ON THE EXPONENT OF FINITE-DIMENSIONAL HOPF ALGEBRAS

Pavel Etingof and Shlomo Gelaki

1. Introduction

One of the classical notions of group theory is the notion of the exponent of a group. The exponent of a group is the least common multiple of orders of its elements.

In this paper we generalize the notion of exponent to Hopf algebras. We define the exponent of a Hopf algebra $H$ (with bijective antipode) to be the smallest $n$ such that $m_n \circ (I \otimes S^{-2} \otimes \cdots \otimes S^{-2n+2}) \circ \Delta_n = \varepsilon \cdot 1$, where $m_n$, $\Delta_n$, $S$, $1$, and $\varepsilon$ are the iterated product and coproduct, the antipode, the unit, and the counit. If $H$ is involutive (for example, $H$ is semisimple and cosemisimple), the last formula reduces to $m_n \circ \Delta_n = \varepsilon \cdot 1$.

We give four other equivalent definitions of the exponent (valid for finite-dimensional Hopf algebras). In particular, we show that the exponent of $H$ equals the order of the Drinfeld element $u$ of the quantum double $D(H)$, and the order of $R_{21} R$, where $R$ is the universal $R$-matrix of $D(H)$.

We show that the exponent is invariant under twisting. We prove that for semisimple and cosemisimple Hopf algebras $H$, the exponent is finite and divides $\dim(H)^3$. For triangular semisimple Hopf algebras in characteristic zero, we show that the exponent divides $\dim(H)$. These theorems are motivated by the work of Kashina [Ka1,Ka2], who conjectured that if $H$ is semisimple and cosemisimple then (using our language) the exponent of $H$ is always finite and divides $\dim(H)$, and showed that the order of the squared antipode of any finite-dimensional semisimple and cosemisimple Hopf algebra in the Yetter-Drinfeld category of $H$ divides the exponent of $H$.

At the end we formulate some open questions, in particular suggest a formulation for a possible Hopf algebraic analogue of Sylow’s theorem.

2. Definition and Elementary Properties of Exponent

Let $H$ be a Hopf algebra over any field $k$, with multiplication map $m$, comultiplication map $\Delta$ and antipode $S$. We will always assume that $S$ is bijective. Let $m_1 = I$ and $\Delta_1 = I$ be the identity map $H \to H$, and for any integer $n \geq 2$ let $m_n : H^\otimes n \to H$ and $\Delta_n : H \to H^\otimes n$ be defined by $m_n = m \circ (m_{n-1} \otimes I)$, and $\Delta_n = (\Delta_{n-1} \otimes I) \circ \Delta$. We start by making the following definition.

Received December 28, 1998.
Definition 2.1. The exponent of a Hopf algebra $H$, denoted by $\exp(H)$, is the smallest positive integer $n$ satisfying $m_n \circ (I \otimes S^{-2} \otimes \cdots \otimes S^{-2n+2}) \circ \Delta_n = \varepsilon \cdot 1$. If such $n$ does not exist, we say that $\exp(H) = \infty$.

Let us list some of the elementary properties of $\exp(H)$.

Proposition 2.2. Let $H$ be a Hopf algebra over $k$. Then:

1. The order of any group-like element of $H$ divides $\exp(H)$ (here we agree that any positive integer $n$ divides $\infty$).
2. For any group $G$, $\exp(k[G])$ equals the exponent of $G$ (see e.g. [Ro, p.12]), i.e. the least common multiple of the orders of the elements of $G$.
3. If $\exp(H) = n < \infty$ then $m_r \circ (I \otimes S^{-2} \otimes \cdots \otimes S^{-2r+2}) \circ \Delta_r = \varepsilon \cdot 1$ if and only if $r$ is divisible by $n$.
4. If $H$ is finite-dimensional, $\exp(H^*) = \exp(H)$.
5. $\exp(H_1 \otimes H_2)$ equals the least common multiple of $\exp(H_1)$ and $\exp(H_2)$.
6. If $\exp(H) = 2$ then $H$ is commutative and cocommutative (this generalizes the fact that a group $G$ with $g^2 = 1$ for all $g \in G$ is abelian).
7. The exponents of Hopf subalgebras and quotients of $H$ divide $\exp(H)$.
8. If $K \supseteq k$ is a field then $\exp(H \otimes_k K) = \exp(H)$.

