Алгебра и анализ
Том 25 (2013), № 5

St. Petersburg Math. J.
Vol. 25 (2014), No. 5, Pages 855–868
S 1061-0022(2014)01319-2
Article electronically published on July 18, 2014

GENERALIZED COCOMMUTATIVITY OF SOME HOPF ALGEBRAS AND THEIR RELATIONSHIP WITH FINITE FIELDS

S. YU. SPIRIDONOVA

Abstract. Semisimple finite-dimensional Hopf algebras with only one summand of dimension not equal to one are considered. The group of group-like elements in the dual Hopf algebra is assumed to have minimal order and to be cyclic. Under these restrictions it is proved that the Hopf algebra is cocommutative up to numerical coefficients in the comultiplication and the antipode. A natural relationship is established between such Hopf algebras and finite fields, and it is proved that these Hopf algebras exist only for $n = p^k - 1$, where n is the order of the group of group-like elements in the dual Hopf algebra, p is prime, and k is a positive integer.

§1. Introduction

The Hopf algebras are of interest as structures that combine the notions of algebra and coalgebra and, like groups, they possess an antipode that takes any element to its inverse (see [4]). In particular, the classification of semisimple finite-dimensional Hopf algebras over algebraically closed fields is of interest. It is known that all semisimple (co)commutative Hopf algebras are either group algebras or dual to them [4]. At the same time, the question concerning the non(co)commutative algebras remains open. The semisimple Hopf algebras with only one summand of dimension not equal to one represent the simplest noncommutative case. The classification of the Hopf algebras of the class next in order of complexity, namely, those with several summands of pairwise distinct dimensions not equal to one, was reduced in [3] to the case of one summand of dimension not equal to one.

As was shown in [4, §3.1], the one-dimensional summands in the semisimple decomposition correspond to group-like elements of the dual Hopf algebra.

If we restrict ourselves to algebras with only one irreducible summand of dimension not equal to one, then any such algebra over an algebraically closed field k has the form

$$H = \bigoplus_{h\in G} ke_h \oplus \mathrm{Mat}(n,k)E, \tag{1.1}$$

where $G = G(H^*)$ is the group of group-like elements of H^*, and the set $\{e_h, h \in G\}$ is a system of orthogonal central idempotents in H.

In the general form, the semisimple Hopf algebras over an algebraically closed field of characteristic not dividing the dimension of the algebra were considered in [1]. As was shown in [1, §§1, 2], the comultiplication in an algebra of the form (1.1) looks like this:

$$\Delta(x) = \begin{cases} \sum_h [(h \rightharpoonup x) \otimes e_h + e_h \otimes (x \leftharpoonup h)] + \Delta'(x), & x \in \mathrm{Mat}(n,k), \\ \sum_{f\in G} e_f \otimes e_{f^{-1}h} + \Delta_h, & x = e_h, \end{cases}$$

2010 *Mathematics Subject Classification.* Primary 16T05.

Key words and phrases. Semisimple Hopf algebras, group of group-like elements, cocommutativity in the wide sense finite fields.

Partially supported by RFBR (grant no. 12-01-00070).

where

$$\Delta_h = [1 \otimes (h^{-1} \rightharpoonup)]\Delta_1 = [(\leftharpoonup h^{-1}) \otimes 1]\Delta_1 \in \mathrm{Mat}(n,k) \otimes \mathrm{Mat}(n,k)$$

for all $h \in G$, the element Δ_1 corresponds to the unit element in the group G, and

$$\Delta' : \mathrm{Mat}(n,k) \longrightarrow \mathrm{Mat}(n,k) \otimes \mathrm{Mat}(n,k)$$

is an algebra homomorphism not preserving the unity. Moreover, the left and right actions $f \rightharpoonup x$ and $x \leftharpoonup f$ of the elements $f \in H^*$ on $x \in H$ are given by the following rule: if

$$\Delta(x) = \sum x_{(1)} \otimes x_{(2)},$$

then

$$f \rightharpoonup x = \sum x_{(1)} \langle f,\ x_{(2)} \rangle, \quad x \leftharpoonup f = \sum \langle f,\ x_{(1)} \rangle x_{(2)}.$$

Next, the order of $G = G(H^*)$ divides n^2, because the number of one-dimensional summands divides the dimension of the algebra (see [4, §3.1]) and $\dim(H) = |G| + n^2$. The case of maximal order, $|G| = n^2$, occurs if and only if $\Delta' = 0$ (see [1, §4]). The algebras of that type were classified in [2]. If $\Delta' \neq 0$, then the order of the group G is equal to nq, where q divides n (see [1, §9]).

In the present paper, we study the case where the group G has minimal order n and is cyclic. The case of a cyclic group G of an arbitrary order n generalizes the case of algebras of the type $(1, p; p, 1)$ treated in [5], i.e., algebras of the form (1.1) with prime $n = p$. That case was completely described in [5], where it was proved that, for $p > 2$, the condition $p = 2^k - 1$ is fulfilled for some natural k.

The main result of the present paper shows that Hopf algebras with a cyclic group G of minimal order may exist only for $n = p^k - 1$ and only in a specific form, namely, when they are cocommutative in a certain wide sense. A Hopf algebra of the form (1.1) is said to be *cocommutative in the wide sense* if for any indices i, j, k, l, p, q the symmetric coefficients ω^{ij}_{klpq} and ω^{ij}_{pqkl} are both equal to zero, or are both not equal to zero. Here the coefficients ω^{ij}_{klpq} determine the algebra homomorphism Δ':

$$\Delta'(E_{ij}) = \sum_{k,l,p,q=1}^{n} \omega^{ij}_{klpq} E_{kl} \otimes E_{pq}. \tag{1.2}$$

The algebra that is not cocommutative in the wide sense is said to be *strongly noncocommutative*. As was shown in [6, §7], a Hopf algebra of the form (1.1) is cocommutative if and only if the homomorphism Δ' is cocommutative, which means that the symmetric coefficients ω^{ij}_{klpq} and ω^{ij}_{pqkl} are equal for all indices. Thus, the class of Hopf algebras of the form (1.1) that are cocommutative in the wide sense does include the class of cocommutative algebras.

In §2, we present some auxiliary definitions and statements from [1] and [6].

In §3, we show that with every Hopf algebra H of the form (1.1) with $\dim(H) = n(n+1)$ we can naturally associate a certain multiplicative group M_H of order $n+1$ on which multiplication is given in accordance with the comultiplication in H. Moreover, an operation of addition can be introduced on the group M_H, which is linked with multiplication by several relations similar to distributivity in a field. Next, in §3 we prove that a Hopf algebra is cocommutative in the wide sense if and only if the corresponding multiplicative group M_H is Abelian.

In §4, we show that if a Hopf algebra is cocommutative in the wide sense, then the corresponding structure M_H is a field. This enables us to conclude that Hopf algebras that are cocommutative in the wide sense exist only for $n = p^k - 1$, where p is prime

and k is a positive integer. Also in §4, we introduce a homomorphism $M_H \to S_n$ and consider the case where H is strongly noncommutative.

