

## ON SEMISIMPLE HOPF ALGEBRAS OF DIMENSION $pq$

SHLOMO GELAKI AND SARA WESTREICH

(Communicated by Lance W. Small)

**ABSTRACT.** We consider the problem of the classification of semisimple Hopf algebras  $A$  of dimension  $pq$  where  $p < q$  are two prime numbers. First we prove that the order of the group of grouplike elements of  $A$  is not  $q$ , and that if it is  $p$ , then  $q = 1 \pmod{p}$ . We use it to prove that if  $A$  and its dual Hopf algebra  $A^*$  are of Frobenius type, then  $A$  is either a group algebra or a dual of a group algebra. Finally, we give a complete classification in dimension  $3p$ , and a partial classification in dimensions  $5p$  and  $7p$ .

In this paper we consider semisimple Hopf algebras of dimension  $pq$  over an algebraically closed field  $k$  of characteristic 0, where  $p$  and  $q$  are distinct prime numbers. Masuoka has proved that a semisimple Hopf algebra of dimension  $2p$  over  $k$ , where  $p$  is an odd prime, is *trivial* (i.e. is either a group algebra or a dual of a group algebra) [Ma1]. Izumi and Kasaki have proved that Kac algebras (i.e. semisimple Hopf algebras over the field of complex numbers, with an additional condition on the existence of an involution), of dimension  $3p$  over  $k$ , where  $p$  is prime, are trivial [IK]. Thus, a natural conjecture is:

**Conjecture 1.** Any semisimple Hopf algebra of dimension  $pq$  over  $k$ , where  $p$  and  $q$  are distinct prime numbers, is trivial.

A well known property of  $A$ , a finite dimensional semisimple group algebra or a dual of a group algebra, is that it is of *Frobenius type*; that is, the dimension of any irreducible representation of  $A$  divides the dimension of  $A$  (the definition is due to Montgomery [Mo]). A special case of Kaplansky's 6th conjecture [K] is:

**Conjecture 2.** Any semisimple Hopf algebra of dimension  $pq$  over  $k$ , where  $p$  and  $q$  are distinct prime numbers, is of Frobenius type.

In this paper we prove among the rest that Conjecture 1 is equivalent to Conjecture 2 (see Theorem 3.5).

A major role in the analysis is played by  $G(A)$  (where  $G(A)$  denotes the group of grouplike elements of  $A$ ). By [NZ],  $|G(A)|$  is either  $1, p, q$  or  $pq$ . We prove in Theorem 2.1 that if  $p < q$ , then  $|G(A)| \neq q$ , and if  $|G(A)| = p$ , then  $q = 1 \pmod{p}$ . Consequently, we prove in Theorem 2.2 that if  $|G(A)| \neq 1$  and  $q \neq 1 \pmod{p}$ , then  $A$  is a commutative group algebra.

---

Received by the editors August 1, 1997 and, in revised form, March 17, 1998.  
1991 *Mathematics Subject Classification.* Primary 16W30.

The second author's research was supported by the Israel Science Foundation founded by the Israel Academy of Sciences and Humanities.

Thus Theorem 2.2 suggests the following question: When is  $|G(A)| \neq 1$ ? In Proposition 3.1 we prove that this is guaranteed when  $A^*$  is of Frobenius type, and in Theorem 3.2 we prove that if moreover  $q \neq 1 \pmod{p}$ , then  $A$  is a commutative group algebra. In Theorem 3.4 we prove that if  $|G(A^*)| \neq 1$  and  $A^*$  is of Frobenius type, then  $A$  is trivial, and  $|G(A)| = p < q$  or  $pq$ . The equivalence of Conjectures 1 and 2 is thus a consequence of Proposition 3.1 and Theorem 3.4.

A complete classification of semisimple Hopf algebras of dimension  $3p$  is then given in Theorem 4.3. Indeed, they are all trivial.

We conclude by using Theorem 2.2 to prove in Theorem 4.5 that if  $A$  is a semisimple Hopf algebra of dimension  $5p$ ,  $p$  an odd prime, and if  $p = 2$  or  $4 \pmod{5}$  or  $p \in \{13, 23\}$ , then  $A$  is a commutative group algebra. Moreover, we obtain in Theorem 4.6 the same result for semisimple  $A$  of dimension  $7p$ ,  $p$  a prime, and  $p = 6 \pmod{7}$  or  $p \in \{17, 31\}$ .

