TOPICS IN ALGEBRA
BANACH CENTER PUBLICATIONS, VOLUME 26, PART 1
PWN POLISH SCIENTIFIC PUBLISHERS
WARSAW 1990

# FORMS OF HOPF ALGEBRAS AND GALOIS THEORY

BODO PAREIGIS

*Mathematisches Institut der Universität München, München, F.R.G.*

The theory of Hopf algebras is closely connected with various applications, in particular to algebraic and formal groups. Although the first occurrence of Hopf algebras was in algebraic topology, they are now found in areas as remote as combinatorics and analysis. Their structure has been studied in great detail and many of their properties are well understood. We are interested in a systematic treatment of Hopf algebras with the techniques of forms and descent.

The first three sections of this paper give a survey of the present state of the theory of forms of Hopf algebras and of Hopf Galois theory, especially for separable extensions. It includes many illustrating examples some of which cannot be found in detail in the literature. The last two sections are devoted to some new or partial results on the same field. There we formulate some of the open questions which should be interesting objects for further study. We assume throughout most of the paper that $k$ is a base field and do not touch upon the recent beautiful results of Hopf Galois theory for rings of integers in algebraic number fields as developed in [C1].

## I. Hopf algebra forms

As a first example of the occurrence of a Hopf algebra let us consider the units functor. In the sequel let $k$ be a commutative, associative ring with unit. Later on it will be a field, in particular the field of rationals or reals. Let $k$-$\mathscr{A}lg$ denote the category of commutative $k$-algebras and $\mathscr{G}rp$ the category of groups. Then there is an important functor

$$U\colon\ k\text{-}\mathscr{A}lg \to \mathscr{G}rp,$$

---

This paper is in final form and no version of it will be submitted for publication elsewhere.
I tank the referee for valuable suggestions to improve the style of this paper.

the *units functor*, which associates with each $k$-algebra its group of invertible elements or units. This functor is representable by the $k$-algebra $k[x, x^{-1}] = k\mathbf{Z}$, the group ring of the infinite cyclic group $\mathbf{Z}$, i.e.

$$U(A) \cong k\text{-}\mathscr{A}lg(k[x, x^{-1}], A).$$

The multiplication of the units group $U \times U \to U$ induces a commutative diagram

$$\begin{array}{ccc} U(A) \times U(A) & \to & U(A) \\ \downarrow & & \downarrow \\ k\text{-}\mathscr{A}lg(k[x, x^{-1}] \otimes k[x, x^{-1}], A) & \to & k\text{-}\mathscr{A}lg(k[x, x^{-1}], A) \end{array}$$

with vertical arrows isomorphisms. By the Yoneda Lemma the bottom horizontal arrow induces a comultiplication on the representing $k$-algebra

$$\Delta\colon k[x, x^{-1}] \to k[x, x^{-1}] \amalg k[x, x^{-1}] = k[x, x^{-1}] \otimes k[x, x^{-1}],$$

defined by $\Delta(x) = x \otimes x$. Observe that the tensor product of commutative algebras is the coproduct in $k$-$\mathscr{A}lg$. Also the inverse inv: $U \to U$ and the neutral element $\{\cdot\} \to U$ define corresponding maps on the representing algebra. All in all we obtain the structure of a Hopf algebra on the algebra $k[x, x^{-1}]$.

DEFINITION. A $k$-algebra $H$ together with $k$-algebra homomorphisms

$$\Delta\colon H \to H \otimes H, \quad \sigma\colon H \to H, \quad \varepsilon\colon H \to k$$

is called a *Hopf algebra* if $H$ together with $\Delta$ and $\varepsilon$ is a coalgebra and if $\sigma$ satisfies the following commutative diagrams:

$$\begin{array}{ccccc} H & \xrightarrow{\varepsilon} & k & \xrightarrow{\eta} & H \\ {\scriptstyle\Delta}\downarrow & & & & \uparrow{\scriptstyle\nabla} \\ H \otimes H & & \xrightarrow{\sigma\otimes 1 \;(1\otimes\sigma)} & & H \otimes H \end{array}$$

Here the map $\nabla\colon H \otimes H \to H$ denotes the multiplication $\nabla(a \otimes b) := ab$ of the algebra $H$ and $\eta\colon k \to H$ is defined by $\eta(a) := a \cdot 1_H$, the canonical map from $k$ into $H$.

The map $\Delta\colon H \to H \otimes H$ is called the *diagonal* or *comultiplication* on $H$. It is awkward to write the images as tensors in the usual way, especially if composites of such maps occur. The following simplified notation has been introduced by Sweedler. For a linear map $f\colon A \to B \otimes C$ we define $\sum a_{(B)} \otimes a_{(C)} := f(a)$ or in the special case of a Hopf algebra $(H, \Delta, \varepsilon)$ we write $\sum h_{(1)} \otimes h_{(2)} := \Delta(h)$. The advantage of this notation is that it can be extended to bilinear maps along the following example. If $g\colon B \times C \to D$ is a bilinear map with induced map $\hat{g}\colon B \otimes C \to D$ on the tensor product, then we can define $\sum g(a_{(B)}, a_{(C)}) := \hat{g}(f(a))$ and thus use the "components" $a_{(B)}$ and $a_{(C)}$ as if they were well-defined ordinary elements, which can be used as arguments in bilinear maps.

Similar to the Hopf algebra $k[x, x^{-1}]$ each commutative (as an algebra) Hopf algebra $H$ represents a functor

$$\tilde{H}\colon k\text{-}\mathscr{A}lg \to \mathscr{G}rp, \qquad \tilde{H}(A) := k\text{-}\mathscr{A}lg(H, A),$$

where the multiplication on $\tilde{H}$ is given by the commutative diagram

$$\begin{array}{ccc} \tilde{H}(A)\times\tilde{H}(A) & \to & \tilde{H}(A) \\ \downarrow & & \downarrow \\ k\text{-}\mathscr{A}lg(H\otimes H, A) & \to & k\text{-}\mathscr{A}lg(H, A) \end{array}$$

So the group ring $k\mathbf{Z}$ has been seen to be a Hopf algebra with the diagonal $\Delta(g) = g\otimes g$ for $g$ in $\mathbf{Z}$. This holds not only for the group $\mathbf{Z}$. Every group ring $kG$ is a Hopf algebra with the same comultiplication, even for noncommutative groups $G$. The noncommutative group rings, however, do not any more represent group-valued functors on $k$-$\mathscr{A}lg$. They are special instances of formal groups.

Another concrete example of a group-valued functor is

$$C\colon k\text{-}\mathscr{A}lg \to \mathscr{G}rp,$$

the *circle group*, defined by $C(A) := \{(a, b)\in A\times A \mid a^2+b^2 = 1\}$. The group structure is given by $(a, b)*(c, d) := (ac-bd, ad+bc)$. The representing Hopf algebra is the "trigonometric algebra" $H = k[c, s]/(c^2+s^2-1)$. The diagonal is defined by

$$\Delta(c) = c\otimes c - s\otimes s, \qquad \Delta(s) = c\otimes s + s\otimes c.$$

The most interesting observation is this. Let $A$ be a commutative $k$-algebra with 2 invertible and containing $i = \sqrt{-1}$. Then the assignment

$$U(A)\ni a \mapsto \left(\frac{1}{2}(a+a^{-1}), \frac{1}{2i}(a-a^{-1})\right)\in C(A)$$

defines a functorial isomorphism of groups. If $2^{-1}, i\in k$ then $U$ and $C$ are isomorphic group-valued functors, hence they have isomorphic representing Hopf algebras

$$k[x, x^{-1}] \cong k[c, s]/(c^2+s^2-1).$$

If $i\notin k$ then the two group-valued functors are not isomorphic, neither are their representing Hopf algebras $k[x, x^{-1}]$ and $k[c, s]/(c^2+s^2-1)$.

