JOURNAL OF ALGEBRA **209,** 658–691 (1998)
ARTICLE NO. JA987643

Lifting of Quantum Linear Spaces and Pointed Hopf Algebras of Order p^3

N. Andruskiewitsch*

FAMAF, UNC, (5000) C. Universitaria, Córdoba, Argentina

and

H.-J. Schneider

Mathematisches Institut der Universität München, Theressienstr. 39, D-80333 München, Germany
E-mail: hanssch@rz.mathematik.uni-muenchen.de

Communicated by Susan Montgomery

Received November 19, 1997

We propose the following principle to study pointed Hopf algebras, or more generally, Hopf algebras whose coradical is a Hopf subalgebra. Given such a Hopf algebra A, consider its coradical filtration and the associated graded coalgebra $\operatorname{gr} A$. Then $\operatorname{gr} A$ is a graded Hopf algebra, since the coradical A_0 of A is a Hopf subalgebra. In addition, there is a projection $\pi: \operatorname{gr} A \to A_0$; let R be the algebra of coinvariants of π. Then, by a result of Radford and Majid, R is a braided Hopf algebra and $\operatorname{gr} A$ is the bosonization (or biproduct) of R and A_0: $\operatorname{gr} A \simeq R\#A_0$. The principle we propose to study A is first to study R, then to transfer the information to $\operatorname{gr} A$ via bosonization, and finally to lift to A. In this article, we apply this principle to the situation when R is the simplest braided Hopf algebra: a quantum linear space. As consequences of our technique, we obtain the classification of pointed Hopf algebras of order p^3 (p an odd prime) over an algebraically closed field of characteristic zero; with the same hypothesis, the characterization of the pointed Hopf algebras whose coradical is abelian and has index p or p^2; and an infinite family of pointed, nonisomorphic, Hopf algebras of the same dimension. This last result gives a negative answer to a conjecture of I. Kaplansky. © 1998 Academic Press

Key Words: Hopf algebras

*Forschungsstipendiat der Alexander von Humboldt-Stiftung. Also partially supported by CONICET, CONICOR, SeCYT (UNC) and FaMAF (República Argentina)m and by TWAS (Trieste)

0021-8693/98 $25.00

0. INTRODUCTION

We assume for simplicity of the exposition that our groundfield k is algebraically closed of characteristic 0; many results below are valid under weaker hypotheses. Let A be a noncosemisimple Hopf algebra whose coradical A_0 is a Hopf subalgebra; for instance, A is pointed, that is, all simple subcoalgebras are one dimensional. Let

$$A_0 \subseteq A_1 \subseteq \cdots \subseteq A$$

be the coradical filtration of A; see [M, Chapter 5]. This is a coalgebra filtration and we consider the associated graded coalgebra $\operatorname{gr} A = \bigoplus_{n \geq 0} \operatorname{gr} A(n)$, $\operatorname{gr} A(n) = A_n / A_{n-1}$, where $A_{-1} = 0$. Since A_0 is a Hopf subalgebra, $\operatorname{gr} A$ is a graded Hopf algebra and the zero term of its own coradical filtration is $\operatorname{gr} A(0) = A_0$, which is a Hopf subalgebra of $\operatorname{gr} A$. Let us denote $B = \operatorname{gr} A$, $H = \operatorname{gr} A(0)$. Let $\gamma\colon H \to B$ be the inclusion and let $\pi\colon B \to H$ be the projection with kernel $\bigoplus_{n \geq 1} \operatorname{gr} A(n)$. Then π is a Hopf algebra retraction of γ. We can describe the situation in the diagram

$$R \hookrightarrow B \underset{\gamma}{\overset{\pi}{\leftrightarrows}} H, \tag{0.1}$$

where $R = B^{\operatorname{co} H} = \{a \in B\colon (\mathrm{id} \otimes \pi)\Delta(a) = a \otimes 1\}$. The setting (0.1) was first considered by Radford [R3]; Majid presented it in categorical terms [Mj]. It turns out that R is a Hopf algebra in the braided category ${}^{H}_{H}\mathcal{YD}$ of Yetter–Drinfeld modules over H; we shall say "braided Hopf algebra," for short. Moreover, B can be recovered as the biproduct (or bosonization, in Majid's terminology) of R and H.

DEFINITION. Let A be a Hopf algebra whose coradical A_0 is a Hopf subalgebra. The braided Hopf algebra R described above shall be called the *diagram* of A.

The general principle we propose is as follows: first we analyze the diagram R of A, then we transfer the information to $\operatorname{gr} A$ by bosonization, and finally we lift it from $\operatorname{gr} A$ to A via the filtration.

R is a *graded* braided Hopf algebra and its coradical is trivial: $R_0 = R(0) = k1$. We denote by $P(R)$ the space of primitive elements of R. We see, considering the coradical filtration, that $P(R) \neq 0$, because $\dim R > 1$; this last condition just means that A is not cosemisimple. In other words, the Hopf algebras R we need to study are of a very special kind.

The first natural examples of such braided Hopf algebras are the well-known quantum linear spaces. We give a characterization of finite-dimensional quantum linear spaces in Section 3; see Proposition 3.5.

If Γ is a finite abelian group, a quantum linear space over Γ is given by elements $g_1, \dots, g_\theta \in \Gamma$, and characters $\chi_1, \dots, \chi_\theta \in \hat{\Gamma}$ satisfying

$$q_i := \chi_i(g_i) \neq 1, \quad \text{for all } i,$$
$$\chi_j(g_i)\chi_i(g_j) \quad = 1, \quad \text{for all } i \neq j.$$

The quantum linear space $\mathscr{R} = \mathscr{R}(g_1, \dots, g_\theta; \chi_1, \dots, \chi_\theta)$ is then the braided Hopf algebra over $k\Gamma$ generated as an algebra by primitive elements $x_1, \dots, x_\theta$, with relations

$$x_1^{N_1} = 0, \dots, x_\theta^{N_\theta} = 0,$$
$$x_i x_j = \chi_j(g_i) x_j x_i, \text{ if } i \neq j.$$

The elements x_i are g_i-graded and the action of Γ on x_i is via the character χ_i. To each such quantum linear space we define a compatible datum $\mathscr{D}$ consisting of scalars $\mu_i \in \{0, 1\}$ for each i, $1 \leq i \leq \theta$, and $\lambda_{ij} \in k$ for each $i, j, 1 \leq i < j \leq \theta$ satisfying conditions (5.1) and (5.2). We define for each such datum a pointed Hopf algebra $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$ in Section 5. Then we prove our main result.

LIFTING THEOREM 5.5. *Let $\mathscr{R} = \mathscr{R}(g_1, \dots, g_\theta; \chi_1, \dots, \chi_\theta)$ be a quantum linear space over the finite abelian group Γ. Then pointed Hopf algebras A with coradical $k(\Gamma)$ and diagram $\mathscr{R}$ are exactly of the form $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$ for some compatible datum $\mathscr{D}$.*

Let p be an odd prime number and let $\mathbb{G}_p$ denote the group of pth roots of 1 in k.

As an application of the Lifting Theorem, we classify pointed Hopf algebras of dimension p^3.

A Hopf algebra of dimension p is isomorphic to a group algebra by Zhu's theorem [Z].

The only pointed noncosemisimple Hopf algebras of dimension p^2 are the Taft algebras $T_k(q) = T(q), q \in \mathbb{G}_p - 1$; see Section 1.

In dimension p^3, we have the following list of pointed noncosemisimple Hopf algebras over k, for each $q \in \mathbb{G}_p - 1$:

(a) The product Hopf algebra $T(q) \otimes k\mathbb{Z}/(p))$.

(b) The Hopf algebra $\widetilde{T(q)} := k\langle g, x \mid gxg^{-1} = q^{1/p}x, g^{p^2} = 1, x^p = 0\rangle$. Here $q^{1/p}$ is a pth root of q. Its comultiplication is determined by $\Delta(x) = x \otimes g^p + 1 \otimes x, \Delta(g) = g \otimes g$.

(c) The Hopf algebra $\widehat{T(q)} := k\langle g, x \mid gxg^{-1} = qx, g^{p^2} = 1, x^p = 0\rangle$. Its comultiplication is determined by $\Delta(x) = x \otimes g + 1 \otimes x, \Delta(g) = g \otimes g$.

(d) The Hopf algebra $\mathbf{r}(q) := k\langle g, x \mid gxg^{-1} = qx, g^{p^2} = 1, x^p = 1 - g^p\rangle$. Its comultiplication is determined by $\Delta(x) = x \otimes g + 1 \otimes x$, $\Delta(g) = g \otimes g$.

(e) The Frobenius–Lusztig kernel $\mathbf{u}(q) := k\langle g, x, y \mid gxg^{-1} = q^2x, gyg^{-1} = q^{-2}y, g^p = 1, x^p = 0, y^p = 0, xy - yx = g - g^{-1}\rangle$. Its comultiplication is determined by $\Delta(x) = x \otimes g + 1 \otimes x$, $\Delta(y) = y \otimes 1 + g^{-1} \otimes y$, $\Delta(g) = g \otimes g$.

(f) For each $m \in \mathbb{Z}/(p) - 0$, the book Hopf algebra $\mathbf{h}(q, m) := k\langle g, x, y \mid gxg^{-1} = qx, gyg^{-1} = q^m y, g^p = 1, x^p = 0, y^p = 0, xy - yx = 0\rangle$. Its comultiplication is determined by $\Delta(x) = x \otimes g + 1 \otimes x$, $\Delta(y) = y \otimes 1 + g^m \otimes y$, $\Delta(g) = g \otimes g$.

We prove the following:

THEOREM 0.1. *Any noncosemisimple pointed Hopf algebra of order p^3 is isomorphic to one in the list above.*

We shall see that there are no isomorphisms between different Hopf algebras in the list, except for book algebras, where $\mathbf{h}(q, m)$ is isomorphic to $\mathbf{h}(q^{-m^2}, m^{-1})$; cf. Section 1.

Let us define the *index* of a Hopf subalgebra H of a finite Hopf algebra A as the ratio $\dim A/\dim H$; it is an integer because of the Theorem of Nichols–Zoeller [NZ].

Theorem 0.1 is a consequence of Theorem 0.2:

THEOREM 0.2. *Let $H = k(\Gamma)$, where Γ is a finite nontrivial abelian group; say $\Gamma = \langle y_1\rangle \oplus \cdots \oplus \langle y_\sigma\rangle$, $y_l \neq 0$. Let M_l denote the order of y_l, $1 \le l \le \sigma$. Let A be a pointed Hopf algebra with coradical H.*

(A) *Assume that the index of H in A is p. Then there exist $g \in \Gamma$ and a character $\chi \in \hat{\Gamma}$ such that $q := \chi(g)$ has order p and A can be represented by generators h_l, $1 \le l \le \sigma$, a, and relations*

$$h_l h_t = h_t h_l, \; h_l^{M_l} = 1 \text{ for all } 1 \le l, t \le \sigma \tag{0.2}$$

$$a^p = \mu(1 - g^p), \text{ with } \mu \text{ either } 0 \text{ or } 1; \tag{0.3}$$

$$h_l a h_l^{-1} = \chi(y_l) a, \text{ for all } 1 \le l \le \sigma. \tag{0.4}$$

The Hopf algebra structure of A is determined by

$$\Delta(h_l) = h_l \otimes h_l, \qquad \Delta(a) = a \otimes 1 + g \otimes a, \qquad 1 \le l \le \sigma.$$

Assume that the index of H in A is p^2. Then there are two possibilities:

(B_1) *There exist* $g \in \Gamma$ *and a character* $\chi \in \hat{\Gamma}$ *such that* $q := \chi(g)$ *has order* p^2 *and* A *can be presented by generators* $h_l, a, 1 \leq l \leq \sigma$, *and relations* (0.2),

$$a^{p^2} = \mu\left(1 - g^{p^2}\right), \text{ with } \mu \text{ either } 0 \text{ or } 1; \tag{0.5}$$

$$h_l a h_l^{-1} = \chi(y_l) a, 1 \leq l \leq \sigma. \tag{0.6}$$

The Hopf algebra structure of A *is determined by*

$$\Delta(h_l) = h_l \otimes h_l, \qquad \Delta(a) = a \otimes 1 + g \otimes a, \quad 1 \leq l \leq \sigma.$$

(B_2) *There exist* $g_1, g_2 \in \Gamma$ *and characters* $\chi_1, \chi_2 \in \hat{\Gamma}$ *such that* $q_1 := \chi_1(g_1)$ *and* $q_2 = \chi_2(g_2)$ *have order* p, $\chi_1(g_2)\chi_2(g_1) = 1$ *and* A *can be presented by generators* $h_l, a_i, 1 \leq l \leq \sigma, i = 1, 2$, *and relations* (0.2),

$$a_i^p = \mu_i(1 - g_i^p), \text{ with } \mu_i \text{ either } 0 \text{ or } 1, i = 1, 2; \tag{0.7}$$

$$h_l a_i h_l^{-1} = \chi_i(y_l) a_i, 1 \leq l \leq \sigma, i = 1, 2; \tag{0.8}$$

$$a_1 a_2 - \chi_2(a_1) a_2 a_1 = \lambda(1 - g_1 g_2), \text{ with } \lambda \text{ either } 0 \text{ or } 1. \tag{0.9}$$

If $\lambda \neq 0$, *then* $\chi_1 \chi_2 = 1$. *The Hopf algebra structure of* A *is determined by*

$$\Delta(h_l) = h_l \otimes h_l, \qquad \Delta(a_i) = a_i \otimes 1 + g_i \otimes a_i, \quad i = 1, 2, \quad 1 \leq l \leq \sigma.$$

The proof of Theorem 0.2 follows from the above principle: we show, via the mentioned characterization, that a braided Hopf algebra of our special type and of dimension p or p^2 is necessarily a quantum linear space (Lemma 5.6). We then deduce Theorem 0.2 from the Lifting Theorem 5.5.

