BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 77, Number 3, May 1971

ON INSEPARABLE GALOIS THEORY

BY STEPHEN U. CHASE[1]

Communicated by Alex Rosenberg, November 23, 1970

Throughout this note k will be a field of characteristic $p \neq 0$, and K will be a modular extension of k [9]; i.e., a finite purely inseparable field extension of k which is a tensor product, over k, of primitive extensions. We shall outline a Galois theory of modular field extensions which, for the special case where the exponent of K/k is one, reduces to the well-known Galois correspondence of Jacobson [5, p. 186] between intermediate fields in the extension and restricted Lie subalgebras of $L(K/k) = \mathrm{Der}_k(K, K)$ which are also K-subspaces ($L(K/k)$ being the restricted Lie k-algebra and K-space of derivations of K over k).

There have recently appeared in the literature a number of other approaches to inseparable Galois theory, in varying stages of development; see, e.g. Sweedler [8], [9], Shatz [7], Davis [2], Gerstenhaber and Zaromp [3]. Our treatment utilizes the Hopf algebraic techniques of [8].

1. Basic concepts. A cocommutative k-coalgebra C [10, p. 63] will be called a *divided power coalgebra* if $[C : k]$ is a power of p and $C \approx C_1 \otimes_k \cdots \otimes_k C_r$, where each coalgebra C_i is spanned by a sequence of divided powers [10, p. 268]. A *divided power Hopf algebra* is a Hopf k-algebra which is a divided power coalgebra. The k-space $P(C)$ of primitive elements of C [10, p. 199] is a restricted Lie k-algebra [4] if C is a Hopf algebra, the Lie multiplication and p-power map in $P(C)$ being defined by the formulae $[x, y] = xy - yx$ and $x^{[p]} = x^p$ for x, y in C.

THEOREM 1. *There exists a divided power Hopf k-algebra $H(K/k)$ and a measuring $\omega_{K/k}: H(K/k) \otimes K \to K$ [10, p. 138] with the following universal property. Given any measuring $\omega: C \otimes K \to K$, with C a divided power k-coalgebra, there is a unique coalgebra map $f: C \to H(K/k)$ such that $\omega = \omega_{K/k}(f \otimes 1_K)$. $H(K/k)$ is uniquely determined by K/k up to Hopf algebra isomorphism, and $[H(K/k) : k] = [K : k]^{[K:k]}$. Moreover, there exists a restricted Lie algebra isomorphism $P(H(K/k)) \approx L(K/k)$,*

AMS 1970 *subject classifications*. Primary 12F15; Secondary 16A24.

Key words and phrases. Inseparable field extensions, approximate automorphisms, higher derivations, Hopf algebras.

[1] Supported in part by NSF GP-9395. The results of §1 were presented to the Society on May 14, 1969.

and if the exponent of K/k is one there is a Hopf algebra isomorphism $H(K/k) \approx U_r(L(K/k))$, the restricted universal enveloping algebra of $L(K/k)$.

If C is a subcoalgebra of $H(K/k)$, we shall denote by K^C the subfield of fixed elements of K under the measuring $\omega_{K/k}$ [10, p. 202].

THEOREM 2. *If C is a divided power subcoalgebra of $H(K/k)$, then K/K^C is modular* [8, p. 274]. *Conversely, if $k \subseteq F \subseteq K$ and K/F is modular, then there is a unique divided power Hopf subalgebra $H(K/F)$ of $H(K/k)$ such that $K^{H(K/F)} = F$ and, if C is as above, then $F \subseteq K^C$ if and only if $C \subseteq H(K/F)$. $[H(K/F):k] = [K:F]^{[K:k]}$.*

In order to characterize those Hopf subalgebras of $H(K/k)$ of the form $H(K/F)$, with F as above, we introduce a Hopf algebraic analogue of Jacobson's K-space structure on $L(K/k)$. Recall that, if X is a cocommutative coalgebra and Y is a commutative, cocommutative Hopf algebra, then $\mathrm{Coalg}_k(X, Y)$, the set of all coalgebra maps from X to Y, is an abelian group, with composition law $*$ defined as in [10, p. 69].

