JOURNAL OF
Algebra

Volume 106, 1987

ACADEMIC PRESS, INC.
Harcourt Brace Jovanovich, Publishers
San Diego Orlando New York Austin Boston
London Sydney Tokyo Toronto

CONTENTS OF VOLUME 106

NUMBER 1, MARCH 1987

NUMBER 2, APRIL 1, 1987

JOURNAL OF ALGEBRA 106, 239–258 (1987)

Hopf Galois Theory for Separable Field Extensions

CORNELIUS GREITHER AND BODO PAREIGIS

Mathematisches Institut der Universität München, Theresienstr. 39, 8000 Munich 2, West Germany

Communicated by A. Frohlich

Received January 21, 1985

INTRODUCTION

It is well known that adjoining $\omega = \sqrt[3]{2}$ to $\mathbb{Q}$ does not give a Galois extension of $\mathbb{Q}$, i.e., there is no set of automorphisms of $\mathbb{Q}(\omega)$ whose set of common fixed elements is precisely $\mathbb{Q}$. However, one can define the following linear maps s, c from $\mathbb{Q}(\omega)$ to itself by

$$c(1)=1, \qquad c(\omega)=-\tfrac{1}{2}\omega, \qquad c(\omega^2)=-\tfrac{1}{2}\omega^2,$$
$$s(1)=0, \qquad s(\omega)=\tfrac{1}{2}\omega, \qquad s(\omega^2)=-\tfrac{1}{2}\omega^2,$$

and $\alpha \in \mathbb{Q}(\omega)$ is in $\mathbb{Q}$ if and only if $c(\alpha)=\alpha$ and $s(\alpha)=0$. In this sense, $\mathbb{Q}$ can be considered as the fixed field of s, c. This in itself is not remarkable. But even though c and s are not automorphisms, they have a close connection with the ring structure of $\mathbb{Q}(\omega)$. For all $\alpha, \beta \in \mathbb{Q}(\omega)$, we have

$$c(\alpha\beta) = c(\alpha)\cdot c(\beta) - 3\cdot s(\alpha)\cdot s(\beta);$$
$$s(\alpha\beta) = c(\alpha)\cdot s(\beta) + s(\alpha)\cdot c(\beta).$$

So $\mathbb{Q}(\omega)$ is some sort of "generalized Galois extension" of $\mathbb{Q}$. This example is an instance of a general concept introduced by Chase and Sweedler [2]. The interrelation between c, s and the ring structure of $\mathbb{Q}(\omega)$ is formalized by the concept of H-Galois extension where H is a finite Hopf algebra.

DEFINITION. Let $K|k$ be a finite extension of fields, H a finite k-Hopf algebra. Then $K|k$ is *H-Galois* if there exists a k-algebra homomorphism

$$\mu: H \to \mathrm{End}_k(K)$$

such that $(1, \mu): K \otimes_k H \to \mathrm{End}_k(K)$ is an isomorphism (where

0021-8693/87 $3.00

$1: K \to \mathrm{End}_k(K)$ is induced by the multiplication in K), and the following conditions are satisfied:

$$\mu(h)(xy) = \sum_{(h)} \mu(h_{(1)})(x) \cdot \mu(h_{(2)})(y),$$
$$\mu(h)(1) = \varepsilon(h)(1) \qquad \text{for} \quad h \in H,\ x, y \in K.$$

Remark 1. Whenever $K|k$ is Galois with group G, $K|k$ is H-Galois, where H is the group ring kG.

Remark 2. In the example at the beginning, take H to be $\mathbb{Q}[c, s]/(3s^2 + c^2 - 1, (2c+1)s, (2c+1)(c-1))$, $\Delta(c) = c \otimes c - 3s \otimes s$, $\Delta(s) = c \otimes s + s \otimes c$, $\varepsilon(c) = 1$, $\varepsilon(s) = 0$.

Remark 3. An equivalent definition would be: There is a k-algebra homomorphism $\mu'': K \to K \otimes_k H^*$, where H^* is the dual Hopf algebra to H, such that μ'' defines an H-comodule structure on K, and the map

$$(\mathrm{mult.} \otimes H^*)(K \otimes \mu''): K \otimes K \to K \otimes K \otimes H^* \to K \otimes H^*$$

is an isomorphism of K-vector spaces.

μ'' and μ are deduced from each other in a canonical way, and there is a third canonical map $\mu': H \otimes K \to K$. We will use whichever is the most convenient.

Many purely inseparable extensions are H-Galois [2]. This is of interest since one can prove a weaker form of the so-called Main Theorem of Galois Theory for arbitrary H-Galois extensions. In this paper, we start with the observation that many nonnormal *separable* extensions are H-Galois extensions for appropriate H (this does not seem to be widely known), and we set out to characterize the extensions $K|k$ which are H-Galois completely in terms of the Galois group G of the normal closure (= splitting field) $\tilde{K}$ of K over k. The result will be stated in Section 2 and proved in Section 3. It will turn out that (in contrast to classical theory) in general there may exist several Hopf algebras H making a given extension $K|k$ H-Galois, the easiest example being $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$. All possible H-Galois structures will be determined.

Let us give a more detailed preview of some results. If $K|k$ has degree $n = 2$, $K|k$ is classically Galois. For $n = 3$ or 4, $K|k$ is always H-Galois. For $n = 5$, there are separable extensions which are not H-Galois for any H. The extensions of degree 3 and 4 have an even nicer structure which we call "almost classically Galois," see Section 4. For extensions with this structure, the Main Theorem holds in the usual form: The sub-Hopf algebras of H are in bijective correspondence with the intermediate fields E, $k \subset E \subset K$. As a further illustration of the nonuniqueness of H, we will show for

classical Galois extensions $K|k$: $K|k$ can be made H-Galois in such a way that in the correspondence between all sub-Hopf algebras and intermediate fields, only those intermediate fields occur which are normal over k.

In the body of the paper, all field extensions (except algebraic closures) are assumed to be *finite*.

1. Galois Theory and Descent

We fix a base field k. Let L be an extension field of k, S a finite set, B the group of all permutations of S. When and in which way is L^S a Galois extension of L in the sense of Galois theory of commutative rings? (See [1].) Any action of a group N on L^S by L-automorphisms is given by an action of N on the index set S. So we can state:

1.1. Lemma. *Let L, S, B be as above. Then giving a Galois action $\mu'\colon L[N]\otimes_L (L^S)\to L^S$ (i.e., providing $L^S \mid L$ with an N-Galois structure) is the same as giving an embedding $N\subset B$ as a regular permutation group.*

(A subgroup of a permutation group is *regular* if it is transitive and the stabilizer of any of the permuted objects is the trivial group.)

Proof. Every map μ' gives an operation of N on S. Since Galois actions are faithful, N is embedded in B. By direct calculation one sees that N is regular on S if and only if the canonical map $L[N]\otimes_L L^S \to \mathrm{End}_L(L^S)$ is bijective.

This lemma explains the Galois theory of L^S over L. We want to apply this to a general field extension $K|k$. One knows that if L is "big enough," then $L\otimes_k K$ is L-isomorphic to L^S for some S. To be precise, we define the setup

$$\begin{aligned} &\tilde{K} = \text{normal closure of } K \text{ over } k \qquad (K|k \text{ separable})\\ &G = \mathrm{Aut}(\tilde{K}|k)\\ &G' = \mathrm{Aut}(\tilde{K}|K)\\ &S = G/G' \qquad \text{(left cosets)}. \end{aligned} \tag{$*$}$$

Let $L^{G/G'}$ be the set of functions from G/G' to L. This is a L-vector space with base $\{e_{\bar{g}} \mid \bar{g}\in G/G'\}$, where $e_{\bar{g}}(\bar{h}) = \delta_{\bar{g},\bar{h}}$.