## 1. PRELIMINARIES

In this paper  $k$  will always denote an algebraically closed field of characteristic 0.

Recall that a finite dimensional Hopf algebra over  $k$  is semisimple if and only if it is cosemisimple [LR].

Let  $A$  be semisimple Hopf algebra over  $k$ , and let  $\rho_V : A \rightarrow \text{End}_k(V)$  be a finite dimensional representation of  $A$ . The associated character  $\chi_V$  is given by  $\chi_V(a) = \text{tr}(\rho_V(a))$  for all  $a \in A$ . A character  $\chi_V$  is called irreducible if the representation  $V$  is irreducible. Let  $R(A)$  denote the character ring of  $A$ ; that is, the  $k$ -subalgebra of  $A^*$  generated by the characters  $\chi_V$  of finite dimensional  $A$ -modules  $V$ . The set of all irreducible characters forms a basis of  $R(A)$  [La]. Zhu has proved that  $R(A)$  is semisimple and if  $e_{A^*}, e_1, \dots, e_k$  are the primitive idempotents of  $R(A)$ , where  $e_{A^*}$  is an integral of  $A^*$ , then

$$(1) \quad \dim A = 1 + \sum_{i=1}^k \dim(e_i A^*)$$

and the dimension of each  $e_i A^*$  divides the dimension of  $A$  [Z]. Note that  $\dim R(A) \geq k + 1$ , and equality holds if and only if  $R(A)$  is commutative.

Let  $f : A \rightarrow A^*$  be the map given by  $f(a) = a \rightharpoonup \lambda = \sum \langle a, \lambda_{(2)} \rangle \lambda_{(1)}$  for all  $a \in A$ , where  $\lambda$  is a non-zero integral of  $A^*$ . Recall that  $f$  gives a linear isomorphism between  $kG(A)$  and the sum of the 1-dimensional ideals of  $A^*$ , and a linear isomorphism between the center  $Z(A)$  of  $A$  and  $R(A)$ . Therefore, using the notation of (1),  $\dim(e_i A^*) = 1$  for some  $i$  if and only if  $G(A) \cap Z(A) \neq \{1\}$ .

Let  $A$  be a semisimple Hopf algebra over  $k$ . Any simple subcoalgebra  $C_l$  of  $A^*$  has a basis  $\{x_{ij}^l \mid 1 \leq i, j \leq n_l\}$ , where  $\Delta(x_{ij}^l) = \sum_{k=1}^{n_l} x_{ik}^l \otimes x_{kj}^l$  and  $\varepsilon(x_{ij}^l) = \delta_{i,j}$ . Note that  $n_l = 1$  if and only if  $C_l = \{g\}$  for some  $g \in G(A)$ . Nichols and Richmond have proved that if  $\dim A$  is odd, then  $A$  does not have a 2-dimensional irreducible module [NR], hence

$$(2) \quad \dim A = |G(A)| + \sum_l n_l^2, \quad n_l \geq 3.$$

Now,  $L$  is an irreducible left coideal of  $C_l$  if and only if

$$(3) \quad L = L_j^l = \text{sp}\{x_{kj}^l \mid 1 \leq k \leq n_l\}$$

for some  $1 \leq j \leq n_l$ . Similarly,  $R$  is an irreducible right coideal of  $C_l$  if and only if

$$(4) \quad R = R_k^l = \text{sp}\{x_{kj}^l | 1 \leq j \leq n_l\}$$

for some  $1 \leq k \leq n_l$ . Note that

$$(5) \quad \dim(L_j^l \cap R_k^l) = 1$$

for any  $1 \leq j, k \leq n_l$ .

In what follows we recall some of the properties of a Hopf algebra with a projection, which we shall use in the sequel.

**Theorem 1.1** ([R]). *If  $H \xrightarrow{i} A \xrightarrow{\pi} H$  is a sequence of finite dimensional Hopf algebra maps where  $i$  is injective,  $\pi$  is surjective and  $\pi \circ i = \text{id}_H$ , then there exists  $B \subseteq A$  so that:*

- (i)  $B$  is a left  $H$ -module algebra and coalgebra via the adjoint action.
- (ii)  $B$  is a left  $H$ -comodule algebra and coalgebra via  $\rho(b) = \sum b^{(1)} \otimes b^{(2)} = \sum \pi(b_{(1)}) \otimes b_{(2)}$ .
- (iii)  $B \cong A/AH^+$  as a coalgebra, via the map  $b \times h \mapsto b\varepsilon(h)$ .
- (iv)  $B$  is a left coideal subalgebra of  $A$ .
- (v) As an algebra  $A = B \times H$  is a smash product.
- (vi) As a coalgebra  $A = B \times H$  is a smash coproduct, that is:  $\Delta(b \times h) = \sum b_{(1)} \times b_{(2)}^{(1)} h_{(1)} \otimes b_{(2)}^{(2)} \times h_{(2)}$ .
- (vii) The map  $B \times H \rightarrow A(b \times h \mapsto bi(h))$  is an isomorphism of bialgebras.