DEFINITION 3. A *formal K-space* is a commutative, cocommutative Hopf k-algebra Y, together with a map $K \times Y \to Y$ such that, for any X as above, the induced map $K \times \mathrm{Coalg}_k(X, Y) \to \mathrm{Coalg}_k(X, Y)$ renders the abelian group $\mathrm{Coalg}_k(X, Y)$ a vector space over K. (Y itself is *not* a K-space; however, $P(Y)$ is.)

Now, if C is a divided power k-coalgebra, we let $k = C(0) \subseteq C(1) \subseteq \cdots \subseteq C(n) \subseteq \cdots$ be the natural (or *coradical*) filtration of C [10, p. 185], and denote by $\mathrm{gr}(C)$ the associated (strictly) graded coalgebra [10, p. 228]; the k-space of homogeneous elements of $\mathrm{gr}(C)$ of degree n is $\mathrm{gr}(C)_n = C(n)/C(n-1)$. There exist natural k-space isomorphisms $\mathrm{gr}(C)_1 \approx P(\mathrm{gr}(C)) \approx P(C)$. Finally, $\mathrm{gr}(C)$ possesses a unique k-algebra structure which renders it a commutative, cocommutative Hopf k-algebra.

THEOREM 4. *There exists a unique map $K \times \mathrm{gr}(H(K/k)) \to \mathrm{gr}(H(K/k))$ rendering $\mathrm{gr}(H(K/k))$ a formal K-space such that the composite isomorphism $\mathrm{gr}(H(K/k))_1 \approx P(H(K/k)) \approx L(K/k)$ is a K-space map.*

If H is a divided power Hopf subalgebra of $H(K/k)$, then the inclusion map $H \hookrightarrow H(K/k)$ induces an injection $\mathrm{gr}(H) \hookrightarrow \mathrm{gr}(H(K/k))$, and so we may identify $\mathrm{gr}(H)$ with a graded Hopf subalgebra of $\mathrm{gr}(H(K/k))$.

THEOREM 5. *If $k \subseteq F \subseteq K$ and K/F is modular, then $\mathrm{gr}(H(K/F))$ is a* *formal K-subspace of* $\mathrm{gr}(H(K/k))$ (*i.e., is closed under the action of K introduced in Theorem* 4). *Conversely, if H is a divided power Hopf subalgebra of $H(K/k)$ such that* $\mathrm{gr}(H)$ *is a formal K-subspace of* $\mathrm{gr}(H(K/k))$, *and K is a tensor product over $F=K^H$ of primitive extensions of F of equal exponent, then $H=H(K/F)$.*

2. **Regular Hopf algebras.** One can deduce Jacobson's theorem [**5**, p. 186] as a special case of Theorem 5. But in order to obtain a more complete and useful theory, it is desirable to examine more closely the various "K-actions" on Lie algebras and Hopf algebras discussed earlier. We begin with the Lie algebra case.

DEFINITION 6. Let A be an (associative) k-algebra containing K, and set $A_K^{\dagger}=\{u \text{ in } A/ux-ux \text{ is in } K \text{ for all } x \text{ in } K\}$. $A_K^{\dagger}$ is a left K-subspace of A, and is a restricted Lie k-algebra under the operations $[u, v]=uv-vu$ and $u^{[p]}=u^p$ for u, v in $A_K^{\dagger}$.

