manuscripta mathematica

Volume 55 1986

Springer-Verlag Berlin Heidelberg New York Tokyo
Printers: Brühlsche Universitätsdruckerei, Giessen

Springer-Verlag GmbH & Co. KG, 1000 Berlin 33

Springer-Verlag Berlin Heidelberg New York Tokyo

Index

Covered by Zentralblatt für Mathematik and Current Mathematical Publications manuscripta math. 55, 121 - 136 (1986)

manuscripta mathematica

HOPF ALGEBRA FORMS OF THE MULTIPLICATIVE GROUP AND OTHER GROUPS

Rudolf Haggenmüller and Bodo Pareigis

The multiplicative group functor, which associates with each k-algebra its group of units, is affine with Hopf algebra $k[x,x^{-1}]$. The purpose of this paper is to determine explicitly all Hopf algebra forms of $k[x,x^{-1}]$ with only minor restrictions on k (2 not a zero-divisor and $Pic_{(2)}(k) = 0$). We also describe explicitly (by generators and relations) the Hopf algebra forms of kC_3 , kC_4 and kC_6 , where C_n is the cyclic group of order n . Some of our results could be drawn from [1,III §5.3.3] where a similar result as ours is indicated (and left as an exercise). We prefer however a less technical approach, in particular we do not use the extended theory of algebraic groups and functor sheaves.

The principal tool of this note is the theory of faithfully flat descent which is used to prove that the Hopf algebra forms of kG with finitely generated group G (with finite automorphism group F) are in one-to-one correspondence with the F-Galois extensions of k. The progress in recent years in describing the quadratic extensions of k and the explicit construction of the correspondence allow us to compute the forms of kG for all groups with $Aut(G) = C_2$ in terms of generators and relations.

Consider the functor $C\colon k\text{-}\mathcal{Alg}_c \longrightarrow \mathcal{Gr}$, the *circle functor*, defined by

$$C(A) = \{(a,b)\in A\times A \mid a^2+b^2=1\} \ .$$

The group structure is given by

$$(a,b)\cdot(c,d) = (ac-bd,ad+bc) \ .$$

The neutral element is $(1,0)$ and the inverse of (a,b) is $(a,-b)$. To understand this multiplication observe that C is represented by the k-algebra $H = k[c,s]/(s^2+c^2-1)$. This must be a Hopf algebra and is called the *trigonometric algebra*. The coalgebra structure of H is given by

$$\Delta(c) = c \otimes c - s \otimes s \qquad \Delta(s) = c \otimes s + s \otimes c$$
$$\varepsilon(c) = 1 \qquad \varepsilon(s) = 0 .$$

The antipode is $S(c) = c$, $S(s) = -s$.

Obviously c and s play the role of cos and sin resp. and the diagonal map reflects the summation formulas for cos and sin:

$$\cos(x + y) = \cos(x)\cos(y) - \sin(x)\sin(y)$$
$$\sin(x + y) = \cos(x)\sin(y) + \sin(x)\cos(y) .$$

ε gives the value at $0°$ and S is the reflection on the x-axis. The geometric meaning of the group structure on C(A) is the addition of the corresponding angles with the x-axis for the points (a,b) resp. (c,d) .

Let us now ask for a *group-like element* $e \neq 1$ in H , i.e. an element e with $\Delta(e) = e \otimes e$, $\varepsilon(e) = 1$. A little calculation shows that such an element exists if and only if there is $i \in k$ with $i^2 = -1$ and all the group-like elements are then of the form $(c + is)^n$, $n \in \mathbb{Z}$. Observe that $e^{-1} = c - is$, if $e = c + is$. The diagonal map on e reflects the summation formula for the exponential function $\exp(x + y) = \exp(x)\exp(y)$. If furthermore 2 is invertible in k then we get an isomorphism of Hopf algebras $k[c,s]/(s^2 + c^2 - 1) \simeq k\mathbb{Z}$ (where $1 \in \mathbb{Z}$ corresponds to $e = c + is$) because of $c = \frac{1}{2}(e + e^{-1})$, $s = \frac{1}{2i}(e - e^{-1})$. The affine k-group represented by $k\mathbb{Z} \simeq k[x,x^{-1}]$ is the *multiplicative group* or the group of units. Hence we have the following:

If A is a k-algebra over a commutative ring k with $2^{-1} \in k$ and $i \in k$, then the circle group C(A) is isomorphic to the multiplicative group U(A) . Moreover if $H = k[c,s]/(s^2 + c^2 - 1)$ is defined over a field k with $2 \neq 0$ and if $K = k[i]$, then $H \otimes_k K \simeq k\mathbb{Z} \otimes_k K$ as Hopf algebras. So we have two Hopf algebras H and $k\mathbb{Z}$ which after faithfully flat extension of the base ring become isomorphic. We say that H is a K-*form* of $k\mathbb{Z}$, the multiplicative group.