Proof. (1) Suppose $\exp(H) < \infty$, and set $n = \exp(H)$. Since $S^2(g) = g$ we have that $g^n = m_n \circ \Delta_n(g) = m_n \circ (I \otimes S^{-2} \otimes \cdots \otimes S^{-2n+2}) \circ \Delta_n(g) = \varepsilon(g)1 = 1$. Therefore the order of $g$ divides $n$.

(6) Since $m \circ (I \otimes S^{-2}) \circ \Delta = \varepsilon \cdot 1$ is equivalent to $S^3 = I$, we have that $I : H \to H$ is an antiautomorphism of algebras and coalgebras, and the result follows.

The proofs of the other parts are obvious. \(\square\)

Remark 2.3. Part (2) of Proposition 2.2 motivated Definition 2.1.

Example 2.4. Let $H$ be a finite-dimensional Hopf algebra over an algebraically closed field $k$ of characteristic zero. Suppose that $H$ contains a non-trivial $1 : g$ skew-primitive element $x$ (i.e. $\Delta(x) = x \otimes 1 + g \otimes x$, where $g$ is a group-like element, and $x \notin k[g]$). It is clear that in this case we may assume that $xg = gqx$ for some root of unity $q$ of order dividing $|g|$. Also, $S^2(x) = qx$, $\varepsilon(x) = 0$, $\{x, gx, \ldots, g^{|q|-1}x\}$ is linearly independent, and hence

$$m_n \circ (I \otimes S^{-2} \otimes \cdots \otimes S^{-2n+2}) \circ \Delta_n(x) = \sum_{i=0}^{n-1} q^{-i} g^i x \neq 0.$$ 

Hence, $\exp(H) = \infty$. In particular, the exponent of any pointed Hopf algebra $H$ over $k$ (which is not a group algebra) is $\infty$, since by [TW], $H$ contains a non-trivial skew-primitive element.
In the sequel, we will assume for simplicity that $H$ is finite-dimensional. Let us formulate four equivalent definitions of $\exp(H)$. Recall that the Drinfeld double $D(H) = H^{\text{cop}} \otimes H$ of $H$ is a quasitriangular Hopf algebra with universal $R$–matrix $\mathcal{R} = \sum_i h_i \otimes h_i^*$, where $\{h_i\}, \{h_i^*\}$ are dual bases for $H$ and $H^*$ respectively. Let $u = m(S \otimes I)\tau(\mathcal{R}) = \sum_i S(h_i^*)h_i$, where $S$ is the antipode of $D(H)$ and $\tau$ is the usual flip map, be the Drinfeld element of $D(H)$. By [D],

$$S^2(x) = uxu^{-1}, \quad x \in D(H) \quad \text{and} \quad \Delta(u) = (u \otimes u)(\mathcal{R}_{21}\mathcal{R})^{-1}.$$  

**Theorem 2.5.** Let $H$ be a finite-dimensional Hopf algebra over $k$. Then

1. $\exp(H)$ equals the smallest positive integer $n$ such that
   $$\mathcal{R}(I \otimes S^2)(\mathcal{R}) \cdots (I \otimes S^{2n-2})(\mathcal{R}) = 1.$$

2. $\exp(H)$ equals the order of $u$.

3. $\exp(H)$ equals the order of $\mathcal{R}_{21}\mathcal{R}$.