THEOREM 7 [**6**], [**1**]. *The following are equivalent for any restricted Lie k-algebra and K-space L:*

(a) *There exists an associative k-algebra A containing K, and a restricted Lie k-algebra and K-space injection $j:L\hookrightarrow A_K^{\dagger}$.*

(b) *There exists a restricted Lie k-algebra map $\delta:L\to L(K/k)$ such that (if $u(x)=\delta(u)(x)$ for u in L and x in K) $[\alpha u, \beta v]=\alpha u(\beta)v-\beta v(\alpha)u+\alpha\beta[u, v]$ and $(\alpha u)^{[p]}=\alpha^p u^{[p]}+u(\alpha)^{p-1}u$ for u, v in L and α, β in K.*

The map δ above is uniquely determined by L. We shall say that L is *K-regular* if it satisfies the conditions of Theorem 7; such Lie algebras were first considered by Hochschild in [**4**].

We introduce analogous notions for Hopf algebras. Let A be a k-algebra containing K, and H be a divided power Hopf k-algebra. A k-algebra map $\varphi:H\to A$ will be called *admissible* if, for any u in H and x in K, $\sum_{(u)} f(u_{(1)})xf(\lambda(u_{(2)}))$ is also in K, where λ and Δ are the antipode [**10**, p. 71] and diagonal maps of H, respectively, and $\Delta(u)=\sum_{(u)} u_{(1)}\otimes u_{(2)}$. Finally, the length of a maximal sequence of divided powers of H is a power of p; this power is called the *exponent* of H.

THEOREM 8. *For any natural number e and k-algebra A containing K, with $[A:k]<\infty$, there exists a divided power Hopf k-algebra $h_K^e(A)$ of exponent e and an admissible map $\zeta_A:h_K^e(A)\to A$ with the following universal property: Given any divided power Hopf k-algebra H of exponent $\leqq e$ and admissible map $\varphi:H\to A$, there is a unique Hopf k-algebra map $f:H\to h_K^e(A)$ such that $\zeta_A f=\varphi$. $h_K^e(A)$ is unique up to Hopf algebra isomorphism; moreover—*

(a) *$P(h_K^e(A))\approx A_K^{\dagger}$ as restricted Lie k-algebras.*

(b) $h_K^1(A) \approx U_r(A_K^{\dagger})$ *as Hopf k-algebras.*

(c) *There exists a unique formal K-space structure on* $\mathrm{gr}(h_K^e(A))$ *such that the composite isomorphism* $\mathrm{gr}(h_K^e(A))_1 \approx P(h_K^e(A)) \approx A_K^{\dagger}$ *is a K-space map.*

(d) *If* $\{1, u_1, u_2, \cdots, u_n\}$ *is a sequence of divided powers of* $h_K^e(A)$ *and* α *is in* K, *then there is a unique sequence* $\{1, \alpha \circ u_1, \alpha \circ u_2, \cdots, \alpha \circ u_n\}$ *of divided powers of* $h_K^e(A)$ *such that* $\zeta_A(\alpha \circ u_i) = \alpha^i \zeta_A(u_i)$ *for* $i \leqq n$.

DEFINITION 9. Let H be a divided power Hopf k-algebra, with $\mathrm{gr}(H)$ a formal K-space. H is called *K-regular* if there exists a k-algebra A containing K, with $[A:k] < \infty$, and a Hopf k-algebra injection $j: H \hookrightarrow h_K^e(A)$ for some natural number e, such that—

(a) $\mathrm{gr}(j): \mathrm{gr}(H) \hookrightarrow \mathrm{gr}(h_K^e(A))$ is a map of formal K-spaces.

(b) If α is in K and $\{1, u_1, \cdots, u_n\}$ is a sequence of divided powers of $\mathrm{Im}(j)$, then $\alpha \circ u_i$ is likewise in $\mathrm{Im}(j)$ whenever $p \mid i$.

If L is a restricted Lie k-algebra and K-space of finite dimension, then one obtains easily a unique formal K-space structure on $\mathrm{gr}(U_r(L))$ such that the composite isomorphism $L \approx P(U_r(L)) \approx P(\mathrm{gr}(U_r(L))) \approx \mathrm{gr}(U_r(L))_1$ is a K-space map.

