ABELIAN EXTENSIONS OF ARBITRARY FIELDS

BY
D. K. HARRISON[1,2]

For k a field, a normal extension of k is a field F containing k such that the group of automorphisms of F leaving k point-wise fixed (the Galois group) is finite and leaves no more than k fixed. It is an untouched classical problem to determine the normal extensions of k. Because of this, realistic work has centered on finding the Abelian extensions (the normal extensions where the Galois group is commutative). Where k is an algebraic number field this makes up the class field theory. Where k is any field of characteristic zero containing all the roots of unity, the Abelian extensions are given by the Kummer theory. In this paper we generalize the Kummer theory to an arbitrary field. In the characteristic p case or in the case where roots of unity do not exist, our answer, although it does not involve field extensions and thus is technically correct, is not as explicit as we could wish. For instance, it is not clear how to use this work in the derivation of the class field theory. Yet our answer is in terms of a cohomology theory in which a great deal of machinery exists simply because the theory is exactly analogous to (i.e., is the same in category theory as) the cohomology of groups, and for this reason we feel it presents a natural, systematic approach to questions involving Abelian extensions in the same way that the less general Kummer theory provides such an approach.

If we replace the word "set" by "commutative algebra with identity over k" and the phrase "map from A to B" by "algebra homomorphism from B to A," then the concept of a group transforms (using category theory for precision) to an object which is often called a group scheme (or equivalently, a Hopf algebra with inverse map). The ordinary cohomology of groups, together with all its formalistic properties, transforms to these schemes. The group rings $k(H)$ and $k(L)$ are such schemes, where H denotes the group of integers and L denotes the rationals modulo the integers. Our result is that the second cohomology group of $k(L)$ with coefficients in $k(H)$ (trivial operation) is naturally isomorphic to the character group of the full Galois group of k. This means that the Abelian extensions of k are in one-one correspondence with the finite subgroups of of $H^2(k(L), k(H))$. This cohomology group is explicitly a certain factor group of

---

Received by the editors August 14, 1961.
(1) This work was done under National Science Foundation Grant NSF-G-23454
(2) The author is indebted to the referee for many helpful suggestions and educating remarks.

a group of units in $k(L\times L)$. The use of a character basis in $k(L \times L)$ (when it exists) gives the ordinary Kummer theory. When written explicitly the complex for our cohomology groups is reminiscent of the Amitsur complex (see [1]); in fact, it is easily checked that the Amitsur groups of a field F are the $H^n(F, k(H)), n = 0, 1, \cdots$ (in any category any object F is a semigroup by

$$F \times F \xrightarrow{\text{proj}_2} F$$

and operates on any "group" G by $F \times G \to 0 \to G$). Our use of group rings is an extension of the methods of Galois algebras (see [2]) with the important difference that we use group rings over the constant group L rather than over the Galois group.

1. **The map and that it is one-one.** Let k be a field, and let $\mathscr{A}_k$ be the dual of the category of commutative algebras with identity over k. For $A, B \in \mathscr{A}_k$, $\text{Map}(A,B)$ is the set, $\text{Alg}(B,A)$, of algebra homomorphisms from B into A which take the identity of B into that of A. $A \times B$ is easily checked to be $A \otimes_k B$. $\text{Map}(A,k)$ has only one element for each A. Hence a group is an object A together with an element $\phi \in \text{Map}(A \times A, A)$ such that there exists a $\lambda \in \text{Map}(k,A)$ (the identity) and a $t \in \text{Map}(A,A)$ (the inverse) which satisfy certain easily guessed properties. If A with ϕ is a commutative group, then for any $B \in \mathscr{A}_k$, $\text{Map}(B,A)$ is an ordinary commutative group in a natural fashion. If B with θ is a group, then an operation of B on A is an element in $\text{Map}(B \times A, A)$ which satisfies certain properties. If B does operate on A we consider the ordinary complex

$$\text{Map}(k,A) \to \text{Map}(B,A) \to \text{Map}(B \times B, A) \to \text{Map}(B \times B \times B, A) \to \cdots,$$

where the maps are analogous to those in the ordinary cohomology of groups, and we let $H^n(B,A)$ denote the kernel modulo the image at $\text{Map}(B^n,A)$.