## 2. ON THE ORDER OF $G(A)$ AND $G(A^*)$

In this section we prove some results concerning the group of grouplike elements of semisimple Hopf algebras of dimension  $pq$ .

**Theorem 2.1.** *Let  $A$  be a semisimple Hopf algebra of dimension  $pq$  over  $k$ , where  $p < q$  are two prime numbers. Then:*

1.  $|G(A)| \neq q$ .
2. If  $|G(A)| = p$ , then  $q = 1 \pmod{p}$ .

*Proof.* 1. Suppose to the contrary that  $|G(A)| = q$ . If  $G(A) \cap Z(A) = G(A)$ , then  $H = kG(A)$  is central in  $A$ , hence is a normal sub-Hopf algebra of  $A$ . Since  $A/AH^+$  is a Hopf algebra of dimension  $p$  it follows by [Z] that  $A/AH^+ \cong kC_p$ . An elementary argument which follows from [Ma2, Section 2], shows that  $A$  is isomorphic as an algebra to the twisted group ring  $kC_q^t[C_p]$  of the cyclic group  $C_p$  over the commutative algebra  $kC_q$ , and hence must be commutative. Thus,  $A^*$  is a group algebra and hence of Frobenius type. By (2),  $pq = q + ap^2 + bq^2$  for some integers  $a, b \geq 0$ . But  $p < q$ , hence  $b = 0$ , which yields a contradiction. We conclude that  $G(A) \cap Z(A) = \{1\}$ . Therefore, using the notation of (1),  $\dim(e_i A^*) \in \{p, q\}$  for all  $i$ . Let  $E_0$  be the integral of  $H = kG(A)$  with  $\varepsilon(E_0) = 1$ . Since  $\dim(A/AH^+) = p$ , it follows that  $AH^+ = A(1 - E_0)$  has dimension  $(q - 1)p$  and thus  $\dim(AE_0) = p$ . Moreover,  $E_0 e_A = e_A$ , hence  $E_0 = e_A + \sum_j e_{i_j}$ . But  $p < q$ , hence counting dimensions yields a contradiction and the result follows.

2. If  $G(A) \cap Z(A) = G(A)$ , then  $H = kG(A)$  is central in  $A$ , and hence  $A$  is commutative. Therefore,  $A^*$  is a group algebra and hence of Frobenius type. By (2),  $pq = p + ap^2 + bq^2$  for some integers  $a, b \geq 0$ . Clearly,  $b = 0$  and hence  $q = 1 + ap$ . If  $G(A) \cap Z(A) = \{1\}$ , then using the notation of (1),  $\dim(e_i A^*) \in \{p, q\}$  for all  $i$ . Since  $\dim(A/AH^+) = q$ , it follows that  $AH^+ = A(1 - E_0)$  has dimension  $(p - 1)q$

and thus  $\dim(AE_0) = q$ . Hence,  $E_0 = e_A + \sum_j e_{i_j}$ . But, counting dimensions yields that  $\dim(e_{i_j}A^*) = p$  for all  $j$ , and the result follows in this case as well.  $\square$

As a direct consequence of Theorem 2.1 we have:

**Theorem 2.2.** *Let  $A$  be a semisimple Hopf algebra of dimension  $pq$  over  $k$ , where  $p < q$  are two prime numbers satisfying  $q \not\equiv 1 \pmod{p}$ . If  $|G(A)| \neq 1$ , then  $A$  is a commutative group algebra.*

### 3. THE MAIN RESULT

In this section we consider semisimple Hopf algebras  $A$  of dimension  $pq$  such that  $A^*$  is of Frobenius type. First we find out when  $|G(A)| \neq 1$  is guaranteed.