If $k$ is a field of characteristic $\neq 2$ and $i\notin k$, then $U$ and $C$ are nonisomorphic but they induce isomorphic functors $U|_{k(i)}$ and $C|_{k(i)}$ if restricted to the $k(i)$-algebras. Let $K = k(i)$ and let $A$ be a $K$-algebra. Then we have

$$\begin{aligned} K\text{-}\mathscr{A}lg(K\otimes k[x, x^{-1}], A) &\cong k\text{-}\mathscr{A}lg(k[x, x^{-1}], A) \\ &\cong U|_K(A) \cong C|_K(A) \\ &\cong k\text{-}\mathscr{A}lg(k[c, s]/(c^2+s^2-1), A) \\ &\cong K\text{-}\mathscr{A}lg(K\otimes k[c, s]/(c^2+s^2-1), A), \end{aligned}$$

hence $K \otimes k[x, x^{-1}] \cong K \otimes k[c, s]/(c^2+s^2-1)$ as $K$-Hopf algebras, where the tensor product is always taken over the base ring $k$. Observe that a cancellation property cannot be expected in this case.

In particular, the $\mathbf{Q}$-Hopf algebras $\mathbf{Q}[x, x^{-1}]$ and $\mathbf{Q}[c, s]/(c^2+s^2-1)$ and the $\mathbf{R}$-Hopf algebras $\mathbf{R}[x, x^{-1}]$ and $\mathbf{R}[c, s]/(c^2+s^2-1)$ are not isomorphic, but the $\mathbf{C}$-Hopf algebras $\mathbf{C}[x, x^{-1}] \cong \mathbf{C}[c, s]/(c^2+s^2-1)$ are. This is an example for the next definition.

DEFINITION. Let $G$ and $G'$ be group-valued functors on $k$-$\mathscr{A}lg$. Let $K$ be a faithfully flat commutative $k$-algebra. If the restrictions to $K$-$\mathscr{A}lg$ are isomorphic group-valued functors: $G|_K \cong G'|_K$, then $G$ and $G'$ are called *$K$-forms* of each other as groups.

Let $H$ and $H'$ be Hopf algebras over the commutative ring $k$. Let $K$ be a faithfully flat commutative $k$-algebra. If $K \otimes H \cong K \otimes H'$ as $K$-Hopf algebras, then $H$ and $H'$ are called *$K$-forms* of each other as Hopf algebras.

We say that $G$ and $G'$ resp. $H$ and $H'$ are *forms* of each other if there exists a faithfully flat $k$-algebra $K$ such that they are $K$-forms of each other.

So for $G$ and $G'$ to be $K$-forms of each other we need an isomorphism of set-valued functors $\alpha$: $G|_K \to G'|_K$ such that

$$\begin{array}{ccc} G|_K \times G|_K & \xrightarrow{\alpha\times\alpha} & G'|_K \times G'|_K \\ \downarrow & & \downarrow \\ G|_K & \xrightarrow{\alpha} & G'|_K \end{array}$$

commutes.

There may be many different Hopf algebras $H'$ which are forms for $H$ with respect to some faithfully flat extension $K$. In particular, the richness of Hopf algebras over $\mathbf{Q}$ should be higher than over $\mathbf{C}$. Granted there may be Hopf algebras defined over $\mathbf{C}$, which do not come about by a base ring extension from $\mathbf{Q}$, but e.g. semisimple cocommutative Hopf algebras over $\mathbf{C}$ are always defined over $\mathbf{Q}$. This is a consequence of a more general structure theorem of Milnor, Moore and Cartier on cocommutative Hopf algebras over algebraically closed fields. Our interests are in this richness of Hopf algebras over "small" fields. One can show for example that over the field $\mathbf{R}$ of reals the circle functor $C$ is the only nontrivial form of the units functor $U$.

There is a description of $K$-forms for quite general algebraic structures given by the theory of faithfully flat descent. We apply it to the case of Hopf algebras. Let $H$ be a Hopf algebra over $k$. The automorphism group of this Hopf algebra will be denoted by $k$-$\mathscr{H}opf$-Aut$(H)$. After a base ring extension by $k \to K$ we get a Hopf algebra $K \otimes H$ over $K$ with automorphism group $K$-$\mathscr{H}opf$-Aut$(K \otimes H)$. Every change of the base ring extension, i.e. every homomorphism of commutative $k$-algebras $K \to L$ induces a group homomorphism $K$-$\mathscr{H}opf$-Aut$(K \otimes H) \to L$-$\mathscr{H}opf$-Aut$(L \otimes H)$. Thus we have a functor $\mathbf{Aut}(H)$: $k$-$\mathscr{A}lg \to \mathscr{G}rp$ defined by $\mathbf{Aut}(H)(K) :=$ $K$-$\mathscr{H}opf$-Aut$(K \otimes H)$. Every

group-valued functor on the category $k$-$\mathcal{A}lg$ of commutative $k$-algebras has an associated Amitsur cohomology $H^n(K/k, \mathbf{Aut}(H))$. It is not necessary to know the precise definition of these cohomology groups to apply the following theorem.

THEOREM 1.1. *Let $H$ be a $k$-Hopf algebra. Then there is a bijection between the set of (isomorphism classes of) $K$-forms of $H$ and the Amitsur cohomology group $H^1(K/k, \mathbf{Aut}(H))$.*

Proofs of this may be found in various forms in [G], [H], or [KO]. Actually, this theorem holds in greater generality and the proof is quite technical and involved.

In view of this theorem the main problem of calculating forms is to determine the set of Hopf algebra automorphisms of a Hopf algebra. In fact, we do not have to calculate the cohomology group, since by a twofold application of this theorem—going from certain forms to the cohomology group and then from the same cohomology group back to some other forms—we will eliminate the explicit computation of the cohomology.

In the case of group rings $kG$ of finitely generated groups $G$ the automorphism group $k$-$\mathcal{H}opf$-Aut$(kG)$ can be calculated, in particular for cyclic groups $C_n$ of order $n$. We assume that the automorphism group $F$ of $G$ is finite. Then one can show that $k$-$\mathcal{H}opf$-Aut$(kG)$ is isomorphic to the automorphism group $\mathcal{G}al$-Aut$(E_k^F)$ of the trivial $F$-Galois extension $E_k^F$ of $k$. This Galois extension can be described by the ring $E_k^F = (kF)^*$, the dual space of the group ring $kF$, on which $F$ acts by automorphisms in such a way that the ring extension $(kF)^*/k$ is an $F$-Galois extension in the sense of [CHR]. Actually, this leads to a functorial isomorphism $\mathbf{Aut}(kG) \cong \mathcal{G}al$-$\mathbf{Aut}(E^F)$, so that the Amitsur cohomology groups of these two group functors also coincide.