4. $\exp(H)$ equals the order of any non-zero element $v \in D(H)$ satisfying
   $$\Delta(v) = (v \otimes v)(\mathcal{R}_{21}\mathcal{R})^{-1}.$$  

**Proof.** First note that since $(\Delta \otimes I)(\mathcal{R}) = \mathcal{R}_{13}\mathcal{R}_{23}$, it follows that

$$(\Delta_n \otimes I)(\mathcal{R}) = \mathcal{R}_{1,n+1} \cdots \mathcal{R}_{n,n+1},$$

for all $n$.

Second, recall that the map $H^* \otimes H \to D(H)$, $p \otimes h \mapsto ph$ is a linear isomorphism [D].

Now we will show the equivalence of Definition 2.1 and the four definitions in the theorem.

(Definition 2.1 $\iff$ 1 $\iff$ 2) Write $\mathcal{R} = \sum_j a_j \otimes b_j$. Using the above we obtain the following equivalences:

$$m_n \circ (I \otimes S^{-2} \cdots \otimes S^{-2n+2}) \circ \Delta_n = \varepsilon \cdot 1 \iff$$

$$(m_n \circ (I \otimes S^{-2} \cdots \otimes S^{-2n+2}) \circ \Delta_n \otimes I)(\mathcal{R}) = 1 \iff$$

$$(m_n \circ (I \otimes S^{-2} \cdots \otimes S^{-2n+2}) \otimes I)(\mathcal{R}_{1,n+1} \cdots \mathcal{R}_{n,n+1}) = 1 \iff$$

$$\sum_{i_1, \ldots, i_n} a_{i_1} S^{-2}(a_{i_2}) \cdots S^{-2n+2}(a_{i_n}) \otimes b_{i_1} \cdots b_{i_n} = 1 \iff$$

$$\mathcal{R}(I \otimes S^2)(\mathcal{R}) \cdots (I \otimes S^{2n-2})(\mathcal{R}) = 1 \iff$$

$$u^n = 1.$$  

(in the last step we applied $m \circ (I \otimes S)\tau$ to both sides of the equation, and used the fact that $uS^{-2}(x) = xu$, for all $x \in D(H)$).

(2 $\iff$ 3) Clearly if $u^n = 1$ then $(\mathcal{R}_{21}\mathcal{R})^n = 1$. In the other direction, first note that $(\mathcal{R}_{21}\mathcal{R})^n = 1$ implies that $u^n \in G(D(H))$ (where $G(A)$ is the group of
grouplike elements of a Hopf algebra $A$). Therefore by $[R]$, $u^n = ab$ where $a \in G(H^*)$ and $b \in G(H)$. Regarding $u$ as an element of $H^* \otimes H$, we have that $m(I \otimes \varepsilon)(u) = m(\varepsilon \otimes I)(u) = 1$. Hence it follows that $1 = m(I \otimes \varepsilon)(u^n) = a$ and $1 = m(\varepsilon \otimes I)(u^n) = b$, so $u^n = 1$.

(2 $\Leftrightarrow$ 4) First note that $v = ug$, where $g \in G(D(H))$. Since $g$ commutes with $u$ we have that $v^n = u^ng^n$. Therefore if $u^n = 1$ then $v^n = 1$ by parts 1 and 3 of Proposition 2.2, and if $v^n = 1$ then $u^n \in G(D(H))$, so $u^n = 1$ as explained above.

\begin{corollary}
Let $H$ be a finite-dimensional Hopf algebra over $k$. Then
\[ \exp(H^{\text{cop}}) = \exp(H^{\text{op}}) = \exp(H). \]
\end{corollary}

\begin{proof}
Since $(D(H^{\text{ cop}}), \mathcal{R}) \cong (D(H)^{\text{op}}, \mathcal{R}_{21})$ as quasitriangular Hopf algebras, it follows from part 1 of Theorem 2.5 that $\exp(H^{\text{cop}}) = \exp(H)$. Hence the result follows from part 4 of Proposition 2.2.
\end{proof}

### 3. Invariance of Exponent Under Twisting

In this section we show that $\exp(H)$ is invariant under twisting. First recall Drinfeld’s notion of a twist for Hopf algebras.