**Proposition 3.1.** *Let  $A$  be a semisimple Hopf algebra of dimension  $pq$  over  $k$ , where  $p < q$  are two prime numbers. If  $A^*$  is of Frobenius type, then either  $|G(A)| = p$  and  $q \equiv 1 \pmod{p}$ , or  $|G(A)| = pq$ .*

*Proof.* If  $A$  is cocommutative, then  $|G(A)| = pq$ . Otherwise,  $|G(A)| \neq pq$ , and by Theorem 2.1,  $|G(A)| \neq q$ . If  $|G(A)| = 1$ , then by (1),  $pq = 1 + ap^2 + bq^2$  for some integers  $a, b \geq 0$ , as  $A^*$  is of Frobenius type. But,  $q^2 > pq$  hence  $b = 0$  which yields a contradiction.  $\square$

As a corollary of Proposition 3.1 we have:

**Theorem 3.2.** *Let  $A$  be a semisimple Hopf algebra of dimension  $pq$  over  $k$ , where  $p < q$  are two prime numbers satisfying  $q \not\equiv 1 \pmod{p}$ . If  $A^*$  is of Frobenius type, then  $A$  is a commutative group algebra.*

In the following proposition we determine the coalgebra structure of  $A$ .

**Proposition 3.3.** *Let  $A$  be a non-cocommutative and non-commutative semisimple Hopf algebra of dimension  $pq$  over  $k$ , where  $p < q$  are prime numbers. Let  $R(A^*)$  be the character ring of  $A^*$ . If  $A^*$  is of Frobenius type, then:*

1.  $R(A^*)$  is commutative.
2. As a coalgebra  $A = k1 \oplus kg \oplus \dots \oplus kg^{p-1} \oplus C_1 \oplus \dots \oplus C_a$ , where  $a = \frac{q-1}{p}$ ,  $g$  is a grouplike element and  $C_i$  is a simple subcoalgebra of  $A$  of dimension  $p^2$  for all  $1 \leq i \leq a$ .
3.  $gC_i = C_i = C_i g$  for all  $1 \leq i \leq a$ .

*Proof.* Set  $H = kG(A)$ . By Theorem 2.1 and Proposition 3.1,  $\dim H = p$ . If  $H$  is central in  $A$ , then (as in the proof of Theorem 2.1)  $A$  must be commutative. Therefore, we conclude that  $G(A) \cap Z(A) = \{1\}$ .

Set  $n = \dim R(A^*) - 1$ . Then, by (1) there exist two natural numbers  $a$  and  $b$  such that:

$$(6) \quad pq = 1 + ap + bq$$

and

$$(7) \quad n \geq a + b.$$

Clearly,  $a \geq 1$  and  $b < p$ . Moreover,  $A^*$  is of Frobenius type and  $p < q$ , hence by (2)

$$(8) \quad pq = p^2(n + 1 - p) + p.$$

Substituting (6) and (7) in (8) yields

$$pq \geq p^2(a+b+1-p) + p = p^2 \left( \frac{(p-b)q-1}{p} + b+1-p \right) + p$$

and hence  $(1-p+b)q \geq (1-p+b)p$ . Since  $p < q$  and  $b < p$ , this is possible if and only if  $b = p-1$  and equality holds in (7). This implies that  $R(A^*)$  is commutative and that  $pq = 1 + ap + (p-1)q$ , and hence  $a = \frac{q-1}{p}$ . Let

$$e_A, e_1, \dots, e_a, e_{a+1}, \dots, e_{a+p-1}$$

be the primitive idempotents of  $R(A^*)$ , where  $e_A$  is the integral of  $A$  with  $\varepsilon(e_A) = 1$ ,  $\dim(Ae_i) = p$  for  $1 \leq i \leq a$  and  $\dim(Ae_{a+j}) = q$  for  $1 \leq j \leq p-1$ . Let  $E_0 = \frac{1}{p} \sum_{i=0}^{p-1} g^i$  be an integral of  $H$  where  $g$  is a generator of  $G(A)$ . Since  $\dim(A/AH^+) = q$ , it follows that  $AH^+ = A(1-E_0)$  has dimension  $(p-1)q$  and thus  $\dim(AE_0) = q$ . Moreover,  $E_0e_A = e_A$ , hence counting dimensions yields that

$$E_0 = e_A + e_1 + \dots + e_a.$$

Since  $R(A^*)$  is commutative,  $\dim(R(A^*)e_A) = \dim(R(A^*)e_i) = 1$  for all  $1 \leq i \leq a$ , and hence