We shall give more applications of this principle in a separate article. We shall generalize the basic Theorem of Taft and Wilson ([TW], [M, Thm. 5.4.1]) to the case of Hopf algebras whose coradical is a Hopf subalgebra. This Theorem is the key point in the proof of the following result (see e.g. [N, p. 1545], [AS2, Prop. 3.1]): If A is a pointed non-cosemisimple finite-dimensional Hopf algebra, with coradical $k(\Gamma)$ where Γ is abelian, then there exist $g \in \Gamma$, a k-character χ of Γ such that $\chi(g) \neq 1$, and $x \in A, x \notin k(\Gamma)$ such that

$$hxh^{-1} = \chi(h)x \quad \forall h \in \Gamma, \quad \Delta(x) = x \otimes g + 1 \otimes x.$$

The preceding statement is the initial point in existing attempts of classifications of various kinds of pointed Hopf algebras.

The Lifting Theorem 5.5 has an extra bonus. In 1975, Kaplansky formulated a series of conjectures on Hopf algebras. Under the hypothesis that the characteristic of the ground field does not divide the positive integer n, one of these conjectures states that there are only a finite number (up to isomorphism) of Hopf algebras of dimension n. In this direction the following result was proved by Stefan: The set of types of semisimple and cosemisimple Hopf algebras of a given dimension is finite (in any characteristic). See [St]; a more direct proof (showing at the same time finiteness of the number of automorphisms and right coideal subalgebras) is given in [S].

Our Lifting Theorem easily produces counterexamples to Kaplansky's conjecture.

THEOREM 0.3. *There exist an infinite family of nonisomorphic pointed Hopf algebras of order* p^4.

Let us say that a Hopf algebra is *very simple* if

(i) it has no nontrivial normal Hopf subalgebra, and

(ii) it cannot be constructed by bosonization in a nontrivial way.

Usually, a Hopf algebra is called simple if it satisfies only (i); see for instance [A]. However, Taft algebras and book algebras are simple in this sense—this follows from the criteria in [AS1]; but they are analogues of solvable algebraic groups and it is hard to accept their simplicity. On the other hand, bosonization is also a mean to build Hopf algebras from smaller ones—though one of them is a braided Hopf algebra. Also, Taft and book algebras can be build by bosonization. For these reasons, we propose this new definition.

Theorem 0. 1 has the following consequence:

COROLLARY 0.4. *The only pointed Hopf algebras of order* p^3, *which are very simple, are the Frobenius–Lusztig kernels* $\mathbf{u}(q)$ *of type* A_1.

The Corollary follows from the considerations in Section 1. So far, the only known very simple Hopf algebras of order p^3 are the Frobenius–Lusztig kernels $\mathbf{u}(q)$ and their duals; see 1.7.

Let us briefly indicate the contents of the paper. In Section 1, we give some information about the Hopf algebras mentioned above. Section 2 is devoted to basic facts supporting the principle. In Section 3 we discuss finite-dimensional quantum linear spaces. In Section 4, we discuss possible quantum linear spaces over abelian groups. Theorem 0.2, respectively Theorem 0.3, Theorem 0.1, are proved in Section 5, respectively Section 6, Section 7.

Theorem 0.1 of this paper was announced at the Colloque "K-theory, cyclic homology and group representations," CIRM, Luminy (July 1997); and at the "XLVI Reunión de Comunicaciones Cientificas de la Unión Matemática Argentina," Córdoba (September 1997), where also a counterexample to Kapklansky's conjecture was described. The list appears already in the preprint version of [AS2], Trabajos de Matemática 42/96, FaMAF.

Theorem 0.1 was independently proved by Caenepeel and Dascalescu [CD] and also by Stefan and van Oystaeyen [SvO]. Theorem 0.3 was independently found by Beattie *et al*. [BDG] and also by Gelaki [G]. The methods of these authors seem to be quite different from ours. It is an interesting coincidence that all these articles, including ours, appeared in preprint form in a period of a few weeks in the fall of 1997.

We thank the referee for helpful comments on this paper.

Conventions. If C is a coalgebra, we denote by $G(C)$ the set of group-like elements of C. If $g, h \in G(C)$, then we denote $P_{g,h}(C) = P_{g,h} = \{x \in C\colon\ \Delta(x) = x \otimes h + g \otimes x\}$; the elements of $P_{g,h}$ are called skew-primitives. When B is a bialgebra, $P_{1,1}(B)$ is just the space $P(B)$ of primitive elements.

If A is an algebra, $\operatorname{Alg}(A, k)$ denotes the set of all algebra maps from A to k.

If Γ is a group, we denote by $\hat{\Gamma}$ the group of characters (one-dimensional representations over k) of Γ.

1. ABOUT THE HOPF ALGEBRAS IN THE LIST

1.0. Let $\xi \in k$ be a root of 1 of order $N \geq 2$. The Taft algebra $T_k(\xi) = T(\xi)$ is the algebra $k\langle g, x \mid gxg^{-1} = \xi x, g^N = 1, x^N = 0\rangle$. Its Hopf algebra structure is given by

$$\Delta(g) = g \otimes g, \quad \mathscr{S}(q) = g^{-1}, \quad \varepsilon(g) = 1,$$

$$\Delta(x) = x \otimes g + 1 \otimes x, \quad \mathscr{S}(x) = -xg^{-1}, \quad \varepsilon(x) = 0.$$

The dimension of $T\xi$ is N^2. It is known that $T(\xi) \simeq T(\xi)^*$ as Hopf algebras, and that $T(\xi) \simeq T(\tilde{\xi})$ only if $\xi = \tilde{\xi}$.

A proper Hopf subalgebra A of $T(\xi)$ is contained in $k[g]$: this follows easily looking at the coradical filtration of A. Therefore, if A is a proper Hopf subalgebra or quotient of $T(\xi)$, then the order of A divides N.

Semisimple Hopf algebras of order p^2 are group algebras [Ma2]. The only pointed noncosemisimple Hopf algebras of order p^2 are the Taft algebras; a more precise characterization of Taft algebras is given in [AS2].

In fact, Taft algebras and group algebras are the only known Hopf algebras of order p^2.

1.1. The pointedness of the Hopf algebras in the list is a consequence of the criteria [M, Lemma 5.5.1]. As in the proof of [M, Lemma 5.5.5], we conclude that a Hopf algebra in the list has coradical $k(\Gamma)$, where Γ is:

(1) $\mathbb{Z}/(p) \times \mathbb{Z}/(p)$, in case (a);

(2) $\mathbb{Z}/(p^2)$, in cases (b), (c), (d);

(3) $\mathbb{Z}/(p)$, in cases (e), (f).

In particular, this is a first step toward deciding the nonexistence of isomorphisms between the different cases.

It is not difficult to see that all the Hopf algebras in the list have dimension p^3; e.g., using the Diamond Lemma. Alternatively, say in case (b), let A be a vector space with a basis $g^i x^j, 0 \leq i \leq p^2 - 1, 0 \leq j \leq p - 1$. It is possible to write down explicitly a multiplication table for A such that the defining relations hold; A is then an associative algebra. Hence there is an epimorphism $\widetilde{T_k(q)} \to A$. But it is easy to see that $\widetilde{T_k(q)}$ has dimension at least p^3; therefore the dimension is p^3. This idea applies to the other cases as well.

1.2. The Hopf algebra $\widetilde{T_k(q)}$ does not depend, modulo isomorphisms, upon the choice of the pth root of q. Indeed, let $\widetilde{T}_j := k\langle h, y \mid hyh^{-1} = q^{1/p+j}y, h^{p^2} = 1, y^p = 0\rangle$, with comultiplication $\Delta(h) = h \otimes h, \Delta(y) = y \otimes h^p + 1 \otimes y$. Then one has an isomorphism of Hopf algebras $\widetilde{T_k(q)} \to \widetilde{T}_j$ determined by $x \mapsto y, g \mapsto h^{1-pj}$.

Notice that $\widetilde{T_k(q)}$ is a cocentral extension of $k(\mathbb{Z}/p)$ by a Taft algebra:

$$1 \to T_k(q) \to \widetilde{T_k(q)} \to k(\mathbb{Z}/p) \to 1.$$

1.3. The Hopf algebra $\widehat{T_k}(q)$ is dual to $\widetilde{T_k(q)}$. It is a central extension of a Taft algebra,

$$1 \to k(\mathbb{Z}/p) \to \widehat{T_k(q)} \to T_k(q) \to 1,$$

where the central Hopf algebra is generated by g^p. It is clear that no group-like element of $\widetilde{T_k(q)}$ is central; hence $\widetilde{T_k(q)}$ and $\widehat{T_k(q')}$ cannot be isomorphic for any q, q'.

1.4. The Hopf algebra $\mathbf{r}(q)$ is also a central extension of a Taft algebra,

$$1 \to k(\mathbb{Z}/p) \to \mathbf{r}(q) \to T_k(q) \to 1,$$

again, the central Hopf algebra is generated by g^p. This Hopf algebra was first considered by Radford [R1]. The dual Hopf algebra $(\mathbf{r}(q))^*$ is not pointed—see *loc. cit.*; hence cases (b), (c), and (d) have no intersection.

In all three cases, the Hopf algebras are not isomorphic for different values of q. This can be shown via the first term of the coradical filtration. Indeed, it is enough to consider $\widetilde{T_k(q)}$, since $\widetilde{T_k(q)} \simeq (\widetilde{T_k(q)})^*$ and gr $\mathbf{r}(q) \simeq \widetilde{T_k(q)}$.

1.5. The Frobenius–Lusztig kernel $\mathbf{u}(q)$ is the simplest example of the finite dimensional Hopf algebras introduced in [L1], [L2]. It is easy to see that it has no nontrivial representation of dimension 1. Looking at its coradical filtration [T], we conclude that $\mathbf{u}(q)$ and $\mathbf{u}(q')$ are not isomorphic unless $q = q'$. It is not difficult to see that $\mathbf{u}(q)$ has no nontrivial quotient Hopf algebra [T]; hence it is very simple. See also [AS1].

1.6. Information about book Hopf algebras can be found in [AS2, Sect. 6]; $\mathbf{h}(q, p-1)$ was already considered in [R2, p. 352]—without assuming that the order of q is prime. $\mathbf{h}(q, m)$ and $\mathbf{h}(\tilde{q}, \tilde{m})$ are isomorphic if, and only if, $(\tilde{q}, \tilde{m}) = (q, m)$ or (q^{-m^2}, m^{-1}) [AS2, Prop. 6.5]. The dual Hopf algebra $(\mathbf{h}(q, m))^*$ is isomorphic to $\mathbf{h}(q, -m)$ [AS2, Prop. 6.7]; in particular, $\mathbf{h}(q, m)$ has p different representations of dimension 1 and hence types (e) and (f) have no intersection.

Book algebras can be obtained by bosonization [AS2]; see also Section 3. By the criteria in [AS1], a book algebra is simple.