THEOREM 10. *If L is as above, then* $U_r(L)$ *is a K-regular Hopf algebra if and only if L is a K-regular restricted Lie algebra.*

3. **The fundamental theorem and an application.** Our Galois correspondence now assumes the following form.

THEOREM 11. *If* K/k *is modular, then there exists a one-to-one lattice-inverting correspondence between the fields F, with* $k \subseteq F \subseteq K$ *and* K/F *modular, and the K-regular Hopf subalgebras H of* $H(K/k)$. *The correspondence is given by the operations* $H \to K^H$, $F \to H(K/F)$.

The theorem below is a consequence of the Galois theory developed here, together with some of the results and techniques of [**10**]. If A is a k-algebra, let $A[t]$ be the ring of "truncated" polynomials over A in the indeterminate t, subject only to the relation $t^m = 0$ for some natural number m. An *approximate automorphism of* K/k (mod degree m) is a $k[t]$-algebra automorphism σ of $K[t]$ such that $\sigma(x) = x$ (mod $tK[t]$) for all x in $K \subseteq K[t]$ [**3**]. If A is a k-algebra containing K, then an approximate automorphism σ of K/k is called *A-inner* if there is an invertible element u of $A[t]$ such that $\sigma(x) = uxu^{-1}$ for all x in $K \subseteq A \subseteq A[t]$.

THEOREM 12. *Let K be a finite extension field of k, and A be a k-algebra containing K, with* $[A:k] < \infty$. *Assume that the subfield of K* *of elements left fixed by all A-inner approximate automorphisms of K/k is precisely k (i.e., if x is in K, then $\sigma(x)=x$ for every A-inner approximate automorphism σ of K/k if and only if x is in k). If $B=\{a$ in $A/ax=xa$ for all x in $K\}$ is the centralizer of K in A, then A is a free left and right B-module of rank $[K:k]$, and the map $\varphi: A\otimes_k K \rightarrow \mathrm{End}_B(A)$ is an isomorphism of K-algebras, where $\varphi(a\otimes x)u=aux$ for a, u in A and x in K, and A is viewed as a right B-module.*

In particular, A is a "form" of the K-algebra of $n\times n$ matrices over B, where $n=[K:k]$.

References

1. G. Angwin, *On regular restricted Lie algebras* (unpublished).

2. R. L. Davis, *A Galois theory for a class of purely inseparable exponent two field extensions*, Bull. Amer. Math. Soc. **75** (1969), 1001–1004. MR **39** #5524.

3. M. Gerstenhaber and A. Zaromp, *On the Galois theory of purely inseparable field extensions*, Bull. Amer. Math. Soc. **76** (1970), 1011–1014.

4. G. Hochschild, *Simple algebras with purely inseparable splitting fields of exponent one*, Trans. Amer. Math. Soc. **79** (1955), 477–489. MR **17**, 61.

5. N. Jacobson, *Lectures in abstract algebra*. Vol. III: *Theory of fields and Galois theory*, Van Nostrand, Princeton, N. J., 1964. MR **30** #3087.

6. G. S. Rinehart, *Differential forms on general commutative algebras*, Trans. Amer. Math. Soc. **108** (1963), 195–222. MR **27** #4850.

7. S. Shatz, *Galois theory*, Lecture Notes in Math., no. 86, Springer-Verlag, Berlin, 1969, pp. 146–158.

8. M. E. Sweedler, *The Hopf algebra of an algebra applied to field theory*, J. Algebra **8** (1968), 262–276. MR **36** #5105.

9. ———, *Structure of inseparable extensions*, Ann. of Math. (2) **87** (1968), 401–410. MR **36** #6391.

10. ———, *Hopf algebras*, Math. Lecture Note Series, Benjamin, New York, 1969. MR **40** #5705.

Cornell University, Ithaca, New York 14850