$$(9) \quad \dim(R(A^*)E_0) = a + 1.$$

Since the set of all the irreducible left  $A^*$ -modules consists of  $p$  1-dimensional modules and  $a = \frac{q-1}{p}$   $p$ -dimensional modules, it follows that

$$A = k1 \oplus kg \oplus \dots \oplus kg^{p-1} \oplus C_1 \oplus \dots \oplus C_a$$

as a coalgebra, where  $C_i$  is a simple subcoalgebra of  $A$  of dimension  $p^2$  for all  $1 \leq i \leq a$ . Let

$$\{1, g, \dots, g^{p-1}, \chi_1, \dots, \chi_a\}$$

be the set of irreducible characters of  $A^*$ , where  $\chi_i$  corresponds to  $C_i$ . This set clearly forms a basis of  $R(A^*)$ . Then

$$R(A^*)E_0 = sp\{E_0, E_0\chi_1, \dots, E_0\chi_a\}$$

which implies by (9) that  $\{E_0, E_0\chi_1, \dots, E_0\chi_a\}$  forms a basis of  $R(A^*)E_0$ . If  $g\chi_i = \chi_j$  for  $i \neq j$ , then  $E_0\chi_i = E_0\chi_j$  which is a contradiction. Therefore,  $g\chi_i = \chi_i$ , and hence

$$gC_i = C_i = C_i g$$

for all  $i$ . This concludes the proof of the proposition.  $\square$

**Theorem 3.4.** *Let  $A$  be a semisimple Hopf algebra of dimension  $pq$  over  $k$ , where  $p < q$  are prime numbers. If  $A^*$  is of Frobenius type and  $|G(A^*)| \neq 1$ , then  $A$  is trivial, and  $|G(A)| = p < q$  or  $pq$ .*

*Proof.* If  $A$  is either cocommutative or commutative, then  $A$  is either a group algebra or a dual of a group algebra respectively. In any event  $A^*$  is of Frobenius type, hence by Proposition 3.1,  $|G(A)| = p < q$  or  $pq$  and we are done.

Suppose that  $A$  is not cocommutative and not commutative. Then Proposition 3.3 is applicable. Set  $H = kG(A)$ . By Proposition 3.1,  $|G(A)| = p$ . Let  $g$  be a generator of  $G(A)$ . By Theorem 2.1,  $|G(A^*)| \neq q$ , hence  $|G(A^*)| = p$  too. Thus we have the following sequence of maps:

$$H \xrightarrow{i} A \xrightarrow{\pi} H$$

where  $i$  is the inclusion map and  $\pi$  is a surjection homomorphism of Hopf algebras. If  $\pi \circ i = \varepsilon$ , then  $H \subseteq K = A^{coH}$ . Since  $K$  is a left coideal of  $A$ , it is a direct sum of irreducible left coideals  $K = k1 \oplus kg \oplus \cdots \oplus kg^{p-1} \oplus V_1 \oplus \cdots \oplus V_n$ . Since  $A^*$  is of Frobenius type it follows that  $\dim V_i = p$  for all  $i$ . But, this is a contradiction since  $p$  does not divide  $\dim K = q$ . Therefore  $\pi \circ i \neq \varepsilon$  and we may assume that  $\pi \circ i = id_H$ . Therefore by Theorem 1.1, there exists  $B \subset A$  so that  $A \cong B \times H$ . By Theorem 1.1(iv),  $B$  is a left coideal of  $A$ , hence a direct sum of irreducible left coideals of  $A$ . By Proposition 3.3(2), the dimensions of these irreducible left coideals are either 1 or  $p$ . Since  $\dim B = q$ , it follows that  $B$  contains an irreducible left coideal  $V$  of  $A$ , of dimension  $p$ . Since  $V \subset C$  for some  $p^2$ -dimensional simple subcoalgebra  $C$ , it follows by Theorem 1.1(vii) and Proposition 3.3(3), that  $V \times H \subseteq C$ . But,  $\dim(V \times H) = p^2 = \dim C$ , hence  $V \times H = C$ . By Theorem 1.1(iii),  $A/AH^+ \cong B$  as coalgebras, and  $V$  is the image of  $C = V \times H$  under this isomorphism, hence

$V$  is a subcoalgebra of  $B$ .