1.2. Lemma. *Let L be any field containing $\tilde{K}$. Then the map*

$$\phi\colon L\otimes_k K \ni \lambda\otimes x \mapsto \sum_{\bar{g}\in G/G'} \lambda g(x)\cdot e_{\bar{g}} \in L^{G/G'}$$

is an L-algebra isomorphism. Set $\Gamma = \mathrm{Aut}(L|k)$. Then Γ maps onto G. $L \otimes_k K$ is a Γ-set via the left factor, and $L^{G/G'}$ is a Γ-set by $\gamma(\lambda e_{\bar{h}}) = \gamma(\lambda)\, e_{\overline{gh}}$, where $\gamma \mapsto g \in G$ and $\{e_{\bar{h}} \mid \bar{h} \in G/G'\}$ is the canonical base of $L^{G/G'}$. Then ϕ is also a Γ-map.

Proof. (well known). Write $K = k[\xi] = k[X]/(f)$ with minimal polynomial f for ξ. For each $h \in \mathrm{Alg}_k(K, \tilde{K}) = \mathrm{Alg}_k(K, L)$ we have a root $h(\xi)$ of f, hence $\{g(\xi) \mid \bar{g} \in G/G'\}$ is the set of roots of f. By the Chinese Remainder Theorem, we get

$$L \otimes_k K \simeq L[X]/(f) \simeq \prod_{\bar{g} \in G/G'} L[X]/(X - g(\xi)) \simeq L^{G/G'},$$

and the map is precisely ϕ. The Γ-map property is checked easily.

Now we begin with an arbitrary Hopf algebra H which gives an H-Galois structure for the separable extension $K|k$. We will show that H is a form of $k[N]$, and N is uniquely embedded in $B = \mathrm{Perm}(G/G')$ as a regular permutation group.

1.3. PROPOSITION. *Let $K|k$ be separable and H-Galois. Then there is, for any extension $L \supset \tilde{K}$, a unique regular subgroup $N \subset B = \mathrm{Perm}(S)$ such that there is an L-isomorphism $\alpha: L \otimes_k H \to L[N]$, and the diagram*

$$\begin{array}{ccc} (L \otimes H) \otimes_L (L \otimes K) & \xrightarrow{L \otimes \mu'} & L \otimes K \\ \downarrow{\scriptstyle \alpha \otimes \phi} & & \downarrow{\scriptstyle \phi} \\ L[N] \otimes_L L^S & \xrightarrow{\nu'} & L^S \end{array}$$

commutes. (The bare symbol $\otimes$ means $\otimes_k$.)

Proof. The only point will be that $L \otimes H$ is a group ring. Since $\tilde{K} \otimes K \cong \tilde{K} \otimes H^*$ as $\tilde{K}$-algebras, we have $L \otimes H^* \cong L \otimes K$ as L-algebras. On the other hand, $L \otimes K$ is L-isomorphic to L^S by Lemma 1.2. Thus the L-Hopf algebra $L \otimes H^*$ has L^S for its underlying algebra. As is well known, this implies $L \otimes H \cong L^N$ as Hopf algebras for some group N, so $L \otimes H \cong L[N]$. (Thanks are due to C. Wenninger for pointing out this short proof.)

Our Galois structure $\mu': H \otimes_k K \to K$ induces a Galois structure $(L \otimes H) \otimes_L (L \otimes K) \to L \otimes K$. Let ν' be defined by the above diagram. Then the Galois action ν' determines an embedding $N \subset B$ as a regular subgroup by 1.1. Since ν' is determined by the diagram, the embedding $N \subset B$ is also uniquely determined.

We close this section by recalling some elements of descent theory (see,

e.g., [4, pp. 44, 65]). Suppose $L|k$ Galois with group G. Let A be an object (vector space, algebra, Hopf algebra) over k. An *L-form* of A is a k-object B such that $L\otimes_k B \cong L\otimes_k A$. Let us agree on $\otimes = \otimes_k$.

G operates on $L\otimes A$ by automorphisms via L. By conjugation, G operates on $\mathrm{Hom}_L(L\otimes A, L\otimes A')$ for k-objects A, A'.

(Example: $A = k^n$, $\mathrm{Aut}_L(L\otimes A) = Gl(n, L)$, and G operates on the matrix entries.)

1.4. THEOREM. *The set* L-$\mathrm{Form}(A)$ *of L-forms of A modulo isomorphism is in bijective correspondence with* $H^1(G, \mathrm{Aut}_L(L\otimes A))$.

Proof. See [4, 8.1 and 9.1].

In this theorem, H^1 denotes as usual the pointed set of cocycles with cohomologous cocycles identified. A cocycle in a G-module P is a family $\{p_\sigma | \sigma\in G\}$, $p_\sigma \in P$, $p_{\sigma\tau} = p_\sigma \cdot {}^\sigma(p_\tau)$. We omit the definition of the relation "cohomologous."

For later use, we make the correspondence explicit: For $B\in L$-$\mathrm{Form}(A)$, $\phi: L\otimes B \to L\otimes A$ an isomorphism, we construct a cocycle as follows:

$$p_\sigma = \phi\cdot \mathrm{op}_B(\sigma)\cdot \phi^{-1}\cdot \mathrm{op}_A(\sigma^{-1}) \in \mathrm{Aut}_L(L\otimes A).$$

Here $\mathrm{op}_A(\sigma)$ denotes the operation of $\sigma\in G$ on $L\otimes A$ through the left factor L. Every cocycle occurs in this way.

DEFINITION. Let B_i be an L-form of A_i, $\phi_i: L\otimes B_i \xrightarrow{\sim} L\otimes A_i$ $(i=1,2)$. Then a morphism $f: L\otimes A_1 \to L\otimes A_2$ is called *descendable* if there is a morphism g such that

$$\begin{array}{ccc} L\otimes B_1 & \xrightarrow{L\otimes g} & L\otimes B_2 \\ {\scriptstyle\phi_1}\downarrow & & \downarrow{\scriptstyle\phi_2} \\ L\otimes A_1 & \xrightarrow{f} & L\otimes A_2 \end{array}$$

commutes. (If g exists, it is unique.)

1.5. LEMMA. *In this notation, let* $p^{(i)}$ *be the associated cocycles to* B_i. *Then f is descendable if and only if*

$$f\cdot p^{(1)}_\sigma = p^{(2)}_\sigma \cdot f \qquad \textit{for all} \quad \sigma\in G.$$

Proof. Easy verification which we omit.

For subsequent use, we make one last remark:

1.6. LEMMA. *Let H be a Hopf algebra over k, $\mu: H \otimes K \to K$ a k-linear map. Then μ defines an H-Galois structure if and only if $L \otimes \mu$ defines an $L \otimes H$-Galois structure on $L \otimes K$.*

Proof. The assertion follows from the general theory of faithfully flat descent applied to $L|k$.

2. STATEMENT OF THE MAIN THEOREM AND FIRST EXAMPLES

Let us begin with another explicit example. Consider the extension $K = \mathbb{Q}(\sqrt[4]{2}) | \mathbb{Q} = k$. The extension $K(i)|\mathbb{Q}(i)$ is Galois with group $N = C_4$, so it is H_0-Galois with $H_0 = \mathbb{Q}(i)[C_4]$. One can show by direct calculation that H_0 contains a sub-Hopf algebra H with $H_0 = H[i]$ and H operates on K in such a way that $K|\mathbb{Q}$ is H-Galois: If e stands for a generator of C_4,

$$H = \mathbb{Q}\left[\frac{e+e^{-1}}{2}, \frac{e-e^{-1}}{2i}\right] \cong \mathbb{Q}[c, s]/(c^2 + s^2 - 1, cs).$$

We omit the details since the example is covered by the general theorem to follow. We resume the setup $(*)$ of the first section: $\tilde{K}$ = normal closure of the separable extension $K|k$, $G = \mathrm{Aut}(\tilde{K}|k)$, $G' = \mathrm{Aut}(\tilde{K}|K)$, and $S = G/G'$.