1.7. Semisimple Hopf algebras of order p^3 were classified by Masuoka [Ma1]: there are $p + 8$ isomorphism types, namely three group algebras of abelian groups; two group algebras of nonabelian groups and their duals; $p + 1$ noncommutative, noncocommutative Hopf algebras constructed by extension.

In addition to the already mentioned Hopf algebras of order p^3 there are also the dual Hopf algebras $(\mathbf{u}(q))^*$ and $(\mathscr{R}(q))^*$. Among all these Hopf algebras of order p^3, only the Frobenius–Lusztig kernels and their duals are very simple in the sense of the Introduction.

2. THE CORADICAL FILTRATION AND THE ASSOCIATED GRADED HOPF ALGEBRA

2.0 Let B, H, and R be as in (0.1). Then R is a braided Hopf algebra in the category ${}_H^H\mathscr{YD}$ of Yetter–Drinfeld modules over H. See [R3], [Mj]. We recall the explicit form of this structure; we follow the conventions of [AS2].

The action of H on R is given by the adjoint representation composed with γ. The coaction is $(\pi \otimes \mathrm{id})\Delta$. These two structures are related by the Yetter–Drinfeld condition:

$$\delta_R(h.r) = h_{(1)} r_{(-1)} \mathscr{S}\big(h_{(3)}\big) \otimes h_{(2)}.r_{(0)}.$$

Hence, R is an object of ${}_H^H\mathscr{YD}$.

Moreover, R is a subalgebra of B and a coalgebra with comultiplication

$$\Delta_R(r) = r_{(1)}\gamma\pi\mathscr{S}(r_{(2)}) \otimes r_{(3)};$$

the counit is the restriction of the counit of B. To avoid confusion, we denote here the comultiplication of R by

$$\Delta_{(R)}(r) = \sum r^{(1)} \otimes r^{(2)},$$

or even we omit sometimes the summation sign.

The multiplication m and the comultiplication Δ of R satisfy

$$\Delta m = (m \otimes m)(\mathrm{id} \otimes c \otimes \mathrm{id})(\Delta \otimes \Delta).$$

Here c is the commutativity constraint of ${}_H^H\mathscr{YD}$; explicitly

$$c_{M,N}(m \otimes n) = m_{(-1)}.n \otimes m_{(0)},$$

for $M, N \in {}_H^H\mathscr{YD}, m \in M, n \in N$.

The map $\mathscr{S}_R\colon R \to R$ given by

$$\mathscr{S}_R(r) = \gamma\pi(r_{(1)})\mathscr{S}_B r_{(2)}$$

(where $\mathscr{S}_B$ is the antipode of B) is the antipode of R, i.e., the inverse of the identity in End R for the convolution product. Hence R is a braided Hopf algebra in ${}_H^H\mathscr{YD}$.

Conversely, given H and a Hopf algebra R in ${}_H^H\mathscr{YD}$, the tensor product $B = R \otimes H$ bears a Hopf algebra structure, denoted $R\#H$, via the smash product and smash coproduct:

$$\begin{aligned}(r\#h)(s\#f) &= r(h_{(1)}.s)\#h_{(2)}f,\\ \Delta(r\#h) &= r^{(1)}\#(r^{(2)})_{(-1)}h_{(1)} \otimes (r^{(2)})_{(0)}\#h_{(2)}\end{aligned} \tag{2.1}$$

Let $\pi\colon R\#H \to H$ and $\gamma\colon H \to R\#H$ be the maps

$$\pi(r\#h) = \varepsilon(r)h, \quad \gamma(h) = 1\#h.$$

Then γ is a section of π and we are in the setting (0.1). We term $B = R\#H$, following Majid, the bosonization of R.

2.1. We recall that a graded Hopf algebra is a Hopf algebra G together with a grading $G = \bigoplus_{n\geq 0} G(n)$ which is simultaneously an algebra and a coalgebra grading [Sw, Section 11.2]. In particular, $\varepsilon(G(n)) = 0$ for $n > 0$ and the antipode is a homogeneous map of degree 0.

It turns out that $G(0)$ is a Hopf subalgebra of G and that the inclusion $\gamma\colon G(0) \hookrightarrow G$ is a section of the projection $\pi\colon G \to G(0)$ with kernel $\bigoplus_{n\geq 1} G(n)$. Let

$$R = \{a \in G\colon (\mathrm{id} \otimes \pi)\Delta(a) = a \otimes 1\}.$$

We know that R is a braided Hopf algebra in ${}^{G(0)}_{G(0)}\mathcal{YD}$ and G is the bosonization of R.

We shall say that a braided Hopf algebra with a grading of Yetter–Drinfeld modules is *graded* if the grading is simultaneously an algebra and coalgebra grading.

LEMMA 2.1. *Keep the notation above.*

(i) *R is a graded subalgebra of G: $R = \bigoplus_{n\geq 0} R(n)$, where $R(n) = R \cap G(n)$.*

(ii) *With respect to this grading, it is a braided graded Hopf algebra.*

(iii) *$G(n) = R(n)\#G(0)$ and $R_0 = R(0) = k1$.*

Proof. Let $r \in R$ and let us decompose $r = \sum_j r_j$, with $r_j \in G(j)$. Then we write

$$\Delta_G(r_j) = \sum_h r_{j,h} \otimes r_j^h,$$

where $r_{j,h} \in G(h)$, $r_j^h \in G(j-h)$. Clearly, $\pi(r_j^h) = 0$ unless $h = 0$. Hence $(\mathrm{id} \otimes \pi)\Delta(r_j) \in G(j) \otimes G(0)$. By definition of R,

$$\sum_j r_j \otimes 1 = \sum_j (\mathrm{id} \otimes \pi)\Delta(r_j);$$

taking homogeneous components, we see that $r_j \otimes 1 = (\mathrm{id} \otimes \pi)\Delta(r_j)$, i.e., that $r_j \in R$. This proves (i).

It follows from the definition of the action and coaction that each $R(n)$ is a submodule and subcomodule. That is, $R = \bigoplus_{n\geq 0} R(n)$ is a grading in ${}^{G(0)}_{G(0)}\mathcal{YD}$.

It is not difficult that R is a graded coalgebra. Indeed, if $r \in R(j)$ then we write

$$(\Delta_G \otimes \mathrm{id})\Delta_G(r) = \sum_{h,t} a_h \otimes b_t \otimes c_{j-t-h},$$

where $a_h \in G(h)$, $b_t \in G(t)$, $c_{j-t-h} \in G(j-t-h)$. Hence

$$\begin{aligned}\Delta_R(r) &= \sum_{h,t} a_h \pi\mathcal{S}(b_t) \otimes c_{j-t-h}\\ &= \sum_h a_h \pi\mathcal{S}(b_0) \otimes c_{j-h} \in \oplus_h R(h) \otimes R(j-h).\end{aligned}$$

Now we prove (iii). The first claim is evident, since $G(n) \supseteq R(n)\#G(0)$ and $G = \bigoplus_{n\geq 0} G(n) = \bigoplus_{n\geq 0} R(n) \otimes G(0)$. As for the second, we know that $R_0 \subseteq R(0)$ and $R(0) = k1$. Indeed, the contention follows since the coradical is contained in the zero part of any coalgebra filtration [M, 5.3.4]; the equality follows by definition. These two facts imply that $R_0 = R(0) = k1$. ∎

2.2. Let A be a Hopf algebra and assume that its coradical A_0 is a Hopf subalgebra (for instance, A is pointed). Then the coradical filtration is in fact a Hopf algebra filtration and the associated graded algebra

$$\operatorname{gr} A = \bigoplus_{n\geq 0} \operatorname{gr} A(n) = \bigoplus_{n\geq 0} An/A_{n-1}$$

(with $A_{-1} = 0$) is a graded Hopf algebra. See [M, 5.2.8]. If A has finite dimension N, then $\operatorname{gr} A$ also has dimension N.

Lemma 2.2. *If* $\operatorname{gr} A$ *is generated as an algebra by* $\operatorname{gr} A(0) \oplus \operatorname{gr} A(1)$ *then* A *is generated as an algebra by* A_1.

Proof. This can be checked directly, or via the following argument: $A_1, \operatorname{gr} A(1)$ are A_0-bimodules, and the projection $A_1 \to \operatorname{gr} A(1)$ is a bimodule homomorphism. Since A_0 is semisimple by [LR], $A_1 \simeq A_0 \oplus \operatorname{gr} A(1)$ as A_0-bimodules. We can consider the tensor algebra $T_{A_0}(\operatorname{gr} A(1))$ and the corresponding map $\pi: T_{A_0}(\operatorname{gr} A(1)) \to A$- see [N, Prop. 1.4.1]. This map is compatible with filtrations and the corresponding graded map is surjective. Then π is surjective [B, Sect. 2, no. 8]. ∎

(2.3). Let A be a Hopf algebra whose coradical A_0 is a Hopf subalgebra.

Lemma 2.3. *The coradical filtration of* $\operatorname{gr} A$ *is given by*

$$(\operatorname{gr} A)_m = \bigoplus_{n\leq m} \operatorname{gr} A(n). \tag{2.2}$$

Definition [CM]. A graded coalgebra satisfying (2.2) is called *coradically graded.*

Proof. We check this for $m = 0, 1$; the general case is similar or else can be deduced from these two cases by [CM, 2.2].

First, $A_0 = \operatorname{gr} A(0) \subseteq (\operatorname{gr} A)_0$ because it is cosemisimple. Conversely, the filtration $\operatorname{gr} A(0) \subset \operatorname{gr} A(0) \oplus \operatorname{gr} A(1) \subset \cdots \subset \bigoplus_{n\leq m} \operatorname{gr} A(n) \subset \cdots$ is a coalgebra filtration hence $\operatorname{gr} A(0) \supseteq (\operatorname{gr} A)_0$ [Sw, 11.1.1].

Now we consider $m = 1$. Again, $A_0 \oplus A_1/A_0 \subseteq (\operatorname{gr} A)_1$ is easy. Let $y \in (\operatorname{gr} A)_1$ and write

$$y = \overline{y_0} + \overline{y_1} + \cdots + \overline{y_m}, \quad \overline{y_j} \in A_j/A_{j-1}, \quad \overline{y_m} \neq 0.$$

Hence

$$\Delta(y) = \sum_{j=0}^{m} \Delta\left(\overline{y_j}\right) \in \Delta\left(\overline{y_m}\right) + \bigoplus_{r+s<m} \operatorname{gr} A(r) \otimes \operatorname{gr} A(s),$$

and $\Delta(\overline{y_m}) = z_1 + z_2 + z_3$, with $z_1 \in \operatorname{gr} A(m) \otimes \operatorname{gr} A(0)$, $z_2 \in \operatorname{gr} A(0) \otimes \operatorname{gr} A(m)$, $z_3 \in \bigoplus_{r+s=m,\, r,s>0} \operatorname{gr} A(r) \otimes \operatorname{gr} A(s)$.

Now assume that $m > 1$. If $z_3 = 0$, $\overline{y_m} = 0$; and if $z_3 \neq 0$, $y \notin (\operatorname{gr} A)_1$. So m should be 1 and $A_0 \oplus A_1/A_0 \supseteq (\operatorname{gr} A)_1$. ∎

2.4. Let $G = \bigoplus_{n \geq 0} G(n)$ be a coradically graded Hopf algebra. Let R be the associated braided graded Hopf algebra, see 2.1.

LEMMA 2.4. (i) *$R_0 = k1 = R(0)$ and $P(R) = R(1)$.*

(ii) *R is a coradically graded coalgebra.*

(iii) *$G_1 = G(0) \oplus [P(R)\#G(0)]$.*

Proof. (i) We know that $R_0 = R(0) = k1$ from Lemma 2.1.

Let $r \in R(1)$. Then $\Delta_R(r) = r_1 \otimes 1 + 1 \otimes r_2$, for some $r_1, r_2 \in R(1)$. Applying $\mathrm{id} \otimes \varepsilon$ and $\varepsilon \otimes \mathrm{id}$ to both sides of this equality, we conclude that $r_1 = r_2 = r$. That is, $P(R) \supseteq R(1)$.

Let now $r \in P(R)$. If $\delta(r) = r_{(-1)} \otimes r_{(0)} \in G(0) \otimes R$, then

$$\Delta_G(r) = r \otimes 1 + r_{(-1)} \otimes r_{(0)}.$$

As $G_0 = G(0)$, we deduce that $r \in G_1$. But by hypothesis, $G_1 = G(0) \oplus G(1)$. Hence $r \in R(0) \oplus R(1)$; since $\varepsilon(r) = 0$, we see that $r \in R(1)$. That is, $P(R) \subseteq R(1)$.