We wish to prove that  $V$  is a simple subcoalgebra of  $B$  and thus to reach a contradiction. Note that since  $V$  is an irreducible left coideal of  $A$  it follows that  $V \times g^i$  is also an irreducible left coideal of  $A$  for all  $0 \leq i \leq p-1$ . By Proposition 3.3(3), it follows that

$$\{V \times g^i \mid 0 \leq i \leq p-1\}$$

is the set of all the irreducible left coideals of  $A$  contained in  $C$ . Since  $V$  is a left coideal of  $A$ , it follows from Theorem 1.1(ii) that  $V$  is an  $H$  subcomodule of  $B$ . Let  $\rho : B \rightarrow H \otimes B$  be the comodule structure map, and write  $V = \bigoplus_{i=0}^{p-1} V_i$ , where  $V_i = \rho^{-1}(g^i \otimes V)$ . We claim that  $\dim V_i = 1$  for all  $i$ . Indeed, let  $\{v_0, \dots, v_{p-1}\}$  be a basis of  $V$  consisting of homogeneous elements; that is,  $\rho(v_i) = g^{m_i} \otimes v_i$  for some  $0 \leq m_i \leq p-1$ . Let  $0 \neq v \in V$  and write  $\Delta_B(v) = \sum_{i=0}^{p-1} b_i \otimes v_i$ . Then by Theorem 1.1(vi),

$$\Delta_A(v \times 1) = \sum_{i=0}^{p-1} b_i \times g^{m_i} \otimes v_i \times 1.$$

Therefore, using Kaplansky's notation [K],  $L(v \times 1) = sp\{b_i \times g^{m_i} \mid 0 \leq i \leq p-1\} \subset C$  is a *right* coideal of  $A$  of dimension  $\leq p$ . Since  $C$  is a simple subcoalgebra of  $A$  of dimension  $p^2$ , it follows that  $\dim(L(v \times 1)) = p$  and  $L(v \times 1)$  is irreducible. Therefore by (5),  $\dim(L(v \times 1) \cap (V \times g^i)) = 1$  for all  $i$ , hence  $\{m_i \mid 0 \leq i \leq p-1\} = \{0, 1, \dots, p-1\}$ . Thus  $V$  has a basis  $\{v_i \mid 0 \leq i \leq p-1\}$ , where  $\rho(v_i) = g^i \otimes v_i$ . Since  $V$  is an  $H$ -comodule coalgebra it follows that  $\Delta_B(V_i) \subseteq \sum_{j=0}^{p-1} V_j \otimes V_{i-j}$ , hence  $\Delta_B(v_i) = \sum_{j=0}^{p-1} \alpha_{ij} v_j \otimes v_{i-j}$  for all  $i$ , for some  $\alpha_{ij} \in k$ . Computing  $\Delta_A(v_i \times 1)$  yields that  $R_i = L(v_i \times 1) = sp\{\alpha_{ij} v_j \times g^{i-j} \mid 0 \leq j \leq p-1\} \subset C$  is a right coideal of  $A$  of dimension  $\leq p$ , for all  $i$ . Hence  $\dim R_i = p$  and

$$(10) \quad R_i = sp\{v_j \times g^{i-j} \mid 0 \leq j \leq p-1\}$$

is irreducible. It is straightforward to verify that  $R_i \neq R_t$  for  $i \neq t$ , and hence the set  $\{R_i \mid 0 \leq i \leq p-1\}$  is the set of *all* the irreducible right coideals of  $A$  which are contained in  $C$ .

Finally, let  $D \subseteq V$  be a subcoalgebra. By Theorem 1.1(vi),  $D \times H \subseteq C$  is a *right* coideal of  $A$  and hence  $D \times H = \bigoplus_l R_{i_l}$ , where  $R_{i_l}$  is as in (10). But, the image of  $D \times H$  under the map  $id \otimes \varepsilon : A \rightarrow B$  equals  $D$ , while the image of  $\bigoplus_l R_{i_l}$  under

this map equals  $V$ . Therefore  $D = V$ , and hence  $V$  is a simple coalgebra. But, this is a contradiction since  $\dim V = p$  is not a square.  $\square$

As a corollary we obtain the following:

**Theorem 3.5.** *Let  $A$  be a semisimple Hopf algebra of dimension  $pq$  over  $k$ , where  $p < q$  are prime numbers. If both  $A$  and  $A^*$  are of Frobenius type, then  $A$  is trivial.*

*Proof.* Follows from Proposition 3.1 and Theorem 3.4.  $\square$

#### 4. THE DIMENSIONS $3p, 5p$ AND $7p$

We start this section with a complete classification of semisimple Hopf algebras of dimension  $3p$ .