\begin{definition}
Let $H$ be a Hopf algebra over $k$. A twist for $H$ is an invertible element $J \in H \otimes H$ which satisfies
\[ (\Delta \otimes I)(J)J_{12} = (I \otimes \Delta)(J)J_{23} \quad \text{and} \quad (\varepsilon \otimes I)(J) = (I \otimes \varepsilon)(J) = 1. \]

Given a twist $J$ for $H$, we can construct a new Hopf algebra $H^J$, which is the same as $H$ as an algebra, with coproduct $\Delta^J$ given by
\[ \Delta^J(x) = J^{-1}\Delta(x)J, \quad x \in H. \]

If $(H, R)$ is quasitriangular then so is $H^J$ with the $R$-matrix
\[ R^J = J_{21}^{-1}RJ. \]

In particular, since $H$ is a Hopf subalgebra of $D(H)$, we can twist $D(H)$ using the twist $J \in D(H) \otimes D(H)$ and obtain $(D(H)^J, \mathcal{R}^J)$.

\begin{proposition}
Let $H$ be a finite-dimensional Hopf algebra over $k$, and let $J$ be a twist for $H$. Then $(D(H^J), \mathcal{R}) \cong (D(H)^J, \mathcal{R}^J)$ as quasitriangular Hopf algebras.
\end{proposition}

\begin{proof}
Let $H_+$ and $H_-$ be the Hopf subalgebras of $D(H)^J$ generated by the left and right components of $\mathcal{R}^J$ respectively. Clearly, $H_+ \subseteq H^J$. In order to prove the theorem it is sufficient to prove that the multiplication map $H_+ \otimes H_- \to D(H)^J$ is a linear isomorphism, since then $H_+ = H^J$ (by dimension counting) and the result will follow.

Clearly, $\dim(H_+) \leq \dim(H)$ and $\dim(H_-) = \dim(H_+)$, so we need to show that $H_+ H_- = D(H)$. Since $JR_{21}^J R_{21}^J = R_{21} R_2$ we have that

\[ HH_- = \]
Let $A = H_+H_-=H_-H_+$, $\dim(H) = d$, $\dim(H_+) = d_+$, $\{v_1, \ldots, v_{d/d_+}\}$ with $v_1 = 1$ be a basis of $H$ as a right $H_+$-module, and $\{w_1, \ldots, w_{d/d_+}\}$ with $w_1 = 1$ be a basis of $H$ as a left $H_+$-module (such bases exist by the freeness theorem for Hopf algebras [NZ]). Then we get by dimension counting that $D(H) = \bigoplus_{i,j=1}^{d/d_+} v_i Aw_j$. Thus, $HH_- \cap H_-H = A$, hence $H \subseteq A$ which implies that $HAH = A$, and the result follows.

**Theorem 3.3.** Let $H$ be a finite-dimensional Hopf algebra over $k$, and let $J$ be a twist for $H$. Then $\exp(H) = \exp(HJ)$.

**Proof.** By part 3 of Theorem 2.5, and Proposition 3.2, it is sufficient to show that the order of $R^J_2 R^{J}$ equals to the order of $R_2 R$. But this is clear since they are conjugate.

**Corollary 3.4.** Let $H$ be a finite-dimensional Hopf algebra over $k$. Then $\exp(D(H)) = \exp(H)$.

**Proof.** By [RS], there exists $J \in D(H) \otimes D(H)$ such that

$$D(D(H)) \cong (D(H) \otimes D(H))^J$$

as Hopf algebras. Then using Theorem 3.3 we get that $\exp(D(H))$ equals the order of $u$ in $(D(H) \otimes D(H))^J$ which equals the order of $u$ in $D(H) \otimes D(H)$, and hence equals $\exp(H)$ (since $u_{D(H) \otimes D(H)} = u_{D(H)} \otimes u_{D(H)}$).