(ii) By [CM, 2.2], it is enough to consider the cases $m = 0, 1$. The case $m = 0$ is covered by (i). For $m = 1$, we have, again by (i),

$$R_1 = k1 \oplus P(R) = R(0) \oplus R(1).$$

(iii) This follows from Lemma 2.1 and (ii). ∎

2.5. Let H be a cosemisimple Hopf algebra. Let R be a braided graded Hopf algebra in the category ${}_H^H\mathcal{YD}$. Let $G = R\#H$; it is easy to see that G is a graded Hopf algebra.

LEMMA 2.5. *If $R_0 = k1 = R(0)$ and $P(R) = R(1)$, then G is a coradically graded Hopf algebra.*

3. QUANTUM LINEAR SPACES

As mentioned in the Introduction, we are interested in braided Hopf algebras R in the category ${}_H^H\mathcal{YD}$ of Yetter–Drinfeld modules over a Hopf algebra H. We use in this section the notation of [AS2, Section 4].

A version of the following result appears in [N, p. 1538].

LEMMA 3.1. *Let H be a finite dimensional Hopf algebra.*

(i) *Let $x \in H$ such that $\Delta(x) = x \otimes 1 + g \otimes x$, $gx = xg$, for some $g \in G(H)$. Then x is a scalar multiple of $g - 1$.*

(ii) *Let R be a finite dimensional braided Hopf algebra in ${}_H^H\mathcal{YD}$. Let $x \in P(R)$ be a nonzero primitive element such that $\delta(x) = g \otimes x$, $h.x = \chi(h)x$, for some $g \in G(H)$, $\chi \in \mathrm{Alg}(H, k)$ and for all $h \in H$. Then $q := \chi(g) \neq 1$.*

Proof. Let S be the subalgebra of H generated by g and x; by hypothesis, it is a commutative Hopf subalgebra and hence it is cosemisimple by the Cartier–Kostant theorem. Looking at the expression of x in terms of the decomposition of S in simple subcoalgebras, one concludes that $x = \lambda(g - 1)$, for some $\lambda \in k$. This shows (i).

For (ii), we apply (i) to the element $x\#1$ of $A = R\#H$; by (2.1), $\Delta(x) = x \otimes 1 + g \otimes x$ and $gx = qxg$. If $q = 1$ then $x = \lambda(g - 1)$, for some $\lambda \in k$. This implies $x = 0$, a contradiction. ∎

Let K be an arbitrary Hopf algebra. Let $g \in G(K)$, $\chi \in \mathrm{Alg}(K, k)$ such that $\chi(h)g = h_{(1)}\chi(h_{(2)})g\mathcal{S}(h_{(3)})$, for all $h \in K$. Let N be the order of $q := \chi(g)$; we assume N is finite.

Let $R = k[y]/(y^N)$. Then R is a braided Hopf algebra in ${}_H^H\mathcal{YD}$ with K-module and K-comodule structures given by

$$h.y^t = \chi^t(h)y^t, \qquad \delta_R(y^t) = g^t \otimes y^t,$$

and comultiplication uniquely determined by $\Delta_R(y) = y \otimes 1 + 1 \otimes y$. This braided Hopf algebra will be denoted $\mathcal{R}(g, \chi)$. The braided Hopf algebras $\mathcal{R}(g, \chi)$ and $\mathcal{R}(\tilde{g}, \tilde{\chi})$ are isomorphic only if $g = \tilde{g}$ and $\chi = \tilde{\chi}$. See [AS2, Lemma 8.1].

THEOREM 3.2. *Let H be a finite-dimensional semisimple Hopf algebra. Let R be a finite-dimensional braided Hopf algebra in ${}_H^H\mathcal{YD}$. Assume that*

(1) $R_0 = k1$, *where R_0 is the coradical of R.*

(2) $\dim P(R) = 1$.

Then there exist $g \in G(H)$, and $\chi \in Alg(H, k)$ such that $R \simeq \mathcal{R}(g, \chi)$.

Proof. By (1), $P(R) \neq 0$. As $P(R)$ is a Yetter–Drinfeld submodule of R, condition (2) implies the existence of $g \in G(H)$ and a character $\chi \in H^*$ such that

$$\delta(x) = g \otimes x, \qquad h.x = \chi(h)x \quad \forall h \in G(H), x \in P(R).$$

Let N be the order of $q = \chi(g)$. Fix $x \in P(R)$, $x \neq 0$. By the quantum binomial formula, $\dim k[x] = N$ and $x^N = 0$. In fact, $k[x] \simeq \mathscr{R}(g, \chi)$. Hence we only need to prove that $R = k[x]$.

Consider the algebra R^*. It has a unique maximal ideal, namely $\mathscr{M} := R_0^{\perp}$. $\mathscr{M}$, and *a fortiori* $\mathscr{M}^2$ and $\mathscr{M}/\mathscr{M}^2$, are Yetter–Drinfeld modules. Observe that $\mathscr{M}/\mathscr{M}^2 \simeq (P(R))^*$ as H-modules. But, since H is semisimple, the projection $\mathscr{M} \to \mathscr{M}/\mathscr{M}^2$ has an H-linear and H-colinear section. Whence there exists $T \in \mathscr{M} - \mathscr{M}^2$ such that

$$\delta(T) = g^{-1} \otimes T, \qquad h.T = \chi^{-1}(h)T \quad \forall h \in H.$$

It is not difficult to show that $R^* = k[T]$. Hence $1, T, T^2, \dots, T^{d-1}$ is a basis of R^*, where $d = \dim R$, and we can consider its dual basis $t_0, t_1, \dots, t_N \dots$ in R. Note that $\delta(T^j) = g^{-j} \otimes T^j, h.T^j = \chi^{-j}(h)T^j, \forall h \in H$; hence $\delta(t_j) = g^j \otimes t_j$, $h.t_j = \chi^j(h)t_j, \forall h \in H$.

On the other hand, consider the coradical filtration of R:

$$R_0 = k1 \subseteq R_1 = k1 \oplus P(R) \subseteq \dots \subseteq R_j \subseteq \dots.$$

If $j \leq N - 1, 1, x, \dots, x^j$ belong to R_j. As $(R_j)^* \simeq R^*/\mathscr{M}^{j+1}$, we conclude that $1, x, \dots, x^j$ form a basis of R_j. Hence there exist $\lambda_j \in k$ such that

$$\lambda_j t_j = x^j, \qquad j \leq N - 1.$$

Now assume $d > N$ and let $z = t_N$. Then

$$\begin{aligned}\Delta(z) = \Delta(t_N) &= \sum_{0 \leq i \leq N} t_i \otimes t_{N-i} = z \otimes 1 + 1 \otimes z \\ &\quad + \sum_{1 \leq i \leq N-1} \lambda_i \lambda_{N-i} x^i \otimes x^{N-i}.\end{aligned}$$

Therefore the subalgebra $k\langle x, z\rangle$ is a Hopf subalgebra of R. Now let us compute

$$\begin{aligned}\Delta(xz) &= (x \otimes 1 + 1 \otimes x)\Big(z \otimes 1 + 1 \otimes z + \sum_{1 \leq i \leq N-1} \lambda_i \lambda_{N-i} x^i \otimes x^{N-i}\Big) \\ &= xz \otimes 1 + x \otimes z + \sum_{1 \leq i \leq N-1} \lambda_i \lambda_{N-i} x^{i+1} \otimes x^{N-i} \\ &\quad + z \otimes x + 1 \otimes zx + \sum_{1 \leq i \leq N-1} \lambda_i \lambda_{N-i} q^i x^i \otimes x^{N+1-i}.\end{aligned}$$

Hence $xz \in R_{N+1}$; similarly, also $zx \in R_{N+1}$. We conclude, looking at the decomposition in H-submodules, that

$$xz = at_{N+1} + bx, \qquad zx = ct_{N+1} + dx,$$

for some $a, b, c, d \in k$. It follows from this that $k[x]$ is a normal Hopf subalgebra of $k\langle x, z\rangle$, and we can form the quotient Hopf algebra. The image of z in this finite dimensional braided Hopf algebra is invariant and primitive, hence 0. Then $k[x] = k\langle x, z\rangle$, a contradiction. ∎

Remark. The referee proposes an alternative proof of Theorem 3.2 which also works for H not semisimple. We sketch now the argument. One shows first the following Proposition:

PROPOSITION. *Let S be a finite-dimensional graded Hopf algebra in the category ${}^H_H\mathcal{YD}$ of Yetter–Drinfeld modules over a finite-dimensional Hopf algebra H (not necessarily semisimple). Suppose* $\dim S(0) = \dim S(1) = 1$. *Then S is generated as an algebra by $S(1)$ if and only if S is coradically graded (i.e., strictly graded in this case).*

In fact, one needs to show only one implication, by duality. The proof uses the quantum binomial formula. Theorem 3.2 follows from the first paragraph of our proof and the Proposition passing to the coradically graded Hopf algebra $S = \operatorname{gr} R$, corresponding now to the coradical filtration of R. The following Corollary is also due to the referee:

COROLLARY. *Let A be a finite-dimensional Hopf algebra whose coradical is a Hopf subalgebra. If* $\dim A_1 = 2 \dim A_0$ *then the algebra A is generated by A_1.*

The proof follows from the Proposition using Lemma 2.4 and 2.2.

Let K be an arbitrary Hopf algebra.

DEFINITION. We shall say that a braided Hopf algebra R in ${}^K_K\mathcal{YD}$ satisfies *hypothesis* (A) if there exist a basis $x_1, \dots, x_\theta$ of $P(R)$, and $g_1, \dots, g_\theta \in G(K)$, $\chi_1, \dots, \chi_\theta \in \operatorname{Alg}(K, k)$ such that for all $j, 1 \le j \le \theta$,

$$\delta(x_j) = g_j \otimes x_j, \quad h.x_j = \chi_j(h)x_j, \quad \text{for all } h \in K,$$

and $\qquad$ the order N_j of $q_j := \chi_j(g_j)$ is finite.

If $K = k(\Gamma)$ is the group algebra of a finite abelian group Γ, hypothesis (A) always holds; see the remarks after Corollary 5.3.

If $q \in k$ and $0 \le i \le n < \operatorname{ord} q$, we set $(0)_q! = 1$,

$$\binom{n}{i}_q = \frac{(n)_q!}{(i)_q!(n-i)_q!}, \quad \text{where } (n)_q! = \prod_{1 \le i \le n} (i)_q, \quad (n)_q = \frac{q^n - 1}{q - 1}.$$

By the quantum binomial formula, if $1 \le n_j < N_j$, then

$$\Delta\left(x_j^{n_j}\right) = \sum_{0 \le i_j \le n_j} \binom{n_j}{i_j}_{q_j} x_j^{i_j} \otimes x_j^{n_j - i_j}.$$

We use the notation

$$\mathbf{n} = (n_1, \dots, n_j, \dots, n_\theta), \quad x^{\mathbf{n}} = x_1^{n_1} \dots x_j^{n_j} \dots x_\theta^{n_\theta},$$
$$|\mathbf{n}| = n_1 + \cdots + n_j + \cdots + n_\theta;$$

accordingly, $\mathbf{N} = (N_1, \dots, N_\theta)$, $\mathbf{1} = (1, \dots, 1)$. Also, we set

$$\mathbf{i} \le \mathbf{n} \quad \text{if } i_j \le n_j, j = 1, \dots, \theta.$$

Then, for $\mathbf{n} \le \mathbf{N} - \mathbf{1}$, we deduce from the quantum binomial formula that

$$\Delta(x^{\mathbf{n}}) = x^{\mathbf{n}} \otimes 1 + 1 \otimes x^{\mathbf{n}} + \sum_{\substack{0 \le \mathbf{i} \le \mathbf{n} \\ 0 \ne \mathbf{i} \ne \mathbf{n}}} c_{\mathbf{n}, \mathbf{i}} x^{\mathbf{i}} \otimes x^{\mathbf{n} - \mathbf{i}},$$

where $c_{\mathbf{n}, \mathbf{i}} \ne 0$ for all $\mathbf{i}$. We shall need

$$\begin{aligned} \Delta(x_j x_i) &= \left(x_j \otimes 1 + 1 \otimes x_j\right)(x_i \otimes 1 + 1 \otimes x_i) \\ &= x_j x_i \otimes 1 + x_j \otimes x_i + \chi_i(g_j) x_i \otimes x_j + 1 \otimes x_j x_i, \end{aligned} \tag{3.1}$$

for $1 \le j, i \le \theta$.