**Proposition 4.1.** *Let  $A$  be a non-cocommutative semisimple Hopf algebra of dimension  $3p$  over  $k$ , where  $p > 3$  is prime. Then  $|G(A)| = 3$ .*

*Proof.* By Theorem 2.1,  $|G(A)| \neq p$ . Since  $A$  is non-cocommutative,  $|G(A)| \neq 3p$ . Assume  $|G(A)| = 1$  and let  $R(A^*) \subseteq A$  be the ring of characters of  $A^*$ . Set  $n = \dim R(A^*) - 1$ . Then by (1), there exist two natural numbers  $a$  and  $b$  such that

$$3p = 1 + 3a + bp \quad \text{and} \quad n \geq a + b.$$

Note that  $a \geq 1$  and hence  $b = 1$  or  $2$ . Since  $2$  does not divide  $3p$ , and  $A^*$  is semisimple we have by [NR] that  $A^*$  does not have a 2-dimensional irreducible module and hence the following two inequalities hold:

$$n \geq a + 1 = \frac{(3-b)p + 2}{3} \quad \text{and} \quad 3p \geq 9n + 1.$$

But these two inequalities are incompatible since they imply that  $(-6 + 3b)p \geq 7$  which is impossible. This concludes the proof of the proposition.  $\square$

**Proposition 4.2.** *Every semisimple Hopf algebra  $A$  of dimension  $3p$  over  $k$ , where  $p > 3$  is prime, is of Frobenius type.*

*Proof.* If  $A$  is a group algebra or a dual of a group algebra, then it is known that  $A$  is of Frobenius type. Otherwise, by Proposition 4.1,  $|G(A)| = 3$ . Since  $A$  is non-commutative we must have  $G(A) \cap Z(A) = \{1\}$ .

Set  $n = \dim R(A^*) - 1$ . Then, by (1) there exist two natural numbers  $a$  and  $b$  such that:

$$3p = 1 + 3a + bp \quad \text{and} \quad n \geq a + b.$$

Clearly,  $a \geq 1$  and hence  $b = 1$  or  $2$ . Since  $2$  does not divide  $3p$  we have by [NR] that  $A^*$  does not have a 2-dimensional irreducible module and hence that the following two inequalities hold:

$$n \geq a + b \quad \text{and} \quad 3p \geq 9(n - 2) + 3.$$

Therefore,  $3p \geq 9\left(\frac{(3-b)p-1}{3} + b - 2\right) + 3$  and hence  $(-2 + b)p \geq 3b - 6$ . Clearly, this is possible if and only if the equalities above hold, and  $b = 2$ . Therefore,  $3p = 1 + 3a + 2p$  and  $a = \frac{p-1}{3}$ . This implies that  $R(A^*)$  is commutative and that

$$A = k1 \oplus kg \oplus kg^2 \oplus C_1 \oplus \cdots \oplus C_a$$

as a coalgebra where  $C_i$  is a simple subcoalgebra of  $A$  of dimension 9 for all  $1 \leq i \leq a$ . Hence  $A^*$  is of Frobenius type. Replacing  $A$  by  $A^*$  yields the same result for  $A$ .  $\square$

As a corollary of the above and of Theorem 3.5 we have:

**Theorem 4.3.** *A semisimple Hopf algebra of dimension  $3p$  over  $k$ , where  $p > 3$  is prime, is trivial.*

We conclude the paper by considering semisimple Hopf algebras of dimensions  $5p$  and  $7p$ .

**Lemma 4.4.** *Let  $A$  be a semisimple Hopf algebra of odd dimension over  $k$ . If  $|G(A)| = 1$ , then there exists an irreducible  $A^*$ -module  $V$  with  $\dim V \geq 4$ .*

*Proof.* Suppose on the contrary that for any non-trivial  $A^*$ -irreducible module  $V$ ,  $\dim V \leq 3$ . Then by [NR],  $\dim V = 3$ . Hence,  $\dim(V \otimes V^*) = 9$  and by [La],  $V \otimes V^* = k \oplus V_1 \oplus \cdots \oplus V_i$ , where  $V_j \neq k$  is an  $A^*$ -irreducible module for all  $j$ . Since  $\dim V_j = 3$ , this is a contradiction.  $\square$

**Theorem 4.5.** *Let  $A$  be a semisimple Hopf algebra over  $k$ . If  $\dim A = 5p$ ,  $p$  an odd prime, and if  $p = 2$  or  $4 \pmod{5}$  or  $p \in \{13, 23\}$ , then  $A$  is a commutative group algebra.*

