollary 3.5, it is clearly sufficient to show $H^2(S, Q/Z) = 0$. Now if $J \cong \varinjlim J_i$, it is clear that $\mathfrak{H}(R, J) \cong \varinjlim \mathfrak{H}(R, J_i)$ and by [4, Prop. 5.9.3*, p. 100] it follows that $H^n(R, J) \cong \varinjlim H^n(R, J_i)$, $n = 0, 1, 2, \ldots$. Since Q/Z is the direct limit of all finite cyclic groups the result now follows.

COROLLARY 3.7. *If R is a field of characteristic zero, S an algebraic closure of R with galois group $\mathfrak{G}_R$, then $H^1(\mathfrak{G}_R, Q/Z) \cong H^2(R, Q/Z)$.*

Proof. Let J be a cyclic group of order n. By Corollary 2.3, $H^2(S, J) = U(S)/(U(S))^n$ and this is 0 since S is algebraically closed. This together with Corollary 3.6 proves the result.

COROLLARY 3.8. *Let J be a cyclic group of order n, R a field of characteristic prime to n containing all the n^{th}-roots of unity, and S a galois extension field of R with galois group $\mathfrak{G}$. Viewing J as a trivial $\mathfrak{G}$-module, there is an exact sequence*

$$0 \to H^1(\mathfrak{G}, J) \to U(R)/(U(R))^n \to U(S)/(U(S))^n$$

Proof. This follows immediately from Corollaries 2.3 and 3.5.

Remark. Since $H^1(\mathfrak{G}, J)$ is the group of continuous homomorphisms of $\mathfrak{G}$ to J, and J may be identified with the group of the n-th roots of unity in R, this exact sequence is the basic part of Kummer theory [1, p. 19; 13, p. 163].

4. Galois algebras and coalgebras. In order to prove Harrison's theorem for fields of arbitrary characteristic, it is necessary to study $H^2(R, J)$ in greater detail. In this section we follow up the original ideas in [8] and exhibit a close connection between $H^2(R, J)$ and the theory of galois algebras initiated by Hasse and his school [16].

Let R be a commutative ring and G a finite group. As before, $R(G^n)$ denotes the group ring of $G^n = G \times \cdots \times G$ (n times) over R, and $R(G^n)$ will be viewed as an $R(G)$-module via diagonal action, i.e.

$$\sigma(\tau_1 \otimes \cdots \otimes \tau_n) = \sigma\tau_1 \otimes \cdots \otimes \sigma\tau_n.$$

By a *galois R-coalgebra* $(R(G), D)$, we mean $R(G)$ together with an $R(G)$-homomorphism

$$D : R(G) \to R(G^2) \cong R(G) \otimes R(G).$$

The coalgebra is coassociative if the diagram

$$\begin{array}{ccccc} R(G) & \xrightarrow{D} & R(G^2) & \xrightarrow{D\otimes 1} & R(G^3) \\ \| & & \| & & \| \\ R(G) & \xrightarrow{D} & R(G^2) & \xrightarrow{1\otimes D} & R(G^3) \end{array} \tag{4.1}$$

is commutative. Two galois R-coalgebras $(R(G), D)$, $(R(G), \tilde{D})$ are defined to be isomorphic if there is an $R(G)$-module automorphism ϕ of $R(G)$ rendering the diagram

$$\begin{array}{ccc} R(G) & \xrightarrow{D} & R(G^2) \\ \uparrow{\scriptstyle \phi} & & \uparrow{\scriptstyle \phi\otimes\phi} \\ R(G) & \xrightarrow{\tilde{D}} & R(G^2). \end{array} \tag{4.2}$$

commutative.

Isomorphism classes of galois R-coalgebras are easily described in terms of elements of $R(G^2)$. Indeed, since D is an $R(G)$-homomorphism, for any x in $R(G)$ we have

$$D(x) = \Delta(x)\, D(1) \tag{4.3}$$

where Δ is the usual diagonal map, as in 2. Let $D(1) = u$. Then it is immediate that (4.1) is commutative if and only if $(D\otimes 1)(D(1)) = (1\otimes D)(D(1))$, since all the mappings are $R(G)$-homomorphisms. This last equation is equivalent to

$$\Delta_1(u)\,\Delta_3(u) = \Delta_2(u)\,\Delta_0(u) \tag{4.4}$$

in the notation of 2. Conversely, given any element u in $R(G^2)$ satisfying (4.4), define $D(u)(x) = \Delta(x)u$. Then it is clear that $(R(G), D(u))$ is a coassociative galois R-coalgebra.

If $(R(G), D) \cong (R(G), \tilde{D})$, then, since ϕ is an $R(G)$-module automorphism

$$\phi(x) = x\phi(1) = xv \tag{4.5}$$

for all x in $R(G)$, where $v = \phi(1)$ is a unit in $R(G)$. Since all maps in the diagram (4.2) are $R(G)$-homomorphisms, commutativity of (4.2) is equivalent to the condition that $D(\phi(1)) = (\phi\otimes\phi)(\tilde{D}(1))$, i.e. that

$$\Delta(v)u = \tilde{u}(v\otimes v). \tag{4.6}$$

Again it is quite clear that, given two galois coalgebras $(R(G), D)$, $(R(G), \tilde{D})$ and a unit v in $R(G)$ satisfying (4.6), then defining ϕ by (4.5) yields an

isomorphism between them. Since (4.6) is easily seen to be an equivalence relation, we have established

PROPOSITION 4.1. *There is a bijection of pointed sets between the set of isomorphism classes of coassociative galois R-coalgebras $(R(G), D)$ and equivalence classes of elements of $R(G^2)$ satisfying* (4.4), *the equivalence relation being given by* (4.6). *The isomorphism class of $(R(G), \Delta)$ corresponds to the equivalence class of* 1. *The bijection is implemented via* (4.3).

Unfortunately, coalgebras are not very familiar objects. In order to obtain more precise results we find it necessary to deal with better known objects, and so we examine the dual of a coalgebra.