Set $B = \mathrm{Perm}(S)$. Since G operates on $S = G/G'$, G maps into B. This map is monic, since its kernel is the intersection of all conjugates of G', or (which is the same) the biggest invariant subgroup of G contained in G', and this group must be trivial because $\tilde{K}$ is the smallest Galois extension of k over K. Thus we have $G \subset B$.

(In our example, S is in canonical bijection with the four complex roots of $X^4 - 2$, and G operates faithfully on S. If we identify S with $\{1, 2, 3, 4\}$, G is the dihedral group $D_4 = \langle (1234), (13) \rangle$ and $G' = \langle (24) \rangle$. G has a normal subgroup $N = \langle (1234) \rangle$ which is a regular permutation group on S. All these remarks show that we do have a particular case of the following result.)

2.1. THEOREM. *Let $K|k$ be a separable field extension, S, B as above. Then the following are equivalent:*

(a) *There is a k-Hopf algebra H such that $K|k$ is H-Galois.*

(b) *There is a regular subgroup $N \subset B$ such that the subgroup G of B normalizes N.*

Furthermore, the group N in (b) *is obtained from* (a) *by the procedure of Lemma* 1.3. *The Hopf algebra H in* (a) *is always a K-form of $k[N]$ and can be computed by means of Galois descent.*

The proof is postponed to Section 3 for the sake of examples.

2.2. EXAMPLE. $K=\mathbb{Q}(\sqrt[3]{2})$, $k=\mathbb{Q}$. Here $\tilde{K}=\mathbb{Q}(\zeta_3, \sqrt[3]{2})$, G is the full permutation group on $S\simeq\{1,2,3\}$, and G' has two elements. Take N to be the alternating group on $S\simeq\{1,2,3\}$. This is the example from the introduction (where H was also explicitly given).

2.3. EXAMPLE. $K=\mathbb{Q}(\sqrt[4]{2})$ revisited. We know $G\cong D_4$ on $\{1,2,3,4\}$. $D_4=\langle\sigma,\tau\rangle$, $\sigma=(1234)$, $\tau=(13)$. If one takes $N=\langle\sigma^2,\sigma\tau\rangle$, then $C_2\times C_2\cong N\lhd G$, and one sees easily that N is regular. This gives rise to a Hopf algebra H' (which is not isomorphic to H constructed at the beginning of this section). One can show: H' is the sub-Hopf algebra $\mathbb{Q}[st, s+t, \sqrt{-2}(t-s)]$ of $\mathbb{Q}(\sqrt{-2})[s,t]=\mathbb{Q}(\sqrt{-2})[C_2\times C_2]$, where $s^2=t^2=1$ and s, t are group-like. Setting $a=(s+t)/2$, $b=(\sqrt{-2}/2)(t-s)$, one obtains $H'\cong\mathbb{Q}[a,b]/(ab, b^2-2a^2+2)$ and $\Delta a=a\otimes a-\frac{1}{2}b\otimes b$, $\Delta b=a\otimes b+b\otimes a$, $\varepsilon(a)=1$, $\varepsilon(b)=0$, $S(a)=a$, $S(b)=b$.

N.B. This is an example of a separable field extension which has two different Hopf Galois structures. Nakajima has given an example of this phenomenon in characteristic 2 using a different approach [6, Remark 2 following 2.7].

Remark. In both these examples, N was actually contained in G. This need not hold in general; see Section 4.

2.4. COUNTEREXAMPLE. Let $K=\mathbb{Q}(\xi)$, $[K:\mathbb{Q}]=5$, $\mathrm{Gal}(\xi\,|\,\mathbb{Q})=\mathrm{Aut}(\tilde{K}\,|\,\mathbb{Q})\cong S_5$. (Plenty of such K exist.) Then $K|\mathbb{Q}$ is not H-Galois for any H.

Proof. $[G:G']=5$, so $B\cong S_5$, $B=G$. Assume there exists a normal subgroup $N\lhd S_5$ which is regular on $S=G/G'$. Since N is then necessarily generated by a 5-cycle, this can be refuted directly, but we argue in a more general way:

2.4.1. LEMMA. *For $N<\Gamma$ (Γ any group), $\#\mathrm{Norm}_\Gamma(N)$ divides $\#\mathrm{Cent}_\Gamma(N)\cdot\#\mathrm{Aut}(N)$.*

Proof. This follows from the left exact sequence

$$1\to\mathrm{Cent}_\Gamma(N)\to\mathrm{Norm}_\Gamma(N)\to\mathrm{Aut}(N).$$

2.4.2. LEMMA. *Let $N<S_n$ be a regular subgroup. Then $\mathrm{Cent}_{S_n}(N)=\{\phi_\sigma\,|\,\sigma\in N\}\cong N^{\mathrm{opp}}$, where ϕ_σ is defined by $\phi_\sigma(i)=\mu_i(\sigma(1))$, $\mu_i\in N$ being determined by $\mu_i(1)=i$.*

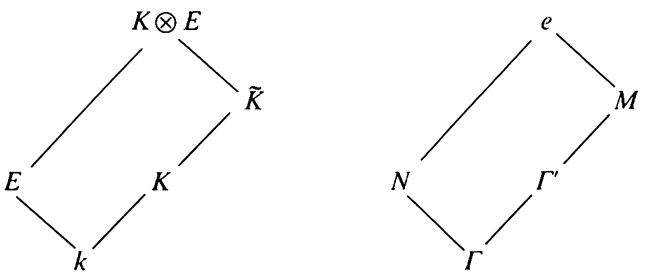
Proof. Take $\phi \in \mathrm{Cent}_{S_n}(N)$ and find $\sigma \in N$ with $\sigma(1) = \phi(1)$. Then $\phi = \phi_\sigma$. In fact, let $i \neq \{1,\ldots,n\}$ and $\mu_i \in N$, $\mu_i(1) = i$. Then $\mu_i\phi = \phi\mu_i$ so that $\phi(i) = \phi\mu_i(1) = \mu_i\phi(1) = \mu_i\sigma(1) = \phi_\sigma(i)$. Conversely, given $\sigma \in N$ define ϕ_σ as in the lemma. Since $\phi_\sigma(i) = \phi_\sigma(j)$ implies $\mu_i\sigma(1) = \mu_j\sigma(1)$, it implies $i = j$ because N is regular, so ϕ_σ is indeed in S_n. One easily checks that $\phi_\sigma \in \mathrm{Cent}_{S_n}(N)$ and that $\phi_{\sigma\tau} = \phi_\tau\phi_\sigma$.

Now the two preceding lemmas imply in the situation of 2.4: $\#\mathrm{Norm}_{S_5}(N) \leqslant \#N^{\mathrm{opp}} \cdot \#\mathrm{Aut}(N)$. But $N \cong C_5$, so the last expression is 20. This contradicts the assumption that the group S_5 normalizes N.

Whole reams of examples for H-Galois extensions can be constructed with the following result:

2.5. THEOREM. *Assume $K|k$ a separable field extension, and assume there exists a Galois extension $E|k$ such that $K \otimes E$ is a field which contains a normal closure $\tilde{K}$ of $K|k$. Then $K|k$ is H-Galois, where H is an E-form of $k[N]$ and $N \cong \mathrm{Aut}(K \otimes E|E)$.*

Proof. (a) First we show E can be shrunk to a Galois extension E' with $K \otimes E' = \tilde{K}$. Let M, N, Γ', Γ be the groups of automorphisms of $K \otimes E$ fixing $\tilde{K}$, E, K, k, respectively:



We claim $\tilde{K} \cap (KE) = K \cdot (\tilde{K} \cap E)$. If we translate this into groups, we have $M \cdot (\Gamma' \cap N) = \Gamma' \cap (M \cdot N)$, and this is correct since N is normal and $\Gamma' \supset M$. So $\tilde{K} = \tilde{K} \cap (KE) = K \cdot (\tilde{K} \cap E) = K \otimes (K \cap E)$, and we may define $E' = \tilde{K} \cap E$.