To describe all such forms we want to use the theory of faithfully flat descent. We sketch the main ideas following [3]. Let us discuss the general notions in two specific cases. Consider a directed graph s such as F-*gal* resp. *hopf* (see diagram below), which comes equipped with functors for all vertices $i \in \{0,1,2\}$ of the graph and all $L \in k\text{-}\mathcal{Alg}_c$:

$$F_i^L: L\text{-}Mod \longrightarrow L\text{-}Mod .$$

In our examples we take

$$F_0^L(N) = L \qquad F_1^L(N) = N \qquad F_2^L(N) = N \otimes_L N .$$

Observe that these functors are in general no additive functors. For $q: L \longrightarrow M$ in $k\text{-}\mathcal{Alg}_c$ there are coherent natural isomorphisms $\varphi_q: F_i^L(\ ) \otimes_L M \simeq F_i^M(\ \otimes_L M)$. These data will be called an *admissible structure* .

We define categories s_L (F-gal_L resp. $hopf_L$) in the following way. Objects will be $(K,\mathcal{K})$ in F-gal_L resp. $(H,\mathcal{H})$ in $hopf_L$ with $K, H \in L\text{-}Mod$ and $\mathcal{K}$: F-*gal* $\longrightarrow$ L-*Mod* resp. $\mathcal{H}$: *hopf* $\longrightarrow$ L-*Mod* graph maps such that $\mathcal{H}(i) = F_i^L(H)$. Morphisms are L-module homomorphisms which are "natural transformations" with respect to the graph maps.

Let F be a finite group with elements $f \in F$ then the above situation is represented by the diagram on the next page where the last part shows the properties of the functors F_i with respect to change of basis.

If $q: L \longrightarrow M$ is a change of basis morphism and $f: (A_L,\mathcal{A}_L) \longrightarrow (B_L,\mathcal{B}_L)$ is a morphism in s_L then $q^*(f)$ denotes the morphism $f \otimes_L M$ obtained by this change of basis.

	s:	F-gal:	$hopf$:
	$i \xrightarrow{\gamma} j$ F_i^L	$0 \xrightarrow{\eta} 1 \xleftarrow{\nabla} 2$ (f ↺ on 1) $F_i^L(N) = N \otimes_L \cdots \otimes_L N$ (i factors)	$0 \underset{\varepsilon}{\overset{\eta}{\rightleftarrows}} 1 \underset{\nabla}{\overset{\Delta}{\leftrightarrows}} 2$
L:	s_L: $F_i^L(N) \longrightarrow F_j^L(N)$	F-gal_L: $(K,\mathcal{K})\colon L \longrightarrow K \longleftarrow K \otimes_L K$ (f ↺ on K)	$hopf_L$: $(H,\mathcal{H})\colon L \rightleftarrows H \leftrightarrows H \otimes_L H$
M:	s_M: $F_i^M(N \otimes_L M) \longrightarrow F_j^M(N \otimes_L M)$ $\wr\!\wr\ \varphi_q \qquad\qquad \wr\!\wr\ \varphi_q$ $F_i^L(N) \otimes_L M \longrightarrow F_j^L(N) \otimes_L M$	F-gal_M: $(K_M,\mathcal{K}_M)\colon\ M \longrightarrow K \otimes_L M \longleftarrow (K \otimes_L M) \otimes_M (K \otimes_L M)$ $\wr\!\wr\ \varphi_q \qquad \wr\!\wr\ \varphi_q \qquad \wr\!\wr\ \varphi_q$ $(K,\mathcal{K})\circ M\colon L \otimes_L M \longrightarrow K \otimes_L M \longleftarrow (K \otimes_L K) \otimes_L M$	$hopf_M$: (similar)

called Amitsur complex. For a functor $G\colon k\text{-}\mathcal{Alg}_c \longrightarrow \mathcal{Gr}$ we define a 1-cocycle $\varphi \in G(L \otimes L)$ by the identity

$$d_2(\varphi) = d_3(\varphi)d_1(\varphi) \; .$$

φ is homologous to ψ if $\varphi = d_2(\pi)\psi d_1(\pi)^{-1}$ for some $\pi \in G(L)$. The pointed set of classes of 1-cocycles is $H^1(L/k,G)$. For $(B,\mathcal{B}) \in \mathcal{s}_k$ we shall use the functor $\mathcal{Aut}(B,\mathcal{B})$ for G, where $\mathcal{Aut}(B,\mathcal{B})(L) = \mathrm{Aut}_L(B_L,\mathcal{B}_L)$, the group of automorphisms of $(B_L,\mathcal{B}_L)$ in $\mathcal{s}_L$ (F-$\mathcal{gal}_L$ resp. $\mathcal{hopf}_L$). Now we can formulate the descent theorem.