For any R-module M we set $M^* = \mathrm{Hom}_R(M, R)$. If M is also an $R(G)$-module, M^* carries the usual $R(G)$-module structure defined by

$$(4.7) \qquad (\sigma\varphi)(m) = \varphi(\sigma^{-1}m) \text{ for } \varphi \text{ in } M^*, \ m \text{ in } M, \text{ and } \sigma \text{ in } G.$$

It is well known that if M is isomorphic to $R(G)$, then M^* is also [6, p. 7]. Let $(R(G), D)$ be a coassociative galois R-coalgebra. Set $A(D) = R(G)^*$. Then there is a $R(G)$-isomorphism $\rho : A(D) \to R(G)$ and the transpose of D, the mapping $D^* : A(D) \otimes A(D) \to A(D)$ yields a multiplication on $A(D)$. Transposing the commutative diagram (4.1) shows that this multiplication is associative and since D is an $R(G)$-homomorphism, G acts as a group of R-algebra automorphisms on $A(D)$. Explicitly the product on $A(D)$ is given by

$$(4.8) \qquad (h \cdot g)(x) = (h \otimes g)(D(x)) = (h \otimes g)(\Delta(x)u)$$

for h, g in $A(D)$ and x in $R(G)$. *In contradistinction to the commutative rings occurring in this paper, $A(D)$ need not have an identity.* Finally, if $\emptyset : (R(G), D) \to (R(G), \tilde{D})$ is an isomorphism of galois R-coalgebras, transposing the commutative diagram (4.2) shows that $\emptyset^* : A(\tilde{D}) \to A(D)$ is both an $R(G)$-module and R-algebra isomorphism.

The foregoing leads to the following

DEFINITION 4.2. Let R be a commutative ring and G a finite group. An associative R-algebra A (not necessarily with identity) is called *a galois R-algebra with galois group G* if

(i) G acts as a group of R-algebra automorphisms of A and

(ii) there is an $R(G)$-isomorphism $\rho : R(G) \to A$ or equivalently

(ii′) A has a normal basis.

Two galois R-algebras A and $\tilde{A}$ with galois group G are said to be *isomorphic* if there is an R-algebra isomorphism $A \to \tilde{A}$ which is also an $R(G)$-isomorphism.

THEOREM 4.3. *The set of isomorphism classes of galois R-algebras with galois group G is bijective with the set of isomorphism classes of coassociative galois R-coalgebras, $(R(G), D)$. The bijection from coalgebras to algebras is given by sending the isomorphism class of $(R(G), D)$ to the isomorphism class of $A(D)$. Under this map the isomorphism class of $(R(G), \Delta)$ corresponds to the isomorphism class of the algebra $\sum_{\sigma \text{ in } G} \oplus Re_\sigma$ with $e_\sigma e_\tau = \delta_{\sigma,\tau} e_\sigma$ and $\sigma(e_\tau) = e_{\sigma\tau}$. This algebra is called the trivial galois R-algebra with galois group G.*

Proof. Let A be a galois R-algebra with galois group G. By (ii) there is an $R(G)$-isomorphism $\rho^* : A^* \to R(G)^* \cong R(G)$, hence an $R(G)$-isomorphism $\eta : A^* \to R(G)$. Denoting the multiplication of A by μ, there is a unique mapping $D(A, \eta) : R(G) \to R(G^2)$ which makes the following diagram commutative,

$$\begin{array}{ccc} A^* & \xrightarrow{\mu^*} & A^* \otimes A^* \\ \downarrow \eta & & \downarrow \eta \otimes \eta \\ R(G) & \xrightarrow{D(A,\eta)} & R(G) \otimes R(G) \end{array}$$

The associativity of μ implies the coassociativity of $(R(G), D(A, \eta))$, and, since for all σ in G we have $\sigma(\mu(x \otimes y)) = \mu(\sigma(x) \otimes \sigma(y))$, the mapping μ^* and hence also $D(A, \eta)$ is an $R(G)$-homomorphism. Thus $(R(G), D(A, \eta))$ is a coassociative galois R-coalgebra.

Now let A_i, $i = 1, 2$, be galois R-algebras with galois group G and $\eta_i : A_i^* \to R(G)$, $i = 1, 2$, be $R(G)$-module isomorphisms. Suppose that there is an R-algebra and $R(G)$-module isomorphism $\lambda : A_1 \to A_2$. We shall show $(R(G), D(A_1, \eta_1)) \cong (R(G), D(A_2, \eta_2))$. Let $\Phi : R(G) \to R(G)^2$ be the composite

$$R(G) \xrightarrow{\eta_2^{-1}} A_2^* \xrightarrow{\lambda^*} A_1^* \xrightarrow{\eta_1} R(G)$$

If μ_i, $i = 1, 2$, denote the multiplications of A_i, then the properties of η_1, η_2, λ ensure the commutativity of

$$\begin{array}{ccccccc} R(G) & \xrightarrow{\eta_2^{-1}} & A_2^* & \xrightarrow{\lambda^*} & A_1^* & \xrightarrow{\eta_1} & R(G) \\ \downarrow{\scriptstyle D(A_2,\,\eta_2)} & & \downarrow{\scriptstyle \mu_2^*} & & \downarrow{\scriptstyle \mu_1^*} & & \downarrow{\scriptstyle D(A_1,\,\eta_1)} \\ R(G) & \xrightarrow{\eta_2^{-1}\otimes\eta_2^{-1}} & A_2^*\otimes A_2^* & \xrightarrow{\lambda^*\otimes\lambda^*} & A_1^*\otimes A_1^* & \xrightarrow{\eta_1\otimes\eta_1} & R(G^2) \end{array}$$

where, as usual, we have identified $(A_i\otimes A_i)^*$ with $A_i^*\otimes A_i^*$. But this is equivalent to the commutativity of

$$\begin{array}{ccc} R(G) & \xrightarrow{D(A_1,\,\eta_1)} & R(G^2) \\ \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Phi\otimes\Phi} \\ R(G) & \xrightarrow{D(A_2,\,\eta_2)} & R(G^2) \end{array}$$

Since Φ is obviously an $R(G)$-automorpism, this proves $(R(G),\ D(A_1,\ \eta_1))\cong (R(G),\ D(A_2,\ \eta_2))$.