We have let H denote the integers and L denote the rationals modulo the integers. The group algebra $k(L) \in \mathscr{A}_k$. If $\phi(\sum \alpha_\sigma \sigma) = \sum \alpha_\sigma \sigma \otimes \sigma$ for $\alpha_\sigma \in k$, $\sigma \in L$, then it is easily checked that $\phi \in \text{Map}(k(L) \times k(L), k(L))$ and that $k(L)$ with ϕ is a commutative group. Similarly, $k(H)$ is a commutative group. If $\psi(a) = 1 \otimes a$ for $a \in k(H)$, then $\psi \in \text{Map}(k(L) \times k(H), k(H))$ and ψ gives an operation of $k(L)$ on $k(H)$. Let Ω be the field of separable elements in an algebraic closure of k, and let G be the group of automorphisms of Ω which leave k point-wise fixed. Then G has a natural topology, and by Galois theory and Pontryagin duality the finite subgroups of the character group $\text{Hom}_c(G, L)$ are in one-one correspondence with the Abelian extensions of k. Our aim is to prove that

$$\text{Hom}_c(G, L) \cong H^2(k(L), k(H))$$

by a natural isomorphism Δ.

For n any positive integer, it is easily checked that $\mathrm{Map}(k(L)^n, k(H)) = \mathrm{Alg}(k(H), k(L)^n)$ is isomorphic to $U(k(L)^n)$, the group of units of $k(L)^n$. This is because every algebra homomorphism from $k(H)$ is determined by the image of a generator of H. Here $k(L)^n = k(L) \otimes \cdots \otimes k(L)$ may be thought of as the single group ring $k(L^n)$, where L^n denotes the direct product $L \times \cdots \times L$ of groups. Thus our complex from which we take cohomology is

$$U(k) \xrightarrow{\delta_0} U(k(L)) \xrightarrow{\delta_1} U(k(L \times L)) \xrightarrow{\delta_2} U(k(L \times L \times L)) \cdots$$

and it is easily checked for n a positive integer and $a \in U(k(L^n))$ that

$$\delta_n(a) = e \otimes a \cdot (\prod \phi_s(a^{(-1)^s})) \cdot (a \otimes e)^{(-1)^{n+1}},$$

where s goes from 1 to n, e is the identity of L, and ϕ_s is defined by linearity and $\phi_s(\sigma_1 \otimes \cdots \otimes \sigma_n) = \sigma_1 \otimes \cdots \otimes \sigma_s \otimes \sigma_s \otimes \cdots \otimes \sigma_n$ (i.e., apply ϕ at the sth place) for $\sigma_1, \cdots, \sigma_n \in L$. This gives a concrete formulation of $H^2(k(L), k(H))$.

LEMMA. *Let G operate on $\Omega(L)$ by operation on the coefficients. Then for any $f \in \mathrm{Hom}_c(G, L)$ there exists a $u \in U(\Omega(L))$ (the units) with $x(u) = u \cdot f(x)$ for all $x \in G$.*

Proof. Let J be the image of f. Since G is compact and L is discrete, J is finite. Let F be the field of elements left fixed by the kernel of f. Then using f^{-1} we may think of J as the Galois group of F over k. Let β give a normal basis of F over k and let $u = \sum \sigma^{-1}(\beta)\sigma \in \Omega(L)$ where the sum is over the $\sigma \in J$. Then for $x \in G$ it is easily checked that $x(u) = u \cdot f(x)$. To show that u is a unit, we use the fact that $F \otimes_k F$ is isomorphic to a direct sum of copies of F, one for each $\tau \in J$, by the correspondence which takes $\alpha \otimes \gamma$ into $\sum \alpha\tau^{-1}(\gamma)$. Thus there is an element in $F \otimes F$ which corresponds to 1 in the eth copy of F and 0 in the other copies. Since β gives a normal basis, this element is of the form $\sum \alpha_\sigma \otimes \sigma(\beta)$. Now it is easily checked that $\sum \alpha_\sigma \sigma$ is an inverse for u.