**4. The Exponent of a Semisimple and Cosemisimple Hopf Algebra**

In this section, we will show that if $H$ is semisimple and cosemisimple then $\exp(H)$ is finite, and give an estimate for it in terms of $\dim(H)$. Let $H$ be a semisimple and cosemisimple Hopf algebra over $k$ (note that by [LR] the cosemisimplicity assumption is redundant if the characteristic of $k$ is 0). Recall that for semisimple and cosemisimple $H$, $D(H)$ is also semisimple and cosemisimple [R]. Also, by [LR, EG2], $S^2 = I$ and hence $u$ is central in $D(H)$. This implies that $\exp(H)$ equals the smallest positive integer $n$ satisfying $m_n \circ \Delta_n = \varepsilon \cdot 1$, and also to the order of $R$ (by part 1 of Theorem 2.5).

**Remark 4.1.** In [Ka1, Ka2] Kashina studied the smallest positive integer $n$ satisfying $m_n \circ \Delta_n = \varepsilon \cdot 1$, for any finite-dimensional Hopf algebra $H$. In particular she observed the analogous properties listed in Proposition 2.2, and proved an analogue to Corollary 3.4 under the assumption that this smallest $n$ is the same for $H$ and $H^{cop}$.

**Theorem 4.2.** Let $(H, R)$ be a semisimple triangular Hopf algebra over a field $k$ of characteristic 0. Then $\exp(H)$ divides $\dim(H)$.
Proof. By part 8 of Proposition 2.2, we may assume that \( k \) is algebraically closed. Now, it is straightforward to check that the theorem holds for \((k[G], 1 \otimes 1)\) where \( G \) is a finite group. But by [EG1, Theorem 2.1], there exist a finite group \( G \) and a twist \( J \in k[G] \otimes k[G] \) such that \( H \cong k[G]_J \) as Hopf algebras. Hence the result follows from Theorem 3.3.

Theorem 4.3. Let \( H \) be a semisimple and cosemisimple Hopf algebra over \( k \). Then \( \exp(H) \) divides \( \dim(H)^3 \).

Theorem 4.3 will be proved later.

Corollary 4.4. Let \( H \) be a semisimple and cosemisimple Hopf algebra over \( k \), and let \( B \) be a finite-dimensional semisimple Hopf algebra in the category of Yetter-Drinfeld modules over \( H \). Then the order of the antipode of \( B \) is finite and divides \( 2\dim(H)^3 \), and if \( H \) is semisimple triangular and the characteristic of \( k \) is 0, then the order of the antipode of \( B \) is finite and divides \( 2\dim(H)^3 \).

Proof. Follows from Theorems 4.2 and 4.3, and [Ka1, Theorem 6].

Remark 4.5. Theorem 4.3 is motivated by Vafa’s theorem [V]. Vafa’s theorem (see [Ki] for the mathematical exposition) states that the twists in a semisimple modular category act on the irreducible objects by multiplication by roots of unity. Thus, the fact that \( u \in D(H) \) has a finite order follows from the fact that the category of representations of \( D(H) \) is modular, with system of twists given by the action of the central element \( u \) (see e.g. [EG1]).

Kashina conjectured the following:

Conjecture 4.6. Let \( H \) be a semisimple and cosemisimple Hopf algebra over \( k \). Then \( \exp(H) \) is finite and divides \( \dim(H) \).

This conjecture was checked by Kashina in a number of special cases [Ka1, Ka2]. Our results presented above give a proof to the first part of the conjecture, and additional supportive evidence for its second part.

Now we will prove Theorem 4.3. In order to do this, we need a lemma.