Hence, $A\to(R(G),\ D(A,\ \eta))$ induces a well defined mapping F, from isomorphism classes of galois algebras to isomorphism classes of galois coalgebras. As was noted above Definition 4.2, $(R(G),\ D)\to A(D)$ induces a well defined mapping F', from isomorphism classes of galois coalgebras to isomorphism classes of galois algebras. To prove that $F'F$ is the identity, we note that transposing the diagram used to define $D(A,\ \eta)$ yields a commutative diagram

$$\begin{array}{ccc} A^{**} & \xleftarrow{\mu^{**}} & A^{**}\otimes A^{**} \\ \uparrow{\scriptstyle \eta^*} & & \uparrow{\scriptstyle \eta^*\otimes\eta^*} \\ R(G)^* & \xleftarrow{D(A,\eta)^*} & R(G)^*\otimes R(G)^*. \end{array}$$

Since A is a finitely generated free R-module there is a natural, whence also $R(G)$-, isomorphism $A^{**}\cong A$ which takes μ^{**} to μ. Identifying A^{**} with A then shows that $\eta^*:\ R(G)^*\to A$ is an algebra isomorphism of $A(D(A,\ \eta))$ with A which is also an $R(G)$-isomorphism. To show FF' is the identity, let $\eta:\ R(G)^{**}\to R(G)$ be the natural isomorphism. Then $D(A(D),\ \eta)$ is defined by the commutative diagram

$$\begin{array}{ccc} R(G)^{**} & \xrightarrow{D^{**}} & R(G)^{**}\otimes R(G)^{**} \\ \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \eta\otimes\eta} \\ R(G) & \xrightarrow{D(A(D),\,\eta)} & R(G)\otimes R(G) \end{array}$$

Again, identifying $R(G)^{**}$ with $R(G)$ and D^{**} with D shows $D(A(D),\ \eta)=D$, and thus $F'=F^{-1}$.

Finally, to compute $F^{-1}((R(G), \Delta))$, let $\{h_\sigma\}$ be the R-basis of $R(G)^*$ dual to the R-basis $\{\sigma \mid \sigma \text{ in } G\}$ of $R(G)$, i.e. $h_\sigma(\tau) = \delta_{\sigma,\tau}$. By (4.8), $(h_\sigma \cdot h_\tau)(\rho) = h_\sigma(\rho)h_\tau(\rho)$, so that the h_σ are orthogonal idempotents. By (4.7), $(\sigma h_\tau)(\rho) = h_\tau(\sigma^{-1}\rho)$ so that $\sigma(h_\tau) = h_{\sigma\tau}$. This completes the proof of Theorem 4.3.

Proposition 4.1 and Theorem 4.3 immediately yield

PROPOSITION 4.1′. *There is a bijection of pointed sets between the set of isomorphism classes of galois R-algebras with galois group G and equivalence classes of elements of $R(G^2)$ satisfying* (4.4), *the equivalence relation being given by* (4.6). *The isomorphism class of the trivial galois R-algebra with galois group G corresponds to the class of the identity element of $R(G^2)$.*

Remark. Proposition 4.1′ is equivalent to Satz 1 and Satz 2 of Chapter 1 of [16]. The element $u = D(1)$ or $D(A, \eta)(1)$, is called a "Resolventenfaktor" there. The use of coalgebras seems to simplify notations and proofs considerably.

Now if $G = J$ is an abelian group and u is a unit in $R(G^2)$, the relation (4.4) is simply the condition that u be a 2-cocycle in $\mathfrak{H}(R, J)$, while (4.6) then asserts that u and $\tilde{u}$ are cohomologous. Hence

COROLLARY 4.4. *If J is a finite abelian group, there is a bijection between $H^2(R, J)$ and the isomorphism classes of galois R-coalgebras $(R(J), D)$ [galois R-algebras with galois group J] for which $D(1)$ is a unit [$D(A, \eta)(1)$ is a unit]. The element 0 of $H^2(R, J)$ corresponds to the class of $(R(J), \Delta)$ [the trivial galois R-algebras with galois group J].*

In order to characterize those algebras and coalgebras for which u is a unit we introduce

DEFINITION 4.5. Let A be a ring with identity, G a finite group of ring automorphisms of A and $R = A^G$. Let E be the ring of functions from G to A under pointwise operations. Then A is called *a galois extension of R with galois group G* if

(i) R is in the centre of A

(ii) the mapping $\Lambda : A \otimes A \to E$ defined by $\Lambda(x \otimes y)(\sigma) = x\sigma(y)$ for x, y in A, σ in G

is an R-module isomorphism.

Remark. This is a slight generalization of a concept introduced in [5]. It

is not difficult to see that the conditions (b) and (c) of [5, Thm. 1.3] are still equivalent to (ii) above, assuming (i).