With the lemma proved we are now in a position to define Δ. Let B^2 be the image of δ_1. Let δ_1^* be the obvious extension of δ_1 to a map from $U(\Omega(L))$ to $U(\Omega(L \times L))$. Now for $f \in \mathrm{Hom}_c(G, L)$ let $\Delta(f) = \delta_1^*(u) \cdot B^2$ where u is chosen as in the lemma. It is easily checked for $x \in G$ that

$$x(\delta_1^*(u)) = \delta_1^*(x(u)) = \delta_1^*(u \cdot f(x)) = \delta_1^*(u) \cdot \delta_1^*(f(x)) = \delta_1^*(u)$$

(here the operation of x on $\Omega(L \times L)$ is on the coefficients) and thus $\delta_1^*(u) \in U(k(L \times L))$. It is clear that $\delta_2(\delta_1^*(u)) = 0$. Finally, if v is another element of $U(\Omega(L))$ with $x(v) = v \cdot f(x)$, then $x(v^{-1}u) = v^{-1}u$ so $v^{-1}u \in U(k(L))$. Thus $\delta_1^*(u) = \delta_1^*(v) \cdot \delta_1(v^{-1}u)$ and we have shown that Δ is well defined.

We show now that Δ is one-one. Let f be in the kernel of Δ and u be chosen as in the lemma. Then there is a $v \in U(k(G))$ with $\delta_1^*(u) = \delta_1(v)$ and thus $\delta_1^*(uv^{-1}) = e \otimes e$. This implies that $\phi^*(uv^{-1}) = (e \otimes uv^{-1}) \cdot (uv^{-1} \otimes e)$ where ϕ^* is the

obvious extension of ϕ to a map from $\Omega(L)$ to $\Omega(L^2)$. By the lemma which follows this implies that $uv^{-1} = \sigma$ for some $\sigma \in L$, and thus for $x \in G$,

$$u \cdot f(x) = x(u) = x(\sigma v) = \sigma v = u.$$

Hence $f(x) = e$ for all $x \in G$.

LEMMA. *Suppose* $w \in \Omega(L)$ *with* $\phi^*(w) = w \otimes w$ *and* $w \neq 0$. *Then* $w \in L$.

Proof. Let $w = \sum \alpha_\sigma \sigma$ where the sum is over a subset S of L and where we may assume $\alpha_\sigma \neq 0$ for $\sigma \in S$. Then

$$\sum \sum \alpha_\sigma \alpha_\tau \sigma \otimes \tau = w \otimes w = \phi^*(w) = \sum \alpha_\sigma \sigma \otimes \sigma$$

and thus $\alpha_\sigma \alpha_\tau = 0$ for $\sigma \neq \tau$. Hence S has only one element.