THEOREM 1. *Let* L *be a faithfully flat* k-*algebra, let* $\mathcal{s}$ *be an admissible structure and let* $(B,\mathcal{B})$ *be in* $\mathcal{s}_k$. *Then there is a bijection between the set of* L-*forms* $\underline{\underline{S}}(L/k,(B,\mathcal{B}))$ *of* $(B,\mathcal{B})$ *and* $H^1(L/k,\mathcal{Aut}(B,\mathcal{B}))$. *The bijection is given in the following way: let the class of* $(C,\mathcal{C})$ *be an* L-*form of* $(B,\mathcal{B})$ *with isomorphism* $\omega\colon (C_L,\mathcal{C}_L) \cong (B_L,\mathcal{B}_L)$, *then*

$$\varphi\colon B \otimes L \otimes L \xrightarrow{d_1^*(\omega)^{-1}} C \otimes L \otimes L \xrightarrow{d_2^*(\omega)} B \otimes L \otimes L$$

is the associated 1-cocycle. If a 1-cocycle $\varphi \in \mathrm{Aut}_{L\otimes L}(B \otimes L \otimes L)$ *is given, then let* C *be the equalizer in* k-*Mod of*

$$B \otimes L \underset{\varphi(B \otimes d_1)}{\overset{B \otimes d_2}{\rightrightarrows}} B \otimes L \otimes L$$

Tensoring with L *induces an isomorphism* $\omega\colon C \otimes L \cong B \otimes L$ *and there is a unique* $\mathcal{s}$-*structure* $\mathcal{C}$, *such that* $\omega\colon (C_L,\mathcal{C}_L) \longrightarrow (B_L,\mathcal{B}_L)$ *is an* $\mathcal{s}_L$-*isomorphism.*

Proofs of this theorem can be found in [2,3].

Now we can describe the L-forms of the Hopf algebra kG by $H^1(L/k,\mathcal{Hopf}\text{-}\mathcal{Aut}(G))$, where $\mathcal{Hopf}\text{-}\mathcal{Aut}(G)(L) = \text{Hopf-Aut}_L(LG)$ for any commutative k-algebra L .

The category F-gal_L contains in particular all Galois extensions of L with group F and hopf_L contains all Hopf algebras over L. A change of basis q: $L \longrightarrow M$ induces functors $\mathit{s}_L \longrightarrow \mathit{s}_M$ (F-$\mathit{gal}_L \longrightarrow$ F-gal_M and $\mathit{hopf}_L \longrightarrow \mathit{hopf}_M$ which also preserve the Galois extensions and Hopf algebras). If M is a faithfully flat extension of L then only F-Galois extensions resp. bialgebras over L can be lifted to F-Galois extensions resp. bialgebras over M , i.e. these properties are preserved and reflected by faithfully flat base extensions.

Let L be a faithfully flat k-algebra. An isomorphism class $(C,\mathcal{C})$ in s_k is called an L-*form* of an object $(B,\mathcal{B})$ in s_k , if after base ring extension the object $(C_L,\mathcal{C}_L) \simeq (C,\mathcal{C}) \otimes L = (C \otimes L, \mathcal{C} \otimes L)$ is isomorphic to $(B,\mathcal{B}) \otimes L$ in s_L . The set of L-forms of $(B,\mathcal{B})$ will be denoted by $\underline{\underline{S}}(L/k,(B,\mathcal{B}))$. $(C,\mathcal{C})$ is called a *form* of $(B,\mathcal{B})$ if there exists a faithfully flat k-algebra L such that $(C,\mathcal{C})$ is an L-form of $(B,\mathcal{B})$. The set of all forms is denoted by $\underline{\underline{S}}(B,\mathcal{B})$. If we simply write lim for the direct limit taken over all faithfully flat extensions of k then we have for our special cases

$$\text{F-}\underline{\underline{Gal}}(K,\mathcal{K}) = \lim \text{F-}\underline{\underline{Gal}}(L/k,(K,\mathcal{K})) \qquad \text{resp.}$$
$$\underline{\underline{Hopf}}(H,\mathcal{H}) = \lim \underline{\underline{Hopf}}(L/k,(H,\mathcal{H})) \ .$$

Our aim is to describe $\underline{\underline{Hopf}}(kG)$ where G is a finitely generated group (with automorphism group $F = C_2$) and k is a commutative ring (where 2 is not a zero-divisor and $\mathrm{Pic}_{(2)}(k) = 0$), i.e. we want to describe all bialgebras H over k which after faithfully flat ring extension L become isomorphic to $kG \otimes_k L \simeq LG$. The trigonometric algebra was a first example with $G = \mathbb{Z}$.

Each $L \in k\text{-}\mathit{Alg}_c$ defines a cosimplicial object

$$k \longrightarrow L \underset{d_2}{\overset{d_1}{\rightrightarrows}} L \otimes L \;\substack{\longrightarrow\\ \longrightarrow\\ \longrightarrow}\; L \otimes L \otimes L$$

Observe that the use of the graph

$$0 \underset{\varepsilon}{\overset{\eta}{\rightleftarrows}} 1 \underset{\nabla}{\overset{\Delta}{\rightleftarrows}} 2$$

actually allows arbitrary bialgebras $(C,\mathcal{C})$ to become L-forms of a Hopf algebra $(H,\mathcal{H})$, i.e. to be in $\mathcal{H}opf(H,\mathcal{H})$. If we had used instead the graph

$$0 \underset{\varepsilon}{\overset{\eta}{\rightleftarrows}} 1 \underset{\nabla}{\overset{\Delta}{\rightleftarrows}} 2 \quad (S \text{ loop at } 1)$$

for $\mathcal{h}opf$ then only Hopf algebras $(C,\mathcal{C})$ would have been admitted as L-forms of the Hopf algebra $(H,\mathcal{H})$. But in both cases the forms are described by $H^1(L/k,\mathcal{H}opf\text{-}\mathcal{A}ut(\ \otimes H))$, since each bialgebra automorphism of $L \otimes H$ is automatically a Hopf algebra automorphism [8, Lemma 4.0.4] . Thus we have