We formulate one of the most interesting consequences of these considerations.

THEOREM 1.2 [HP]. *Let $k$ be a commutative ring with 2 not a zero divisor in $k$ and $\mathrm{Pic}_{(2)}(k) = 0$, the two-torsion of the Picard group. Then*

(a) *the Hopf algebra forms of $k\mathbf{Z}$ are*

$$H = k[c, s]/(s^2 - asc - bc^2 + u),$$

(b) *the Hopf algebra forms of $kC_3$ are*

$$H = k[c, s]/(s^2 - asc - bc^2 + u, (c+1)(c-2), (c+1)(s-a)),$$

(c) *the Hopf algebra forms of $kC_4$ are*

$$H = k[c, s]/(s^2 - asc - bc^2 + u, c(ac - 2s)),$$

(d) *the Hopf algebra forms of* $kC_6$ *are*

$$H = k[c, s]/(s^2 - asc - bc^2 + u,\ (c-2)(c-1)(c+1)(c+2),\ (c-1)(c+1)(sc-2a)).$$

*In all cases* $a, b, u \in k$ *satisfy* $a^2 + 4b = u$ *and* $u$ *is a unit in* $k$. *The Hopf algebra structure in all cases is defined by*

$$\Delta(c) = u^{-1}((a^2+2b)c \otimes c - a(c \otimes s + s \otimes c) + 2c \otimes s),$$
$$\Delta(s) = u^{-1}(-abc \otimes c + 2b(c \otimes s + s \otimes c) + as \otimes s),$$
$$\varepsilon(c) = 2, \quad \varepsilon(s) = a, \quad \sigma(c) = c, \quad \sigma(s) = ac - s.$$

We give an indication of the way how this result is obtained. In all cases of the theorem the group $F$ is the cyclic group with two elements. The theory of $C_2$-Galois extensions (= quadratic Galois extensions) is well known. Actually, every quadratic Galois extension of $k$ is a form of the trivial quadratic Galois extension $(kC_2)^* \cong k \times k$ of $k$ as will be seen below. Since the automorphism groups $\mathbf{Aut}(kG) \cong \mathscr{G}al\text{-}\mathbf{Aut}(k \times k)$ coincide, the first Amitsur cohomology groups describing the forms coincide, too. So there is a bijective correspondence between the forms of the group rings in the theorem and the quadratic Galois extensions of $k$ [see Thm. 4.1]. This correspondence was used to explicitly calculate the forms given in the theorem.

## II. Hopf Galois extensions

A different class of "forms" is obtained if one considers the following cancellation problem.

DEFINITION. Let $G$: $k\text{-}\mathscr{A}lg \to \mathscr{G}rp$ be a group-valued functor. Then the multiplication of $G$ on itself $G \times G \to G$ makes $G$ a $G$-set-valued functor. Here we define the functor $G \times G$ by $(G \times G)(K) := G(K) \times G(K)$, so that the multiplication of each group $G(K)$ defines a functorial homomorphism $G \times G \to G$, briefly the multiplication on $G$, and the $G$-set structure is defined "componentwise".

Let $X$: $k\text{-}\mathscr{A}lg \to \mathscr{S}et$ be another functor which is also a $G$-set-valued functor by $X \times G \to X$. Let $K$ be a faithfully flat commutative ring extension of $k$. If the restrictions $G|_K$ and $X|_K$ to $K\text{-}\mathscr{A}lg$ are isomorphic as $G|_K$-set-valued functors, then $G$ and $X$ are called *$K$-forms* of each other as $G$-set-valued functors.

So for $G$ and $X$ to be $K$-forms of each other we need an isomorphism of set-valued functors $\alpha$: $G|_K \to X|_K$ such that

$$\begin{array}{ccc} G|_K \times G|_K & \xrightarrow{\alpha \times 1} & X|_K \times G|_K \\ \downarrow & & \downarrow \\ G|_K & \xrightarrow{\alpha} & X|_K \end{array}$$

commutes.

A Hopf-algebraic description of this is somewhat more complicated. The notions of a $G$-set and of forms of a $G$-set translated to the representing objects of the representable functors $G$ and $X$ give the following definition.

DEFINITION. Let $H^*$ be a commutative Hopf algebra and let $A$ be a commutative algebra. $A$ is called an *$H^*$-comodule algebra* if there is an algebra map $\chi\colon A \to A \otimes H^*$ such that the diagrams

$$\begin{array}{ccc} A & \xrightarrow{\iota} & A \otimes H^* \\ {\scriptstyle\chi}\downarrow & & \downarrow{\scriptstyle 1\otimes\Delta} \\ A \otimes H^* & \xrightarrow{\chi\otimes 1} & A \otimes H^* \otimes H^* \end{array} \qquad \text{and} \qquad \begin{array}{ccc} A & \xrightarrow{\iota} & A \otimes H^* \\ {\scriptstyle \mathrm{id}}\downarrow & & \downarrow{\scriptstyle 1\otimes\varepsilon} \\ A & \xleftarrow{\sim} & A \otimes k \end{array}$$

commute.

Let $H^*$ be a commutative Hopf algebra and let $A$ be a commutative $H^*$-comodule algebra. Let $K$ be a faithfully flat commutative ring extension of $k$. If $K \otimes H^* \cong K \otimes A$ as $K \otimes H^*$-comodule algebras, then $A$ is called a *$K$-form* of $H^*$.

Closely connected with $K$-forms of $G$-set-valued functors is the notion of a principal homogeneous space.

DEFINITION. If $G$ is a group and $X$ is a set, then a $G$-set $X$ is called *homogeneous* if for each pair $x, y \in X$ there exists a $g \in G$ such that $xg = y$. A $G$-set $X$ is *principal homogeneous* if $X$ is homogeneous and $xg = x$ for any $x \in X$ implies $g = e$.

It is easy to verify that a $G$-set $X$ is principal homogeneous iff the map $\varphi\colon X \times G \ni (x, g) \mapsto (x, xg) \in X \times X$ is bijective. This holds also in the case $X = \emptyset$. If $X \neq \emptyset$ then $X$ and $G$ are isomorphic as $G$-sets. These statements are easily rephrased in terms of functors.

The map $\varphi\colon X \times G \to X \times X$ which is defined for any $G$-set-valued functor $X$ induces the algebra homomorphism $\psi\colon A \otimes A \ni s \otimes t \mapsto \sum st_{(A)} \otimes t_{(H^*)} \in A \otimes H^*$ on the representing objects. $\varphi$ is an isomorphism iff $\psi$ is.

PROPOSITION 2.1. *Let $G$ be a representable group-valued functor and let $X$ be a representable $G$-set-valued functor on $k$-$\mathcal{A}lg$. Let the representing algebra $A$ of $X$ be faithfully flat. Then $G$ and $X$ are $K$-forms of each other as $G$-sets for some faithfully flat commutative $k$-algebra $K$ iff $X$ is a principal homogeneous space over $G$.*

*Proof.* We first remark the following. Let $X$ and $Y$ be representable functors, let $f\colon X \to Y$ be a natural transformation, and let $K$ be faithfully flat.