2. **That the map is "onto."** Let u be any unit in $k(L \times L)$ with $\delta_2(u) = e \otimes e \otimes e$. Clearly $u \in k(J \times J)$ for some finite subgroup J of L. We now use an idea which in slightly different form and for different reasons is presented in [2]. Let A_u denote the dual vector space of $\Omega(J)$ made into an algebra over Ω by $(f \cdot g)(b) = f \otimes g(\phi(b) \cdot u)$ for all functionals f, g and all $b \in \Omega(J)$. Since $\delta_2(u) = e \otimes e \otimes e$, $e \otimes u \cdot \phi_2(u) = u \otimes e \cdot \phi_1(u)$ which when applied to the definition of multiplication gives associativity. We let J operate on A_u by defining $f^\sigma(a)$ as $f(\sigma a)$ for $\sigma \in J, f \in A_u, a \in \Omega(J)$. Let $h \in A_u$ be defined by linearity, $h(\sigma) = 0$ if $\sigma \neq e$, and $h(e) = 1$. Then it is easily checked that J operates on A_u as a group of automorphisms, and also that the h^σ, $\sigma \in J$, give a normal basis. We let $t = \sum h^\sigma$. Using the normal basis we can check that the αt, $\alpha \in \Omega$, are exactly the elements in A_u left fixed by the operation of J. Hence for $f \in A_u$, $\sum f^\sigma = \mathrm{tr}(f)t$ for some $\mathrm{tr}(f) \in \Omega$. Now if we combine the map from $\Omega(J \times J)$ to $\Omega(J)$ where $\sigma \otimes \tau \in J \times J$ goes to $\sigma^{-1}\tau$ with that from $\Omega(J)$ to $\mathrm{Hom}_\Omega(\Omega(J),\Omega(J))$ where $\rho \in J$ goes into left multiplication by ρ, then we get a composite algebra homomorphism Γ from $\Omega(J \times J)$ to $\mathrm{Hom}_\Omega(\Omega(J),\Omega(J))$. It is easily checked by direct computation (writing u in terms of $J \times J$ as a basis) that $\det(\Gamma(u)) = \det(\mathrm{tr}(h^\sigma \cdot h^\tau))$, and also that $\det(\Gamma(e \otimes e)) = 1$. Since Γ preserves multiplication and u has an inverse we get $\det(\mathrm{tr}(h^\sigma \cdot h^\tau)) \neq 0$. This implies that $\sum \alpha_\sigma \mathrm{tr}(h^\sigma \cdot h^\tau) = 0$ for all τ has no nontrivial solution in Ω. Hence $a \neq 0$ with $\mathrm{tr}(a \cdot b) = 0$ for all $b \in A_u$ is an impossibility. Now just suppose that A_u has a nontrivial radical N (we aim for a contradiction). Let $N^n \neq 0$ with $N^{n+1} = 0$. With $a \in N^n$, $a \neq 0$, choose $b \in A_u$ with $\mathrm{tr}(a \cdot b) \neq 0$. Since each $\sigma \in J$ is an automorphism, $t = \mathrm{tr}(a \cdot b)^{-1} \cdot \sum (a \cdot b)^\sigma$ gives that $t \in N^n$. Hence $t \cdot t = 0$. But t is easily checked to be just the usual augmentation from $\Omega(J)$ to Ω, and thus both t and $t \otimes t$ are algebra homomorphisms. Hence u having an inverse and $(t \otimes t)(e \otimes e) = 1$, give $(t \otimes t)(u) \neq 0$. But

$$(t \cdot t)(e) = (t \otimes t)(\phi(e) \cdot u) = (t \otimes t)(u) \neq 0$$

which contradicts $t \cdot t = 0$. We have proved that A_u is semisimple. Clearly, the

argument we have given holds if we replace Ω by any extension field, and thus A_u is separable.

LEMMA. *If ε is a minimal central idempotent of A_u, then the ε^σ, $\sigma \in J$, are exactly (no repeats) all the minimal central idempotents. In particular, A_u is isomorphic as an algebra to a direct sum of copies of Ω.*