(b) Suppose $K \otimes E = \tilde{K}$. Let $N = \mathrm{Aut}(\tilde{K}|E)$, $G' = \mathrm{Aut}(\tilde{K}|K)$. Then N is a normal complement to G' in G (since $E|k$ is Galois, $K \cap E = k$, and $KE = \tilde{K}$), so N is regular on $S = G/G'$. Now we take the opposed group $N^{\mathrm{opp}} = \{\phi_\sigma | \sigma \in N\} \subset \mathrm{Perm}(S) = B$ as in Lemma 2.4.2. We claim N^{opp} is normalized by $G \subset B$ and centralized by $N \subset B$. *Proof*: The second half follows from the lemma. So we take $g \in G$ and have to show $g \cdot N^{\mathrm{opp}} \cdot g^{-1} \subset N^{\mathrm{opp}}$. Since N^{opp} is transitive, we may change g so that $g(1) = 1$. Take $\phi_\sigma \in N^{\mathrm{opp}}$. *Claim*: $g\phi_\sigma g^{-1} = \phi_{g\sigma g^{-1}}$. (This makes sense since

$g\sigma g^{-1} \in N$.) To prove the claim, we evaluate at i. In the notation of 2.4.2, this gives the equation

$$g\mu_{g^{-1}(i)}\sigma(1) = \mu_i(g\sigma g^{-1}(1)) \qquad (= \mu_i(g\sigma(1))).$$

So it suffices to prove $g\mu_{g^{-1}(i)} = \mu_i g$, or equivalently $\mu_{g^{-1}(i)} = g^{-1}\mu_i g$. Now both sides are in N, so we only need to evaluate at 1. Then we get $\mu_{g^{-1}(i)}(1) = g^{-1}(i) = g^{-1}(\mu_i(1)) = g^{-1}\mu_i g(1)$, and the claim is proved.

Thus $N^{\mathrm{opp}} \subset B$ satisfies condition (b) of 2.1, so (a) also holds. Moreover, N operates trivially on N^{opp}, so by Corollary 3.2 (see third section) the isomorphism $\tilde{K} \otimes H \simeq \tilde{K}[N]$ is already defined over the fixed field of N, i.e., over E.

(*Remark.* In the proof above, one could take N in the place of N^{opp}, and this would also yield most of the result, but with a different Hopf algebra H which is not necessarily an E-form of $k[N]$. See Section 5.)

2.6. COROLLARY. *Any radical extension of the form* $K = k(a)$, $a^n \in k$, $\mathrm{char}(k) \nmid n$, *which is linearly disjoint to* $k(\zeta_n)$ *over* k, *is H-Galois.* (*This covers, e.g.,* $\mathbb{Q}(\sqrt[3]{2})$ *and* $\mathbb{Q}(\sqrt[4]{2})$, *which were considered above, and many other cases.*)

Proof. $K \otimes_k k(\zeta_n) = K(\zeta_n)$ is the splitting field of $X^n - a^n$ over k, so it is Galois over k, and we may apply 2.5.

Remark 1. In some special cases, one can do without the linear disjointless by replacing $k(\zeta_n)$ by an appropriate subfield.

Remark 2. $k(a)$ is a graded k-algebra with group C_n if $X^n - a^n$ is irreducible over k. By [2, p. 39, remark preceding 4.16] this already implies that $k(a)$ is H-Galois over k, where H is the dual Hopf algebra of $k[C_n]$.

3. PROOF OF THE MAIN THEOREM

It is convenient to restate the main Theorem 2.1 in a more technical form. Let the notation be as in (*) (first section).

3.1. THEOREM. *Let* $N \subset B$ *be a subgroup. The following are equivalent*:

(a) *There is a k-Hopf algebra H and an H-Galois structure on* $K|k$ *which induces* $N \subset B$ *by way of Proposition* 1.3.

(b) N *is regular on* $S = G/G'$, *and the subgroup* $G \subset B$ (*see the remarks preceding* 2.1) *normalizes* N.

More succinctly stated, there is a bijection between isomorphism classes of H-Galois structures on $K|k$ and regular subgroups $N \subset B$ normalized by G.

Theorem 3.1 is a sharpened version of 2.1 (see Proposition 1.3). Before beginning the proof, we still state a corollary which will be proved along the way.

3.2. COROLLARY. *Assume the notation of the theorem, and assume* (a) *and* (b) *hold. Let $G_0 \subset G$ be the group of elements operating trivially on N, and let $L_0 \subset \tilde{K}$ be the fixed field of G_0. Then L_0 is the smallest extension of k with $L_0 \otimes H \cong L_0[N]$.*

Proof of 3.1. (b) implies (a): Recall $S = G/G'$. Define μ': $\tilde{K}[N] \otimes_{\tilde{K}} \tilde{K}^S \to \tilde{K}^S$ by $\mu'(\rho \otimes x e_{\bar{g}}) = x \cdot e_{\rho(\bar{g})}$ for $\rho \in N$, $g \in G$. (Recall $\{e_{\bar{g}} \mid \bar{g} \in G/G'\}$ is the canonical base of $\tilde{K}^S$.) Moreover, define $p_g: N \to N$ by $p_g(n) = gng^{-1}$ for $n \in N$, $g \in G$. Then $\{p_g \mid g \in G\}$ is a G-cocycle of $\tilde{K}$-Hopf automorphisms of $\tilde{K}[N]$. (Here we have used that the operation of G on $\mathrm{Aut}_{\tilde{K}\text{-Hopf}}(\tilde{K}[N])$ via $\tilde{K}$ is trivial, because the Hopf automorphisms of the group ring $\tilde{K}[N]$ are just the group automorphisms of N.)

Any element $h \in G$ operates on $\tilde{K}[N]$ via $\tilde{K}$, and on $\tilde{K}^S$ by virtue of $h(x \cdot e_{\bar{g}}) = h(x) \cdot e_{\overline{hg}}$. We define as earlier: ${}^h\mu' = h \cdot \mu' \cdot h^{-1}$. Let us check that the following diagram commutes:

$$\begin{array}{ccc} \tilde{K}[N] \otimes_{\tilde{K}} \tilde{K}^S & \xrightarrow{{}^h\mu'} & \tilde{K}^S \\ {\scriptstyle p_h \otimes 1}\downarrow & & \| \\ \tilde{K}[N] \otimes_{\tilde{K}} \tilde{K}^S & \xrightarrow{\mu'} & \tilde{K}^S \end{array}$$

We start with $\rho \otimes x e_{\bar{g}}$. Then ${}^h\mu'(\rho \otimes x e_{\bar{g}}) = h\mu' h^{-1}(\rho \otimes x e_{\bar{g}}) = h\mu'(\rho \otimes h^{-1}(x) \cdot e_{\overline{h^{-1}g}}) = h(h^{-1}(x) \cdot e_{\rho(\overline{h^{-1}g})}) = x \cdot e_{h\rho(\overline{h^{-1}g})}$. Going the other way gives: $\mu'(p_h \otimes 1)(\rho \otimes x e_{\bar{g}}) = \mu'(h\rho h^{-1} \otimes x e_{\bar{g}}) = x \cdot e_{h\rho h^{-1}(\bar{g})}$ which is the same.