Assume that $f|_K\colon X|_K \to Y|_K$ is an isomorphism. Then $f$ is an isomorphism. This is due to the fact that the corresponding statement holds for the representing algebras.

Now let there be a natural isomorphism of $G|_K$-set-valued functors $\alpha\colon G|_K \to X|_K$. Then since $(X \times Y)|_K = X|_K \times Y|_K$ the following diagram commutes:

$$\begin{array}{ccc} (G \times G)|_K & \xrightarrow{\varphi|_K} & (G \times G)|_K \\ {\scriptstyle \alpha \times 1}\downarrow & & \downarrow{\scriptstyle \alpha \times \alpha} \\ (X \times G)|_K & \xrightarrow{\varphi|_K} & (X \times X)|_K \end{array}$$

Since $G|_K$ is a principal homogeneous space over $G|_K$ "componentwise", the top morphism is an isomorphism. So are the two vertical arrows. Thus the bottom arrow is an isomorphism. By the above argument $\varphi\colon X \times G \to X \times X$ is an isomorphism.

Conversely, if $\varphi\colon X \times G \to X \times X$ is an isomorphism, then in particular the induced $k$-algebra homomorphism $\psi\colon A \otimes A \ni s \otimes t \mapsto \sum st_{(A)} \otimes t_{(H^*)} \in A \otimes H^*$ of the representing algebras is an isomorphism. (Here we use the Sweedler notation in context with a bilinear map.) This is even an isomorphism of $A$-algebras. So we get for any $A$-algebra $B$

$$\begin{aligned} G|_A(B) &\cong k\text{-}\mathscr{A}lg(H^*, B) \cong A\text{-}\mathscr{A}lg(A \otimes H^*, B) \\ &\cong A\text{-}\mathscr{A}lg(A \otimes A, B) \cong k\text{-}\mathscr{A}lg(A, B) \cong X|_A(B). \end{aligned}$$

It is now easy to verify that this is an isomorphism of $G|_A$-set-valued functors.

The translation of the notion of principal homogeneous spaces into the language of Hopf algebras has a most interesting variation. Let $A$ be an $H^*$-comodule algebra. Assume now that $H^*$ is finitely generated and projective as a $k$-module and that $A$ is faithfully flat. The dual $H := \mathrm{Hom}_k(H^*, k)$ is a finitely generated projective cocommutative Hopf algebra which acts on $A$ by $h \cdot t = \sum t_{(A)} h(t_{(H^*)})$. Then the following holds:

THEOREM AND DEFINITION 2.2. *Under the above assumption the following are equivalent:*

(a) *$A$ is a Hopf Galois extension of $k$ with Hopf algebra $H$ (or simply $H$-Galois).*

(b) *$\psi\colon A \otimes A \ni s \otimes t \mapsto \sum st_{(A)} \otimes t_{(H^*)} \in A \otimes H^*$ is an isomorphism.*

(c) *There is a faithfully flat extension $K$ of $k$ with $K \otimes A \cong K \otimes H^*$ as $K \otimes H^*$-comodule algebras.*

(d) *$\delta\colon H \otimes A \ni h \otimes s \mapsto (t \mapsto \sum s(h \cdot t)) \in \mathrm{End}_k(A)$ is an isomorphism and $A$ is finitely generated faithful projective as a $k$-module.*

(e) *$k$ is the fix ring*

$$A^H := \{s \in A \mid \forall h \in H\colon\ h \cdot s = \varepsilon(h)s\}$$

*of $A$ under the action of $H$ and the rings $A^H$ and $A \# H$ are Morita equivalent.*

*Proof.* (a) A Hopf Galois extension is defined to be one of the equivalent conditions (b)–(e). (b) implies (c) with $K = A$. The equivalence of (b) and (c) is the preceding proposition. The equivalence between (b) and (d) is a simple calculation with dual bases for $H$ and $H^*$ and use of faithful flatness. (e) is essentially a translation of (d) in terms of Morita equivalences. Detailed proofs of this can be found in [P].

There are various different generalizations of Galois extensions. Noncommutative algebras with Hopf algebras acting on them have been investigated. Commutative algebras with finite groups acting on them have been studied in [CHR]. The definition used here has been introduced in [CS] and is also described in [S1]. Special instances of Galois extensions are included in this general concept.

Let $k$ be a field and $H = kG$ the group (Hopf) algebra of a finite group. Let $K$ be a field extension of $k$ which is $H$-Galois. Then $G$ acts by automorphisms on $K$. Furthermore, we have $k = \{s \in K \mid \forall g \in G\colon\ g(s) = s\} = K^G$. Since $[K\colon\ k] = |G|$ we deduce that $K$ is a "classical" Galois extension of $k$ with Galois group $G$. Conversely, if $K$ is a "classical" Galois extension of $k$ with Galois group $G$ then by Dedekind's lemma and (d) of the above theorem $K$ is Hopf Galois with Hopf algebra $H = kG$.

Jacobson's extension [J] of Galois theory to purely inseparable field extensions can be incorporated into the general framework of Hopf Galois theory in the following way. Jacobson uses restricted Lie algebras acting by derivations on purely inseparable field extensions of exponent one. The restricted universal enveloping algebras of the restricted Lie algebras are Hopf algebras and the action extends to a Hopf Galois action on the same extension. Details and an extension to a larger class of purely inseparable field extensions can be found e.g. in [S2] and [W].

The question arises which parts of the "classical" Galois theory can be transferred to Hopf Galois theory. The definition of a Hopf subalgebra $H' \subseteq H$ causes some problems on the coalgebra side. If we always assume, however, that $H'$ is a direct summand of $H$ as a $k$-module, these problems can be resolved. The fundamental theorem of Galois theory can be extended to

THEOREM 2.3 [CS]. *Let $K$ be Hopf Galois with Hopf algebra $H$. For $H'$ a Hopf subalgebra of $H$ let*

$$\mathrm{Fix}(H')\colon = \{x \in K \mid \forall h \in H'\colon\ h \cdot x = \varepsilon(h)x\}.$$

*Then*

$$\mathrm{Fix}\colon\ \{H' \subseteq H \mid H' \text{ Hopf subalgebra}\} \to \{L \mid k \subseteq L \subseteq K \text{ subalgebra}\}$$

*is injective and inclusion-reversing.*

We say that the fundamental theorem of Galois theory holds in its *strong form* if the map Fix is bijective. This, however, is not the case in general, as we

will see below. There is another deviation from the "classical" Galois theory. The Hopf algebra acting on a Galois extension $K$ of $k$ is not uniquely determined. Examples have been known for inseparable field extensions.