LEMMA 3.3. *Let R be a braided Hopf algebra in ${}_K^K\mathcal{YD}$ satisfying hypothesis* (A). *Then $\{x^{\mathbf{n}}: \mathbf{n} \le \mathbf{N} - \mathbf{1}\}$ is linearly independent. Hence,* $\dim R \ge N_1 \dots N_\theta$. *In particular if any element of $G(K)$ has order p, then* $\dim R \ge p^\theta$.

Proof. We shall prove by induction on r that the set

$$\{x^{\mathbf{n}}: |\mathbf{n}| \le r, \quad \mathbf{n} \le \mathbf{N} - \mathbf{1}\}$$

is linearly independent.

Let $r = 1$ and let $a_0 + \sum_{i=1}^{\theta} a_i x_i = 0$, with $a_j \in k, 0 \le j \le \theta$. Applying ε, we see that $a_0 = 0$; by hypothesis we conclude that the other a_j's are also 0.

Now let $r > 1$ and suppose that $z = \sum_{\mathbf{n}: |\mathbf{n}| \le r} a_{\mathbf{n}} x^{\mathbf{n}} = 0$. Then

$$0 = \Delta(z) = z \otimes 1 + 1 \otimes z + \sum_{1 < |\mathbf{n}| \le r} a_{\mathbf{n}} \sum_{\substack{0 \le \mathbf{i} \le \mathbf{n} \\ 0 \ne \mathbf{i} \ne \mathbf{n}}} c_{\mathbf{n}, \mathbf{i}} x^{\mathbf{i}} \otimes x^{\mathbf{n} - \mathbf{i}}$$

$$= \sum_{1 < |\mathbf{n}| \le r} \sum_{\substack{0 \le \mathbf{i} \le \mathbf{n} \\ 0 \ne \mathbf{i} \ne \mathbf{n}}} a_{\mathbf{n}} c_{\mathbf{n}, \mathbf{i}} x^{\mathbf{i}} \otimes x^{\mathbf{n} - \mathbf{i}}.$$

Now, if $|\mathbf{n}| \le r, 0 \le \mathbf{i} \le \mathbf{n}$, and $0 \ne \mathbf{i} \ne \mathbf{n}$, the $|\mathbf{i}| < r$ and $|\mathbf{n} - \mathbf{i}| < r$. By inductive hypothesis, the elements $x^{\mathbf{i}} \otimes x^{\mathbf{n}-\mathbf{i}}$ are linearly independent. Hence $a_{\mathbf{n}} c_{\mathbf{n},\mathbf{i}} = 0$ and $a_{\mathbf{n}} = 0$ for all $\mathbf{n}$, $|\mathbf{n}| > 1$. By the step $r = 1$, $a_{\mathbf{n}} = 0$ for all $\mathbf{n}$. ∎

Let now $\theta \in \mathbb{N}$ and $g_1, \dots, g_\theta \in G(K)$, $\chi_1, \dots, \chi_\theta \in \mathrm{Alg}(A, k)$. We assume that

$$\text{the order } N_j \text{ of } q_j := \chi_j(g_j) \text{ is finite. To avoid degenerate cases we also assume } N_j > 1\text{; cf. Lemma 3.1.} \tag{3.2}$$

$$g_i g_j = g_j g_i, \quad \chi_i \chi_j = \chi_j \chi_i, \quad \text{for all } i, j. \tag{3.3}$$

$$\chi_i(h) g_i = h_{(1)} \chi_i(h_{(2)}) g_i \mathscr{S}(h_{(3)}), \text{ for all } h \in K, 1 \le i \le \theta. \tag{3.4}$$

$$\chi_j(g_i) \chi_i(g_j) = 1, \quad \text{for all } i \ne j. \tag{3.5}$$

For $K = k(\Gamma)$ with Γ finite abelian, the following Lemma was essentially proved in [N, p. 1539].

Let R be the algebra generated by $x_1, \dots, x_\theta$, with relations

$$x_1^{N_1} = 0, \dots, x_\theta^{N_\theta} = 0, \tag{3.6}$$

$$x_i x_j = \chi_j(g_i) x_j x_i, \text{ if } i \ne j. \tag{3.7}$$

LEMMA 3.4. *R has a unique braided Hopf algebra structure in ${}_K^K\mathscr{YD}$ such that the action and coaction are determined by*

$$\delta(x_j) = g_j \otimes x_j, \qquad h.x_j = \chi_j(h) x_j \quad \forall h \in \Gamma, \quad 1 \le j \le \theta,$$

and the x_i's are primitive. The dimension of R is $N_1 \dots N_\theta$. The coradical of R is $k1$ and the space $P(R)$ of primitive elements is the span of the x_i's. R is a coradically graded Hopf algebra, with respect to the grading where the x_i's are homogeneous of degree 1.

We denote this braided Hopf algebra by $\mathscr{R}(g_1, \dots, g_\theta; \chi_1, \dots, \chi_\theta)$; it will be called a *quantum linear space* over K.

Proof. We first observe that R is a K-module algebra and a K-comodule algebra because of conditions (3.3). Indeed, we can extend the preceding action and coaction of K to the free algebra on generators $x_1, \dots, x_\theta$; then we have to see that the ideal generated by the relations (3.6) and (3.7) is stable by the action and coaction. This is clear for (3.6); for (3.7), it follows from (3.3). In addition, the Yetter−Drinfeld condition on R holds because of, and indeed is equivalent to, (3.4).

We verify next that the elements $1 \otimes x_i + x_i \otimes 1 \in R \otimes R$ satisfy relations (3.6) and (3.7). The first follows from the quantum binomial formula; the second, by direct computation using (3.5). The counit is determined by $\varepsilon(x_i) = 0$. The existence of the antipode follows from a Lemma of Takeuchi, see [M, 5.2.10]: it is enough to check that the restriction of the identity to the coradical of R is invertible. But is not difficult to see that $R_0 = k1$. Indeed R is a graded coalgebra whose homogeneous part of degree 0 is $k1$; then use [Sw, 11.1.1]. Thus R is a braided Hopf algebra. By Lemma 3.3, $\dim R \geq N_1 \dots N_\theta$. But (3.6) and (3.7) guarantee that the monomials $\{x^{\mathbf{n}}: \mathbf{n} \leq \mathbf{N} - \mathbf{1}\}$ generate R as vector space; whence $\dim R = N_1 \dots N_\theta$.

Finally, it is clear that $R = \bigoplus_{n \geq 0} R(n)$ is a graded Hopf algebra, where $R(n)$ is generated by the monomials $x^{\mathbf{n}}$ such that $|\mathbf{n}| = n$. Let $z \in P(R)$; we can assume that z is homogeneous. By the same argument as in the proof of Lemma 3.3, $n = 1$. That is, $R_1 = P(R)$. The last assertion follows from [CM, 2.2]. ∎

Quantum linear spaces are characterized by the following Proposition.

PROPOSITION 3.5. *Let R be a braided Hopf algebra in ${}^K_K\mathcal{YD}$ satisfying hypothesis* (A). *Assume that*

$$\dim R = N_1 \dots N_\theta .$$

Then:

(i) $\chi_j(g_j)\chi_i(g_i) = 1$, *for all $i \neq j$; and*

(ii) *R is a quantum linear space.*

Proof. Relations (3.6) hold by Lemma 3.1. By Lemma 3.3, $\{x^{\mathbf{n}}: \mathbf{n} \leq \mathbf{N} - \mathbf{1}\}$ is a basis of R, which is then generated as an algebra by $x_1, \dots, x_\theta$. If $i > j$, $x_i x_j$ can be expressed by

$$x_i x_j = \sum_n c_{\mathbf{n}} x^{\mathbf{n}},$$

for some $c_{\mathbf{n}} \in k$. Applying Δ, we see that $c_{\mathbf{n}} = 0$ unless $x^{\mathbf{n}} = x_j x_i$; so $x_i x_j = c x_j x_i$, for some $c \in k$. By (3.1), we have

$$\begin{aligned} x_i x_j \otimes 1 + x_i \otimes x_j + \chi_j(g_i) x_j \otimes x_i + 1 \otimes x_i x_j \\ = c x_j x_i \otimes 1 + c x_j \otimes x_i + c \chi_i(g_j) x_i \otimes x_j + 1 \otimes c x_j x_i . \end{aligned}$$

By Lemma 3.3 again, $c = \chi_j(g_i)$ and $c\chi_i(g_j) = 1$. Hence (i) and relations (3.7) hold. Applying the action and coaction to both sides of the equality (3.7), the conditions (3.3) follow.

We can define now a surjective algebra homomorphism

$$\mathscr{R}(g_1, \dots, g_\theta; \chi_1, \dots, \chi_\theta) \to R,$$

which is also a morphism of Yetter–Drinfeld modules. It is easy to conclude that it is a homomorphism of braided Hopf algebras. By a dimension argument, this map is an isomorphism. ∎

4. QUANTUM LINEAR SPACES OVER ABELIAN GROUPS

Let Γ be a finite nontrivial abelian group and let $H = k(\Gamma)$. We discuss in this section the existence of quantum linear spaces over H.

Let $\theta \in \mathbb{N}$. A *datum for a quantum linear space* consists of elements $g_1, \dots, g_\theta \in \Gamma$, $\chi_1, \dots, \chi_\theta \in \hat{\Gamma}$ such that conditions (3.2), ..., (3.5) hold. Explicitly, and because Γ is abelian, we are then requiring the following conditions:

$$q_j := \chi_j(g_j) \neq 1. \tag{4.1}$$

$$\chi_j(g_i)\chi_i(g_j) = 1, \quad \text{for all } i \neq j. \tag{4.2}$$

We shall say that the datum, or its associated quantum linear space, has *rank* θ. Given θ, we are interested in describing all the data of rank θ. This description could be very cumbersome. Let $\theta(\Gamma)$ be the greatest integer θ such that a datum of rank θ exists.

LEMMA 4.1. *Let $\Gamma = K \times H$, where K and H are finite abelian groups. Then $\theta(\Gamma) \geq \theta(K) + \theta(H)$. If the orders of K and H are coprime, then $\theta(\Gamma) = \theta(K) + \theta(H)$.*

Proof. We identify H, K with subgroups of Γ, and $\hat{H}$, $\hat{K}$ with subgroups of $\hat{\Gamma}$. Let $h_1, \dots, h_\mu, \eta_1, \dots, \eta_\mu$ be a datum for H and let $k_1, \dots, k_\nu, \zeta_1, \dots, \zeta_\nu$ be a datum for H. Then

$$h_1, \dots, h_\mu, k_1, \dots, k_\nu \text{ in } \Gamma, \qquad \eta_1, \dots, \eta_\mu, \zeta_1, \dots, \zeta_\nu \text{ in } \hat{\Gamma},$$

is clearly a datum for Γ. Hence $\theta(\Gamma) \geq \theta(K) + \theta(H)$.

Conversely, assume that the orders of H and K are coprime and let $g_1, \dots, g_\theta \in \Gamma$, $\chi_1, \dots, \chi_\theta \in \hat{\Gamma}$ be a datum for Γ. Let us decompose

$$g_i = h_i k_i, \text{ where } h_i \in H, k_i \in K,$$

and

$$\chi_i = \eta_i \zeta_i, \text{ where } \eta_i \in \hat{H}, \xi_i \in \hat{K}, \quad 1 \leq i \leq \theta.$$

We claim that $h_i, \eta_i, i \in I$, where $I := \{i\colon \eta_i(h_i) \neq 1\}$ is a datum for H, and, similarly, that $k_i, \zeta_i, i \in J$, where $J := \{i\colon \zeta_i(k_i) \neq 1\}$ is a datum for K. Clearly,

$$\chi_i(g_i) \neq 1 \text{ implies } \eta_i(h_i) \neq 1 \text{ or } \zeta_i(k_i) \neq 1;$$

that is, the claim implies $\theta(\Gamma) \leq \theta(K) + \theta(H)$. We check then the claim. Condition (4.1) is forced by the choice of the index sets. For (4.2), observe that

$$1 = \chi_j(g_i)\chi_i(g_j) = \eta_j(h_i)\eta_i(h_j)\zeta_j(k_i)\zeta_i(k_j)$$

implies $1 = \eta_j(h_i)\eta_i(h_j) = \zeta_j(k_i)\zeta_i(k_j)$, because the orders of $\eta_j(h_i)\eta_i(h_j)$ and $\zeta_j(k_i)\zeta_i(k_j)$ are coprime. ∎

By the preceding Lemma, we are reduced to investigate the behavior of $\theta(\Gamma)$ when Γ is an abelian p-group, p a prime.