In §5, using the group M_H and the homomorphism mentioned above, we prove that all the Hopf algebras of the form (1.1) are cocommutative in the wide sense; thus, they exist only for $n = p^k - 1$, where n is prime and k is natural.

§2. Auxiliary definitions and statements

In the Hopf algebras (1.1) under consideration, the coassociativity of comultiplication is equivalent to the following conditions on Δ' (see [1, §§1, 2]):

$$(1 \otimes \Delta')\Delta_1 = (\Delta' \otimes 1)\Delta_1, \tag{2.1}$$

$$\Delta'(x \leftharpoonup h) = [(\leftharpoonup h) \otimes 1]\Delta'(x)\ , \tag{2.2}$$

$$[1 \otimes (h \rightharpoonup)]\Delta'(x) = \Delta'(h \rightharpoonup x)\ , \tag{2.3}$$

$$[1 \otimes (\leftharpoonup h)]\Delta'(x) = [(h \rightharpoonup) \otimes 1]\Delta'(x)\ , \tag{2.4}$$

$$[\Delta'(E) \otimes E][y \otimes \Delta_1] = [(\Delta' \otimes 1)\Delta'(y)](E \otimes \Delta_1)\ , \tag{2.5}$$

$$(\Delta_1 \otimes E)[(1 \otimes \Delta')\Delta'(y)] = [\Delta_1 \otimes y][E \otimes \Delta'(E)]\ , \tag{2.6}$$

$$[\Delta'(E) \otimes E][(1 \otimes \Delta')\Delta'(x)] = [(\Delta' \otimes 1)\Delta'(x)][E \otimes \Delta'(E)] \tag{2.7}$$

for all $x \in \mathrm{Mat}(n, k)$, $h \in G$, where E denotes the identity matrix in $\mathrm{Mat}(n, k)$.

Moreover, in [1, §4] it was shown that the actions $\rightharpoonup$ and $\leftharpoonup$ of the group G on H can be represented in the form

$$h \rightharpoonup x = A_h x A_h^{-1}, \quad x \leftharpoonup h = B_h x B_h^{-1}, \tag{2.8}$$

where the matrices A_h, $B_h \in GL(n,\ k)$ and $h \in G$ satisfy

$$A_h A_f = \lambda_{hf} A_{hf}, \quad \lambda_{hf} \in k^*, \tag{2.9}$$

$$B_h = \omega_h U A_h^t U^{-1}, \quad \omega_h \in k^*, \tag{2.10}$$

$$\operatorname{tr} A_h = n\delta_{e,h}, \tag{2.11}$$

$U \in GL(n,\ k)$ being a (skew-)symmetric matrix.

Moreover, the antipode in H has the form

$$S(x) = \begin{cases} U x^t U^{-1}, & x \in \mathrm{Mat}(n, k), \\ e_{h^{-1}}, & x = e_h, \end{cases}$$

and for Δ_1 we have

$$\Delta_1 = \frac{1}{n} \sum_{i,j=1}^{n} E_{ij} \otimes S(E_{ji}),$$

where the E_{ij} are matrix units. Next, in view of [1, §1], yet another condition

$$\mu(1 \otimes S)\Delta'(x) = \mu(S \otimes 1)\Delta'(x) = 0 \tag{2.12}$$

is imposed on the antipode and the homomorphism Δ'.

Thus, to endow a semisimple finite-dimensional algebra of the form considered with the structure of a Hopf algebra, it is necessary to specify the matrices A_h, B_h, $h \in G$, the matrix U, and the algebra homomorphism Δ' in such a way that all the above conditions be fulfilled.

In [6], it was proved that if the group G is cyclic, then there exists a basis in which the matrix U is monomial, i.e.,

$$U = \sum_{r=1}^{n} u_r E_{r\sigma(r)}, \tag{2.13}$$

where $\sigma \in S_n$ is a permutation of order 2. At the same time, in that basis, the two matrices A_g and B_g, where g is a generator of the group G, have a diagonal form; moreover, the entries on the diagonals are distinct roots of unity:

$$A_g = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}, \quad B_g = \begin{pmatrix} \lambda_{\sigma(1)} & 0 & \dots & 0 \\ 0 & \lambda_{\sigma(2)} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_{\sigma(n)} \end{pmatrix},$$

where λ_i, $i = 1, \dots, n$, are distinct roots of unity of degree n.

If we consider the algebra homomorphism Δ' in the general form (1.2), then the conditions (2.1)–(2.7) are equivalent to the following system of conditions on the coefficients ω^{ij}_{klpq} and the entries of the matrix U (see [6]):

$$\frac{u_i}{u_j}\omega^{\sigma(i)\sigma(j)}_{klpq} = \frac{u_p}{u_q}\omega^{\sigma(p)\sigma(q)}_{ijkl} = \frac{u_k}{u_l}\omega^{\sigma(k)\sigma(l)}_{pqij} \quad \text{for all} \quad i,j,k,l,p,q; \tag{2.14}$$

$$\text{if} \quad \frac{\lambda_{\sigma(i)}}{\lambda_{\sigma(j)}} \neq \frac{\lambda_{\sigma(k)}}{\lambda_{\sigma(l)}}, \quad \text{then} \quad \omega^{ij}_{klpq} = 0 \quad \text{for all} \quad p,q; \tag{2.15}$$

$$\text{if} \quad \frac{\lambda_{\sigma(p)}}{\lambda_{\sigma(q)}} \neq \frac{\lambda_k}{\lambda_l}, \quad \text{then} \quad \omega^{ij}_{klpq} = 0 \quad \text{for all} \quad i,j; \tag{2.16}$$

$$\text{if} \quad \frac{\lambda_i}{\lambda_j} \neq \frac{\lambda_p}{\lambda_q}, \quad \text{then} \quad \omega^{ij}_{klpq} = 0 \quad \text{for all} \quad k,l; \tag{2.17}$$

$$\omega^{ij}_{klpq}\omega^{kl}_{ij\sigma(p)\sigma(q)} = \frac{u_p}{u_q}, \quad \omega^{ij}_{klpq}\omega^{pq}_{\sigma(k)\sigma(l)ij} = \frac{u_k}{u_l}; \tag{2.18}$$

$$\omega^{ij}_{klpq}\omega^{kl}_{stuv} = \omega^{ij}_{st\alpha\beta}\omega^{\alpha\beta}_{uvpq} \quad \text{for nonzero coefficients.} \tag{2.19}$$

Moreover, the form of $\Delta'(E_{ij})$ simplifies in the case where $i = j$:

$$\Delta'(E_{ii}) = \sum_{k,p=1}^{n} \omega^{ii}_{kkpp} E_{kk} \otimes E_{pp}, \tag{2.20}$$

where every coefficient ω^{ii}_{kkpp} is equal either to 0 or to 1.

For completeness, we mention statements from [6] without proofs.