REMARK: *A bialgebra form of a Hopf algebra is a Hopf algebra.*

Let G be a group and $x \in LG$ be a group-like element, i.e. $\Delta(x) = x \otimes x$ and $\varepsilon(x) = 1$. If $x = \sum_{g\in G} a_g g$, then x is group-like iff

$$(*) \quad \begin{cases} a_g = 0 \quad \text{for almost all} \quad g \in G \\ a_g \cdot a_h = 0 \quad \text{if} \quad g \neq h \\ a_g \cdot a_g = a_g \\ \sum_{g\in G} a_g = 1 \ . \end{cases}$$

Let $V(LG)$ denote the set of all group-like elements of LG .

THEOREM 2. *Let* G *be a finitely generated group. Then*

$$\text{Hopf-Aut}_L(LG) \simeq V(LF)$$

where $F = \text{Gr-Aut}(G)$, *the set of group automorphisms of* G .

Proof: Let $\sum a_f f \in V(LF)$. Then the L-linear map φ with

$$\varphi(g) = \sum_{f\in F} a_f f(g) \quad \text{for all} \quad g \in G$$

is a Hopf algebra automorphism. In fact we have

$$\begin{aligned}\varphi(g)\varphi(g') &= \textstyle\sum_f a_f f(g) \sum_{f'} a_{f'} f'(g') \\ &= \textstyle\sum_f a_f f(g) f(g') \quad \text{(by (*))} \\ &= \textstyle\sum_f a_f f(gg') \\ &= \varphi(gg')\end{aligned}$$

and

$$\varphi(1) = \textstyle\sum_f a_f f(1) = \sum_f a_f = 1 ,$$

hence φ is an algebra homomorphism.

$$\begin{aligned}(\varphi \otimes \varphi)(\Delta(g)) &= \varphi(g) \otimes \varphi(g) \\ &= \textstyle\sum_f a_f f(g) \otimes \sum_{f'} a_{f'} f'(g) \\ &= \textstyle\sum_f a_f f(g) \otimes f(g) \\ &= \textstyle\sum_f a_f \Delta(f(g)) \\ &= \Delta(\textstyle\sum_f a_f f(g)) \\ &= \Delta\varphi(g)\end{aligned}$$

and

$$\varepsilon\varphi(g) = \varepsilon(\textstyle\sum_f a_f f(g)) = \sum_f a_f = 1 = \varepsilon(g)$$

give that φ is a Hopf algebra homomorphism. But with $\psi(g) = \sum_f a_f f^{-1}(g)$ we get

$$\begin{aligned}\varphi\psi(g) &= \varphi(\textstyle\sum_f a_f f^{-1}(g)) \\ &= \textstyle\sum_f a_f \sum_{f'} a_{f'} f' f^{-1}(g) \\ &= \textstyle\sum_f a_f g \\ &= g\end{aligned}$$

hence $\psi = \varphi^{-1}$. So we have a group homomorphism

$$V(LF) \longrightarrow \text{Hopf-Aut}_L(LG) \quad .$$

Now let $\sum_f a_f f$ define the identity on LG . Define $a(g,h) := \sum \{a_f | f \in F \wedge f(g) = h\}$ for $g,h \in G$. Because of $\sum_f a_f f(g) = g$ for all $g \in G$ we have $a(g,h) = \delta_{g,h}$. Use the fact that the a_f are orthogonal idempotents to get

$$a_{f'} = \Pi_g \; a(g,f'(g)) = \Pi_g \; \delta_{g,f'(g)} = \delta_{f',id} ,$$

so $\sum_f a_f f = id \in V(LF)$ which shows $V(LF) \leq \text{Hopf-Aut}_L(LG)$.

Before we continue we remark the following. For any group G and Hopf algebra homomorphism $\varphi: LG \longrightarrow LG$ let $\varphi(g) = \sum_{g'} a_{g',g} g'$ for $g \in G$. Since g is group-like so is $\varphi(g)$ hence the coefficients $\{a_{g',g} | g' \in G\}$ satisfy (*) for each g .