*Proof.* We wish to show that  $|G(A)| \neq 1$ . Suppose on the contrary that  $|G(A)| = 1$ . Set  $n = \dim R(A^*) - 1$ . By (1), there exist two natural numbers  $1 \leq a$  and  $1 \leq b \leq 4$  such that

$$\begin{aligned} 5p &= 1 + 5a + bp, \\ n &\geq a + b \quad \text{and} \\ 5p &\geq 9(n - 1) + 16 + 1 \end{aligned}$$

where the last inequality follows from (2) and Lemma 4.4. Hence  $(-20 + 9b)p \geq 45b + 31$ . But, if  $p = 2$  or  $4 \pmod{5}$ , then  $b = 2$  or  $1$  respectively and if  $p \in \{13, 23\}$ , then  $b = 3$ . In any event this is impossible and we have proved that  $|G(A)| \neq 1$ . The result follows now from Theorem 2.2.  $\square$

**Theorem 4.6.** *Let  $A$  be a semisimple Hopf algebra over  $k$ . If  $\dim A = 7p$ ,  $p$  a prime, and if  $p = 6 \pmod{7}$  or  $p \in \{17, 31\}$ , then  $A$  is a commutative group algebra.*

*Proof.* Suppose  $|G(A)| = 1$  and set  $n = \dim R(A^*) - 1$ . By (1), there exist two natural numbers  $1 \leq a$  and  $1 \leq b \leq 6$  so that

$$\begin{aligned} 7p &= 1 + 7a + bp, \\ n &\geq a + b \quad \text{and} \\ 7p &\geq 9(n - 1) + 16 + 1 \end{aligned}$$

where the last inequality follows from (2) and Lemma 4.4. Thus,  $(-14 + 9b)p \geq 63 + 47$ . But, if  $p = 6 \pmod{7}$  or  $p \in \{17, 31\}$ , then this is impossible. The result follows now from Theorem 2.2.  $\square$

## REFERENCES

- [IK] M. Izumi and I. Kosaki, *Finite-dimensional Kac algebras arising from certain group actions on a factor*, International Math. Research Notes **8** (1996), 357–370. MR **97e**:46082
- [K] I. Kaplansky, *Bialgebras*, University of Chicago, 1975. MR **55**:8087
- [La] R. G. Larson, *Characters of Hopf algebras*, J. Algebra **17** (1971), 352–368. MR **44**:287
- [LR] R. G. Larson and D. E. Radford, *Finite Dimensional Cosemisimple Hopf Algebras in Characteristic 0 are Semisimple*, J. of Algebra **117** (1988), 267–289. MR **89k**:16016
- [Ma1] A. Masuoka, *Semisimple Hopf Algebras of Dimension  $2p$* , Communication in Algebra **23** No. 5 (1995), 1931–1940. MR **96e**:16050
- [Ma2] A. Masuoka, *The  $p^n$  Theorem for Semisimple Hopf Algebras*, Proceedings of the AMS **124** (1996), 735–737. MR **96f**:16046
- [Mo] S. Montgomery, private communication.
- [NR] W. D. Nichols and B. Richmond, *The Grothendieck Group of a Hopf Algebra*, J. of Pure and Applied Algebra **106** (1996), 297–306. MR **97a**:16075
- [NZ] W. D. Nichols, M. B. Zoeller and M. Bettina, *A Hopf algebra freeness theorem*, Amer. J. of Math. **111** (1989), 381–385. MR **90c**:16008
- [R] D. E. Radford, *The Structure of Hopf Algebras with a Projection*, J. of Algebra **2** (1985), 322–347. MR **86k**:16004
- [Z] Y. Zhu, *Hopf algebra of prime dimension*, International Mathematical Research Notices No. 1 (1994), 53–59. MR **94j**:16072

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MASSACHUSETTS 02138  
*Current address*: Department of Mathematics, University of Southern California, Los Angeles,  
California 90089

*E-mail address*: [gelaki@math.usc.edu](mailto:gelaki@math.usc.edu)

INTERDISCIPLINARY DEPARTMENT OF THE SOCIAL SCIENCE, BAR-ILAN UNIVERSITY, RAMAT-  
GAN, ISRAEL

*E-mail address*: [swestric@mail.biu.ac.il](mailto:swestric@mail.biu.ac.il)