THEOREM 4.6. *A galois R-algebra with galois group G is a galois extension of R with galois group G if and only if the class of elements in $R(G^2)$ corresponding to its isomorphism class consists of units.*

Proof. It is clear from (4.6) that if the equivalence class of an element of $R(G^2)$ contains one unit then the entire class consists of units. Hence we may assume that our galois algebra is of the form $A = A(D(u))$ with u in $R(G^2)$ satisfying (4.4). Thus $A = R(G)^*$ with multiplication defined by (4.8). Let h be the element of A defined by $h(1) = 1$, $h(\sigma) = 0$ for $\sigma \neq 1$ in G. Then $\sigma(h) = h_\sigma$, where h_σ is defined by $h_\sigma(\tau) = \delta_{\sigma,\tau}$. Clearly, the elements h_σ ($h_1 = h$) form an R-basis of A. Now, let $u = \sum r_{\sigma,\tau}(\sigma \otimes \tau)$ with $r_{\sigma,\tau}$ in R, and σ, τ in G. Then it is easily checked that

$$r_{\sigma,\tau} = (h_\sigma \cdot h_\tau)(1)$$

and so

$$h_\sigma \cdot h_\tau = r_{\sigma,\tau} h + \sum_{\rho \neq 1} \tilde{r}_\rho h_\rho \qquad \tilde{r}_\rho \text{ in } R. \tag{4.9}$$

As usual, we identify $(A \otimes A)^*$ with $R(G) \otimes R(G)$ by setting

$$(\sigma \otimes \tau)(h_\lambda \otimes h_\rho) = h_\lambda(\sigma) h_\rho(\tau).$$

Next, we define an R-module homomorphism $\Gamma : R(G^2) \to E^*$, where E is the ring of functions from G to A, by

$$\Gamma(\sigma \otimes \tau)(\varphi) = \varphi(\sigma)(\tau) \text{ for } \sigma, \tau \text{ in } G \text{ and } \varphi \text{ in } E.$$

Consider the composite map $R(G^2) \xrightarrow{\Gamma} E^* \xrightarrow{\Lambda^*} (A \otimes A)^* = R(G^2)$. We shall compute $\Lambda^*\Gamma$ explicitly in a number of steps.

(i) $(\Lambda^*\Gamma)(1 \otimes 1) = u$

Proof. For any σ, τ, λ, ρ in G we have

$$[(\Lambda^*\Gamma)(\sigma \otimes \tau)](h_\lambda \otimes h_\rho) = \Gamma(\sigma \otimes \tau)[\Lambda(h_\lambda \otimes h_\rho)] = (\Lambda(h_\lambda \otimes h_\rho)(\sigma))(\tau) = (h_\lambda \cdot h_{\sigma\rho})(\tau)$$

In particular, $(\Lambda^*\Gamma)(1 \otimes 1)(h_\lambda \otimes h_\rho) = r_{\lambda,\rho}$ by (4.9). In view of the identification of $(A \otimes A)^*$ with $R(G^2)$ this means that $(\Lambda^*\Gamma)(1 \otimes 1) = \sum r_{\lambda,\rho}(\lambda \otimes \rho) = u$,

(ii) Define a left $R(G^2)$-module structure on E by $[(\lambda\otimes\rho)\varphi](\sigma) = \lambda[\varphi(\lambda^{-1}\sigma\rho)]$ for λ, ρ, σ in G, φ in E. That this is indeed a well defined left $R(G^2)$-module structure follows from the fact that this is just the tensor product of the two standard left module structures

$$(\lambda\varphi)(\sigma) = \lambda[\varphi(\lambda^{-1}\sigma)] \text{ and } (\rho\varphi)(\sigma) = \varphi(\sigma\rho)$$

which clearly commute. Then E^* becomes a right $R(G^2)$-module in the usual way, viz. for ψ in E^*, φ in E and z in $R(G^2)$

$$(\psi z)(\varphi) = \psi(z\varphi).$$

Now, define a right $R(G^2)$-module structure on $R(G^2)$ by

$$(\sigma\otimes\tau)*(\lambda\otimes\rho) = (\lambda^{-1}\sigma\rho)\otimes(\lambda^{-1}\tau) \text{ for } \sigma,\ \tau,\ \lambda,\ \rho \text{ in } G.$$

Again, this is a tensor product of two standard $R(G)$-module structures. Keeping the $R(G)$-module structure of A, (4.7), in mind, it is then easily verified that $\Gamma : R(G^2)\to E^*$ is a right $R(G^2)$-module homomorphism.

(iii) $A\otimes A$ has a left $R(G^2)$-module structure given by

$$(\lambda\otimes\rho)(h_\sigma\otimes h_\tau) = \lambda(h_\tau)\otimes\rho(h_\tau) = h_{\lambda\sigma}\otimes h_{\rho\tau} \tag{4.10}$$

With this module structure $\Lambda : A\otimes A\to E$ is an $R(G^2)$-module homomorphism using the $R(G^2)$-module structure of E defined in (ii), as can readily be checked. Now, when $(A\otimes A)^*$ is identified with $R(G)\otimes R(G)$, the right $R(G^2)$-module structure of $(A\otimes A)^*$ arising from (4.10) carries over to the right $R(G^2)$-module structure of $R(G^2)$ given by

$$(\sigma\otimes\tau)\circ(\lambda\otimes\rho) = \lambda^{-1}\sigma\otimes\rho^{-1}\tau.$$

Hence, $\Lambda^* : E^*\to R(G^2)$ is a right $R(G^2)$-module homomorphism, using the $\circ R(G^2)$-module structure on $R(G^2)$.

(iv) $(\Lambda^*\Gamma)(\sigma\otimes\tau) = (\tau\otimes\sigma\tau^{-1})u$ and so $(\Lambda^*\Gamma)(R(G^2)) = R(G^2)u$.

Proof. Combining (iii) and (ii) shows that $(\Lambda^*\Gamma)(x*(\lambda\otimes\rho)) = [(\Lambda^*\Gamma)(x)]\circ\lambda\otimes\rho$, for x in $R(G^2)$ and λ, ρ in G. Now $\sigma\otimes\tau = (1\otimes 1)*(\tau^{-1}\otimes\tau^{-1}\sigma)$, hence $(\Lambda^*\Gamma)(\sigma\otimes\tau) = [(\Lambda^*\Gamma)(1\otimes 1)]\circ(\tau^{-1}\otimes\tau^{-1}\sigma) = (\tau\otimes\sigma^{-1}\tau)u$ by (iii) and (i). Choosing $\tau = \lambda$ and $\sigma = \rho\lambda$, leads to $(\Lambda^*\Gamma)(\rho\lambda\otimes\lambda) = (\lambda\otimes\rho)u$, proving $(\Lambda^*\Gamma)(R(G^2)) = R(G^2)u$.