Lemma 4.7. Let \( H \) be a Hopf algebra of finite dimension \( d \) over \( k \), \( \mathcal{R} \in H \otimes H^{*\text{cop}} \subset D(H) \otimes D(H) \) be the universal \( R \)-matrix, and \( u \in D(H) \) be the Drinfeld element. Then:

1. For any finite-dimensional \( H - \)module \( V_+ \) and finite-dimensional \( H^{*} - \)module \( V_- \), one has \((\det(\mathcal{R}_{|V_+ \otimes V_-}))^d = 1\).
2. For any finite-dimensional \( D(H) - \)module \( V \), one has \((\det(u|_V))^{d^2} = 1\).
Proof. (1) Recall that $(\Delta \otimes I)(R) = R_{13}R_{23}$. Apply this identity to $V_+ \otimes H \otimes V_-$, where $H$ is the regular representation of $H$. Since $V_+ \otimes H = (\dim V_+)H$, this yields, after taking determinants:
\[ (\det(R_{|H \otimes V_-}))^{\dim V_+} = (\det(R_{|V_+ \otimes V_-}))^d(\det(R_{H \otimes V_-}))^{\dim V_+}. \]
The result follows after cancellation.

(2) We use Drinfeld's formula, $\Delta(u) = (u \otimes u)(R_{21}R)^{-1}$. Using part 1, and the fact that $D(H) = H^* \otimes H$ as $H^*$—module and $H$—module, we compute:
\[ \det(\Delta(u)|_{V \otimes D(H)}) = (\det(u_V))^d(\det(u_{|D(H)}))^{\dim V}. \]
Since $V \otimes D(H) = (\dim V)D(H)$, the result follows. \hfill \square

Proof of Theorem 4.3. By part 8 of Proposition 2.2, we may assume that $k$ is algebraically closed. Since $u$ is central, we have for any irreducible $D(H)$—module $V$ that $\det(u_V) = \lambda(u, V)^{\dim V}$, where $\lambda(u, V)$ is the eigenvalue of $u$ on $V$. So by Lemma 4.7, $\lambda(u, V)^{\dim V \cdot d^2} = 1$. But by [EG1, Theorem 1.5], and in positive characteristic by [EG2, Theorem 3.7], $\dim V$ divides $d$, so $\lambda(u, V)^d = 1$. Thus, $u^{d^2} = 1$ and we are done by part 2 of Theorem 2.5. \hfill \square

In the non-semisimple case, as we know, Theorem 4.3 fails, and the order of $u$ may be infinite. The analogue of Theorem 4.3 in this case is the following theorem.

Let $A$ be a finite-dimensional algebra. For any two irreducible $A$—modules $V_1$ and $V_2$, write $V_1 \sim V_2$ if they occur as constituents in the same indecomposable $A$—module. Extend $\sim$ to an equivalence relation. For an irreducible module $W$, let $[W]$ be the equivalence class of $W$. For an indecomposable module $V$ let $[V]$ be the equivalence class of any constituent $W$ of $V$. Let $N_V$ be the greatest common divisor of dimensions of elements of $[V]$.

**Theorem 4.8.** Let $H$ be a Hopf algebra of dimension $d$ over an algebraically closed field $k$. Then:

1. For any indecomposable $D(H)$—module $V$, the unique eigenvalue of the central element $z = uS(u)$ on $V$ is a root of unity of order dividing $d^2N_V$.
2. For any indecomposable $D(H)$—module $V$, every eigenvalue of $u$ on $V$ is a root of unity of order dividing $2d^2N_V$ (so the eigenvalues of $u$ on any $D(H)$ module are roots of unity).

Proof. (1) Recall that $z = u^2g$, where $g$ is a grouplike element of $D(H)$. By [NZ], the order of $g$ divides $\dim(H) = d$. Since $V$ is indecomposable and $z$ is central, $z$ has a unique eigenvalue $\lambda(z, V)$ on $V$. For any $W \in [V]$, $\lambda(z, V) = \lambda(z, W)$, so we get, $(\det(u_{|W}))^{2d} = \lambda(z, V)^{d \cdot \dim W}$, which implies by part 2 of Lemma 4.7, that $\lambda(z, V)^{d^2 \cdot \dim W} = 1$.  