LEMMA 4.2. *Let Γ be a cyclic p group, where p is an odd prime. Then* $\theta(\Gamma) = 2$.

Proof. We first prove that $\theta(\Gamma) \leq 2$. It is enough to show that no datum of rank 3 exists. Let us assume, on the contrary, that $g_1, g_2, g_3 \in \Gamma$, $\chi_1, \chi_2, \chi_3 \in \hat{\Gamma}$, satisfy (4.1), (4.2). Let g be a generator of the subgroup $\langle g_1, g_2, g_3 \rangle$ and let p^s be the order of g, where s is a positive integer. Let ζ be a primitive p^sth root of 1. Let $a_1, a_2, a_3, b_1, b_2, b_3$ be integers such that

$$g_i = g^{b_i}, \quad \chi_i(g) = \zeta^{a_i}, \quad 1 \leq i \leq 3.$$

Then condition (4.1) means that $a_i b_i \not\equiv 0 \bmod p^s$ and (4.2) that

$$a_1 b_2 + a_2 b_1 \equiv 0 \bmod p^s \tag{4.3}$$

$$a_1 b_3 + a_3 b_1 \equiv 0 \bmod p^s \tag{4.4}$$

$$a_2 b_3 + a_3 b_2 \equiv 0 \bmod p^s. \tag{4.5}$$

On the other hand, there exist integers r_1, r_2, r_3 such that

$$b_1 r_1 + b_2 r_2 + b_3 r_3 \equiv 1 \mod p^s. \tag{4.6}$$

Now, we multiply (4.3) by b_3, (4.4) by b_2, (4.5) by b_1, and conclude (since p is odd) that

$$a_1 b_2 b_3 \equiv 0 \mod p^s, \quad a_2 b_1 b_3 \equiv 0 \mod p^s, \quad a_3 b_1 b_2 \equiv 0 \mod p^s.$$

Let us write

$$a_1 = p^t \widetilde{a_1}, \qquad \text{where } t \geq 0, p \nmid \widetilde{a_1}.$$

Then $p^{s-t} \mid b_2 b_3$ and hence there exist positive integers h, j such that $p^h | b_2, p^j | b_3$ and $h + j = s - t$. From (4.3), (4.4) we deduce that $p^{t+h} | a_2 b_1$ and $p^{t+j} | a_3 b_1$. Now assume that $p \nmid b_1$. Then

$$p^{t+h} | a_2 \Rightarrow p^{t+2h} | a_2 b_2 \Rightarrow t + 2h < s,$$

and similarly, $t + 2j < s$. But then $h < (s-t)/2, j < (s-t)/2$ and therefore $h + j < s$, which is not possible. Hence $p \mid b_1$. By symmetry, $p | b_2, p | b_3$. This contradicts (4.6) and finishes the proof of $\theta(\Gamma) \leq 2$.

Let g denote now a generator of Γ and let again p^s be the order of g and ζ a primitive p^sth root of 1. Then $g_1 = g, g_2 = g^a, \chi_1$ given by $\chi_1(g) = \zeta$ and χ_2 given by $\chi_2(g) = \zeta^{-a}$ is a datum of rank 2 whenever $a^2 \not\equiv 0 \bmod p^s$. ∎

5. POINTED HOPF ALGEBRAS WHOSE DIAGRAMS ARE QUANTUM LINEAR SPACES

Let Γ be a finite abelian group. We fix a decomposition $\Gamma = \langle y_1 \rangle \oplus \cdots \oplus \langle y_\sigma \rangle$ and we denote by M_l the order of $y_l, 1 \leq l \leq \sigma$.

Let $g_1, \ldots, g_\theta \in \Gamma, \chi_1, \ldots, \chi_\theta \in \hat{\Gamma}$ be a datum for quantum linear space; i.e., (4.1), (4.2) hold. We set $q_i = \chi_i(g_i)$, N_i the order of q_i. We abbreviate $\mathscr{R} := \mathscr{R}(g_1, \ldots, g_\theta; \chi_1, \ldots, \chi_\theta)$ for the quantum linear space defined in Section 3.

A compatible datum $\mathscr{D}$ for Γ and $\mathscr{R}$ consists of

(5.1) a scalar $\mu_i \in \{0, 1\}$ for each $i, 1 \leq i \leq \theta$; it is arbitrary if $g_i^{N_i} \neq 1$ and $\chi_i^{N_i} = 1$, but 0 otherwise;

(5.2) a scalar $\lambda_{ij} \in k$ for each $i, j, 1 \leq i < j \leq \theta$; it is is arbitrary if $g_i g_j \neq 1$ and $\chi_i \chi_j = 1$, but 0 otherwise.

Remark. If $\lambda_{ij} \neq 0$ and $\lambda_{ih} \neq 0$, then $\chi_i \chi_j = 1$ and $\chi_i \chi_h = 1$; hence $\chi_j = \chi_h$. If in addition the order N_i of $q_i := \chi_i(g_i)$ is odd, then $j = h$. Indeed, suppose $j \neq h$. Then

$$1 = \chi_j(g_h)\chi_h(g_j) = \chi_i(g_h)^{-1}\chi_i(g_j)^{-1} = \chi_i(g_i)^{-2}.$$

Here, the first equality is by (4.2); the second, because $\chi_j = \chi_h = \chi_i^{-1}$; the third, because $\chi_i(g_i)^{-1} = \chi_j(g_i) = \chi_i(g_j)^{-1}$ and similar with h instead of j. Now N_i odd forces $1 = \chi_i(g_i)$, which is excluded by (3.2).

Let η be the injective map from Γ to the free algebra $k\langle h_1, \ldots, h_\sigma, a_1, \ldots, a_\theta \rangle$ given by

$$\eta(y_1^{n_1}, \ldots, y_\sigma^{n_\sigma}) = h_1^{n_1} \ldots h_\sigma^{n_\sigma}, \quad 0 \leq n_l \leq M_l - 1, \quad 1 \leq l \leq \sigma.$$

We shall identify elements of Γ with elements of the free algebra $k\langle h_1, \ldots, h_\sigma, a_1, \ldots, a_\theta \rangle$ via η without further notice.

DEFINITION. Let Γ be a finite abelian group, $\mathscr{R}$ a quantum linear space, and $\mathscr{D}$ a compatible datum. Keep the notation above. Let $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$ be the algebra presented by generators $h_l, 1 \le l \le \sigma$, and $a_i, 1 \le i \le \theta$ with defining relations

$$h_l^{M_l} = 1, 1 \le l \le \sigma; \tag{5.3}$$

$$h_l h_t = h_t h_l, 1 \le t < l \le \sigma; \tag{5.4}$$

$$a_i h_l = \chi_i^{-1}(y_l) h_l a_i, 1 \le l \le \sigma, 1 \le i \le \theta; \tag{5.5}$$

$$a_i^{N_i} = \mu_i\big(1 - g_i^{N_i}\big), 1 \le i \le \theta; \tag{5.6}$$

$$a_j a_i = \chi_i(g_j) a_i a_j + \lambda_{ij}\big(1 - g_i g_j\big), 1 \le i < j \le \theta. \tag{5.7}$$

We shall denote in what follows by the same letters the generators of the free algebra $k\langle h_1, \dots, h_\sigma, a_1, \dots, a_\theta\rangle$ and their classes in $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$; no trouble should arise.

LEMMA 5.1. *There exists a unique Hopf algebra structure on* $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$ *such that*

$$\Delta(h_l) = h_l \otimes h_l, \qquad \Delta(a_i) = a_i \otimes 1 + g_i \otimes a_i, \quad 1 \le l \le \sigma, \quad 1 \le i \le \theta. \tag{5.8}$$

Proof. Let also $\Delta\colon k\langle h_1, \dots, h_\sigma, a_1, \dots, a_\theta\rangle \to \mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D}) \otimes \mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$ denote the algebra map defined by (5.8). Clearly, $\Delta(h) = h \otimes h$ whenever h is a monomial in the h_l's. We have to verify that the elements $H_l = h_l \otimes h_l$, $A_i = a_i \otimes 1 + g_i \otimes a_i$ satisfy the defining relations. This is not difficult for (5.3), (5.4), (5.5). For relations (5.6), (5.7), the reason is the same: both sides of each equality are skew-primitive elements related to the same group-likes. For instance, we have

$$\begin{aligned}\Delta(a_i)^{N_i} &= a_i^{N_i} \otimes 1 + g_i^{N_i} \otimes a_i^{N_i} = \mu_i\big(1 - g_i^{N_i}\big) \otimes 1 + g_i^{N_i} \otimes \mu_i\big(1 - g_i^{N_i}\big)\\ &= \Delta \mu_i\big(1 - g_i^{N_i}\big).\end{aligned}$$

Here the first equality follows from (5.4) and the definition of Δ via the quantum binomial formula, since the order of q_i is N_i; the second, from (5.6); the third is clear. This proves that H_l, A_i satisfy (5.6). For (5.7), the computation is also direct. It is clear that Δ is coassociative.

The algebra map $\varepsilon\colon \mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D}) \to k$ uniquely determined by $\varepsilon(h_l) = 1$, $\varepsilon(a_i) = 0$, for all l and i, is the counit of $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$. We claim that there is a unique algebra map $\mathscr{S}\colon \mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D}) \to \mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})^{op}$ such that for all l and i,

$$\mathscr{S}(h_l) = h_l^{-1}, \qquad \mathscr{S}(a_i) = -g_i^{-1} a_i.$$

The verification of relations (5.3), (5.4), (5.5), (5.7) is straightforward. For (5.6), we first check by induction that

$$\mathscr{S}(a_i)^n = (-1)^n q_i^{n(n-1)/2} g_i^{-n} a_i^n.$$

As q_i is a primitive N_ith root of $1, (-1)^{N_i} q_i^{N_i(N_i-1)/2} = -1$. Hence

$$\mathscr{S}(a_i)^{N_i} = -g_i^{-N_i} a_i^{N_i} = \mu_i\left(1 - g_i^{-N_i}\right) = \mu_i\left(1 - \mathscr{S}(g_i)^{N_i}\right).$$

The map $\mathscr{S}$ is clearly an antipode and the Lemma follows. ∎

PROPOSITION 5.2. *Let Γ be a finite abelian group, $\mathscr{R}$ a quantum linear space, and $\mathscr{D}$ a compatible datum. Keep the notation above. The set of monomials*

$$h_1^{r_1} \dots h_\sigma^{r_\sigma} a_1^{s_1} \dots a_\theta^{r_\theta}, \qquad 0 \le r_l < M_l, \quad 0 \le s_i < N_i, \quad 1 \le l \le \sigma, \quad 1 \le i \le \theta$$

is a basis of $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$. In particular,

$$\dim \mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D}) = \prod_{1 \le l \le \sigma} M_l \prod_{1 \le i \le \theta} N_i = |\Gamma| \dim \mathscr{R}. \tag{5.9}$$

Proof. Let us assume that the scalars μ_i, λ_{ij} are arbitrary. It is not difficult to conclude from relations (5.4), (5.5), and (5.7) that these monomials generate the vector space $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$. By the Diamond Lemma [Be], it is then enough to verify that the following overlaps can be reduced to the same normal form:

$$(a_i h_l) h_l^{M_l - 1} = a_i\left(h_l h_l^{M_l - 1}\right); \tag{5.10}$$

$$(a_i h_l) h_t = a_i(h_l h_t), t < l; \tag{5.11}$$

$$\left(a^{N_i - 1} a_i\right) h_l = a_i^{N_i - 1}(a_i h_l); \tag{5.12}$$

$$\left(a_j^{N_j - 1} a_j\right) a_i = a_j^{N_j - 1}(a_j a_i), i < j; \tag{5.13}$$

$$(a_j a_i) a_i^{N_i - 1} = a_j\left(a_i a_i^{N_i - 1}\right), i < j; \tag{5.14}$$

$$(a_j a_i) h_l = a_j(a_i h_l), i < j. \tag{5.15}$$

Here we order the monomials in the following way. If $z_1 < z_2 < \cdots < z_m$ are indeterminates, we define the standard ordering on monomials A, B in $z_1, \dots, z_m$ in the usual way; $A < B$ if length$(A) <$ length(B), or A and B have the same length and A is lexicographically smaller than B. If A is a monomial in $h_1, \dots, a_\theta$, let $\phi(A)$ be its a-part, that is the image under the monoid homomorphism ϕ with $\phi(h_l) = 1, \phi(a_i) = a_i$ for all l, i. We order the monomials in $h_1, \dots, a_\theta$ as follows: $h_1 < \cdots < h_\sigma < a_1 < \cdots <$

a_θ; $A < B$ if $\phi(A) < \phi(B)$ in the standard ordering of the monomials in $a_1, \dots, a_\theta$, or $\phi(A) = \phi(B)$ and A is smaller than B in the standard ordering of $h_1, \dots, a_\theta$.