(v) Γ is an isomorphism of $R(G^2)$-modules.

Proof. Since E and $R(G^2)$ are finitely generated free R-modules we may

identify E^{**} with E and $R(G^2)^*$ with $A\otimes A$. It will therefore be sufficient to show $\Gamma^* : E\to A\otimes A$ is an isomorphism. To this end, define $\varphi_{\sigma,\tau}$ in E by $\varphi_{\sigma,\tau}(\lambda)=\delta_{\sigma,\tau}h_\tau$, σ, τ, λ in G. Since $\{h_\tau\}$ is an R-basis of A, it is clear that $\{\varphi_{\sigma,\tau}\}$ is an R-basis of E. Now $(\Gamma^*(\varphi_{\sigma,\tau}))(\lambda\otimes\rho)=\varphi_{\sigma,\tau}(\Gamma(\lambda\otimes\rho))=(\varphi_{\sigma,\tau}(\lambda))(\rho)$ $=\delta_{\sigma,\tau}\delta_{\tau,\rho}=(h_\sigma\otimes h_\tau)(\lambda\otimes\rho)$. Thus $\Gamma^*(\varphi_{\sigma,\tau})=h_\sigma\otimes h_\tau$ and so Γ^* carries an R-basis of E to one of $A\otimes A$ and is, consequently, an isomorphism.

(vi) Λ is an isomorphism if and only if u is a unit.

Proof. If Λ is an isomorphism then, in view of (v) so is $\Lambda^*\Gamma$, and thus by (iv), $R(G^2)u=R(G^3)$. Hence there is an element u' in $R(G^2)$ with $u'u=1$. Now, if for an element $z=\sum r_{\lambda,\rho}(\lambda\otimes\rho)$ in $R(G^2)$, $zu=0$, then by (iv) $(\Lambda^*\Gamma)(\sum r_{\lambda,\rho}(\rho\lambda\otimes\lambda))=0$, so that $\sum r_{\lambda,\rho}(\rho\lambda\otimes\lambda)=0$ or $r_{\lambda,\rho}=0$, i.e. $z=0$. But $(uu'-1)u=0$ and so $uu'=1$ also, which proves that u is a unit.

By (iv) $\Lambda^*\Gamma$ is the composite of the left multiplication by u and the R-module homomorphism defined by linearity and $\sigma\otimes\tau\to\tau\otimes\sigma\tau^{-1}$. But the latter is an isomorphism whose inverse is defined by $\sigma\otimes\tau\to\tau\sigma\otimes\sigma$ and linearity. Thus, if u is a unit, $\Lambda^*\Gamma$ is an isomorphism, and since by (v), Γ is an isomorphism, Λ^* and hence also Λ must be one too.

(vii) If u is a unit, then $A=A(D(u))$ has an identity.

Proof. Let $\varepsilon : R(G)\to R$ be the algebra homomorphism defined by linearity and $\varepsilon(\sigma)=1$ for σ in G. A routine computation then yields the following formulae, valid for any element u in $R(G^2)$.

$$(\varepsilon\otimes\varepsilon\otimes 1)(\Delta_1(u))=(\varepsilon\otimes 1)(u) \qquad (1\otimes\varepsilon\otimes\varepsilon)(\Delta_1(u))=(1\otimes\varepsilon)(u)$$
$$(\varepsilon\otimes\varepsilon\otimes 1)(\Delta_3(u))=(\varepsilon\otimes\varepsilon)(u) \qquad (1\otimes\varepsilon\otimes\varepsilon)(\Delta_3(u))=(1\otimes\varepsilon)(u)$$
$$(\varepsilon\otimes\varepsilon\otimes 1)(\Delta_2(u))=(\varepsilon\otimes 1)(u) \qquad (1\otimes\varepsilon\otimes\varepsilon)(\Delta_2(u))=(1\otimes\varepsilon)(u)$$
$$(\varepsilon\otimes\varepsilon\otimes 1)(\Delta_0(u))=(\varepsilon\otimes 1)(u) \qquad (1\otimes\varepsilon\otimes\varepsilon)(\Delta_0(u))=(\varepsilon\otimes\varepsilon)(u).$$

Applying the two R-algebra homomorphisms $\varepsilon\otimes\varepsilon\otimes 1$ and $1\otimes\varepsilon\otimes\varepsilon : R(G^3)\to R(G)$ to (4.4) and bearing in mind that both $(\varepsilon\otimes 1)(u)$ and $(1\otimes\varepsilon)(u)$ are units in $R(G)$ then shows

$$(\varepsilon\otimes\varepsilon)(u)=(\varepsilon\otimes 1)(u)=(1\otimes\varepsilon)(u).$$

For $u=\sum r_{\sigma,\tau}(\sigma\otimes\tau)$ this implies, $\sum_\tau r_{\sigma,\tau}=0$, $\sigma\neq 1$, $\sum_\sigma r_{\sigma,\tau}=0$, $\tau\neq 1$ and $\sum_\tau r_{1,\tau}$ $=\sum_\sigma r_{\sigma,1}=(\varepsilon\otimes\varepsilon)(u)$ a unit, r, in R. Now ε is an element of $A=R(G)^*$ and

we compute $\varepsilon \cdot h_1$ and $h_1 \cdot \varepsilon$. By (4.8), $(\varepsilon \cdot h_1)(\lambda) = (\varepsilon \otimes h_1)((\lambda \otimes \lambda)u) = (\varepsilon \otimes h_1)(\sum r_{\sigma,\tau} \lambda\sigma \otimes \lambda\tau) = \sum_\sigma r_{\sigma,\lambda^{-1}} = r\delta_{\lambda,1}$. Similarly, $(h_1 \cdot \varepsilon)(\lambda) = r\delta_{\lambda,1}$. Hence $(r^{-1}\varepsilon)h_1 = h_1(r^{-1}\varepsilon) = h_1$. Now set $e = r^{-1}\varepsilon$. Then for all σ in G, $\sigma(e) = e$ and so $eh_\sigma = h_\sigma e = \sigma(h_1) = h_\sigma$. Thus e is the identity of A, cf. [16. § 7].