Proposition 2.1. *If the summand $E_{kk} \otimes E_{pp}$ in $\Delta'(E_{ii})$ occurs in the decomposition* (2.20) *with a nonzero coefficient, then in all other $\Delta'(E_{jj})$ the coefficient of this element $E_{kk} \otimes E_{pp}$ is equal to* 0.

Proposition 2.2. *In $\Delta'(E_{ij})$, the coefficient of a certain $E_{ku} \otimes E_{pv}$ in the decomposition* (1.2) *is not equal to zero if and only if in $\Delta'(E_{ii})$ the coefficient of $E_{kk} \otimes E_{pp}$ in* (2.20) *is equal to* 1. *Symmetrically, in $\Delta'(E_{ij})$ the coefficient of a certain $E_{ul} \otimes E_{vq}$ in* (1.2) *is not equal to zero if and only if in $\Delta'(E_{jj})$ the coefficient of $E_{ll} \otimes E_{qq}$ in* (2.20) *is equal to* 1.

Proposition 2.3. *In a Hopf algebra of the form* (1.1), *for any i and j there are precisely $n-1$ nonzero coefficients in the decomposition* (1.2). *Moreover,*

1) *for any $k \neq i$, precisely one coefficient ω^{ij}_{klpq} is different from zero*;
2) *for any $p \neq i$, precisely one coefficient ω^{ij}_{klpq} is different from zero*;
3) *for any $l \neq j$, precisely one coefficient ω^{ij}_{klpq} is different from zero*;
4) *for any $q \neq j$, precisely one coefficient ω^{ij}_{klpq} is different form zero.*

Proposition 2.4. *In a Hopf algebra of the form* (1.1) *with a matrix* U *as in* (2.13)*, the following six conditions on the coefficients in the general decomposition* (1.2) *are equivalent*:

$$1)\ \omega^{ij}_{klpq} \neq 0, \qquad 2)\ \omega^{kl}_{ij\sigma(p)\sigma(q)} \neq 0, \qquad 3)\ \omega^{pq}_{\sigma(k)\sigma(l)ij} \neq 0,$$
$$4)\ \omega^{\sigma(p)\sigma(q)}_{\sigma(i)\sigma(j)kl} \neq 0, \qquad 5)\ \omega^{\sigma(k)\sigma(l)}_{pq\sigma(i)\sigma(j)} \neq 0, \qquad 6)\ \omega^{\sigma(i)\sigma(j)}_{\sigma(p)\sigma(q)\sigma(k)\sigma(l)} \neq 0.$$

Since, after permutation of vectors in the canonical basis, A_g and B_g remain diagonal and U remains monomial, there is no loss of generality in assuming that

$$A_g = \sum_{i=1}^{n} \varepsilon^i E_{ii}, \tag{2.21}$$

where ε is a primitive root of degree n of unity.

Proposition 2.5. *In a Hopf algebra of the form* (1.1) *with a matrix* A_g *as in* (2.21) *and a matrix* U *as in* (2.13)*, the following statement is valid: if* $\omega^{ij}_{klpq} \neq 0$*, then*

$$i - j = p - q, \quad \sigma(p) - \sigma(q) = k - l, \quad \sigma(k) - \sigma(l) = \sigma(i) - \sigma(j),$$

where the addition (*subtraction*) *is meant modulo* n*.*

We introduce another auxiliary definition.

Definition 2.1. We say that a permutation $\sigma \in S_n$ *preserves difference* if for any $i, j \in \{1, 2, \dots, n\}$, we have $\sigma(i) - \sigma(j) = i - j \pmod n$.

As was shown in [6], for a permutation $\sigma \in S_n$ from (2.13) the following statement is valid.

Proposition 2.6. *If a Hopf algebra of the form* (1.1) *with a matrix* A_g *as in* (2.21) *is cocommutative in the wide sense, then the corresponding permutation* $\sigma \in S_n$ *from* (2.13) *preserves difference.*

§3. The group M_H

Suppose a Hopf algebra of the form (1.1) is given for some n. Consider the set $M = \{1, 2, \dots, n\}$ and add an element ϵ to it: $M^\epsilon = \{\epsilon, 1, 2, \dots, n\}$. On the set M^ϵ, we can introduce an operation of multiplication related naturally to the comultiplication in the Hopf algebra H. Let $k, p \in M^\epsilon$. We set

$$k *_H p = \begin{cases} i \ \text{ such that } \ \omega^{ii}_{kkpp} \neq 0 & \text{if } \ k, p \neq \epsilon, k \neq \sigma(p), \\ \epsilon & \text{if } \ k, p \neq \epsilon, k = \sigma(p), \\ k & \text{if } \ p = \epsilon, \\ p & \text{if } \ k = \epsilon. \end{cases} \tag{3.1}$$

Since

$$\sum_{j=1}^{n} \Delta'(E_{jj}) = \Delta'(E) = \sum_{s,t\,:\,s \neq \sigma(t)}^{n} E_{ss} \otimes E_{tt},$$

it follows that $k *_H p$ exists for any $k, p \in M^\epsilon$, and, by Proposition 2.1, this element is defined uniquely. Now we can rewrite (2.20) in the form

$$\Delta'(E_{ii}) = \sum_{\substack{k,p \neq \epsilon \\ k *_H p = i}} E_{kk} \otimes E_{pp}, \tag{3.2}$$

and, by Proposition 2.5, for the nondiagonal matrix units we have

$$\Delta'(E_{i(i+t)}) = \sum_{\substack{k,p\neq\epsilon \\ k *_H p = i}} \omega^{i(i+t)}_{k(k+\sigma(p+t)-\sigma(p))p(p+t)} E_{k(k+\sigma(p+t)-\sigma(p))} \otimes E_{p(p+t)}. \tag{3.3}$$

Using Proposition 2.3, we conclude that the coefficients ω in (3.3) are all nonzero.

Theorem 3.1. *For a Hopf algebra H as in* (1.1)*, the structure $M_H = (M^\epsilon, *_H)$ is a group with respect to the operation $*_H$ defined in* (3.1).

Proof. From (3.1) it is seen that ϵ is a unit element with respect to $*_H$. Moreover, every element in M^ϵ has an inverse: $\sigma(k)$ is an inverse of $k \neq \epsilon$ and an inverse of ϵ is ϵ. It remains to prove the associativity of this operation. We prove that $s *_H (u *_H p) = (s *_H u) *_H p$ for any $s, u, p \in M^\epsilon$. If at least one of s, u, and p is equal to ϵ, then the proof is trivial; therefore, we may assume that $s, u, p \neq \epsilon$.