By Lemma 1.2, $\tilde{K}^S = \tilde{K} \otimes_k K$ as $\tilde{K}$-algebras and G-sets, so one gets a new map $\tilde{\mu}$ such that

$$\begin{array}{ccc} \tilde{K}[N] \otimes_{\tilde{K}} (\tilde{K} \otimes K) & \xrightarrow{{}^h\tilde{\mu}} & \tilde{K} \otimes K \\ {\scriptstyle p_h \otimes 1}\downarrow & & \| \\ \tilde{K}[N] \otimes_{\tilde{K}} (\tilde{K} \otimes K) & \xrightarrow{\tilde{\mu}} & \tilde{K} \otimes K \end{array}$$

commutes. Let H be the $\tilde{K}$-form of $k[N]$ defined by the cocycle $\{p_h\}$. Trivially, K is the $\tilde{K}$-form of K defined by 1. By Lemma 1.5, $\tilde{\mu}$ is descendable, i.e., $\tilde{\mu} = \tilde{K} \otimes \mu_0$ where μ_0 is a k-linear map $H \otimes K \to K$. By Lemma 1.6, μ_0 defines an H-Galois structure since μ defines a $\tilde{K} \otimes H$-Galois structure.

(a) implies (b): Define $L = \tilde{K}$. Then by Proposition 1.3, we have $L \otimes H \cong L[N]$ for some group N. The following argument works for any extension L of K which is Galois over k and which satisfies $L \otimes H \cong L[N]$.

L is Galois over k. Let $\Gamma = \mathrm{Aut}(L|k)$. Then Γ maps onto $G = \mathrm{Aut}(\tilde{K}|k)$. So Γ operates on $L \otimes K$ via the left factor, and on L^S as before: $\gamma(\lambda \cdot e_{\bar{g}}) = \gamma(\lambda) \cdot e_{\overline{hg}}$, where $\gamma \mapsto h \in G$. Let $\mu_0 : H \otimes K \to K$ be the given H-Galois structure. The L-form H of $k[N]$ belongs to a cocycle $\{p_\gamma | \gamma \in \Gamma\}$, and in the notation of 1.5, the lower horizontal map which is defined by the following diagram is descendable:

$$\begin{array}{ccc} (L \otimes H) \otimes_L (L \otimes K) & \xrightarrow{L \otimes \mu_0} & (L \otimes K) \\ \cong \downarrow & & \| \\ L[N] \otimes_L (L \otimes K) & \xrightarrow{\tilde{\mu}} & (L \otimes K) \end{array}$$

By 1.5, this means that the following diagram commutes for all elements $\gamma \in \Gamma$:

$$\begin{array}{ccc} L[N] \otimes_L (L \otimes K) & \xrightarrow{{}^{\gamma}\tilde{\mu}} & L \otimes K \\ {\scriptstyle p_\gamma \otimes 1} \downarrow & & \| \\ L[N] \otimes_L (L \otimes K) & \xrightarrow{\tilde{\mu}} & L \otimes K \end{array}$$

We again replace (by Lemma 1.2) $L \otimes K$ by the isomorphic L-algebra and Γ-set L^S and get a commutative diagram:

$$\begin{array}{ccc} L[N] \otimes_L L^S & \xrightarrow{{}^{\gamma}\mu'} & L^S \\ {\scriptstyle p_\gamma \otimes 1} \downarrow & & \| \\ L[N] \otimes_L L^S & \xrightarrow{\mu'} & L^S \end{array}$$

Now p_γ is certainly induced by a group automorphism of N. Let g be the image of γ in G. We claim: $p_\gamma | N =$ conjugation with g. (N is a permutation group on S by virtue of μ'.) In order to use the commutativity of the preceding diagram, we chase the element $v \otimes e_s$ either way (where $v \in N$, $s \in S$): ${}^{\gamma}\mu'(v \otimes e_s) = \gamma\mu'\gamma^{-1}(v \otimes e_s) = \gamma\mu'(v \otimes e_{g^{-1}(s)}) = \gamma(e_{vg^{-1}(s)}) = e_{gvg^{-1}(s)}$. In the other way, we get $\mu'(p_\gamma \otimes 1)(v \otimes e_s) = \mu'(p_\gamma(v) \otimes e_s) = e_{p_\gamma(v)(s)}$, so indeed $p_\gamma(v) = gvg^{-1}$. In particular, N is normalized by G. The regularity of N was already observed in 1.3.

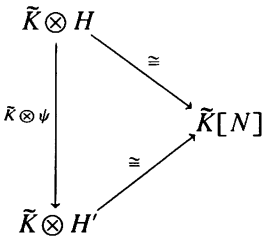
Proof of 3.2. We look at the proof of 3.1, (a) implies (b). The cocycle $\{p_\gamma | \gamma \in \Gamma\}$ was defined as the composition $\Gamma \to G \to^{c} \mathrm{Aut}_{Gr}(N)$, where c sends g to conjugation with g. Let $G_0 = \mathrm{Cent}_G(N)$ be the kernel of c. Then $G_0 = \mathrm{Aut}(\tilde{K}|L_0)$ for some field $L_0 \subset \tilde{K}$. We have an isomorphism

$\phi: L \otimes H \to L[N]$ such that $p_\gamma = \phi \cdot \mathrm{op}_H(\gamma) \cdot \phi^{-1} \cdot \mathrm{op}_{L[N]}(\gamma^{-1})$. Now $p_\gamma = \mathrm{id}$ implies $\phi \cdot \mathrm{op}_H(\gamma) = \mathrm{op}_{L[N]}(\gamma) \cdot \phi$, so this equation holds for all γ mapping into G_0, i.e., for all γ leaving L_0 fixed, so by classical Galois theory the map ϕ is already defined over L_0, i.e., $L_0 \otimes H \cong L_0[N]$. Using similar arguments, it is easy to check that L_0 is the smallest field with this property, and $L_0 \subset \tilde{K}$.

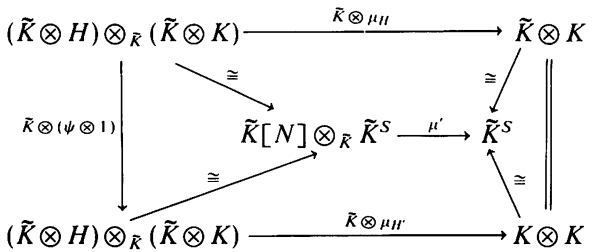
We conclude the section with some remarks on uniqueness. First we show that the Hopf algebra H and the H-Galois structure are uniquely determined by $N \supset B$:

3.3. LEMMA. *Let $K|k$ be H- and H'-Galois with Hopf algebras H and H' which are both $\tilde{K}$-forms of $k[N]$ and induce the same embedding $N \subset B$. Then there is an isomorphism $\psi: H \to H'$ of Hopf algebras compatible with the two Galois structures μ_H and $\mu_{H'}$.*

Proof. H and H' induce the same cocycle $\{p_h | h \in G\}$ on $K[N]$ by $p_h(v) = hvh^{-1}$ as in the proof of 3.1. So there is an isomorphism $\psi: H \to H'$ of k-Hopf algebras such that



commutes. So we get a commutative diagram



Reading the outer frame and using that $\tilde{K}|k$ is faithfully flat, we obtain $\mu_{H'} \cdot (\psi \otimes 1) = \mu_H$. Q.E.D.

Remark. We know already that N along with its embedding in B is uniquely determined by H and its operation. The converse was proved above. If we now forget operations and permutations, the picture is different. The

abstract group N is still determined by the Hopf algebra H (up to isomorphism), since it is "the" group with $\bar{k} \otimes H \cong \bar{k}[N]$. But the Hopf algebra H need not be determined by the abstract group N (see an example in Section 4). Even if we are not interested to know how H operates, and only want to know H up to isomorphism, in general we already have to know how N operates, not just what abstract group N is.

4. The "Almost Classical" Case, and More Examples

We recall the setup (*): $K|k$ separable, $\tilde{K}$ = normal closure of $K|k$, $G = \mathrm{Aut}(\tilde{K}|k)$, $G' = \mathrm{Aut}(\tilde{K}|K)$, $S = G/G'$, $B = \mathrm{Perm}(S)$. The main theorem 2.1 does not tell us whether the subgroup N is contained in $G \subset B$ or not. It turns out that in practice this may or may not happen. The case $N \subset G$ leads to an interesting class of extensions $K|k$ which encompasses all previous examples and deserves study:

4.1. Proposition. *The following conditions are equivalent*:

(a) *There exists a Galois extension $E|k$ such that $k \otimes E$ is a field containing $\tilde{K}$.*

(b) *There exists a Galois extension $E|k$ such that $K \otimes E = \tilde{K}$.*

(c) *G' has a normal complement N in G.*

(d) *There exists a regular subgroup $N \subset B$ normalized by G* and contained in G (*see* 3.1).