The verification of (5.10), (5.11) is easy and gives no condition. The verification of (5.12) amounts to

$$\mu_i\left(1 - g_i^{N_i}\right)h_l = \mu_i\,\chi_i^{-1}(y_l)^{N_i}h_l\left(1 - g_i^{N_i}\right).$$

This imposes the condition

$$\text{if } g_i^{N_i} \neq 1 \text{ and } \chi_i^{N_i} \neq 1 \text{ then } \mu_i = 0. \tag{5.16}$$

The verification of (5.13) turns to

$$\begin{aligned}\mu_j\left(1 - g_j^{N_j}\right)a_i = \mu_j\,\chi_i(g_j)^{N_j}a_i - \mu_j g_j^{N_j}a_i \\ + \lambda_{ij}\left(1 + \chi_i(g_j) + \chi_i(g_j)^2 + \cdots + \chi_i(g_j)^{N_j-1}\right)a_j^{N_j-1};\end{aligned}$$

and so we need the conditions

$$\lambda_{ij}\left(1 + \chi_i(g_j) + \chi_i(g_j)^2 + \cdots + \chi_i(g_j)^{N_j-1}\right) = 0. \tag{5.17}$$

$$\text{If } g_j^{N_j} \neq 1 \text{ and } \chi_i(g_j)^{N_j} \neq 1 \text{ then } \mu_j = 0. \tag{5.18}$$

In the same vein, for (5.14) and (5.15) it is necessary that

$$\lambda_{ij}\left(1 + \chi_i(g_j) + \chi_i(g_j)^2 + \cdots + \chi_i(g_j)^{N_i-1}\right) = 0. \tag{5.19}$$

$$\text{If } g_i^{N_i} \neq 1 \text{ and } \chi_i(g_j)^{N_i} \neq 1 \text{ then } \mu_i = 0. \tag{5.20}$$

$$\text{If } g_i g_j \neq 1 \text{ and } \chi_i\,\chi_j \neq 1 \text{ then } \lambda_{ij} = 0. \tag{5.21}$$

Now it is harmless to assume that

$$\mu_i = 0 \text{ if } g_i^{N_i} = 1,\ \lambda_{ij} = 0 \text{ if } g_i g_j = 1.$$

The combination of this last assumption and (5.16) is exactly the constraint in (5.1); in turn, the constraint in (5.2) is equivalent to the assumption together with (5.21). Also, condition (5.16) implies (5.18) and (5.20). It remains to show that (5.17) and (5.19) are consequences of (5.21).

Indeed, assume that $\lambda_{ij} \neq 0$; by (5.21), this is only possible if $g_i g_j \neq 1$ and $\chi_i\,\chi_j = 1$. But then $\chi_i(g_i) = \chi_j(g_j)^{-1}$, thanks to (4.2). Thus $N_i = N_j$. Moreover, $\chi_i(g_j)^{N_j}\chi_j(g_j)^{N_j} = 1$ and hence $\chi_i(g_j)^{N_j} = 1$. Therefore (5.17) and (5.19) hold. ∎

COROLLARY 5.3. *The Hopf algebra $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$ is pointed and its coradical filtration is given by*

$$\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})_n = \left\langle h_1^{r_1} \dots h_\sigma^{r_\sigma} a_1^{s_1} \dots a_\theta^{s_\theta}, \;\; 0 \le r_l < M_l, \;\; 0 \le s_i < N_i, \;\; \forall l, i, \sum_i s_i \le n \right\rangle. \tag{5.22}$$

In particular,

$$\begin{aligned} P_{g_i,1}(\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})) &= k(1 - g_i) \oplus \left(\bigoplus_{j:\, g_j = g_i} k a_j \right), \quad 1 \le i \le \theta, \\ P_{g,1}(\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})) &= k(1 - g) \quad \text{if } g \ne g_i. \end{aligned} \tag{5.23}$$

Proof. The subalgebra $k[h_1, \dots, h_\sigma]$ of $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$ coincides with its coradical. Indeed, $k[h_1, \dots, h_\sigma] \supset \mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})_0$ by [M, 5.5.1] and the other inclusion is evident. Hence, $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$ is pointed and $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})_0$ is isomorphic to the group algebra of Γ.

Now we consider the graded Hopf algebra $\operatorname{gr} \mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$ associated to the coradical filtration, and the diagram of $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$. It follows from Proposition 5.2 that the diagram is isomorphic to $\mathscr{R}$. By Lemma 3.4, we know the coradical filtration of $\mathscr{R}$. By Lemmas 2.3 and 2.4, we know then the coradical filtration of $\operatorname{gr} \mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$. We conclude, by a recursive argument that the coradical filtration of $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$ is given by (5.22). In particular,

$$\begin{aligned} \mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})_1 = \mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})_0 \oplus \mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})_0 a_1 \oplus \mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})_0 a_2 \cdots \\ \oplus \mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})_0 a_\theta. \end{aligned}$$

The claim (5.23) follows by a direct computation. ∎

Let now A be a finite-dimensional pointed Hopf algebra such that the group $G(A)$ of its group-like elements is isomorphic to Γ. We denote $H = k(\Gamma)$. By the Theorem of Taft and Wilson [M, Thm. 5.4.1], $A_1 = k(\Gamma) + (\bigoplus_{g, h \in \Gamma} P_{g,h})$.

If M is an H-module (respectively, comodule) then M^χ (resp., M_g) denotes the isotypic component of type $\chi \in \hat{\Gamma}$ (resp., of type $g \in \Gamma$). If M is an object in ${}_H^H\mathscr{YD}$ then $M_g^\chi := M_g \cap M_\chi$. Any finite-dimensional $M \in {}_H^H\mathscr{YD}$ decomposes as

$$M = \bigoplus_{g \in \Gamma,\, \chi \in \hat{\Gamma}} M_g^\chi.$$

The adjoint action of Γ on A leaves stable each space $P_{g,h}$; hence, we can further decompose $P_{g,h} = \bigoplus_{\chi \in \hat{\Gamma}} P_{g,h}^\chi$.

LEMMA 5.4. *Let* gr A *be the graded Hopf algebra associated to the coradical filtration and let* R *be the diagram of* A.

(i) *The first term of the coradical filtration of* A *is given by*

$$A_1 = k(\Gamma) \oplus \left(\bigoplus_{\substack{g,h\in\Gamma \\ \chi\in\hat{\Gamma},\, \chi\neq\epsilon}} P^{\chi}_{g,h} \right).$$

Thus the second summand is isomorphic to gr $A(1)$.

(ii) *If* $P(R) = \oplus_{1\le i\le M} P(R)_{g_i}$ *with* $P(R)_{g_i} \neq 0$, *then* $P_{g,h}(A)$ *contains properly* $P_{g,h}(A) \cap k(\Gamma) = k(g-h)$ *if and only if* $(g,h) = (g_i s, s)$, *for some* $s \in \Gamma$.

Proof. If ϵ is the trivial character of Γ, then $P^{\epsilon}_{g,h} \subset k(\Gamma)$ by Lemma 3.1. Since Γ is abelian, $P^{\epsilon}_{g,h} = P_{g,h} \cap k(\Gamma)$. This shows part (i). Part (ii) follows at once from part (i) and formulas (2.1). ∎

LIFTING THEOREM 5.5. *Let* A *be a pointed finite-dimensional Hopf algebra with coradical* $H = k(\Gamma)$, *where* Γ *is an abelian group as above. Let* gr A *be the graded Hopf algebra associated to the coradical filtration. Let* $\mathscr{R}$ *be the diagram of* A. *We assume that* $\mathscr{R}$ *is a quantum linear space.*

Then there exists a compatible datum $\mathscr{D}$ *such that* A *is isomorphic to* $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$ *as Hopf algebras.*

Proof. Let $x_1, \dots, x_\theta$ be the generators of $\mathscr{R}$ satisfying the relations (3.6), (3.7). We identify x_j, resp. $h \in \Gamma$, with $x_j\#1$, resp. $1\#h$, in $\mathscr{R}\#k(\Gamma) \simeq \mathrm{gr} A$. By (2.1), we see that gr A can be presented by generators $h_l, 1 \le l \le \sigma, x_i, 1 \le i \le \theta$ and relations (5.3), (5.4),

$$x_i^{N_i} = 0, \tag{5.24}$$

$$h_l x_i = \chi_i(h_l) x_i h_l, \tag{5.25}$$

$$x_i x_j - \chi_j(g_i) x_j x_i = 0, \tag{5.26}$$

for all $1 \le l \le \sigma, 1 \le i \neq j \le \theta$. The Hopf algebra structure of gr A is determined by

$$\Delta(h) = h \otimes h, \qquad \Delta(x_i) = x_i \otimes 1 + g_i \otimes x_i,$$

$1 \le i \le \theta, h \in \Gamma$. Hence $x_i \in P_{g_i,1}(\mathrm{gr}\, A)^{\chi_i}$. According to Lemma 5.4, we can choose $a_i \in P_{g_i,1}(A)^{\chi_i}$ such that $\overline{a_i} = x_i$ in gr $A(1) = A_1/A_0$. By Lemma 2.2, A is generated by $h_l, 1 \le l \le \sigma$, $a_i, 1 \le i \le \theta$. It is clear that relations (5.3) and (5.4) also hold in A. We verify now that relations (5.5), (5.6), (5.7) hold for some collection of scalars μ_i, λ_{ij}, and at the same time, that this choice must fulfill the constraints in (5.1) and (5.2). For (5.5), this follows from the choice of the a_i's. We check (5.6). By the quantum binomial formula,

$$a_i^{N_i} \in P_{g_i^{N_i},1}(A)^{\chi_i^{N_i}}.$$

We know that

$$g_i a_i^{N_i} g_i^{-1} = \chi_i^{N_i}(g_i) a_i^{N_i} = q_i^{N_i} a_i^{N_i} = a_i^{N_i};$$

by Lemma 3.1, $a_i^{N_i} \in k(g_i^{N_i} - 1)$. Dividing out a_i by an appropriate scalar, we see that relations (5.6) hold, for μ_i either 0 or 1. If $g_i^{N_i} = 1$ we can assume without trouble that $\mu_i = 0$. So let us suppose that $g_i^{N_i} \neq 1$. If $\mu_i = 1$ then

$$h_l a_i^{N_i} h_l^{-1} = a_i^{N_i} = \chi_i^{N_i}(h_l) a_i^{N_i};$$

hence $\chi_i^{N_i}$ is forced to be 1.

We prove now (5.7). By (4.2) and the choice of the a_i's, it follows that

$$a_i a_j - \chi_j(g_i) a_j a_i \in P_{1, g_i g_j}(A)^{\chi_i \chi_j}.$$

By Lemma 5.4, if $a_i a_j - \chi_j(g_i) a_j a_i \notin k(\Gamma)$, then for some $h \neq i, j$, $\chi_i \chi_j = \chi_h$ and $g_i g_j = g_h$. By (4.2) again,

$$1 = \chi_h(g_i)\chi_i(g_h) = \chi_i(g_i)\chi_j(g_i)\chi_i(g_i)\chi_i(g_j) = \chi_i(g_i)^2$$

and hence $\chi_i(g_i) = -1$. Similarly, $\chi_j(g_j) = -1$. So

$$\chi_h(g_h) = \chi_i(g_i)\chi_j(g_i)\chi_i(g_j)\chi_j(g_j) = 1,$$

a contradiction. Therefore, $a_i a_j - \chi_j(g_i) a_j a_i \in k(\Gamma)$ and by Lemma 3.1, there exist scalars λ_{ij} such that $a_i a_j - \chi_j(g_i) a_j a_i = \lambda_{ij}(1 - g_i g_j)$; i.e., (5.7) holds. If $g_i g_j = 1$ we assume without harm that $\lambda_{ij} = 0$. If $g_i g_j \neq 1$ and $\lambda_{ij} \neq 0$ then, arguing as for the μ_i's, we see that $\chi_i \chi_j = 1$. Hence the collection λ_{ij} satisfies the constraints of (5.2).