Case 1. Suppose $s, u, p \neq \epsilon$, $s \neq \sigma(u)$ and $u \neq \sigma(p)$, $s \neq \sigma(u *_H p)$. Then $i = s *_H (u *_H p)$ is an element of $M \subset M^\epsilon$, so that we can consider the matrix unit E_{ii}. We apply relation (2.7) to it, obtaining

$$\sum_{\substack{s',u',p'\neq\epsilon \\ s'*_H(u'*_H p')=i \\ s'\neq\sigma(u')}} E_{s's'} \otimes E_{u'u'} \otimes E_{p'p'} = \sum_{\substack{s'',u'',p''\neq\epsilon \\ (s''*_H u'')*_H p''=i \\ u''\neq\sigma(p'')}} E_{s''s''} \otimes E_{u''u''} \otimes E_{p''p''}. \tag{3.4}$$

Since the indices of the tensor triple $E_{ss} \otimes E_{uu} \otimes E_{pp}$ satisfy the relations under the summation sign on the left-hand side, this triple occurs in (3.4) on the left. Consequently, it occurs in (3.4) on the right, and, therefore, satisfies the relations under summation sign on the right. In particular, $(s *_H u) *_H p = i$.

Case 1b. Let $s, u, p \neq \epsilon$, $s \neq \sigma(u)$ and $u \neq \sigma(p)$, $s *_H u \neq \sigma(p)$. Then $i = (s *_H u) *_H p$ is an element of $M \subset M^\epsilon$, so that we can consider the matrix unit E_{ii}. We apply relation (2.7) to it, obtaining (3.4). Since the indices of the tensor triple $E_{ss} \otimes E_{uu} \otimes E_{pp}$ satisfy the relations under the summation sign on the right-hand side of (3.4), this triple occurs in (3.4) on the right. Consequently, it occurs in (3.4) on the left as well, thus satisfying the relations under the summation sign on the left. In particular, $s *_H (u *_H p) = i$.

Case 1c. Let $s, u, p \neq \epsilon$, $s \neq \sigma(u)$ and $u \neq \sigma(p)$, $s = \sigma(u *_H p)$ and $s *_H u = \sigma(p)$. Then $s *_H (u *_H p) = (s *_H u) *_H p = \epsilon$.

Case 2a. Let $s, u, p \neq \epsilon$, $s = \sigma(u)$, and $u \neq \sigma(p)$. We prove that

$$s *_H (\sigma(s) *_H p) = (s *_H \sigma(s)) *_H p.$$

We have p on the right. Let $x = \sigma(s) *_H p$. This means that $\omega^{xx}_{\sigma(s)\sigma(s)pp} \neq 0$. Using Proposition 2.4, we deduce that $\omega^{pp}_{ssxx} \neq 0$, i.e., $p = s *_H x$, as required.

Case 2b. Let $s, u, p \neq \epsilon$, $s \neq \sigma(u)$, $u = \sigma(p)$. The analysis is similar to that in case 2a.

Case 3. Let $s, u, p \neq \epsilon$, $s = \sigma(u)$, and $u = \sigma(p)$. It is required to prove that $s *_H (\sigma(s) *_H s) = (s *_H \sigma(s)) *_H s$. We use the relations $s *_H \sigma(s) = \sigma(s) *_H s = \epsilon$ and $\epsilon *_H s = s *_H \epsilon = s$. □

Moreover, M is a group with respect to addition modulo n, where n plays the role of zero. We set

$$k + \epsilon = \epsilon + k = \epsilon \tag{3.5}$$

for any $k \in M^\epsilon$. Then, in M^ϵ, the operation $+$ is associative and commutative, n is the unit element, and an inverse exists for each element except for ϵ.

As was mentioned above, in the Hopf algebra H, the coefficients of the form

$$\omega^{i(i+t)}_{k(k+\sigma(p+t)-\sigma(p))p(p+t)},$$

where $k \neq \sigma(p)$ and $k *_H p = i$, and only they, are different from zero. By Proposition 2.2, this implies that

$$(k + \sigma(p+t) - \sigma(p)) *_H (p+t) = k *_H p + t \tag{3.6}$$

for all $k \neq \sigma(p)$, $k, p, t \in M$.

Also, Proposition 2.5 shows that

$$\sigma(k *_H p + t) - \sigma(k *_H p) = \sigma(k + \sigma(p+t) - \sigma(p)) - \sigma(k) \tag{3.7}$$

for any $k, p, t \neq \epsilon, k \neq \sigma(p)$.

Theorem 3.2. *A Hopf algebra H as in* (1.1) *is cocommutative in the wide sense if and only if the group M_H is Abelian.*

Proof. If a Hopf algebra is cocommutative in the wide sense, then the definition (3.1) immediately implies that the group M_H is Abelian. Now we prove the "if" part. First, we prove that for any $t \in M$ there exists $k \in M$ such that $\sigma(k+t) - \sigma(k) = t$. For any t, there exist distinct $k_1, k_2 \in M$ such that $\sigma(k_1 + t) - \sigma(k_1) = \sigma(k_2 + t) - \sigma(k_2)$. This follows from the fact that, at n points from 1 to n, the expression $\sigma(k+t) - \sigma(k)$ as a function of k can take only $(n-1)$ values, namely, from 1 to $n-1$. Now we rewrite (3.6) in the form

$$\sigma(p+t) - \sigma(p) = (k *_H p + t) *_H \sigma(p+t) - k$$

and substitute $\sigma(k_1) *_H k_2$ for p and k_1 for k. We get

$$\begin{aligned} &\sigma(\sigma(k_1) *_H k_2 + t) - \sigma(\sigma(k_1) *_H k_2) \\ &\qquad = (k_1 *_H \sigma(k_1) *_H k_2 + t) *_H \sigma(\sigma(k_1) *_H k_2 + t) - k_1. \end{aligned} \tag{3.8}$$

Using the relations $k_1 *_H \sigma(k_1) = \epsilon$,

$$\sigma(k_1) *_H k_2 + t = (\sigma(k_1) + \sigma(k_2 + t) - \sigma(k_2)) *_H (k_2 + t)$$

and property (3.6), we can rewrite (3.8) in the form

$$\begin{aligned} &(k_2 + t) *_H \sigma\left[(\sigma(k_1) + \sigma(k_2 + t) - \sigma(k_2)) *_H (k_2 + t)\right] - k_1 \\ &\quad = (k_2 + t) *_H \sigma\left[(\sigma(k_1) + \sigma(k_1 + t) - \sigma(k_1)) *_H (k_2 + t)\right] - k_1 \\ &\quad = (k_2 + t) *_H \sigma(k_2 + t) *_H (k_1 + t) - k_1 = t. \end{aligned}$$

Thus, for $k(t) = \sigma(k_1) *_H k_2$ we obtain $\sigma(k+t) - \sigma(k) = t$.

Now we use (3.6) and the fact that M_H is Abelian:

$$\begin{aligned} &(k + \sigma(p+t) - \sigma(p)) *_H (p+t) = k *_H p + t = p *_H k + t \\ &\quad = (p + \sigma(k+t) - \sigma(k)) *_H (k+t) = (k+t) *_H (p + \sigma(k+t) - \sigma(k)) \end{aligned}$$

for any k, p, and t. For k we take the element $k(t)$ for which $\sigma(k+t) - \sigma(k) = t$. Now the right factors cancel, and we obtain $\sigma(p+t) - \sigma(p) = t$ for any p and t. Therefore, we see that (3.3) takes the form

$$\Delta'(E_{i(i+t)}) = \sum_{\substack{k,p \neq \epsilon \\ k *_H p = i}} \omega^{i(i+t)}_{k(k+t)p(p+t)} E_{k(k+t)} \otimes E_{p(p+t)}.$$

Since the sum on the right is symmetric, we conclude that the Hopf algebra H is cocommutative in the wide sense. □

Now we prove that if the structure M_H exists, then conditions (3.6) and (3.7) ensure the existence of a Hopf algebra and, in a sense, they determine it uniquely.