Proof. We know that $G \subset B$ and that G is transitive on S. By definition, G' is the stabilizer in G of $\bar{e} \in S$. For $N \subset G$ we have

$$N \cdot G' = G \qquad \text{iff } N \text{ is transitive;}$$

$$N \cap G' = e \qquad \text{iff } \mathrm{Stab}_N(\bar{e}) \text{ is the trivial group.}$$

Together this means: N is regular on S iff N is a complement to G' in G, which proves (c) $\Leftrightarrow$ (d).

(b) $\Rightarrow$ (a) is trivial, and (a) $\Rightarrow$ (b) was proved in 2.5.

(b) $\Rightarrow$ (c): Take $N = \mathrm{Aut}(\tilde{K}|E)$. By usual Galois theory, the statement $KE = \tilde{K}$ translates into $N \cap G' = e$, $K \cap E = k$ means $NG' = G$. N is normal in G since E is Galois over k.

(c) $\Rightarrow$ (b): Take E = fixed field of N. $KE = \tilde{K}$ and $K \cap E = k$ follow again from usual Galois theory. For $KE \cong K \otimes E$, one computes all degrees involved and uses $[G : N] \cdot [G : G'] = [G : e]$.

Remark. Proposition 4.1(d) is satisfied when G is a Frobenius group with respect to its subgroup G'. In this case, N is uniquely determined as the Frobenius kernel of G. In Example 2.2, G is Frobenius, and in Example 2.3 it is not (but 4.1(d) holds all the same). We are grateful to M. Takeuchi for drawing our attention to this point.

4.2. DEFINITION. If $K|k$ satisfies the four conditions of 4.1, we say that $K|k$ is an *almost classical Galois extension.* Examples: All H-Galois extensions we have seen so far. Compare Corollary 2.6.

It is not trivial to find an extension which is H-Galois but not almost classically Galois but it can be done. To this end, we begin with some remarks about realizing a given group-theoretical situation by fields. Let $G \subset S_n$ be a transitive subgroup and let G' be the stabilizer of n. Then $\{1,..., n\}$ is canonically identified with the left cosets G/G', so we call G/G' again S so that G maps into $B = \mathrm{Perm}(S) = S_n$. One knows that the Galois group G is realized by some field extension $\tilde{K}|k$. Let $K = \mathrm{Fix}(G')$. Then $\tilde{K}$ is the normal closure of $K|k$ if and only if G' contains no proper normal subgroups of G, and this is equivalent to the injectivity of $G \to B$. (The kernel of $G \to B$ is the biggest normal subgroup contained in G'.)

When constructing examples, we will begin with $G \subset S_n$ transitive, form G' as above, check that G' contains no normal subgroups, and only then will be bother about finding "nice" fields which realize the situation.

Some conventions: The underlying set of the cyclic group $C_n = \mathbb{Z}/n\mathbb{Z}$ will be taken to be $\{1, 2, 3,..., n\}$, n being the zero element. Via group addition, C_n becomes a subgroup of S_n. Similarly, the automorphism group $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = \{\text{invertible elements of the ring } \mathbb{Z}/n\mathbb{Z}\}$ is via multiplication a subgroup of S_n, and C_n together with $\mathrm{Aut}(C_n)$ forms a semidirect product inside S_n. The elements of $C_n \ltimes \mathrm{Aut}(C_n)$ will be denoted (a, m) ("first multiply by $\bar{m} \in Z/nZ$, then add $\bar{a} \in Z/nZ$"). Most overhead bars will be omitted.

4.3. LEMMA. *For $n = 16$, there exists $G \subset S_n$ as above such that:*

(a) *There is a regular subgroup $N \subset S_{16}$, $G \subset \mathrm{Norm}_{S_{16}}(N)$.*

(b) *There is no regular subgroup $\tilde{N}$ of S_{16} with $\tilde{N} \subset G \subset \mathrm{Norm}_{S_{16}}(\tilde{N})$.*

Proof. Let $M \subset \mathrm{Aut}(C_{16}) \subset S_{16}$ be the four-element group (!) generated by $(0, 3)$ (= multiplication by three on C_{16}). Set $\tilde{G} = C_{16} \ltimes M$. Then $\#G = 64$, and $\tilde{G}$ normalizes $N = C_{16}$. G will be a subgroup of $\tilde{G}$ of index two. Put $G_0 = \langle (2, 1) \rangle \cong C_8$ and define $\sigma = (1, 3)$. One checks the following: σ normalizes G_0, $\sigma^2 = (4, 9) \notin G_0$, $\sigma^4 = (8, 1) \in G_0$. Let G be generated by G_0 and σ. We have the diagram

$$\begin{array}{ccccccccc} e & \longrightarrow & C_{16} & \longrightarrow & \tilde{G} & \longrightarrow & M & \longrightarrow & e \\ & & \cup & & \cup & & \| & & \\ e & \longrightarrow & G_0 & \longrightarrow & G & \xrightarrow{t} & C_4 & \longrightarrow & e, \end{array}$$

where t maps σ to a generator of C_4. Since $G \subset \tilde{G}$, G normalizes N. G is transitive since G_0 is already transitive on even numbers and $\sigma(0) = 1$. G' contains no normal subgroups of G: Since $\#G = 32$, G' has two elements, so $G' = \{e, (0, 9)\}$ and one checks that G' is not normal in G. So (a) is proved.

For (b), assume the contrary. Then $\#\tilde{N} = 16$, so $\tilde{N}$ has index two in G. $\tilde{N}$ is transitive. Set $N_0 = \tilde{N} \cap G_0$. Then

$$e \to N_0 \to \tilde{N} \to C_4$$

is left exact, and because of $\#\tilde{N} = 16$ there are two cases:

(i) $\#N_0 = 4$, $\tilde{N}$ maps onto C_4,

(ii) $\#N_0 = 8$, $\tilde{N}$ maps onto the nontrivial subgroup of C_4.

Suppose (i) holds. Then $N_0 = \langle (4, 1) \rangle$. Pick $\tilde{\sigma} \in N$ which gives the same image in C_4 as σ under t. Then $\tilde{\sigma} = (a, 3)$, and since $\tilde{\sigma} \in G$, a has to be odd. We look at the $\tilde{N}$-orbit of 16: Under N_0 one gets $\{4, 8, 12, 16\}$. Applying $\tilde{\sigma}$ gives $\{a, a+4, a+8, a+12\} = \{b \mid b \equiv a \bmod 4\}$. Applying N_0 again doesn't produce anything new, and applying $\tilde{\sigma}$ again gives $\{a+3a, a+3a+12, a+3a+8, a+3a+8\} = \{4, 8, 12, 16\}$. So the orbit consists of the eight elements b congruent to 0 or a modulo 4, which contradicts the transitivity of $\tilde{N}$.

Suppose (ii) holds. Then $N_0 = G_0 = \langle (2, 1) \rangle$. The image of $\tilde{N}$ in C_4 is generated by the class of $\sigma^2 = (4, 9)$, i.e., $\tilde{N} = \langle (2, 1), (a, 9) \rangle$ for some a, and if a were odd, $(a, 9)$ would not be in G. Here one sees at once that the $\tilde{N}$-orbit of 16 consists only of even numbers, so we arrive at a contradiction also in this case.