Now let $\varphi\colon LG \longrightarrow LG$ be a Hopf algebra automorphism with inverse ψ . Assume that $g_1,\ldots,g_n$ is a generating system for the group G . Then φ is completely described by its action on the g_i . Let $\varphi(g_i) = \sum a_{ij}x_{ij}$ with $a_{ij} \in L$, $x_{ij} \in G$. Since the $(a_{ij})_j$ are orthogonal idempotents we can refine this set by $1 = \Pi_i(\Sigma_j\, a_{ij}) = \Sigma\, b_k$ where all the b_k are products $\Pi_i\, a_{ij_i}$. Then the b_k satisfy (*) and the a_{ij} are sums of certain b_k's . Hence $\varphi(g_i) = \sum b_k y_{ik}$ for certain group elements y_{ik} . If $g \in G$ and

$$g = g_{i_1}^{n_1} \cdots g_{i_r}^{n_r} \quad \text{then} \quad \varphi(g) = \varphi(g_{i_1})^{n_1} \cdots \varphi(g_{i_r})^{n_r} \quad .$$

Taking the product of the sum expressions for the $\varphi(g_i)$ we get $\varphi(g) = \sum b_k f_k(g)$ where the $f_k(g)$ are suitable products of the y_{ij} . The f_k are homomorphisms since φ is multiplicative. So we have $\varphi = \sum b_k f_k$. If $\psi = \sum b'_r f'_r$ we can again refine the set of idempotents and get $\varphi = \sum b_k f_k$ and $\psi = \sum b_k f'_k$ (with possibly new idempotents but the same homomorphisms). Then $g = \varphi\psi(g) = \sum b_k f_k f'_k(g)$ shows $f_k f'_k(g) = g$ for all $g \in G$ and all k . By symmetry we get the result $\varphi = \sum b_k f_k \in V(LF)$.

We wish to acknowledge that the argument given above as well as the following example were kindly communicated to us by Pere Menal. The example shows that the theorem does not hold for infinitely generated abelian groups.

If $G = \langle g_1, g_2, \ldots \rangle$ is such a group and if L has an infinite series of idempotents $e_1, e_2, \ldots$ with $e_i e_j = e_i$ for $i \leqq j$ and $e_i \neq e_j$ for $i \neq j$, then

$$LG \ni \prod_{i=1}^{n} g_i^{r_i} \longmapsto \prod_{i=1}^{n} (e_i g_i^{r_i} + (1 - e_i) g_i^{-r_i}) \in LG$$

is a Hopf algebra automorphism but not in $V(L(\mathrm{Aut}(G)))$.

We now introduce some facts about Galois extensions of commutative rings. Let F be a finite group. A commutative k-algebra K is called an F-*Galois extension* of k if

1) F is a subgroup of $\mathrm{Aut}_k(K)$,
2) K is a finitely generated projective k-module,
3) $F \subseteq \mathrm{End}_k(K)$ is a free generating system over K .

The k-algebra $E_k^F = \mathrm{Map}(F,k)$, the set of maps with algebra structure induced by the ring structure on k , is called the *trivial* F-*Galois extension*, where F acts by $(fa)(f') = a(f^{-1}f')$, $f,f' \in F$, $a \in \mathrm{Map}(F,k)$. E_k^F has the k-basis v_f^k with $v_f^k(f') = \delta_{f,f'}$. For Galois extensions there is the following

PROPOSITION 3. $\text{Gal-Aut}_k(E_k^F) \simeq V(kF)$.

For a proof see [3, Prop. 2.14].

COROLLARY 4. *Let* G *be a finitely generated group with finite automorphism group* $F = \text{Gr-Aut}(G)$. *Then there is a bijection between the Hopf algebra forms* $\underline{\underline{Hopf}}(kG)$ *of* kG *and the (pointed) set of* F-*Galois extensions* $\mathrm{Gal}(k,F)$ *of* k .

Proof: We first observe that each F-Galois extension K over k is faithfully flat. Furthermore there is a K-isomorphism $\omega\colon K \otimes K \simeq E_K^F \simeq E_k^F \otimes K$ of F-Galois extensions of K defined by $\omega(a \otimes b)(f) = f^{-1}(a)b$, where $K \otimes K$ is a K-algebra by $a\cdot(b \otimes c) = b \otimes ac$ and F acts on $K \otimes K$ by $f(a \otimes b) = f(a) \otimes b$. So every F-Galois extension K of k is a K-form of E_k^F and $\mathrm{Gal}(k,F) = F\text{-}\underline{\underline{Gal}}(E_k^F)$. By Theorem 1 together with Proposition 3 we have $F\text{-}\underline{\underline{Gal}}(L/k,E_k^F) \simeq H^1(L/k,V(-F))$ and Theorems 1 and 2 give $H^1(L/k,V(-F)) \simeq \underline{\underline{Hopf}}(L/k,kG)$. By going to the limit we get $F\text{-}\underline{\underline{Gal}}(E_k^F) \simeq \underline{\underline{Hopf}}(kG)$.

If F is a commutative group then all the objects mentioned in the proof above are abelian groups and all morphisms are group homomorphisms.

We want to make the isomorphism of the Corollary explicit, so that we can construct the Hopf algebra form associated with an F-Galois extension of k. For that purpose we first construct a 1-cocycle for a given F-Galois extension K of k. Then we use this 1-cocycle to construct the corresponding form of kG. In between we have to identify $\text{Gal-Aut}_k(E_k^F) \simeq V(kF)$ and $V(kF) \simeq \text{Hopf-Aut}_k(kG)$.