Steps (vi) and (vii) complete the proof of Theorem 4.6.

An associative R-algebra with identity, A, is a *separable* R-algebra if the two-sided A-module A is projective [4, Chap. IX, § 7]. If R is a field this is equivalent to the usual definition, i.e. $[A : R] < \infty$ and $A \otimes R'$ is semisimple for every extension field R' of R [12, Thm. 1 and 4, Thm. 7.10, p. 179].

LEMMA 4.7. *A galois extension of R with galois group G is a separable R-algebra.*

Proof. By [4, Prop. 7.7, p. 179] an algebra A is separable if and only if there are elements x_i, y_i, $i = 1, \ldots, n$ in A such that $\sum x_i y_i = 1$ and $\sum x x_i \otimes y_i = \sum x_i \otimes y_i x$ in $A \otimes A$ for all x in A. Now let φ be the element of E defined by $\varphi(\sigma) = \delta_{\sigma,1}$ for σ in G and let $(\Lambda^{-1})(\varphi) = \sum x_i \otimes y_i$. Then for all σ in G, $\sum x_i \sigma(y_i) = \delta_{\sigma,1}$. Hence, $\sum x_i y_i = 1$. Moreover, $\Lambda(\sum x x_i \otimes y_i)(\sigma) = \sum x x_i \sigma(y_i) = x\delta_{1,\sigma}$ and $\Lambda(\sum x_i \otimes y_i x)(\sigma) = \sum x_i \sigma(y_i)\sigma(x) = \sigma(x)\delta_{1,\sigma}$. Thus $\Lambda(\sum x x_i \otimes y_i) = \Lambda(\sum x_i \otimes y_i x)$ and since Λ is an isomorphism, $\sum x x_i \otimes y_i = \sum x_i \otimes y_i x$, which proves the lemma.

Corollary 4.4, Theorem 4.6 and Lemma 4.7 yield

COROLLARY 4.8. *If u is a unit of $R(G^2)$, $A = A(D(u))$ is a separable R-algebra. If J is a finite abelian group, $H^2(R, J)$ is bijective with the set of isomorphism classes of galois R-algebras with galois group J which are also galois extensions with galois group J. The bijection carries 0 in $H^2(R, J)$ to the trivial galois algebra.*

Remarks. 1. If u is not a unit there are galois algebras which fail to be galois extension. The algebra of dual numbers over a field is an example of this.

2. In case R is a field, the first result of Corollary 4.8 is contained in [16, Satz 3, p. 33].

5. Galois extensions with cyclic galois groups. We begin with two lemmas which are slight adaptations of [5, Lemma 1.7 and Thm. 4.2] to the non-

commutative case. Their proofs are given here for the reader's convenience.

LEMMA 5.1. *Let A be a galois extension of R with galois group G and R' a commutative R-algebra. Let G act on $A\otimes R'$ via the formula $\sigma(a\otimes r')=\sigma(a)\otimes r'$ for a in A, r' in R', σ in G. Then $A\otimes R'$ is a galois extension of R' with galois group G.*

Proof. As in the proof of Lemma 4.7, there are elements $x_1, \ldots, x_n$; $y_1, \ldots, y_n$ in A such that $\sum x_i\sigma(y_i)=\delta_{1,\sigma}$. As usual let $tr : A\to R$ denote the trace, i.e. $tr(x)=\sum_{\sigma \text{ in } G}\sigma(x)$. Then $\sum x_i tr(y_i)=1$, so $tr(A)A=A$. It is clear that $tr(A)$ is an ideal of R. Moreover, for any x in A, $\sum x_i\sigma(y_i)\sigma(x)=\sigma(x)\delta_{1,\sigma}$, so by summing over all σ in G we have $\sum x_i tr(y_i x)=x$, which proves that A is a finitely generated R-module. By [17, Lemma 2, p. 215] there is an element r of $tr(A)$ such that $(1-r)A=0$. Thus $r=1$ and there is an element a in A with $tr(a)=1$. It is then clear that R is an R-module direct summand of A, a complement being the kernel of the map $A\to R$ defined by $x\to tr(ax)$.

Since R is a direct summand of A, it follows that $1\otimes R'\cong R'$ as R'-algebras and we identify the two objects by means of this isomorphism. Now let z be in $(A\otimes R')^G$, then $z=z\{(tr\otimes 1)(a\otimes 1)\}=(tr\otimes 1)(z(a\otimes 1))$ clearly lies in $R\otimes R'=R'$, which proves $(A\otimes R')^G=R'$.

Let φ_σ be the elements of E defined by $\varphi_\sigma(\tau)=\delta_{\sigma,\tau}$. Then clearly the φ_σ are orthogonal central idempotents in E and $E=\sum\oplus A\varphi_\sigma$. Hence if E' denotes the ring of functions from G to $A\otimes R'$, it is clear that $E'\cong E\otimes R'$ and that $\Lambda\otimes 1 : A\otimes A\otimes R'\cong (A\otimes R')\otimes_{R'}(A\otimes R')\to E\otimes R'\cong E'$ is still an isomorphism, which proves the lemma.

LEMMA 5.2. *Let R be a field and A a galois extension of R with galois group G, then A is a galois R-algebra with galois group G.*

Proof. From the definitions it is clear that we must prove $A\cong R(G)$ as $R(G)$-modules. Define an $R(G)$-module structure on $A\otimes A$ by $(r\sigma)(x\otimes y)=x\otimes r\sigma(y)$ for r in R, x, y in A, σ in G, and an $R(G)$-module structure on E by $[(r\sigma)(\varphi)](\tau)=r\varphi(\tau\sigma)$ for r in R, σ, τ in G and φ in E. It is readily verified that Λ is then an $R(G)$-isomorphism. Moreover, the mapping $E\to A\otimes R(G)$ defined by $\varphi\to\sum_{\sigma \text{ in } G}\varphi(\sigma)\otimes\sigma^{-1}$ is easily seen to be an isomorphism of left $R(G)$-modules where $A\otimes R(G)$ is viewed as $R(G)$-module via the action of $R(G)$ on

the second factor. Hence $A \otimes A \cong A \otimes R(G)$ as $R(G)$-modules. If the order of G is n, this means that the direct sum of n copies of the $R(G)$-module A is a free $R(G)$-module on n generators. By the Krull-Schmidt theorem, which is applicable because R is a field, $A \cong R(G)$.