## III. Separable field extensions

We give an example of a separable field extension which is not Galois in the classical sense, but which is Hopf Galois with two different Hopf algebras. Let $K = \mathbf{Q}(\sqrt[4]{2})$ and $k = \mathbf{Q}$. It is well known that this is not a "classical" Galois extension. Let

$$H = \mathbf{Q}[c, s]/(c^2+s^2-1, cs)$$

with the coalgebra structure as given in part I. Abbreviate $\omega := \sqrt[4]{2}$. Then the operation of $H$ on $K$ is given by

| | 1 | $\omega$ | $\omega^2$ | $\omega^3$ |
|---|---|---|---|---|
| $c$ | 1 | 0 | $-\omega^2$ | 0 |
| $s$ | 0 | $-\omega$ | 0 | $\omega^3$ |

If $K = k(\sqrt[4]{2})$ were a classical Galois extension for example over the base field $\mathbf{Q}(i)$ then the Galois group is cyclic with generator $e$. Here the generator $e$ has been replaced by the two operators $c$ and $s$ which operate $k$-linearly and according to the rules

$$c(xy) = c(x)c(y)-s(x)s(y), \qquad s(xy) = s(x)c(y)+c(x)s(y).$$

Similarities with the trigonometric equalities are intended. If one extends the base field from $\mathbf{Q}$ to $\mathbf{Q}(i)$ then $(\mathbf{Q}(i)\otimes\mathbf{Q}(\sqrt[4]{2}))\colon \mathbf{Q}(i)$ becomes a classical Galois extension and the Hopf algebra $H$ is extended to the group ring $\mathbf{Q}C_4$. By further extending the base field to $\mathbf{Q}(i, \sqrt[4]{2})$ the ring extension $\mathbf{Q}(i, \sqrt[4]{2})\otimes\mathbf{Q}(\sqrt[4]{2})$ becomes isomorphic to the dual of the extended group algebra $(\mathbf{Q}(i, \sqrt[4]{2})C_4)^*$. This isomorphism is compatible with the comodule algebra structure. So we see that the original $H^*$-comodule algebra $K$ is a form of the trivial $H^*$-comodule algebra $H^*$.

One can show that there is a second Hopf algebra over $\mathbf{Q}$ and an action on $K = \mathbf{Q}(\sqrt[4]{2})$ such that the setup is a Hopf Galois extension. The Hopf algebra is

$$H = \mathbf{Q}[c, s]/(s^2-2c^2+2, cs)$$

with the action

| | 1 | $\omega$ | $\omega^2$ | $\omega^3$ |
|---|---|---|---|---|
| $c$ | 1 | 0 | $-\omega^2$ | 0 |
| $s$ | 0 | $\omega^3$ | 0 | $-2\omega$ |

The maps $c$ and $s$ are $k$-linear and satisfy the multiplicative relations

$$c(xy) = c(x)c(y) - \tfrac{1}{2}s(x)s(y), \qquad s(xy) = c(x)s(y) + s(x)c(y).$$

To see that this gives a Hopf Galois extension one has to extend the base field to $\mathbf{Q}(\sqrt{-2})$ and then proceed as above.

This is an example of a $k$-algebra which is a Hopf Galois extension with two different Hopf algebras. We will see below that this happens *very* often. Even the "classical" Galois extensions often have more than one Hopf algebra for which they are Hopf Galois. On the other hand, there are separable field extensions which are not Hopf Galois at all. The separable field extensions which are Hopf Galois can be classified by the following theorem.

To formulate the theorem we fix the following notation. Let $K$ be a finite separable field extension of $k$. Assume

$\tilde{K}$ = normal closure of $K$ over $k$,

$G = \mathrm{Aut}(\tilde{K}/k)$,

$G' = \mathrm{Aut}(\tilde{K}/K)$,

$S = G/G'$ (left cosets),

$B = \mathrm{Perm}(S)$ (group of permutations of $S$).

THEOREM 3.1 [GP]. *Under the assumptions made above the following are equivalent*:

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

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

The examples given above are of a rather special type which we call "almost classical" Hopf Galois extensions. They are characterized by the following

THEOREM 3.2 [GP]. *The following conditions are equivalent*:

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

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

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

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

The last condition of this theorem shows that we are indeed talking about Hopf Galois extensions. These extensions are particularly well behaved because they satisfy the fundamental theorem of Galois theory in its strong form.

THEOREM 3.3 [GP]. *If $K/k$ is almost classically Galois, then there is a Hopf algebra $H$ such that $K/k$ is $H$-Galois and the map* Fix *is bijective.*

The ambiguity of the Hopf algebra acting on a Hopf Galois extension is exposed in the following

THEOREM 3.4 [GP]. *Any classical Galois extension $K/k$ can be endowed with an $H$-Galois structure such that the following variant of the fundamental theorem holds: There is a canonical bijection between Hopf subalgebras of $H$ and normal intermediate fields $k \subseteq E \subseteq K$.*

One of the simplest examples of a classical Galois extension with this new $H$-Galois structure is the following. Let $\zeta$ be a 3rd primitive root of unity and let $\omega := \sqrt[3]{2}$. Then $K = \mathbf{Q}(\omega, \zeta)$ is a classical Galois extension of $\mathbf{Q}$ with Galois group $S_3$. It is also Hopf Galois with Hopf algebra

$$H = \mathbf{Q}[c, s, t]/(c(c-1)(c+1),\ 2c^2+st+ts-2,\ cs,\ sc,\ ct,\ tc,\ s^2,\ t^2).$$

The action of $H$ on $K$ is described by the table

| | 1 | $\omega$ | $\zeta$ |
|---|---|---|---|
| $c$ | 1 | 0 | $\zeta^2$ |
| $s$ | 0 | $\omega^2$ | 0 |
| $t$ | 0 | 0 | 0 |

The action of the three generating elements $c, s, t$ on $K$ satisfies

$$c(xy) = c(x)c(y)+\tfrac{1}{2}s(x)t(y)+\tfrac{1}{2}t(x)s(y),$$

$$s(xy) = c(x)s(y)+s(x)c(y)+\tfrac{1}{2}t(x)t(y),$$

$$t(xy) = c(x)t(y)+t(x)c(y)+s(x)s(y).$$

We finish this section on separable field extensions which are Hopf Galois by giving a family of examples of separable field extensions which are not Hopf Galois: no field extension $K$ over $\mathbf{Q}$ of degree 5 with automorphism group $S_5$ of $\tilde{K}/k$ can be Hopf Galois [GP].

## IV. Hopf algebra forms revisited

Many of the following results have been obtained in cooperation and discussions with students and colleagues of mine. In particular, I gratefully acknowledge the cooperation of C. Greither, R. Haggenmüller, and C. Wenninger.