4.4. COROLLARY. *If* $K = \mathbb{Q}(\sqrt{-2}, \sqrt[16]{2})$, $k = \mathbb{Q}(\sqrt{-2})$, *then* $K|k$ *is H-Galois for some* H, *but not almost classically Galois.*

Proof. $K \subset \tilde{K} = \mathbb{Q}(\sqrt[16]{2}, \zeta_{16})$ where ζ_{16} is a primitive 16th root of unity. Let $G = \mathrm{Aut}(\tilde{K}|k)$. G operates faithfully on the sixteen roots $\zeta_{16}\sqrt[16]{2}$, $\zeta_{16}^2\sqrt[16]{2}, \ldots, \zeta_{16}^{16} \cdot \sqrt[16]{2}$ (which we number canonically from 1 to 16), i.e., $G \subset S_{16}$. By definition of K, $G' = \mathrm{Aut}(\tilde{K}|K)$ consists of those permutations leaving $\sqrt[16]{2}$ fixed.

Claim. G is exactly the group $\langle (2, 1), (1, 3) \rangle$ from Lemma 4.3.

For this we prove:

(i) $\#G = 32$,

(ii) (2, 1) and (1, 3) are in G.

(i) This just means $[\tilde{K}:k] = 32$. Now $[\tilde{K}:\mathbb{Q}] = [\mathbb{Q}(\zeta_{16}):\mathbb{Q}] \cdot [\tilde{K}:\mathbb{Q}(\zeta_{16})]$. The first factor is 8, and so is the second factor (reason: $\sqrt{2}$ is in $\mathbb{Q}(\zeta_{16})$ but $\sqrt[4]{2}$ is not because it does not lie in any abelian extension of $\mathbb{Q}$). So $[\tilde{K}:\mathbb{Q}] = 64$, i.e., $[\tilde{K}:k] = 32$.

(ii) We know that $\tilde{G} = \mathrm{Aut}(\tilde{K}|\mathbb{Q})$ is via operation on the roots of $X^{16} - 2$ a 64-element subgroup of $C_{16} \ltimes \mathrm{Aut}(C_{16}) \subset S_{16}$, and since $\sqrt[16]{2}$ has degree 8 over $\mathbb{Q}(\zeta_{16})$, the automorphism $\sigma_{(2,1)}$ which sends $\sqrt[16]{2}$ to $\zeta_{16}^2 \cdot \sqrt[16]{2}$ and fixes ζ_{16} exists. Furthermore, since $\mathrm{Aut}(\mathbb{Q}(\zeta_{16})|\mathbb{Q}) = \mathrm{Aut}(C_{16})$, for some $a \in C_{16}$ we must have an automorphism $\sigma_{(a,3)}$ in G, to be precise: $\sigma_{(a,3)}(\sqrt[16]{2}) = \zeta_{16}^a \cdot \sqrt[16]{2}$ and $\sigma_{(a,3)}(\zeta_{16}) = \zeta_{16}^3$.

Suppose a is even. Then we can make it vanish since we have $\sigma_{(2,1)} \in G$, so we find an automorphism σ fixing $\sqrt[16]{2}$ and sending ζ_{16} to ζ_{16}^3. But then σ sends $\zeta_8 + \overline{\zeta_8}$ to $\zeta_8^3 + \overline{\zeta_8}^3$, i.e., it sends $\sqrt{2}/2$ to $-\sqrt{2}/2$, so σ cannot fix $\sqrt[16]{2}$, a contradiction. This shows that a was odd, so as above we can suppose $a = 1$. Now the only thing left to do is to check that $\sigma_{(2,1)}$ and $\sigma_{(1,3)}$ indeed leave k fixed, i.e., they leave $\sqrt{-2}$ fixed:

$$\sigma_{(2,1)}(\sqrt{-2}) = \sigma_{(2,1)}(\zeta_{16}^4 \cdot \sqrt[16]{2^8}) = \zeta_{16}^4 \cdot (\zeta_{16}^2)^8 \cdot \sqrt[16]{2^8} = \sqrt{-2},$$

$$\sigma_{(1,3)}(\sqrt{-2}) = \sigma_{(1,3)}(\zeta_{16}^4 \cdot \sqrt[16]{2^8}) = \zeta_{16}^{12}(\zeta_{16} \cdot \sqrt[16]{2})^8$$

$$= \zeta_{16}^{20} \cdot \sqrt[16]{2^8} = \sqrt{-2}. \qquad \text{Q.E.D.}$$

4.5. *Remark.* In the same setting one can find a transitive group $G \subset S_n$ and subgroups $N_1, N_2 \subset B = \mathrm{Perm}(S)$ such that the operations of G on N_i are essentially different, i.e., there is no G-invariant isomorphism between N_1 and N_2. By descent theory, this means that the two Hopf algebras H_i obtained from $N_i \subset B$ are not isomorphic over k; see the remark at the end of Section 3. Take $N_1 = C_{16} \subset S_{16}$ and N_2 generated by (1, 9), $G = C_{16} \ltimes M$. One checks that N_2 is also cyclic of order 16, but not G-isomorphic to N_1. We omit the details.

At the end of this section we now classify in detail all H-Galois extensions with small degrees, and we prove a theorem on the possible "size" of the normal closures of H-extensions. Let as always $K|k$ be separable, $G = \mathrm{Aut}(\tilde{K}|k)$, $G' = \mathrm{Aut}(\tilde{K}|k)$, and set $n = [K:k]$.

4.6. THEOREM. (a) *If $n = 2$, $K|k$ is (classically or) H-Galois.*

(b) *If $n = 3$, $K|k$ is H-Galois for appropriate H.*

(c) *If $n = 4$, $K|k$ is H-Galois for appropriate H.*

(*Comment*: *In* (b) *and* (c), *the notions H-Galois and "almost classically Galois" coincide.*)

(d) *If* $n = 5$, *either* $\#G \geqslant 60$ *and* $K|k$ *is not H-Galois or* $\#G \leqslant 20$ *and* $K|k$ *is H-Galois.* ($\#G \in \{21, \ldots, 59\}$ *does not happen.*)

Proof. Part (a) is clear. For the rest of the proof, let us assume that $K \neq \tilde{K}$, i.e., K is not classically Galois over k. We will always tacitly use the main theorem 2.1.

(b) $G = S_3$, and we may take $N = A_3$. (See also the Introduction.)

(c) $G \subset S_4$ is transitive, $\#G \in \{8, 12, 24\}$.

If $\#G = 12$ or 24, then $G \cong A_4$ and S_4 resp., and one can take $N = D_2$ (the four-group of Klein, alias the commutator group of S_4).

If $\#G = 8$, then G is a D_4 (since S_4 does not contain copies of the quaternion group or any 8-element abelian group), so $G = \langle \sigma, \tau \rangle$ with σ a 4-cycle and τ a transposition such that $\tau\sigma\tau = \sigma^{-1}$. Here one may take $N = \langle \sigma \rangle$ or $N = \langle \sigma^2, \sigma\tau \rangle$. (Compare Example 2.3 and the beginning of Section 2.)

(d) Assume $\#G \geqslant 60$. Then G is A_5 or S_5, and G has no transitive normal subgroups.

If $\#G < 60$, then $\#G \leqslant 24$ (there is no subgroup of index 3, 4,..., $n-1$ in S_n for $n \neq 4$ by [3, II5.3]). But $\#G = 24$ is impossible since $5 | G$, so we are left with $\#G \in \{10, 15, 20\}$. In all three cases the Sylow 5-subgroup of G is normal, and it has to be generated by a 5-cycle, so it is also regular and it serves as our N.

4.7. THEOREM. *Suppose* $K|k$ *is H-Galois. Then* $\#G \leqslant n \cdot n^{[\log_2 n]}$.

Proof. By 2.1 there is an n-element group N normalized by $G \subset S_n$. By 2.4.1, $\#G \leqslant \#\mathrm{Cent}_{S_n}(N) \cdot \#\mathrm{Aut}(N)$, and the first factor equals n by 2.4.2. N is generated by at most $[\log_2 n]$ elements as a group (exercise!), so $\#\mathrm{Aut}(N) \leqslant n^{[\log_2 n]}$.