The main result of this section is

THEOREM 5.3. *Let R be a commutative ring, J a finite cyclic group and A a galois extension of R with galois group J. Then A is commutative.*

The proof will be conducted in a series of lemmas.

LEMMA 5.4. *Let A be a separable R-algebra which is a finitely generated R-module. Then A is commutative if and only if $A \otimes R/\mathfrak{m}$ is commutative for all maximal ideals $\mathfrak{m}$ of R.*

Proof. Let C be the centre of A. Then the exact sequence $0 \to C \to A \to A/C \to 0$ splits as an exact sequence as C-, and hence also as R-, modules [2, Prop. 1.2]. Thus the sequence $0 \to C \otimes R/\mathfrak{m} \to A \otimes R/\mathfrak{m} \to (A/C) \otimes R/\mathfrak{m} \to 0$ is still exact, i.e. $(A \otimes R/\mathfrak{m})/(C \otimes R/\mathfrak{m}) \cong (A/C) \otimes R/\mathfrak{m}$. By [2, Cor. 1.6], $C \otimes R/\mathfrak{m}$ is still the centre of $A \otimes R/\mathfrak{m}$ and thus, if $A \otimes R/\mathfrak{m}$ is commutative, we have $(A/C) \otimes R/\mathfrak{m} = 0$. If $R_{\mathfrak{m}}$ is the local ring of R at $\mathfrak{m}$, this is equivalent to $(A/C) \otimes R_{\mathfrak{m}} = \mathfrak{m}((A/C) \otimes R_{\mathfrak{m}})$. Since A/C is a finitely generated R-module, Nakayama's lemma shows that $(A/C) \otimes R_{\mathfrak{m}} = 0$. Hence if $A \otimes R/\mathfrak{m}$ is commutative for all $\mathfrak{m}$, $(A/C) \otimes R_{\mathfrak{m}} = 0$ for all $\mathfrak{m}$, so that $A/C = 0$ [4, Exc. 11, p. 142], i.e. $A = C$ and so is commutative. The converse is obvious.

COROLLARY 5.5. *It is sufficient to prove Theorem 5.3 assuming that R is a field and A a separable galois algebra with galois group J.*

Proof. Let A be a galois extension of R with galois group J. By Lemma 5.1, $A \otimes R/\mathfrak{m}$ is a galois extension of $R/\mathfrak{m}$ and so by Lemma 5.2, $A \otimes R/\mathfrak{m}$ is a galois algebra. By Lemma 4.7, A and $A \otimes R/\mathfrak{m}$ are both separable algebras, hence Lemma 5.4 completes the proof of the corollary.

LEMMA 5.6. *Let R be a field, J a finite abelian group and A a galois R-algebra with galois group J. Let e be a minimal central idempotent of A and let H be the isotropy subgroup of e, i.e. $H = \{\sigma \text{ in } J \mid \sigma(e) = e\}$. If A contains an identity, A is the algebra direct sum of galois R-algebras isomorphic to Ae which is a galois R-algebra with galois group H.*

Proof. Let $\sigma_1 = 1, \sigma_2, \ldots, \sigma_k$ be distinct coset representatives of J modulo H, i.e. $J = \cup \sigma_i H$. The elements $\sigma_i(e)$ are clearly distinct minimal central idempotents of A, and so are orthogonal. Hence $e' = \sum_1^k \sigma_i(e)$ is an idempotent of A. Now for σ in J, $\sigma\sigma_i = \sigma_{\pi(i)}\eta$ with π a permutation of $\{1, \ldots, k\}$ and η in H. Thus e' is in A^J. But, since $A \cong R(J)$ as $R(J)$-module, $A^J = R \cdot 1$ and since R is a field, $e' = 0$ or 1. The hypothesis $e' = 0$ yields $e = 0$ upon multiplication by e, a contradiction, so $e' = 1$. Therefore $\sigma_i(e)$, $i = 1, 2 \ldots, k$, is the set of *all* primitive central idempotents of A. It follows that $A \cong \sum \oplus A\sigma_i(e)$ as R-algebra and since $\sigma_i : Ae \to A\sigma_i(e)$ is an algebra isomorphism, A is the direct sum of k copies of Ae.

For η in H, we have $\eta\sigma_i(e) = \sigma_i(e)$ and thus $A\sigma_i(e)$ is an H-module. Moreover, $\sigma_i : Ae \to A\sigma_i(e)$ is an H-module isomorphism Hence the $R(H)$-module A is isomorphic to the direct sum of k copies of the $R(H)$-module Ae. But A is also $R(H)$-isomorphic to $R(J)$ which in turn is $R(H)$-isomorphic to the direct sum of k copies of $R(H)$. Thus the Krull-Schmidt theorem shows $Ae \cong R(H)$, proving the lemma.

Remarks. Lemma 5.6 is also proven, assuming A separable, in [10, Lemma 4]. In the terminology of [16], the lemma asserts that under its hypotheses, A is "kerngaloissch" cf. [16, Satz 3, p. 48].

COROLLARY 5.7. *It is sufficient to prove Theorem* 5.3 *assuming that R is a field and A a simple galois R-algebra with cyclic galois group.*

Proof. Let R be a field and A a separable galois R-algebra with cyclic galois group. By Corollary 5.5 it is sufficient to consider this situation. Lemma 5.6 shows that A is a direct sum of indecomposable galois algebras with galois groups subgroups of the galois group of A. Since A is separable, so are its indecomposable direct summands and they are therefore simple. The galois group of A is cyclic and so is, therefore, that of each indecomposable summand.