The techniques to prove Theorem 1.2 can be used to calculate more forms of group rings. The advantage in the proof of Theorem 1.2 was that all quadratic extensions of a commutative ring can be explicitly described if the ring satisfies only minor conditions [Sm]. If 2 is not a zero divisor in $k$ and if $\mathrm{Pic}_{(2)}(k) = 0$ then all quadratic extensions of $k$ are free and can be described as $K = k[x]/(x^2-ax-b)$ where $a^2+4b = u$ is a unit in $k$. The nontrivial

automorphism is $f(x) = a - x$. This information was translated into the language of Hopf algebra forms using the following

THEOREM 4.1 [HP]. *Let $G$ be a finitely generated group with finite automorphism group $F = \mathcal{G}rp\text{-}\mathrm{Aut}(G)$. Then there is a bijection between $\mathrm{Gal}(k, F)$, the set of isomorphism classes of $F$-Galois extensions of $k$, and $\mathrm{Hopf}(kG)$, the set of Hopf algebra forms of $kG$. This bijection associates with each $F$-Galois extension $K$ of $k$ the Hopf algebra*

$$H = \{\textstyle\sum c_g g \in KG \mid \forall f \in F\colon \sum f(c_g) f(g) = \sum c_g g\}.$$

*Furthermore, $H$ is a $K$-form of $kG$ by the isomorphism*

$$\omega\colon H \otimes K \cong KG, \quad \omega(h \otimes a) = ah.$$

On the other hand, it is not trivial to describe $F$-Galois extensions of a field $k$. They are not just the classical Galois field extensions of $k$. The simple example of the trivial $F$-Galois extension $k^F \cong k \times \ldots \times k$ is not a field. Actually, $F$-Galois extensions are just Hopf Galois extensions with Hopf algebra $kF$ [CHR, Thm. 1.3]. Arbitrary commutative rings $K$ are admitted as Galois extensions. The action of the group $F$ on the extension $K$ by different elements $f, f'$ has to be "strongly distinct", i.e. for every idempotent $e \in K$ there is an $x \in K$ such that $f(x)e \neq f'(x)e$. This is the key to the following

THEOREM 4.2. *Let $F$ be a finite group and $k$ a field. $K/k$ is an $F$-Galois extension if and only if*

$$K \cong L \times \ldots \times L \quad (n \text{ times})$$

*where $L/k$ is a $U$-Galois field extension with $U \subseteq F$ a subgroup of index $n$.*

*Proof.* Let $K/k$ be an $F$-Galois extension. $K$ is a commutative separable $k$-algebra by [CHR, Thm. 1.3], hence is a product $K \cong L_1 \times \ldots \times L_n$ of separable field extensions $L_i/k$. The automorphisms in $F$ map the primitive idempotents to primitive idempotents and $F$ operates transitively on the set of primitive idempotents, since the sum of idempotents in an orbit is in the fixed field. For any two idempotents $e_i$ and $e_j$ the automorphism $f$ of $F$ mapping $e_i$ to $e_j$ also maps $L_i$ to $L_j$. Hence $L_i$ is isomorphic to a subfield of $L_j$. By symmetry all the fields $L_i$ are mutually isomorphic. The stabilizer $U \subseteq F$ of $e_1$ acts as Galois group on $L_1/k$ since it acts strongly distinctly and $|U| = [L\colon k]$

Conversely, let $U \subseteq G$ be a subgroup and let $L\colon k$ be $U$-Galois. Let $g_1, \ldots, g_n$ be a set of representatives for $G/U = \{g_1 U, \ldots, g_n U\}$. Let $K = L \times \ldots \times L$ with idempotents $e_1, \ldots, e_n$. Define the action $\sigma\colon G \to S_n$ by $\sigma(g)(i) = j$ if $g g_i U = g_j U$, the regular representation of $G$ on $G/U$. We define $g(le_i) := g^{-1}_{\sigma(g)(i)} g g_i(l) e_{\sigma(g)(i)}$. Observe that $g g_i U = g_{\sigma(g)(i)} U$ implies $u_{g,i} := g^{-1}_{\sigma(g)(i)} g g_i \in U$. Then the fix ring of $K$ under the action of $G$ is $k$, for let $\sum l_i e_i \in K^G$. Then for all $g \in G$ we have $\sum u_{g,i}(l_i) e_{\sigma(g)(i)} = \sum l_i e_i$. For $g := g_i u g_i^{-1}$ we get $g g_i U = g_i U$, hence $\sigma(g)(i) = i$ and $u_{g,i} = g_i^{-1} g_i u g_i^{-1} g_i = u$, so that

$u(l_i) = l_i$ for all $u \in U$, hence $l_i \in k$. For $g := g_j g_i^{-1}$ we get $gg_iU = g_jU$, hence $\sigma(g)(i) = j$ and $u_{g,i} = g_j^{-1} g_j g_i^{-1} g_i = \mathrm{id}$, so that $l_i e_j = l_j e_j$, hence $l_i = l_j$ for all $i, j$. This shows $\sum l_i e_i = \lambda \sum e_i = \lambda \in k$. Obviously all elements of $k$ remain fixed under the action of $G$ so that $k = K^G$. Furthermore, $K$ is separable by definition.

To show that $G$ operates strongly distinctly it suffices to find for every $g \in G$, $g \neq \mathrm{id}$, and $e_i \in K$ an $x \in K$ such that $g(x)e_i \neq xe_i$. Assume first that $\sigma(g)(i) \neq i$. Choose $x = e_i$. Then $g(e_i)e_i = e_{\sigma(g)(i)}e_i = 0 \neq e_i = e_i e_i$. If $\sigma(g)(i) = i$ then $g_i^{-1} g g_i \in U$ and $u \neq \mathrm{id}$ since $g \neq \mathrm{id}$. Choose an $l \in L$ with $u(l) \neq l$ and $x = le_i$. Then

$$g(x)e_i = g(le_i)e_i = g_i^{-1} g g_i(l) e_i u(l) e_i \neq le_i = le_i e_i = xe_i.$$

This concludes the proof.

Observe by the way that $kC_2$ has no nontrivial forms, since $C_2$ has trivial automorphism group, so the corresponding Galois extension of a form must be $k$ itself. Already the next simplest cases after studying the forms of $k\mathbf{Z}$, $kC_3$, $kC_4$, and $kC_6$ cause unsatisfactory calculations. We discuss the case of $\mathbf{Q}C_5$.

The automorphism group of $C_5$ is $C_4$ which has exactly one nontrivial subgroup $C_2$. The $C_4$-Galois extensions $K$ of $\mathbf{Q}$ can be of the following forms:

1) $K$ is a $C_4$-Galois field extension of $\mathbf{Q}$,
2) $K \cong L \times L$ where $L$ is a quadratic field extension of $\mathbf{Q}$,
3) $K \cong \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q}$.

The problem is now to describe as explicitly as possible all $C_2$- resp. $C_4$-Galois field extensions $K$ of $\mathbf{Q}$, to describe the action of $C_4$ on $K$ and then calculate the forms according to Theorem 4.1. Associated with a $C_4$-Galois field extension $K$ is the following form of $\mathbf{Q}C_5$:

$$H \cong \mathbf{Q}[a]/\left(a^5 - 5pa^3 + (5(p^2 - 3q) - 10\sqrt{q(p^2 - 4q)})a\right).$$

Here $K$ is the splitting field of $x^4 + px^2 + q$ and $\sqrt{q(p^2 - 4q)} \in k$ necessarily holds if $K$ is a $C_4$-Galois field extension. The diagonal maps can be described by

$$\Delta(a) = \frac{1}{uv(u^2 - v^2)^2}\left((u^5 + v^5)(a \otimes a) - (u^3 + v^3)(a \otimes b + b \otimes a) + (u + v)(b \otimes b)\right),$$

where

$$u = \sqrt{\frac{-p + \sqrt{p^2 - 4q}}{2}}, \qquad v = \sqrt{\frac{-p - \sqrt{p^2 - 4q}}{2}}.$$

The case of $K \cong L \times L$ with quadratic extension $L/\mathbf{Q}$ is somewhat easier. We get

$$H \cong \mathbf{Q}[a]/(a^5 + 5p(a^3 + pa)) \quad \text{with} \quad \Delta(a) = u^{-1}(1, -1)(a \otimes a)$$

where $L = \mathbf{Q}(u)$ is the splitting field of $x^2 - p$.