Proof. Since A_u is semisimple, it has an identity 1. The elements left fixed by J are those in $\Omega \cdot t$, so this must be $\Omega \cdot 1$. Let S be the group of elements in J which leave the minimal central idempotent ε fixed. Let $\tau_1, \cdots, \tau_r$ be coset representatives for J/S. Then $\sum \varepsilon^{\tau_i}$ is a nonzero idempotent left fixed by J (it is easily checked that the ε^i are distinct and thus orthogonal), and thus it is 1. Hence the ε^{τ_i} are all the minimal central idempotents. To prove now that S is trivial let ρ be a generator of S (all finite subgroups of L are cyclic). Since A_u is separable, the center of $A_u \cdot \varepsilon$ is a separable field extension of $\Omega \cdot \varepsilon$, which by the nature of Ω implies that $A_u \cdot \varepsilon$ is central simple. Thus every automorphism of $A_u \cdot \varepsilon$ is an inner automorphism. In particular there is an $a = a \cdot \varepsilon \in A_u \cdot \varepsilon$ with $aba^{-1} = b^\rho$ for all $b \in A_u \cdot \varepsilon$. In particular $a^\rho = aaa^{-1} = a$. Thus a is left fixed by all elements in S, which implies that $\sum a^{\tau_i} = \sum a^{\tau_i}\varepsilon^{\tau_i}$ is left fixed by all elements in J. Hence $\sum a^{\tau_i} \in \Omega \cdot 1$ which implies that $a \in \Omega \cdot \varepsilon$, and thus that ρ is trivial on $A_u \cdot \varepsilon$. But now for any $b \in A_u$

$$b^\rho = (\sum b\varepsilon^{\tau_i})^\rho = \sum (b^{\tau_i^{-1}}\varepsilon)^{\tau_i \rho} = \sum (b^{\tau_i^{-1}}\varepsilon)^{\rho\tau_i} = \sum (b^{\tau_i^{-1}}\varepsilon)^{\tau_i} = \sum b\varepsilon^{\tau_i} = b,$$

and since A_u has a normal basis, $\rho = e$. This proves the lemma.

Now let $h = \sum \mu_\sigma \varepsilon^\sigma$ and $\varepsilon = \sum \nu_\sigma h^\sigma$. Then $h = \sum\sum \mu_\sigma \nu_\tau h^{\tau\sigma}$ which after equating coefficients implies that $c = \sum \mu_\sigma \sigma$ is a unit in $\Omega(J)$ with $c^{-1} = \sum \nu_\sigma \sigma$. Now by direct computation

$$h^\rho \cdot h^\tau = \sum_\omega \mu_{\omega\rho^{-1}}\mu_{\omega\tau^{-1}}\varepsilon^\omega = \sum_\sigma \sum_\omega \mu_{\omega\rho^{-1}}\mu_{\omega\tau^{-1}}\nu_{\sigma\omega^{-1}} h^\sigma,$$

and using this it is easily checked directly that

$$(h^\rho \cdot h^\tau)(e) = h^\rho \otimes h^\tau(\phi(c^{-1}) \cdot (c \otimes c))$$

for all $\rho, \tau \in J$. Hence $u = \phi(c^{-1}) \cdot (c \otimes c) = \delta_1^*(c)$. Since $u \in k(L \times L)$, $y(u) = u$ for all $y \in G$, and thus

$$\phi(y(c)^{-1}) \cdot (y(c) \otimes y(c)) = \phi(c^{-1}) \cdot (c \otimes c)$$

which implies that

$$\phi((y(c) \cdot c^{-1})^{-1}) \cdot ((y(c) \cdot c^{-1}) \otimes (y(c) \cdot c^{-1})) = e \otimes e.$$

But this with the lemma at the end of the last section implies that $y(c) \cdot c^{-1} \in L$. Denote $y(c) \cdot c^{-1}$ by $g(y)$. Then

$$c \cdot g(yz) = yz(c) = y(c \cdot g(z)) = y(c) \cdot g(z) = c \cdot g(y) \cdot g(z),$$

so $g(yz) = g(y) \cdot g(z)$ for $y, z \in G$. The coefficients of c generate a finite extension of k. Let G_0 be the automorphisms of G which leave this extension fixed. Then G_0 is closed and of finite index in G (implying all the cosets by G_0 are open) and since g is trivial on G_0, g is continuous. Hence $g \in \mathrm{Hom}_c(G, L)$ with $\Delta(g) = u \cdot B^2$.

BIBLIOGRAPHY

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

2. Paul Wolf, *Algebraische Theorie der Galoisschen Algebren*, Deutscher Verlag, Berlin 1956.

UNIVERSITY OF PENNSYLVANIA,
PHILADELPHIA, PENNSYLVANIA