In general if the class of $(C,\mathcal{C})$ is a K-form of $(B,\mathcal{B})$ with isomorphism $\omega\colon C \otimes K \simeq B \otimes K$ then the 1-cocycle $\varphi = d_2^*(\omega)\, d_1^*(\omega)^{-1}$ is given by the commutative diagram

$$
\begin{array}{ccccc}
B \otimes K \otimes K & & \simeq & & B \otimes K \otimes_{d_1} (K \otimes K) \\
\big| & \searrow{\scriptstyle d_1^*(\omega)^{-1}} & & & \big\downarrow {\scriptstyle \omega^{-1} \otimes 1} \\
\big| & & & \nearrow\!\!\!\!\simeq & C \otimes K \otimes_{d_1} (K \otimes K) \\
\varphi & & C \otimes K \otimes K & & \\
\big| & & & \searrow\!\!\!\!\simeq & C \otimes K \otimes_{d_2} (K \otimes K) \\
\big\downarrow & \swarrow{\scriptstyle d_2^*(\omega)} & & & \big\downarrow {\scriptstyle \omega \otimes 1} \\
B \otimes K \otimes K & & \simeq & & B \otimes K \otimes_{d_2} (K \otimes K) .
\end{array}
$$

Let $(B,\mathcal{B})$ be the trivial F-Galois extension E_k^F and K some (K-)form $(C,\mathcal{C})$ of it. Then $\omega\colon K \otimes K \simeq E_K^F \simeq E_k^F \otimes K$ was given by $\omega(a \otimes b)(f) = f^{-1}(a)b$ or equivalently $\omega(a \otimes b) = \sum_f f^{-1}(a)b \cdot v_f^K$. The corresponding 1-cocycle $\varphi \in \text{Gal-Aut}_{K\otimes K}(E_k^F \otimes K \otimes K)$ describes an element $\sum a_{f^{-1}} f$ in $V(K \otimes KF)$ by

$$\varphi(v_e^{K\otimes K}) = \sum a_f v_f^{K\otimes K} .$$

Let $\omega^{-1}(v_e^K) = \sum a_i \otimes b_i \in K \otimes K$, i.e. $\sum f(a_i)b_i = \delta_{f,e}$, then by the diagram above

$$\varphi(v_e^{K\otimes K}) = \sum_f \sum_i (f^{-1}(a_i) \otimes b_i) v_f^{K\otimes K}$$

so the corresponding element in $V(K \otimes KF)$ is $\psi = \sum_f \sum_i (f(a_i) \otimes b_i) f$.

Consider ψ as an element of $\text{Hopf-Aut}_{K\otimes K}(K \otimes KG)$. Then by the construction given in Theorem 1 the associated K-form of kG is the equalizer H in

$$H \longrightarrow KG \overset{d_2}{\underset{\psi d_1}{\rightrightarrows}} K \otimes KG .$$

From

$$\psi(\sum_g 1 \otimes c_g g) = \sum_f \sum_i \sum_g (f(a_i) \otimes b_i c_g) f(g)$$
$$= \sum_g (\sum_{f,i} f(a_i) \otimes b_i c_{f^{-1}(g)}) g$$

we have

$$H = \{\sum c_g g \in KG \mid \sum (c_g \otimes 1) g = \sum_g (\sum_{f,i} f(a_i) \otimes b_i c_{f^{-1}(g)}) g ,$$

where $g \in G$, $f \in F = \text{Gr-Aut}(G)$.

We claim now that $H = (KG)^F$, the subset of fixed elements in KG under the diagonal action of F given by $f(ag) = f(a)f(g)$. Let $\sum c_g g$ be in H and $f \in F$. Then

$$f(\sum c_g g) = \sum \nabla(f \otimes 1)(c_g \otimes 1) f(g)$$
$$= \nabla \sum (f \otimes 1)(f'(a_i) \otimes b_i c_{f'^{-1}(g)}) f(g)$$
$$= \nabla \sum (ff'(a_i) \otimes b_i c_{(ff')^{-1}(h)}) h$$
$$= \sum c_h h ,$$

hence $H \subseteq (KG)^F$. Let $\sum c_g g \in KG$ satisfy $\sum f(c_g) f(g) = \sum c_g g$ for all $f \in F$, then by applying f^{-1} to the group elements we get $\sum f(c_g) g = \sum c_g f^{-1}(g)$. Furthermore observe that $\sum_f f(a_i c_g)$ is fixed under all $f' \in F$ hence an element in k . The inverse map of $\psi = \sum a_f f$ in $V(K \otimes KF) \simeq \text{Hopf-Aut}_{K \otimes K}(K \otimes KG)$ is $\sum a_f f^{-1}$ since $\sum_f a_f f \cdot \sum_{f'} a_{f'} f'^{-1} = 1$ by the orthogonality of the a_f . Using all this we get

$$(\sum a_f f^{-1})(\sum (c_g \otimes 1) g) = \sum (f(a_i) c_g \otimes b_i) f^{-1}(g)$$
$$= \sum (f(a_i c_g) \otimes b_i) g$$
$$= \sum (1 \otimes f(a_i) b_i f(c_g)) g$$
$$= \sum (1 \otimes c_g) g .$$