Theorem 3.3. *Let M^e be the multiplicative group of order $n+1$ in which the elements are enumerated in a one-to-one manner by the elements of M^ϵ; moreover, the unit element $e \in M^e$ is associated with $\epsilon \in M^\epsilon$, and the following relations are valid for all $k, p, t \in M^\epsilon$:*

$$(m_k + (m_p + m_t)^{-1} - (m_p)^{-1}) \cdot (m_p + m_t) = m_k \cdot m_p + m_t, \tag{3.9}$$

$$(m_k \cdot m_p + m_t)^{-1} - (m_k \cdot m_p)^{-1} = (m_k + (m_p + m_t)^{-1} - (m_p)^{-1}) - (m_k)^{-1}, \tag{3.10}$$

where the sum of two elements $m_{i_1}, m_{i_2} \in M^e$, $i_1, i_2 \in M^\epsilon$, is defined in accordance with the rule $m_{i_1} +_{M^e} m_{i_2} = m_{i_1 +_{M^\epsilon} i_2}$. Then up to the values of nonzero entries in the matrix U and nonzero coefficients ω and Δ', there exists a unique Hopf algebra (1.1) *such that the enumeration M^e $m_p \mapsto p \in M_\epsilon$ of elements of the group M^e is an isomorphism between the multiplicative groups M^e and M_H.*

Proof. We define multiplication on the set M^ϵ: $k \star p = s$ if $m_k \cdot m_p = m_s$. Since M^e is a group, it follows that $(M^\epsilon, \star)$ is also a group, and ϵ is the unit element relative to the operation $\star$. Moreover, by the definition of $\star$, the enumeration of elements of the group M is an isomorphism of the groups M^e and $(M^\epsilon, \star)$.

We prove that there exists a unique Hopf algebra H of the form (1.1) such that $(M_H, *_H) = (M^\epsilon, \star)$. We recall that there is no loss of generality in assuming that the matrix A_g, where g is a generator of the group G as in (1.1), is equal to (2.21).

Existence. We find a permutation σ that determines the matrix U by (2.13). We set $\sigma(t)$, $t \in M$, equal to the element $s \in M$ satisfying $m_t = (m_s)^{-1}$, $m_s, m_t \in M^e$. Note that σ defined in this way is a permutation of order 2. Moreover, $\sigma(t)$ is the inverse element for $t \in M$ relative to the operation $\star$. In the matrix (2.13), we set $u_i = 1$, $1 \le i \le n$, and for the role of Δ' we take the mapping

$$\Delta'(E_{i(i+t)}) = \sum_{\substack{k,p \neq \epsilon \\ k \star p = i}} E_{k(k+\sigma(p+t)-\sigma(p))} \otimes E_{p(p+t)}, \tag{3.11}$$

where $i, t \in M$. Note that for $t = n \in M$, from (3.11) we get

$$\Delta'(E_{ii}) = \sum_{\substack{k,p \neq \epsilon \\ k \star p = i}} E_{kk} \otimes E_{pp}. \tag{3.12}$$

One can verify straightforwardly that Δ' defined in this way is a homomorphism. We prove that the matrices A_g and U and the homomorphism Δ' as above satisfy conditions (2.14)–(2.19) and (2.12).

We show that formulas (2.14), namely,

$$\omega_{klpq}^{\sigma(i)\sigma(j)} = \omega_{ijkl}^{\sigma(p)\sigma(q)} = \omega_{pqij}^{\sigma(k)\sigma(l)},$$

are fulfilled for all $i, j, k, l, p, q \in M$. Since, by (3.11), the coefficients can take only two values, 0 or 1, it suffices to verify that they are equal to zero or are not equal to zero simultaneously.

Note that the operation $+$ on M^e and the permutation σ on M are defined so that conditions (3.9) and (3.10) for elements of M^e imply conditions (3.6) and (3.7) for elements of M^ϵ, where the operation $*_H$ is applied instead of the operation $\star$. The definition (3.11) shows that the coefficient $\omega_{klpq}^{\sigma(i)\sigma(j)}$ is nonzero if and only if

$$l = k + \sigma(p + t) - \sigma(p), \quad q = p + t, \ \text{ where } \ t = \sigma(j) - \sigma(i).$$

Moreover, $k \star p = \sigma(i)$ and (3.6) implies $l \star q = \sigma(j)$. From (3.7) we obtain $j - i = \sigma(l) - \sigma(k)$. Thus, $\omega_{klpq}^{\sigma(i)\sigma(j)}$ is nonzero if and only if

$$\sigma(k) - \sigma(l) = i - j, \quad k - l = \sigma(p) - \sigma(q),$$
$$p - q = \sigma(i) - \sigma(j), \quad k \star p = \sigma(i), \quad l \star q = \sigma(j).$$

Similarly, for $\omega_{ijkl}^{\sigma(p)\sigma(q)} \neq 0$ we have

$$\sigma(i) - \sigma(j) = p - q, \quad i - j = \sigma(k) - \sigma(l),$$
$$\sigma(p) - \sigma(q) = k - l, \quad i \star k = \sigma(p), \quad j \star l = \sigma(q).$$

If $\omega_{pqij}^{\sigma(k)\sigma(l)} \neq 0$, then

$$\sigma(p) - \sigma(q) = k - l, \quad p - q = \sigma(i) - \sigma(j),$$
$$i - j = \sigma(k) - \sigma(l), \quad p \star i = \sigma(k), \quad q \star j = \sigma(l).$$

It is clear that the first three conditions for all three coefficients coincide. The equivalence of the three pairs of the remaining conditions follows from the fact that $(M^\epsilon, \star)$ is a group.

Similarly, we can check conditions (2.15)–(2.18).