Proof of Theorem 5.3. Let A be a simple galois algebra over a field R whose galois group J is cyclic. Denote the centre of A by C. Then C is a field extension of R and J induces a group of automorphisms on C whose fixed field is R, since $A^J = R$. Let $K = \{\sigma \text{ in } J \mid \sigma(c) = 1 \text{ for all } c \text{ in } C\}$. Then C is a normal separable extension of R with galois group J/K and so $[C : R] =$

$[J:K]$. Now, as a subgroup of J, the group K is also cyclic generated by κ, say. By the Skolem-Noether theorem κ is an inner automorphism, $\kappa(x) = axa^{-1}$ for x, a in A. Clearly a is in A^K and so $A^K \supset C(a) \supset C$ which implies $[A^K : R] \geq [J : K]$. On the other hand, $A \cong R(J)$ as $R(J)$-module and it is readily seen that $(R(J))^K = \sum RN\sigma_i$ where $N = \sum_{\sigma \text{ in } K} \sigma$ and σ_i are coset representatives of J modulo K. Thus $[(R(J))^K : R] = [J : K]$. Hence $[A^K : R] = [J : K] = [C : R]$ and so $A^K = C(a) = C$. This forces $K = 1$, and so $[C : R] = [J : 1] = [A : R]$ or $A = C$, A is commutative.

Remarks. 1. The main ideas of the last part of the proof of Theorem 6.3 are already found in [8, Lemma, p. 234]. The theorem for galois algebras over rings has also been noted by F. de Meyer, [Osaka Math. J., 2 (1965), pp. 117-127].

2. There are examples of noncommutative galois extensions with non-cyclic abelian galois groups: The four group can be made to act on the 2×2 matrix algebra over a field in such a manner as to turn it into a galois algebra. Hoechsmann in [10] has determined the number of non-commutative separable galois algebras over a field for all finite abelian groups. Quotation of his result makes the last part of the proof of Theorem 5.3 unnecessary.

THEOREM 5.8. (Harrison). *Let R be a field, S a separable algebraic closure of R with galois group $\mathfrak{G}_R$. Then* $\mathrm{Hom}_c(\mathfrak{G}_R, Q/Z)$ [3] $= H^1(\mathfrak{G}_R, Q/Z) \cong H^2(R, Q/Z)$.

Proof. By Corollary 3.6 it is sufficient to show $H^2(S, J) = 0$ for any finite cyclic group J. By Corollary 4.8, $H^2(S, J)$ is bijective with the isomorphism classes of galois extensions of S with galois group J which are also galois S-algebras with galois group J. But these algebras are, by Theorem 5.3, commutative, and by Corollary 4.8, separable. Since S is separably closed, such an algebra may be written as $\sum_1^n \oplus Se_i$ where n is the order of J and $e_i e_j = \delta_{ij}$. Lemma 5.6 shows that e_1 is not left fixed by any element of J besides 1 and that, renumbering if necessary, $e_i = \sigma_i(e_1)$ where $J = \{1, \sigma_2, \ldots, \sigma_n\}$. Thus there is only the trivial galois algebra over S and so by Corollary 4.8, $H^2(S, J) = 0$.

---

[3] $\mathrm{Hom}_c(\mathfrak{G}, Q/Z)$ means the group of continuous homomorphisms from $\mathfrak{G}$ to Q/Z.

Bibliography

[1] E. Artin and J. Tate, Class field theory, Mimeographed Notes, Harvard, 1961.
[2] M. Auslander and O. Goldman, The Brauer group of a commutative ring, Trans. Amer. Math. Soc., vol. **97** (1960), pp. 367-409.
[3] N. Bourbaki, Algèbre commutative, chap. I-II, Hermann, Paris, 1962 (Act. scient. et ind. 1290).
[4] H. Cartan and S. Eilenberg, Homological Algebra, Princeton University Press Princeton, 1956.
[5] S. Chase, D. Harrison and A. Rosenberg, Galois theory and galois cohomology of commutative rings, Memoirs Amer. Math. Soc., **52** (1965), pp. 15-33.
[6] S. Eilenberg and T. Nakayama, On the dimension of modules and algebras II, Nagoya Math. J., vol. **9** (1955), pp. 1-16.
[7] R. Godement, Theórie des faisceaux, Hermann, Paris 1958 (Act. scient. et ind. 1252).
[8] D. K. Harrison, Abelian extensions of arbitrary fields, Trans. Amer. Math. Soc., vol. **106** (1963), pp. 230-235.
[9] D. K. Harrison, Abelian extensions of commutative rings, Memoirs Amer. Math. Soc., **52** (1965), pp. 1-14.
[10] K. Hoechsmann, Über nicht-kommutative abelsche Algebren, J.f.d. reine u. angw. Math., vol. **218** (1965), pp. 1-5.
[11] S. MacLane, Homology, New York, Academic Press, 1963.
[12] A. Rosenberg and D. Zelinsky, Cohomology of infinite algebras Trans. Amer. Math. Soc., vol. **82** (1956), pp. 85-98.
[13] J. P. Serre, Corps locaux, Paris, Hermann, 1962 (Act. scient. et ind. 1296).
[14] J. P. Serre, Cohomologie galoisienne, Lecture Notes in Math. 5, Heidelberg, Springer, 1964.
[15] van der Waerden, Moderne Algebra vol. 2, 2nd ed., Springer, Heidelberg, 1940.
[16] P. Wolf, Algebraische Theorie der galoisschen Algebren, Math. Forschungsberichte III, Deutscher Verlag der Wissenschaften, Berlin, 1956.
[17] O. Zariski and P. Samuel, Commutative algebra, vol. 1, van Nostrand, Princeton, 1958.

Cornell University
Ithaca, New York, U.S.A.