So we have proved the following

THEOREM 5. *Let* G *be a finitely generated group with finite automorphism group* $F = \text{Gr-Aut}(G)$. *Then there is a bijection* *between* Gal(k,F) *and* *Hopf*(kG) *which associates with each* F-*Galois extension* K *of* k *the Hopf algebra*

$$H = \{ \sum c_g g \in KG \mid \sum f(c_g)f(g) = \sum c_g g \quad \textit{for all} \quad f \in F \} .$$

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

$$\omega : H \otimes K \simeq KG , \ \omega(h \otimes a) = ah .$$

This Theorem can be favorably applied in the situation $F = C_2$, the cyclic group with two elements, because in this case the C_2-Galois extensions or "quadratic extensions" of k are well known. So the groups G which are of interest are C_3, C_4, C_6, and $\mathbb{Z}$. We will give a complete description of all forms of kG for these groups with minor restrictions on k .

Assume in the following that 2 is not a zero divisor in k and that $\mathrm{Pic}_{(2)}(k) = 0$. Then all quadratic extensions of k are free [7] and can be described as $K = k[x]/(x^2-ax-b)$ where $a^2+4b = u$ is a unit in k . Their non-trivial automorphism is $f(x) = a - x$. If 2 is invertible in k , then a can be chosen zero thus $K = k[x]/(x^2-b)$ with b a unit in k . In this case two such extensions are isomorphic iff $b \cdot b'$ is a square in k . For the general equivalence of two such extensions we refer to [3,4,5,7].

THEOREM 6. a) *The Hopf algebra forms of* $k\mathbb{Z}$, *the multiplicative group, 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 of* k . *These forms are split by* $K = k[x]/(x^2-ax-b)$. *The Hopf algebra structure is defined by*

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

In the special case of $2 \in U(k)$, $a \in k$ can be taken zero. If we replace c by $2c'$, s by $2bs'$ and u by $4b$ then the forms of $k\mathbb{Z}$ are $H = k[c',s']/(c'^2-bs'^2-1)$. For $b = -1$ this is the trigonometric algebra discussed in the beginning of this note, for $b = 1$ this is isomorphic to $k\mathbb{Z}$. If $k = \mathbb{R}$, the field of reals, then there are precisely two quadratic extensions of $\mathbb{R}$, the complex numbers and $\mathbb{R} \times \mathbb{R}$. Hence these are the only two possible forms of $\mathbb{R}\mathbb{Z}$. If $k = \mathbb{Q}$, the field of rational numbers, then there are infinitely many forms of $\mathbb{Q}\mathbb{Z}$ namely

$$H = k[c',s']/(c'^2+ds'^2-1)$$

where d runs through all positive squarefree natural numbers or $d = -1$.

Proof of the Theorem: Let $G = \mathbb{Z}$ and $k\mathbb{Z} = k[t,t^{-1}]$. Let $\sum a_i t^i$ be an element of a form H . If $a_i = \alpha_i + \beta_i x \in K$, then $\sum (\alpha_i + \beta_i x)t^i = \sum f(\alpha_i + \beta_i x)t^{-i}$ implies $\alpha_{-i} + \beta_{-i}x = \alpha_i + \beta_i(a-x)$, hence

$$H = \{ \alpha_o t^o + \textstyle\sum_{i>o} \alpha_i(t^i + t^{-i}) + \beta_i(xt^i + (a - x)t^{-i}) \} .$$

Define $c_i := t^i + t^{-i}$, $s_i := xt^i + (a - x)t^{-i}$ for $i \geq 0$. Then H is generated by the c_i and s_i as a k-module. Observe $c_o = 2$, $s_o = a$ and $a^2 + 4b \in U(k)$. Define furthermore $c := c_1$ and $s := s_1$. Then the following relations hold:

$$c_i \cdot c = c_{i+1} + c_{i-1} \ , \quad s_i \cdot c = s_{i+1} + s_{i-1} \ , \quad \text{for } i \geq 1 \ .$$

Since c_o , $s_o \in k$ this shows by induction that c and s are k-algebra generators of H . They satisfy the following relation $s^2 - asc - bc^2 + u = 0$ which is easily checked in $k\mathbb{Z}$. So there is an epimorphism $k[c,s]/(s^2-asc-bc^2+u) \longrightarrow H$. This map is injective iff it is injective after tensoring with K . But in the situation $K[c,s]/(s^2-asc-bc^2+u) \longrightarrow H \otimes K \cong K[t,t^{-1}]$ there is an inverse homomorphism $t \longmapsto (a - 2x)^{-1}((a - x)c - s)$. By $(a - 2x)^2 =$

u it is clear that $(a - 2x)$ is invertible. Furthermore

$$(a - 2x)^{-1}((a - x)c - s)\cdot(a - 2x)^{-1}(-xc + s) = 1$$

shows that this map is well defined and maps t^{-1} to $(a - 2x)^{-1}(-xc + s)$. Now it is easy to see that

$$K[c,s]/I \longrightarrow H \otimes K \longrightarrow K[c,s]/I$$

is the identity hence the given map is an isomorphism.