Instead of condition (2.19), we check condition (2.7), equivalent to (2.19). On the left-hand side in (2.7), we have

$$\begin{aligned}
&(\Delta'(E) \otimes E)\big[(1 \otimes \Delta')\Delta'(E_{i(i+t)})\big] \\
&\quad = (\Delta'(E) \otimes E)\Bigg[\sum_{\substack{u,p\neq\epsilon \\ u\star p = i}} E_{u(u+\sigma(p+t)-\sigma(p))} \otimes \Delta'(E_{p(p+t)})\Bigg] \\
&\quad = (\Delta'(E) \otimes E)\Bigg[\sum_{\substack{u,p\neq\epsilon \\ u\star p = i}} E_{u(u+\sigma(p+t)-\sigma(p))} \otimes \Bigg(\sum_{\substack{v,w\neq\epsilon \\ v\star w = p}} E_{v(v+\sigma(w+t)-\sigma(w))} \otimes E_{w(w+t)}\Bigg)\Bigg] \\
&\quad = \sum_{\substack{u,v,w\neq\epsilon \\ u\star(v\star w) = i \\ u\neq\sigma(v), v\neq\sigma(w)}} E_{u(u+\sigma(v\star w+t)-\sigma(v\star w))} \otimes E_{v(v+\sigma(w+t)-\sigma(w))} \otimes E_{w(w+t)}.
\end{aligned}$$

On the right-hand side, we have

$$\begin{aligned}
&[(\Delta' \otimes 1)\Delta'(E_{i(i+t)})]\big(E \otimes \Delta'(E)\big) \\
&\quad = \Bigg[\sum_{\substack{k',w'\neq\epsilon \\ k'\star w' = i}} \Delta'(E_{k'(k'+\sigma(w'+t)-\sigma(w'))}) \otimes E_{w'(w'+t)}\Bigg]\big(E \otimes \Delta'(E)\big) \\
&\quad = \Bigg[\sum_{\substack{k',w'\neq\epsilon \\ k'\star w' = i}} \Bigg(\sum_{\substack{u',v'\neq\epsilon \\ u'\star v' = k'}} E_{u'(u'+\sigma(v'+\sigma(w'+t)-\sigma(w'))-\sigma(v'))} \\
&\qquad\qquad \otimes E_{v'(v'+\sigma(w'+t)-\sigma(w'))}\Bigg) \otimes E_{w'(w'+t)}\Bigg]\big(E \otimes \Delta'(E)\big) \\
&\quad = \sum_{\substack{u',v',w'\neq\epsilon \\ (u'\star v')\star w' = i \\ u'\neq\sigma(v'), v'\neq\sigma(w')}} E_{u'(u'+\sigma(v'+\sigma(w'+t)-\sigma(w'))-\sigma(v'))} \otimes E_{v'(v'+\sigma(w'+t)-\sigma(w'))} \otimes E_{w'(w'+t)}
\end{aligned}$$

From the associativity in the group $(M^\epsilon, \star)$, it follows that any triple of indices u, v, w occurring in the first sum occurs in the second. Let $u = u'$, $v = v'$, $w = w'$. Then (3.7) implies the formula

$$u + \sigma(v \star w + t) - \sigma(v \star w) = u' + \sigma(v' + \sigma(w' + t) - \sigma(w')) - \sigma(v').$$

Consequently, all indices in the corresponding tensor triples coincide, which proves (2.7).

We prove that condition (2.12) is fulfilled:

$$\mu(1\otimes S)(\Delta'(E_{i(i+t)})) = \mu(1\otimes S)\Big(\sum_{\substack{k,p\neq\epsilon\\ k\star p=i}} E_{k(k+\sigma(p+t)-\sigma(p))}\otimes E_{p(p+t)}\Big)$$
$$= \sum_{\substack{k,p\neq\epsilon\\ k\star p=i}} E_{k(k+\sigma(p+t)-\sigma(p))}E_{\sigma(p+t)\sigma(p)} = 0,$$

because $k+\sigma(p+t)-\sigma(p)=\sigma(p+t)$ if and only if $k=\sigma(p)$, i.e., $k\star p=\epsilon$. Similarly, $\mu(S\otimes 1)(\Delta'(E_{i(i+t)}))=0$. Thus, condition (2.12) is also valid, and the matrices A_g and U and the homomorphism Δ' determine a Hopf algebra H.

To complete the proof of existence, it remains to note that $M_H=(M^\epsilon,\star)$ by (3.11).

Uniqueness. Suppose that there exist two Hopf algebras such that $M_{H_1}=M_{H_2}=(M^\epsilon,\star)$. Then the permutations σ_{H_1} and σ_{H_2} are equal, because $\sigma_{H_1}(t)=t_{H_1}^{-1}=t_{H_2}^{-1}=\sigma_{H_2}(t)$, $t\in M$. Then the matrices U_{H_1} and U_{H_2} coincide up to the values of nonzero elements. Finally, the homomorphisms Δ'_{H_1} and Δ'_{H_2} coincide up to the values of nonzero coefficients ω, because formulas (3.2)–(3.3) are valid for them, where the operations $*_{H_1}$ and $*_{H_2}$ coincide with the operation $\star$. □

§4. The permutation σ and the homomorphism of M_H to S_n

Consider a Hopf algebra H of the form (1.1) and the corresponding group M_H with operations $+$ and $*_H$. For a while, we interchange the multiplicative and additive notation of the operations. We shall denote the operation $+$ on the elements of M^ϵ by $\times$, and the operation $*_H$ by $+_H$.

Theorem 4.1. *If the permutation σ corresponding to a Hopf algebra H as in* (1.1) *preserves difference, then $(M^\epsilon,+_H,\times)$ is a field.*

Proof. If σ preserves difference, then we have $\sigma(p+t)=\sigma(p)+t$ for any $p,t\in M$. Condition (3.6) is converted to the distributivity of addition with respect to multiplication:

$$(k+t)*_H(p+t)=k*_H p+t \tag{4.1}$$

for any $k,p,t\neq\epsilon, k\neq\sigma(p)$. Note that, by the definition (3.5), condition (4.1) is in fact fulfilled for any $k,p,t\in M^\epsilon$. We also note that if σ preserves difference, then condition (3.7) is converted to the simple identity $t=t$. If the operations are denoted as was mentioned above, relation (4.1) becomes the usual distributivity of multiplication with respect to addition:

$$k\times t+_H p\times t=(k+_H p)\times t \tag{4.2}$$

for any $k,p,t\in M^\epsilon$. Since $(M,\times)$ is a commutative (cyclic) group, to prove that $(M^\epsilon,+_H,\times)$ is a field it remains to establish that the group $(M^\epsilon,+_H)$ is Abelian. Note that $(M^\epsilon,+_H,\times)$ is a near-field, i.e., its elements form a group with respect to addition, the nonzero elements form a group with respect to multiplication, and at least one distributivity holds true (see, e.g., [8]). We invoke the result of [7] saying that the additive group of a finite near-field is always Abelian, to conclude that $(M^\epsilon,+_H)$ is Abelian. Thus, $(M^\epsilon,+_H,\times)$ is a field. □

Corollary 4.1. *A Hopf algebra of the form* (1.1) *is cocommutative in the wide sense if and only if the corresponding σ preserves difference.*

Proof. The "only if" part was proved in Proposition 2.6, and the "if" part follows from Theorem 4.1, because $(M^{\epsilon}, +_H)$ is an Abelian group, and thus, in the previous notation, M_H is an Abelian group with respect to $*_H$. By Theorem 3.2, this implies that the corresponding Hopf algebra is cocommutative in the wide sense. □

Combining Theorems 3.3 and 4.1 with Corollary 4.1, we get the following statement.