Finally, the case of $K \cong \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q}$ leads to the trivial form $\mathbf{Q}C_5$.

Another simple example is that of forms of $\mathbf{Q}(C_2 \times C_2)$. The automorphism group of $C_2 \times C_2$ is the symmetric group $S_3$. Now we have to study the different cases of $S_3$-Galois extensions:

1) $K$ is an $S_3$-Galois field extension of $\mathbf{Q}$,
2) $K \cong L \times L$ where $L$ is a $C_3$-Galois field extension of $\mathbf{Q}$,
3) $K \cong L \times L \times L$ where $L$ is a quadratic field extension of $\mathbf{Q}$,
4) $K \cong \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q}$.

In the first and second cases we get

$$H = \mathbf{Q}[a]/(a(a^3 + ua + v))$$

where $K$ is the splitting field of $x^3 + ux + v$ irreducible. If $D = -4u^3 - 27v^2$ is the discriminant then

$$\Delta(a) = \frac{1}{D}\Big[-2u(3va \otimes a - u(a \otimes c + c \otimes a))$$

$$+ \frac{v}{2}(4u^2 b \otimes b + 9c \otimes c + 6u(b \otimes c + c \otimes b)) - 9v^2(a \otimes b + b \otimes a)\Big]$$

where

$$b = \frac{4}{v}a^3 + \frac{4u}{v}a + 3,$$

$$c = -\frac{4u}{v}a^3 + 2a^2 - \frac{4u^2}{v}a - 4u.$$

In the third case of $K \cong L \times L \times L$ we get

$$H = \mathbf{Q}[a]/((a^2 - 1)(a^2 - u))$$

where $L$ is the splitting field of $x^2 - u$ and the diagonal is

$$\Delta(a) = \frac{1}{u^2 - u}\left[(u^2 - u - 1)\, a \otimes a - a^3 \otimes a^3 + a^3 \otimes a + a \otimes a^3\right].$$

The case of $K \cong \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q}$ leads to the trivial form $\mathbf{Q}(C_2 \times C_2)$.

PROBLEMS. The generators of Hopf algebra forms and their diagonals are rather arbitrary. It often turns out that either the diagonal or the ideal to be factored out can be chosen to be relatively simple, but not both. Is there a canonical choice of the generators of a Hopf algebra form? ([1]) Is there a way

---

([1]) A complete answer to this question for the case of group rings has recently been given by the author in *Twisted group rings* submitted to Comm. Algebra.

to determine the minimal number of generators? Can one describe the "cyclic" Hopf algebra forms? This seems to be of interest for the representation theory of Hopf algebras, like cyclic groups are for the representation theory of groups.

Another problem area arises from the following considerations. Let $kC_n$ be the group algebra of a finite cyclic group and let $k$ be a field with $\mathrm{char}(k) \nmid n$. Then the group algebra is semisimple by Maschke's theorem. Let $K$ be a field extension of $k$ or a commutative separable algebra. Then every $K$-form $H$ of $kC_n$ is again semisimple, since a nilpotent ideal of $H$ would remain nilpotent in $K \otimes H \cong KC_n$ in both cases, but $KC_n$ is still semisimple. There may be forms which are even better in their representation properties as the example of part I shows.

The Hopf algebra $H = \mathbf{R}[c, s]/(c^2+s^2-1, cs)$ is a $\mathbf{C}$-form of $\mathbf{R}C_4$. It is easy to see that $H \cong \mathbf{R} \times \mathbf{R} \times \mathbf{R} \times \mathbf{R}$ as $\mathbf{R}$-algebras. Thus $H$ is absolutely semisimple, i.e. all its simple modules are one-dimensional over the base field. $\mathbf{R}C_4$, however, is not absolutely semisimple. It decomposes as $\mathbf{R}C_4 \cong \mathbf{R} \times \mathbf{R} \times \mathbf{C}$ as an algebra, so it has a two-dimensional simple module.

So there is the problem of determining which group algebras have absolutely semisimple forms, and of describing all those forms. If every semisimple group algebra had an absolutely semisimple form this would mean that one does not need to extend the base field of a group algebra $kG$ to obtain total splitting, but that the splitting can already be obtained over the base ring for a suitable form $H$. Since we are not talking about algebra forms but about Hopf algebra forms the possibility of tensoring $H$-modules over the base field—an important technique for representation theory—is preserved.

THEOREM 4.3. *If $k$ is a field of characteristic not dividing $n$, then the Hopf algebra $kC_n$ has a uniquely determined absolutely semisimple Hopf algebra form $k^{C_n} = (kC_n)^*$.*

*Proof.* Any absolutely semisimple form of $kC_n$ has underlying algebra $k^I$. But $k^I$ is a Hopf algebra iff $I$ is a finite group. After base field extension the group structure of $I$ remains unchanged, so there can be at most one group structure on $I$ and at most one Hopf algebra structure on $k^I$ so that $k^I$ is a form of $kC_n$. So an absolutely semisimple form of $kC_n$ is a Hopf algebra $k^G$ with a uniquely determined commutative group $G$ of order $n$. We show $G \cong C_n$ so that $k^{C_n}$ becomes the absolutely semisimple form of $kC_n$. It suffices to show this over a field $k$ containing an $n$th primitive root of unity. But then $kC_n$ splits completely and the statement is well known.

This unique absolutely semisimple form of $kC_n$ is associated with an $F$-Galois extension $K$ of with $F \cong \mathrm{Aut}(C_n)$. It turns out that $k[x]/(\varphi_n(x))$ is an $F$-Galois extension and is associated to $k^{C_n}$. $\varphi_n(x)$ is the $n$th cyclotomic polynomial. In general $k[x]/(\varphi_n(x))$ will not be a field extension of $k$. According to Theorem 4.2 and with some additional calculations one can see that $k[x]/(\varphi_n(x)) \cong k(\zeta_n) \times \ldots \times k(\zeta_n)$.

PROBLEMS. It would be interesting to know which group algebras over $\mathbf{Q}$ have absolutely semisimple forms. The Hopf algebra $\mathbf{Q}S_n$ is itself absolutely semisimple. There are also examples of groups $G$ whose group algebras have no absolutely semisimple forms.

## V. Separable Hopf Galois extensions

PROBLEMS. In part III we have seen examples of separable field extensions $K/k$ which are Hopf Galois. All the examples were in fact "almost classically" Galois. A 16-dimensional example of a Hopf Galois extension which is not "almost classically" Galois is given in [GP]. M. Takeuchi has checked that all Hopf Galois extensions of dimension less than 8 are "almost classically" Galois. The obvious question is: are there proper Hopf Galois extensions of dimension less than 16? Questions about the correspondence between "normal" Hopf subalgebras and Hopf Galois subfields have been addressed in [C2] Many of those questions are still open. Childs also addresses the question of the uniqueness of the Hopf algebra $H$ w.r.t. which a separable field extension is Hopf Galois. He obtains results for "classical" Galois field extensions. He shows that the Hopf algebra $H$ is never unique if $G$ is cyclic of odd prime power order. $H$ is never unique for nonabelian $G$. This needs a different proof, however, than given in [C2]. Childs also shows that $H$ is unique if $G$ is cyclic of prime order, a result which we will extend below.