Since, any eigenvalue $\mu$ of $u|_V$, has the property $\mu^2 = \lambda(z,V)\nu$, where $\nu$ is an eigenvalue of $g^{-1}$, we have by part 1 that $\mu^{2d^2\dim W} = 1$, and the result follows.

\textbf{Corollary 4.9.} If $\exp(H) = \infty$, then $u$ is not semisimple.

\textbf{Corollary 4.10.} Let $H$ be a finite-dimensional Hopf algebra over a field $k$ of positive characteristic $p$. Then $\exp(H) < \infty$.

\textit{Proof.} Let $u$ be the Drinfeld element of $D(H)$. By part 2 of Theorem 4.8, the eigenvalues of $u$ are roots of unity. Hence there exists a positive integer $a$ such that $u^a = 1 + n$ where $n \in D(H)$ is a nilpotent element. But then $u^{ap^b} = 1$ for a sufficiently large positive integer $b$, and the result follows from part 2 of Theorem 2.5.

\section{5. Concluding Remarks}

In conclusion we would like to formulate some questions.

\textbf{Question 5.1.} Suppose that $H$ is a semisimple and cosemisimple Hopf algebra of dimension $d$ over $k$. If a prime $p$ divides $d$, must it divide $\exp(H)$?

We do not know the answer to this question even in characteristic zero, even for $p = 2$. However, if $H$ is a group algebra then the answer is positive, since the statement is equivalent to (a special case of) Sylow’s first theorem: a finite group whose order is divisible by $p$ has an element of order $p$. So positive answer to Question 5.1 would be a “quantum Sylow theorem”.

\textbf{Question 5.2.} Let $H$ be a semisimple and cosemisimple Hopf algebra over $k$ whose exponent is a power of a prime $p$. Must the dimension of $H$ be a power of the same prime?

This is a special case of Question 5.1, but we still do not know the answer, except for the case $\exp(H) = 2$, when the answer is trivially positive. For group algebras, the statement is equivalent to the well-known group-theoretical result that a finite group where orders of all elements are powers of $p$ is a p-group (a special case of Sylow’s theorem).

\textbf{Question 5.3.} Let $H$ be a finite-dimensional Hopf algebra over $k$ such that the element $u \in D(H)$ is semisimple in the regular representation. Does it follow that $H$ and $H^*$ are semisimple

(1) In characteristic zero?

(2) In positive characteristic $p$?
By Theorem 4.8, part (1) of Question 5.3 is equivalent to the question whether for a finite-dimensional Hopf algebra $H$ in characteristic 0, $\exp(H) < \infty$ implies that $H$ is semisimple.

A positive answer to part (2) of Question 5.3 implies a positive answer to Question 5.1 for involutive Hopf algebras defined over $\mathbb{Z}$ and free as $\mathbb{Z}$-modules (which includes group algebras, i.e. this would generalize Sylow’s theorem). Indeed, if $H$ is such a Hopf algebra then for any prime $p$ dividing the dimension of $H$, either $H/pH$ or $(H/pH)^*$ is not semisimple (as $tr(S^2) = 0$), and hence $D(H)$ is not semisimple. If the answer to part (2) of Question 5.3 is positive, then this would imply that $u$ is not semisimple over $F_p$, i.e. the order of $u$ is divisible by $p$, as desired.

For group algebras, the answer to part (2) of Question 5.3 is positive: in this case semisimplicity of $u$ is equivalent to semisimplicity of $R = \sum g \otimes \delta_g$, which implies that all group elements $g$ are semisimple. This would imply that their orders are not divisible by $p$, which by Sylow’s theorem implies that $p$ does not divide the order of the group.

Acknowledgment

The authors thank Yevgenia Kashina for suggesting the problem, and Susan Montgomery for useful discussions.

References


Department of Mathematics, Harvard University, Cambridge, MA 02138
E-mail address: etingof@abel.math.harvard.edu

Department of Mathematics, University of Southern California, Los Angeles, CA 90089
E-mail address: gelaki@mathg.usc.edu