Using this theorem and some easy estimates, one deduces:

4.8. COROLLARY. *Suppose* $n \geqslant 5$ *and* $G \cong S_n$ *or* A_n. *Then* $K|k$ *is not H-Galois for any H.*

5. THE SO-CALLED MAIN THEOREM OF GALOIS THEORY

Assume the field extension $K|k$ is H-Galois with respect to the k-Hopf algebra H. The main theorem of Galois theory in its general form says:

5.1. THEOREM [2, Theorem 7.6]. *If we define for a k-sub-Hopf algebra W of H*

$$\mathrm{Fix}(W) = \{x \in K \mid \mu(w)(x) = \varepsilon(w) \cdot x \text{ all } w \in W\},$$

then the map Fix:

$$\{W \subset H \text{ sub-Hopf algebra}\} \to \{E \mid k \subset E \subset k,\ E \text{ field}\}$$

is injective and inclusion-reversing.

Let us say that the main theorem holds in its *strong form* if Fix is also surjective. This is the classical situation (we are completely ignoring the classical statements concerning normal subgroups and intermediate Galois extensions). Now we get some justification for our notion of an almost classical Galois extension:

5.2. THEOREM. *If $K|k$ is almost classically Galois, then there is a Hopf algebra H such that $K|k$ is H-Galois and the main theorem holds in its strong form.*

Proof. Let as always $\tilde{K}$ be the normal closure of $K|k$, $G = \mathrm{Aut}(\tilde{K}|k)$, $G' = \mathrm{Aut}(\tilde{K}|K)$, and let $N \subset G$ be a normal complement of G'. We are in the same situation as in part (b) of the proof of 2.5. $N^{\mathrm{opp}} \subset B$ is constructed as in 2.4.2, and the form H of $k[N^{\mathrm{opp}}]$ is defined by the G-cocycle $\{p_g \mid g \in G\}$, $p_g =$ conjugation with g in B. (N^{opp} is indeed normalized by G; see the proof of 2.5.) We intend to show that domain and range of the map Fix have the same (finite) number of elements (this will prove surjectivity by 5.1). By general descent theory, the sub-Hopf algebras $W \subset H$ are in bijection with the set of subgroups $U \subset N^{\mathrm{opp}}$ stable under all p_g. Now $G = N \ltimes G'$ and N centralizes N^{opp}, so U is p_g-stable for all $g \in G$ iff U is p_h-stable for all $h \in G'$. Let us call these groups U "G'-stable" for short.

LEMMA. *There is a canonical bijection between the set of intermediate groups V, $G' \subset V \subset G$, and the set of G'-stable subgroups of N^{opp}.*

Proof of the Lemma. By the proof of 2.5, the operation of G' on N and N^{opp} is the same. So the second set in the lemma is in bijection with the set of G'-stable subgroups of N. To any V with $G' \subset V \subset G$ we associate $V \cap N \subset N$, and to a G'-stable group $U \subset N$ we associate $V(U) = U \ltimes G'$. It is then routine to check that these assignments are well-defined and mutally inverse.

End of the Proof of 5.2. Now we know that $\#\mathrm{dom}(\mathrm{Fix}) = \#\{W \subset H$ sub-Hopf algebra$\} = \#\{U \mid U \subset N\ G'$-stable$\} = \#\{V \mid G' \subset V \subset G\}$. By the

classical Galois theory, this last number equals $\#\{E \mid k \subset E \subset K, E \text{ field}\} = \#$ range(Fix). Q.E.D.

Remark. It is not very satisfying that this "Main Theorem in the Hopf Case" is proved in essence by reduction to the classical case. However, the theorems shows that the "almost classical Galois extensions" are still quite close to the classical case. Its proof demonstrates again the technique of Galois descent which reduces the property of being H-Galois to certain properties of the Galois group of the normal closure.

Theorem 5.2. prompts the question: What happens if we chose "the wrong H"? We recall the construction of 2.5. What happens if we take N in the place of N^{opp} in the construction? We only deal with the case $N = G$, i.e., $K \mid k$ is classically Galois. Then N is trivially normalized by G (not necessarily centralized), the cocycle $\{p_g \mid g \in G\}$ on N is just conjugation, and we get a form H' of $k[N]$. The sub-Hopf algebras W of H' correspond to p_g-invariant, i.e., normal subgroups U of N. So we know already: The image of Fix has the same cardinality as the set of Galois extensions E between K and k. But actually these two sets are equal. In order to show this, let H'_U be the sub-Hopf algebra of H' which belongs to $U \lhd N$. We claim $\text{Fix}(H'_U) = \text{Fix}(U) \subset K$. Set $E = \text{Fix}(U)$. We tensor from the left with $\tilde{K} = K$ (retaining the $\tilde{}$ for clarity) and obtain

$$\begin{array}{ccccc} \tilde{K}[U] \otimes_{\tilde{K}} \tilde{K}^S \subset & & \tilde{K}[N] \otimes_{\tilde{K}} \tilde{K}^S & \xrightarrow{\mu} & \tilde{K}^S \\ \| & & \| & & \| \\ (\tilde{K} \otimes H'_U) \otimes_{\tilde{K}} (\tilde{K} \otimes K) \subset & & (\tilde{K} \otimes H'_U) \otimes_{\tilde{K}} (\tilde{K} \otimes K) & \longrightarrow & (\tilde{K} \otimes K) \end{array}$$

$\tilde{K} \otimes H'_U$ corresponds under the vertical isomorphism to $\tilde{K}[U]$. So $\tilde{K} \otimes \text{Fix}(H'_U) = \text{Fix}(\tilde{K} \otimes H'_U)$ is the subalgebra of $\tilde{K} \otimes K$ which corresponds to the subalgebra $\text{Fix}_\mu(\tilde{K}[U]) = \{x \in \tilde{K}^S \mid \text{For all } u \in U,\ \mu(u)(x) = x\}$ under the vertical isomorphism. Let E' be the image of $\tilde{K} \otimes E$ in $\tilde{K}^S$. Now it will be enough to show $E' = \text{Fix}(\tilde{K}[U])$ (since by faithful flatness this implies $E = \text{Fix}(H'_U)$). By reasons of dimension, it suffices to show $E' \subset \text{Fix}(\tilde{K}[U])$. Take $x \in E$ and its image $\tilde{x} = \sum g(x) e_g$ in $\tilde{K}^S$. U permutes the e_g, i.e., for $u \in U$ we have $\mu(u)(\tilde{x}) = \sum g(x) e_{ug}$. This is equal to x iff $g(x) = ug(x)$ for all $u \in U$, but this is true since U is normal and U leaves x fixed. Let us sum this up in our final result:

5.3. THEOREM. *Any Galois extension $K \mid k$ can be endowed with an H-Galois structure such that the following variant of the Main Theorem holds: There is a canonical bijection between sub-Hopf algebras of H and* normal *intermediate fields $k \subset E \subset K$.*

This (and earlier results) shows that in the construction of Hopf Galois extensions there is a certain arbitrariness, in contrast to the classical case, where the Galois group always comes with the field.

REFERENCES

1. S. U. CHASE, D. K. HARRISON, AND A. ROSENBERG, Galois theory and Galois cohomology of commutative rings, *Mem. Amer. Math. Soc.* **52** (1965), 15–33.
2. S. U. CHASE AND M. SWEEDLER, "Hopf Algebras and Galois Theory," Lecture Notes in Mathematics, Vol. 97, Springer-Verlag, New York/Berlin.
4. M.-A. KNUS AND M. OJANGUREN, "Théorie de la descente et algèbres d'Azumaya," Lecture Notes in Mathematics, Vol. 389, Springer-Verlag, New York/Berlin.
5. M. SWEEDLER, "Hopf Algebras," Benjamin, New York, 1969.
6. A. NAKAJIMA, *P*-polynomials and *H*-Galois extensions, preprint, 1984.