Assume that we have the same setup $K/k$, $\tilde{K}/k$, $G$, $G'$, $S$, $B$ as in III. In [C2] the following result is shown.

PROPOSITION 5.1. *$G$ normalizes the regular subgroup $N$ of $B$ iff $G$ is a subgroup of the holomorph* $\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$.

We extend Theorem 2 of [C2] as follows:

THEOREM 5.2. *Let $K/k$ be a separable field extension of degree $[K:k] = p$ a prime. The following are equivalent:*

(1) *$K/k$ is Hopf Galois.*
(2) *$K/k$ is almost classically Galois.*
(3) *$G$ is solvable.*

*If any (and all) of these conditions hold then the Hopf algebra $H$ is unique for $K/k$ $H$-Galois.*

*Proof.* If $K/k$ is $H$-Galois then there is a regular subgroup $N$ of $S_p$ such that $G \subseteq \mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$, the holomorph of $N$. Since $N \cong C_p$ the holomorph $\mathrm{Hol}(N) \cong C_p \rtimes C_{p-1}$, hence $G$ is solvable.

Let $G$ be solvable. Since $K = k(a)$ with $a$ a zero of an irreducible polynomial $f$ of degree $p$, $G$ is a subgroup of $S_p$, hence $p \| |G|$ and $p^2 \nmid |G|$. Below

we show that for a solvable group $G$ there is a chain of normal subgroups of $G$ (!)

$$e \lhd \ldots \lhd G_2 \lhd G_1 \lhd G_0 = G$$

with $G_i/G_{i+1} \cong (\mathbf{Z}/p_i\mathbf{Z})^{e_i}$. Consider the sequence of subfields

$$k = k_0 \subset k_1 \subset \ldots \subset k_{m-1} \subset k_m = \tilde{K},$$

with $k_{i+1}/k_i$ Galois with Galois group $(\mathbf{Z}/p_i\mathbf{Z})^{e_i}$ and $k_{i+1}/k$ normal. We get $a \in k_m$ and $a \notin k_{m-1}$, otherwise $\tilde{K} \subseteq k_{m-1}$ since $k_{m-1}/k$ is normal. Then the minimal polynomial $f$ of $a$ is irreducible over $k_{m-1}$ by the last lemma. So all the $k$-generating elements $1, a, \ldots, a^{p-1}$ of $K$ are linearly independent over $k_{m-1}$. Thus $K$ and $k_{m-1}$ are linearly disjoint and $p_m = p$. Since $p^2 \nmid [\tilde{K}:k]$ and $p = p_m = [k_m : k_{m-1}]$ we get $k_{m-1} \otimes K \cong k_{m-1} \cdot K = k_m = \tilde{K}$. So by Theorem 3.2 the field extension $K/k$ is almost classically Galois.

To see that the Hopf algebra $H$ together with the Galois operation is uniquely determined, observe that $p \| |G|$ and $G \subseteq N \rtimes \mathrm{Aut}(N)$ and $N$ the only Sylow $p$-subgroup of $\mathrm{Hol}(N)$ imply that the Sylow $p$-subgroup of $G$ is $N$, which is unique. Thus $G = N \rtimes A$ with a subgroup $A \subseteq \mathrm{Aut}(N)$. Consequently $N = G_p \subseteq B$ is uniquely determined and so is $H$ by Theorem 3.1.

To finish the proof of the theorem we prove the following lemmas.

LEMMA 5.3. *Let $G$ be finite solvable group. Then there is a sequence*

$$e \lhd \ldots \lhd G_2 \lhd G_1 \lhd G_0 = G$$

*with $G_i/G_{i+1} \cong (\mathbf{Z}/p_i\mathbf{Z})^{e_i}$, $p_i$ prime and $G_i \lhd G$ normal subgroups.*

*Proof*: by induction. We only indicate how to construct $G_{i+1}$ from $G_i$. Let $M \lhd G_i$ be a normal subgroup of prime index $p_i$. Define $G_{i+1} := \bigcap_{g \in G} gMg^{-1}$. It has all the required properties.

LEMMA 5.4. *Let $K/k$ be a normal separable finite field extension. Let $f \in k[x]$ be separable and irreducible of degree $p$ a prime. Then either $f$ is irreducible over $K$ or $f$ completely splits into linear factors.*

*Proof.* Let $a_1, \ldots, a_p$ be the zeros of $f$ in the algebraic closure and let $G$ be the automorphism group of $K(a_1, \ldots, a_p)/k$. $G$ operates transitively on the zeros, since $f$ is irreducible. Let $N$ be the fix group of $K$. Since $K/k$ is normal, $N \lhd G$ is a normal subgroup. $N$ decomposes $\{a_1, \ldots, a_p\}$ into orbits of equal cardinality since $G$ operates transitively and $N$ is normal. So either $N$ operates transitively or trivially. Hence $f$ is irreducible or splits completely.

## References

[C1] L. Childs, *Taming wild extensions with Hopf algebras*, Trans. Amer. Math. Soc. 304 (1987), 111–140.

[C2] —, *On the Hopf Galois theory for separable field extensions*, Comm. Algebra, to appear.
[CHR] S. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and cohomology of commutative rings*, Mem. Amer. Math. Soc. 52 (1965).
[CS] S. Chase and M. Sweedler, *Hopf Algebras and Galois Theory*, Lecture Notes in Math. 97, Springer, 1969.
[GP] C. Greither and B. Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra 106 (1987), 239–258.
[G] A. Grothendieck, *Technique de descente I*, Sém. Bourbaki, exp. 190, 1959/60.
[H] R. Haggenmüller, *Über Invarianten separabler Galoiserweiterungen kommutativer Ringe*, Dissertation, Universität München, 1979.
[HP] R. Haggenmüller and B. Pareigis, *Hopf algebra forms of the multiplicative group and other groups*, Manuscripta Math. 55 (1986), 121–136.
[J] N. Jacobson, *An extension of Galois theory to non-normal and non-separable fields*, Amer. J. Math. 66 (1944), 1–29.
[KO] M.-A. Knus and M. Ojanguren, *Théorie de la Descente et Algèbres d'Azumaya*, Lecture Notes in Math. 389, Springer, 1974.
[P] B. Pareigis, *Descent theory applied to Galois theory*, technical report, Univ. California, San Diego 1986.
[Sm] C. Small, *The group of quadratic extensions*, J. Pure Appl. Algebra 2 (1972), 83–105, 395.
[S1] M. Sweedler, *Hopf Algebras*, Benjamin, New York 1969.
[S2] —, *Structure of purely inseparable extensions*, Ann. of Math. 87 (1968), 401–411.
[W] C. H. Wenninger, *Hopf-Galois Theorie einer Klasse rein inseparabler Körpererweiterungen*, Diplom Thesis, Universität München, 1984.