Corollary 4.2. *For any $n = p^m - 1$, where p is prime and m is a positive integer, the number of Hopf algebras of the form* (1.1) *that are cocommutative in the wide sense is equal to the number of ways of defining multiplication on the residue group $Z_{p^m-1} = \{1, 2, \dots, p^m - 1\}$, cyclic with respect to addition, so that, upon adding zero and interchanging the operations of multiplication and addition, the resulting structures $\mathbf{F} = Z_{p^m-1} \cup \{0\}$ are (isomorphic) fields. Moreover, two different (isomorphic) fields on $Z_{p^m-1} \cup \{0\}$ lead to different Δ'. For $n \neq p^m - 1$, there are no Hopf algebras of the form* (1.1) *that are cocommutative in the wide sense.*

For a Hopf algebra H of the form (1.1) and the corresponding group M_H, we define a mapping $\tau : M_H \to S_n$, $k \mapsto \tau_k$, by setting $\tau_k(r) = \sigma(k + r) - \sigma(k)$, $r \in M$, for $k \in M$ and $\tau_\epsilon = id \in S_n$. Condition (3.7) means that τ is a homomorphism of the group M_H to S_n, because the left-hand side of (3.7) contains $\tau_{k*_H p}(t)$ by definition, and the right-hand side contains $(\tau_k \circ \tau_p)(t)$, where $\circ$ is the usual composition of permutations. We also note that (3.6) can be written as

$$(k + \tau_p(t)) *_H (p + t) = k *_H p + t. \tag{4.3}$$

We prove several claims.

Proposition 4.1. *$\tau_k(n) = n$ for any $k \in M_H$.*

Proof. By the definition of τ_k with $k \neq \epsilon$ we have

$$\tau_k(n) = \sigma(k + n) - \sigma(k) = \sigma(k) - \sigma(k) = n.$$ □

Proposition 4.2. *$\tau_{a+k}(s - k) = \tau_a(s) - \tau_a(k)$ for any $a, k, s \in M$.*

Proof. $\tau_{a+k}(s - k) = \sigma(a + s) - \sigma(a + k) = \sigma(a + s) - \sigma(a) - (\sigma(a + k) - \sigma(a)) = \tau_a(s) - \tau_a(k)$. □

Proposition 4.3. *The permutation σ preserves difference if and only if the kernel of the homomorphism τ is nontrivial.*

Proof. If σ preserves difference, then $\tau_k(r) = \sigma(k + r) - \sigma(k) = r$ for any $k, r \in M$, i.e., $\operatorname{Ker} \tau = M_H$. Now we prove the "if" part. Suppose there exists $k \in M$ such that $\tau_k(r) = \sigma(k + r) - \sigma(k) = r$ for any $r \in M$. We take arbitrary $x, y \in M$. Then, since M is an additive cyclic group, there exist $r_1, r_2 \in M$ such that $x = k + r_1$, $y = k + r_2$. Then $\sigma(x) - \sigma(y) = \sigma(k + r_1) - \sigma(k + r_2) = \sigma(k) + r_1 - (\sigma(k) + r_2) = r_1 - r_2 = x - y$. □

Proposition 4.4. *If σ does not preserve difference, then* (3.6) *follows from* (3.7).

Proof. We deduce from (4.3) that τ is an embedding of M_H in S_n. Then (3.6) is equivalent to the fact that $\tau_{(k+\tau_p(r))*_H(p+r)} = \tau_{k*_H p+r}$. Since τ is a homomorphism, we have

$$\tau_{(k+\tau_p(r))*_H(p+r)} = \tau_{k+\tau_p(r)} \circ \tau_{p+r}.$$

It remains to prove that $\tau_{k+\tau_p(r)} \circ \tau_{p+r} = \tau_{k*_H p+r}$:

$$\begin{aligned}
\tau_{k+\tau_p(r)} \circ \tau_{p+r}(s - r) &= \tau_{k+\tau_p(r)}(\tau_p(s) - \tau_p(r)) \\
&= \tau_k(\tau_p(s)) - \tau_k(\tau_p(r)) \\
&= \tau_{k*_H p}(s) - \tau_{k*_H p}(r) \\
&= \tau_{k*_H p+r}(s - r),
\end{aligned}$$

where s, and, thus, $s-r$, ranges over the entire set M. □

As was shown in Corollary 4.1, the permutation σ that does not preserve difference corresponds to the strong noncocommutativity of the Hopf algebra H of the form (1.1). By Proposition 4.3, this means that, in a strongly noncocommutative Hopf algebra H, the group M_H is isomorphic to a non-Abelian subgroup of S_n the elements of which have the form $v_{-\sigma(k)} \circ \sigma \circ v_k$, where σ is certain permutation of order two in S_n that is common for all the subgroup and v_x is the translation that takes any $t \in M$ to $t+x$.

§5. The commutativity of M_H and the cocommutativity of H in the wide sense

Consider a Hopf algebra H of the form (1.1) and the corresponding group M_H with operations $+$ and $*_H$.

Lemma 5.1. *$\sigma(q) - \sigma(p+\sigma(n))$, where $q = (p+\sigma(n)) *_H n$ ranges over all $M \setminus \{n\}$ for p ranging over all $M \setminus \{n\}$.*

Proof. We have the following chain of relations:

$$\begin{aligned}
&\sigma(q) - \sigma(p+\sigma(n)) \\
&\quad = \sigma((p+\sigma(n)) *_H n) - \sigma(p+\sigma(n)) \\
&\quad = \sigma(n) *_H \sigma(p+\sigma(n)) - \sigma(p+\sigma(n)) \\
&\quad = [\sigma(n) + \tau_{\sigma(p+\sigma(n))}(-\sigma(p+\sigma(n)))] *_H [\sigma(p+\sigma(n)) + (-\sigma(p+\sigma(n)))] \\
&\quad = [\sigma(n) + \sigma(n) - \sigma(\sigma(p+\sigma(n)))] *_H n = (\sigma(n) - p) *_H n.
\end{aligned}$$

The third relation in this chain is obtained from (3.6) for $k' = \sigma(n)$, $p' = \sigma(p+\sigma(n))$, $t' = -\sigma(p+\sigma(n))$, and the fourth relation follows from the definition of τ. Note that $(\sigma(n)-p) *_H n \in M \setminus \{n\}$ for $p \in M \setminus \{n\}$. Moreover, for $p_1 \neq p_2, p_1, p_2 \in \{1, 2, \ldots, n-1\}$ we have $(\sigma(n) - p_1) *_H n \neq (\sigma(n) - p_2) *_H n$. Otherwise, multiplying this relation from the right by $\sigma(n)$ and subtracting $\sigma(n)$ from the two sides, we get $p_1 = p_2$. Also we have

$$(\sigma(n) - p) *_H n = \begin{cases} \epsilon, & p = n, \\ n, & p = \epsilon. \end{cases} \tag{5.1}$$

□

Theorem 5.1. *All Hopf algebras of the form* (1.1) *are cocommutative in the wide sense and exist only if $n = p^k - 1$, where p is prime and k is a positive integer.*