The coalgebra structure on H is induced by that of $k\mathbb{Z}$ and is expressed by the given formulas.

For the Hopf algebra forms of kC_3, kC_4, and kC_6 take those of $k\mathbb{Z}$ and express the relation $t^n = 1$ (n = 3, 4, or 6) in terms of c and s .

Case $n = 3$: $t^2 = t^{-1}$ iff $c_2 = c$ and $s_2 = ac - s$ iff $(c + 1)(c - 2) = 0$ and $(c + 1)(s - a) = 0$. To show that $c_2 = c$ and $s_2 = ac - s$ implies $t^2 = t^{-1}$ observe that $xt^2 + (a-x)t^{-2} = xt^{-1} + (a-x)t$ implies $t^2 - t^{-2} = t^{-1} - t$ as coefficients of x . Then $2t^2 = 2t^{-1}$ implies $t^2 = t^{-1}$ since 2 is not a zero divisor in KC_3 .

Case $n = 4$: $t^2 = t^{-2}$ iff $((a-x)c - s)^2 = (-xc + s)^2$ iff $c(ac - 2s)(a - 2x) = 0$ iff $c(ac - 2s) = 0$.

Case $n = 6$: $t^4 = t^{-2}$ iff $c_4 = c_2$ and $s_4 = ac_2 - s_2$ iff $(c^2 - 1)(c^2 -4) = 0$ and $(c^2 - 1)(sc - 2a) = 0$.

REMARK: There is an interesting example of a separable field extension which is (Hopf-)Galois with the Hopf algebra $H = \mathbb{Q}[c,s]/(c^2+s^2-1,sc)$, which is a form of $\mathbb{Q}C_4$. The extension is $\mathbb{Q}(\mu):\mathbb{Q}$ with $\mu = \sqrt[4]{2}$, which is definitely not Galois in the ordinary Galois theory. The operation of H on $\mathbb{Q}(\mu)$ is given by

$$c(1) = 1 \qquad c(\mu) = 0 \qquad c(\mu^2) = -\mu^2 \qquad c(\mu^3) = 0$$
$$s(1) = 0 \qquad s(\mu) = -\mu \qquad s(\mu^2) = 0 \qquad s(\mu^3) = \mu^3 .$$

This operation satisfies

1. $c^2(a) + s^2(a) = a$ for $a \in K$
2. $c(ab) = c(a)c(b) - s(a)s(b)$
   $s(ab) = s(a)c(b) + c(a)s(b)$ for $a, b \in K$,
3. $c(1) = 1$ $s(1) = 0$.

A straightforward computation shows that $\mathbb{Q}(\mu)$ is Galois over $\mathbb{Q}$ with the Hopf algebra H and this operation.

Another example of such a Galois extension is $\mathbb{Q}(\mu):\mathbb{Q}$ with $\mu = \sqrt[3]{2}$ and the Hopf algebra $H = \mathbb{Q}[c,s]/(3s^2+c^2-1,(2c+1)s)$, which is a form of $\mathbb{Q}C_3$ with coalgebra structure $\Delta(c) = c \otimes c - 3s \otimes s$, $\Delta(s) = c \otimes s + s \otimes c$, $\varepsilon(c) = 1$, $\varepsilon(s) = 0$. The operation is defined by

$$c(1) = 1 \qquad c(\mu) = -\frac{1}{2}\mu \qquad c(\mu^2) = -\frac{1}{2}\mu^2$$
$$s(1) = 0 \qquad s(\mu) = \frac{1}{2}\mu \qquad s(\mu^2) = -\frac{1}{2}\mu^2 \ .$$

In a separate paper we will determine all separable field extensions which are Galois with a Hopf algebra H [9] .

REFERENCES

[1] DEMAZURE, M. and GABRIEL, P.: "Groupes algébriques" (Tome I). North Holland - Amsterdam (1970).

[2] GROTHENDIECK, A.: Technique de descente I. Seminaire Bourbaki, Exp. 190 (1959/60).

[3] HAGGENMÜLLER, R.:"Über Invarianten separabler Galoiserweiterungen kommutativer Ringe" Dissertation, Universität München, (1979).

[4] HAGGENMÜLLER, R.: Diskriminanten und Picard-Invarianten freier quadratischer Erweiterungen. *Manuscripta math.* 36 (1981), 83-103.

[5] KITAMURA, K.: On the free quadratic extensions of a commutative ring. *Osaka J.Math.* 10 (1973), 15-20.

[6] KNUS, M.A. and OJANGUREN, M.:"Theorie de la Descente et Algèbres d'Azumaya." Springer LN 389 (1974) .

[7] SMALL, C.: The group of quadratic extensions. *J. Pure Appl. Alg.* 2 (1972), 83-105, 395.

[8] SWEEDLER, M.: "Hopf Algebras" W.A.Benjamin - New York (1969) .

[9] GREITHER, C. and PAREIGIS, B.: Hopf Galois Theory of Separable Field Extensions. To appear in *J. Alg.*

Mathematisches Institut der Univ.
Theresienstraße 39
D-8000 München 2
Federal Republic of Germany

(Received August 2, 1985)