Proof. We argue by contradiction. Let H be a strongly noncocommutative algebra of the form (1.1). Then the group M_H corresponding to it is non-Abelian. By Corollary 4.1, σ does not preserve difference, and, by Proposition 4.3, τ is an isomorphism. We consider an arbitrary $p \in M \setminus \{n\}$ and set $q = (p+\sigma(n)) *_H n$. Note that $q \in M \setminus \{n\}$. Consider the permutation τ_q on an element $r \in M$. Using the definition of τ and Proposition 4.2, we do the following calculations:

$$\begin{aligned}
\tau_q(r) &= \tau_{(p+\sigma(n)) *_H n}(r) \\
&= \tau_{p+\sigma(n)}(\tau_n(r)) \\
&= \tau_{p+\sigma(n)}(\sigma(r) - \sigma(n)) \\
&= \tau_p(\sigma(r)) - \tau_p(\sigma(n)) \\
&= \sigma(p+\sigma(r)) - \sigma(p) - \sigma(p+\sigma(n)) + \sigma(p) \\
&= \sigma(p+\sigma(r)) - \sigma(p+\sigma(n)).
\end{aligned}$$

Since $\tau_q(r) = \sigma(q+r) - \sigma(q)$ by definition, we obtain

$$\sigma(q+r) - \sigma(q) = \sigma(p+\sigma(r)) - \sigma(p+\sigma(n)).$$

We transfer $\sigma(p+\sigma(r))$ to the left-hand side and $\sigma(q)$ to the right-hand side. Note that now the left-hand side can be written as $\tau_{p+\sigma(r)}\big(q+r-p-\sigma(r)\big)$. Thus, we get

$$\tau_{p+\sigma(r)}\big(q+r-p-\sigma(r)\big) = \sigma(q) - \sigma(p+\sigma(n)).$$

Now we apply $\tau_{\sigma(p+\sigma(r))}$ to the two sides and subtract $q-p$, obtaining

$$r - \sigma(r) = \tau_{\sigma(p+\sigma(r))}\big(\sigma(q) - \sigma(p+\sigma(n))\big) + p - q \tag{5.2}$$

for any $p, r \in M$, $p \neq n$, $q = (p+\sigma(n)) *_H n$. Note that the left-hand side does not depend on p. Let C be the number of pairwise distinct values of the expression $r-\sigma(r)$, where r ranges over M. Note that when r ranges over all the set M, the subscript of the permutation $\tau_{\sigma(p+\sigma(r))}$ also ranges over all of M. Thus, $\tau_{\sigma(p+\sigma(r))}\big(\sigma(q) - \sigma(p+\sigma(n))\big)$ runs through the entire orbit of the element $\sigma(q) - \sigma(p+\sigma(n))$. The addition of $p-q$, which is constant relative to r, does not affect the number of pairwise distinct values. We see that the order of the orbit of the element $\sigma(q) - \sigma(p+\sigma(n))$ is equal to C, i.e., to the number of pairwise distinct values of the right-hand side, and does not depend on p.

By Lemma 5.1, any $x \in \{1, 2, \dots, n-1\}$ can uniquely be represented in the form $\sigma(q) - \sigma(p+\sigma(n))$, where $p \in \{1, 2, \dots, n-1\}$. Since, as we have checked, the order of the orbit of any such element is equal to C, we conclude that the order of the orbit of any $x \in \{1, 2, \dots, n-1\}$ is equal to C.

Now we analyze more closely how the set $\{1, 2, \dots, n\}$ is split into orbits under the action of the group of permutations τ_k, $k \in M_H$. From Proposition 4.1 it follows that $\mathrm{Orb}(n) = \{n\}$. The above arguments show that the set $\{1, 2, \dots, n-1\}$ is split into orbits having C elements each. This implies that C divides $n-1$. Moreover, the order of an orbit always divides the order of the acting group. In the case under consideration, we conclude that C divides $|M_H| = n+1$. As a common divisor of $n-1$ and $n+1$, C may be equal only to 1 or 2.

The case of $C = 1$. We have $\tau_x(y) = y$ for any $y \in \{1, 2, \dots, n\}$ and any $x \in M_H$. Proposition 4.3 implies that σ preserves difference, which, by Corollary 4.1, is equivalent to the fact that M_H is Abelian, a contradiction.

The case of $C = 2$. For any $x \in \{1, 2, \dots, n\}$, the permutation τ_x is expanded into a product of independent cycles of length at most 2 each. Indeed, if the length of some independent cycle is greater than 2, then, applying the powers of the permutation τ_x to any element t of this cycle, we conclude that the order of the orbit of t is greater than 2. Therefore, $(\tau_x)^2 = \tau_{x^2} = \mathrm{id}$ and, since τ is an isomorphism, $x^2 = \epsilon$ for any $x \in M_H$. Take any two elements $a, b \in M_H$ and consider their commutator. Since $a^{-1} = a$, $b^{-1} = b$, $(a *_H b)^{-1} = a *_H b$, we have

$$a *_H b *_H a^{-1} *_H b^{-1} = a *_H b *_H a *_H b = \epsilon.$$

Thus, the group M_H is Abelian, a contradiction. □

References

[1] V. A. Artamonov, *On semisimple finite-dimensional Hopf algebras*, Mat. Sb. **198** (2007), no. 9, 3–28; English transl., Sb. Math. **198** (2007), no. 9–10, 1221–1245. MR2360805 (2008i:16049)

[2] V. A. Artamonov and I. A. Chubarov, *Properties of some semisimple Hopf algebras*, Algebras, Representations and Applications, Contemp. Math., vol. 483, Amer. Math. Soc., Providence, RI, 2009, pp. 23–26. MR2497948 (2010k:16045)

[3] V. A. Artamonov, *On semisimple Hopf algebras with few representations of dimension greater than one*, Rev. Un. Mat. Argentina **51** (2010), no. 2, 91–105. MR2840164 (2012h:16061)

[4] S. Montgomery, *Hopf algebras and their actions on rings*, CBMS Reg. Conf. Ser. Math., vol. 82, Amer. Math. Soc., Providence, RI, 1993. MR1243637 (94i:16019)

[5] S. Natale and J. Y. Plavnik, *On fusion categories with few irreducible degrees*, Algebra Number Theory **6** (2012), no. 6, 1171–1197. MR2968637

[6] S. Yu. Spiridonova, *On finite-dimensional semisimple Hopf algebras of dimension* $n(n+1)$, Mat. Zametki **91** (2012), no. 2, 253–269; English transl., Math. Notes **91** (2012), no. 1–2, 243–258.
[7] H. Zassenhaus, *Über endliche Fastkörper*, Abh. Math. Semin. Hamburg Univ. **11** (1935), 187–220. MR3069653
[8] J. L. Zemmer, *The additive group of an infinite near-field is Abelian*, J. London Math. Soc. **44** (1969), 65–67. MR0231902 (38:228)

Department of Mechanics and Mathematics, Lomonosov Moscow State University, Leninskie gory, GSP-1, Moscow 119991, Russia
E-mail address: sonya.spr@gmail.com

Received 7/JUL/2012

Translated by N. B. LEBEDINSKAYA