Then the datum $\mathscr{D} = (\mu_i, \lambda_{ij})$ is compatible and we have a Hopf algebra surjection $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D}) \to A$. As $\mathscr{A}(\Gamma, \mathscr{R}, \mathscr{D})$ and A have the same dimension, they are isomorphic. ∎

We deduce now Theorem 0.2 from Theorem 5.5. We need the following Lemma.

LEMMA 5.6. *Let Γ be a finite nontrivial abelian group and let $H = k(\Gamma)$. Let R be a braided Hopf algebra in ${}^H_H\mathcal{YD}$, with trivial coradical*: $R_0 = R(0) = k1$.

(a) *If* $\dim R = p$ *then* $\dim P(R) = 1$ *and R is a quantum line*.

(b) *If* $\dim R = p^2$ *then* $\dim P(R) = 1$ *or* 2, *and R is respectively a quantum line or a quantum plane*.

Proof. Let R be a finite-dimensional braided Hopf algebra in ${}^H_H\mathcal{YD}$, with trivial coradical. Since $R_0 = k1$ and $R \supsetneq R_0$, $P(R) \neq 0$. On the other hand, $P(R)$ is a Yetter–Drinfeld submodule of R, hence $P(R) = \bigoplus_{g \in \Gamma, \chi \in \hat{\Gamma}} P(R)^{\chi}_{g}$.

Let $x \in P(R)^{\chi}_{g}$, $x \neq 0$, for some $g \in \Gamma$, $\chi \in \hat{\Gamma}$. Let $q = \chi(g)$ and let N be the order of q; $q \neq 1$ by Lemma 3.1; that is, $N > 1$. It is not difficult to see that the subalgebra $k[x]$ of R is a braided Hopf subalgebra of dimension N. It follows from the Nichols–Zoeller Theorem that N divides the dimension of R, see [AS2, Proposition 4.9].

Let $x_1, \dots, x_\theta$ be a basis of $P(R)$ such that $x_j \in P(R)^{\chi_j}_{g_j}$, for some $g_j \in \Gamma$, $\chi_j \in \hat{\Gamma}$, for all j. Let N_j be the order of $\chi_j(g_j)$.

If the dimension of R is p, the considerations above show that $R = k[x_1]$. This proves part (a).

We now assume that the dimension of R is p^2. If $N_1 = p^2$, then $\theta = 1$ and R is a quantum line. So we can further suppose that $N_j = p$ for all j. By Lemma 3.3, $\theta \leq 2$. If $\theta = 1$, then Theorem 3.2 forces $\dim R = p$. This a contradiction and therefore $\theta = 2$. We conclude then, by Proposition 3.5, that r is a quantum plane. ∎

Proof of Theorem 0.2. Let $\operatorname{gr} A$ be the graded Hopf algebra associated to the coradical filtration and let R by the braided Hopf algebra in ${}^H_H\mathcal{YD}$ such that $\operatorname{gr} A \simeq R\#H$ as in 2.2. If the index of H in A is p or p^2, then R is a quantum line or plane, according to Lemma 5.6. The description follows now from Theorem 5.5. ∎

6. FAMILIES OF HOPF ALGEBRAS OF THE SAME DIMENSION

We shall specialize Proposition 5.2 to the simplest possible Γ and $\mathcal{R}$ and suitable $\mathcal{D}$.

Let us assume that Γ is a cyclic group of order MN, where $M > 1$ and $N > 2$. Let us fix a generator y of Γ. Let q be a primitive Nth root of 1. We consider the following datum of quantum linear plane:

$$g_1 = g_2 = y \in \Gamma, \quad \chi_1, \chi_2 \in \hat{\Gamma}, \quad \chi_1(y) = q, \quad \chi_2(y) = q^{-1}.$$

We consider the compatible datum

$$\mathscr{D} = \big(\, \mu_1 = 1, \quad \mu_2 = 1, \quad \lambda_{ij} = \lambda \big),$$

where $\lambda \in k$ is arbitrary.

As above, given a positive integer $n, \mathbb{G}_n$ denotes the group of nth roots of 1 in k.

THEOREM 6.1. *Let $\mathscr{B}(M, N, q, \lambda)$ be the algebra presented by generators h, a_1, a_2 with defining relations*

$$h^{NM} = 1; \tag{6.1}$$

$$ha_1 = qa_1 h, ha_2, = q^{-1} a_2 h; \tag{6.2}$$

$$a_1^N = 1 - h^N, a_2^N = 1 - h^N; \tag{6.3}$$

$$a_2 a_1 - qa_1 a_2 = \lambda(1 - h^2). \tag{6.4}$$

Then $\mathscr{B}(M, N, q, \lambda)$ has dimension MN^3 and carries a Hopf algebra structure given by

$$\Delta(h) = h \otimes h, \qquad \Delta(a_i) = a_i \otimes 1 + h \otimes a_i, \quad 1 \le i \le 2.$$

It is pointed and its coradical filtration is given by

$$\mathscr{B}(M, N, q, \lambda)_n = \langle h^i a_1^{j_1} a_2^{j_2} \colon 0 \le i \le NM, 0 \le j_1, 0 \le j_2, j_1 + j_2 \le n \rangle. \tag{6.5}$$

In particular,

$$\begin{aligned} P_{h,1}(\mathscr{B}(M, N, q, \lambda)) &= k(1 - h) \oplus ka_1 \oplus ka_2 \\ P_{g,1}(\mathscr{B}(M, N, q, \lambda)) &= k(1 - g) \quad \textit{if}\, g \in \Gamma, g \ne h. \end{aligned} \tag{6.6}$$

The Hopf algebras $\mathscr{B}(M, N, q, \lambda)$ and $\mathscr{B}(M, N, q, \tilde{\lambda})$ are isomorphic if and only if $\tilde{\lambda} = u\lambda$ for some $u \in \mathbb{G}_N$.

Proof. The Hopf algebra structure and the dimension statements follow from Lemma 5.1 and Proposition 5.2. The description of the coradical follows from Corollary 5.3.

We prove now the isomorphism statement. We denote by $\tilde{h}, \widetilde{a_i}$, the generators of $\mathscr{B}(M, N, q, \tilde{\lambda})$. We assume first that $\mathscr{B}(M, N, q, \lambda)$ and $\mathscr{B}(M, N, q, \tilde{\lambda})$ are isomorphic; let $\phi\colon \mathscr{B}(M, N, q, \lambda) \to \mathscr{B}(M, N, q, \tilde{\lambda})$ by a Hopf algebra isomorphism. Then ϕ induces a linear isomorphism

$$P_{h,1}(\mathscr{B}(M, N, q, \lambda)) \xrightarrow{\sim} P_{\phi(h),1}\big(\mathscr{B}\big(M, N, q, \tilde{\lambda}\big)\big).$$

By (6.6), dim $P_{h,1}(\mathscr{B}(M, N, q, \lambda)) = 3$; hence dim $P_{\phi(h),1}(\mathscr{B}(M, N, q, \tilde{\lambda})) = 3$ and by (6.6) again, we have $\phi(h) = \tilde{h}$.

Let us write $\phi(a_1) = \alpha_1(1 - \tilde{h}) + \alpha_2 \widetilde{a_1} + \alpha_3 \widetilde{a_1}$, for some $\alpha_i \in k$.

By (6.2), we have $\phi(h)\phi(a_1)\phi(h)^{-1} = q\phi(a_1)$. Hence $\alpha_1 = 0 = \alpha_3$ and $\phi(a_1) = \alpha_2 \widetilde{a_1}$, with $\alpha_2 \neq 0$. By a similar reason, $\phi(a_2) = \beta_3 \widetilde{a_2}$, with $\beta_3 \neq 0$. Now, by (6.3),

$$1 - \tilde{h}^N = \phi(1 - h^N) = \phi\left(a_1^N\right) = a_2^N \widetilde{a_1}^N = \alpha_2^N (1 - \tilde{h}^N).$$

Hence $\alpha_2^N = 1$, and similarly $\beta_3^N = 1$. Notice finally that (6.4) implies

$$\alpha_2 \beta_3 \tilde{\lambda} = \lambda.$$

Conversely suppose that $\tilde{\lambda} = u\lambda$ for some $u \in \mathbb{G}_N$. Then there is a Hopf algebra isomorphism ϕ: $\mathscr{B}(M, N, q, \lambda) \to \mathscr{B}(M, N, q, \tilde{\lambda})$ uniquely determined by

$$\phi(h) = \tilde{h}, \quad \phi(a_1) = \widetilde{a_1}, \quad \phi(a_2) = u\widetilde{a_2}.$$

∎

The following result is a consequence of the argument of the proof of the Theorem and answers a question of Masuoka.

COROLLARY 6.2. *The group of Hopf algebra automorphisms of* $\mathscr{B}(M, N, q, \lambda)$ *is finite.*

Proof. Indeed, any automorphism T has the following form, for some $j \in \mathbb{Z}/N$:

$$T(h) = h, \qquad T(a_1) = q^j a_1, \qquad T(a_2) = q^{-j} a_2.$$

∎

Remark. The Hopf algebra $\mathscr{B}(M, N, q, \lambda)$ arises as a central extension,

$$1 \to k[h^N] \to \mathscr{B}(M, N, q, \lambda) \xrightarrow{\pi} \mathscr{A}\left(\hat{\Gamma}, \hat{\mathscr{R}}, \hat{\mathscr{D}}\right) \to 1,$$

but π has no Hopf algebra section. As M and N could be coprime, this shows that Zassenhaus theorem does not generalize to Hopf algebras.

Proof of Theorem 0.3. It is an immediate consequence of Theorem 6.1, letting $M = N = p$. ∎

Remark. There are also easy examples with $\Gamma = \mathbb{Z}/NM_1 \oplus \mathbb{Z}/NM_2$ of families of pointed nonisomorphic Hopf algebras of dimension $N^4 M_1 M_2$, in particular of dimension p^6. The construction and proof are very similar.

7. POINTED HOPF ALGEBRAS OF ORDER p^3

Let A be a noncosemisimple pointed Hopf algebra of order p^3, and let Γ be the group of its group-like elements. By Nichols–Zoeller Theorem [NZ], we have the following possibilities:

$$\text{(i) } \Gamma = \mathbb{Z}/(p) \times \mathbb{Z}/(p), \qquad \text{(ii) } \Gamma = \mathbb{Z}/(p^2), \qquad \text{(iii) } \Gamma = \mathbb{Z}/(p).$$

We shall discuss the cases separately and deduce from Theorem 0.2 that in case (i) A should be of type (a), in case (ii) A should be of type (b), (c), or (d) and in case (iii) A should be of type (e) or (f).

Case (i). Here $k(\Gamma)$ has index p in A and Theorem 0.2 (ii) applies. Relation (0.3) turns to $a^p = 0$, because any element in Γ has order p. It is easy to see that $A \simeq k(\ker\chi) \otimes k\langle g, a\rangle$, and that the second factor is isomorphic to a Taft algebra.

Case (ii). Again, $k(\Gamma)$ has index p in A and Theorem 0.2 (ii) applies. Let g, χ, q, a be as in Theorem 0.2 (ii); the order of q is p.

We assume first that the order of g is also p. Then the relation (0.3) implies $a^p = 0$. On the other hand, let $h \in \Gamma$ be the generator such that $h^p = g$. Clearly, $\xi := \chi(h)$ has order p^2. We claim that there is an isomorphism of Hopf algebras

$$A \simeq k\langle h, x \mid hxh^{-1} = \xi x, h^{p^2} = 1, x^p = 0\rangle,$$

where the comultiplication in the right-hand side is as in type (b). Indeed the existence of a surjective homomorphism from the right-hand side to the left follows from the considerations above; by a dimension argument it is an isomorphism. So, we are in type (b).

We assume next that the order of g is p^2. Hence, $a^p = \lambda(1 - g^p)$ for some $\lambda \in k$. If $\lambda = 0$, A is of type (c); otherwise we replace a by $(\sqrt[p]{\lambda})^{-1}a$ and conclude that A is of type (d).

Case (iii). Now $k(\Gamma)$ has index p^2 in A and Theorem 0.2 (iii) applies. We observe that possibility (a) is excluded, since every element of Γ has order p. Let g_i, χ_i, q_i, a_i be as in Theorem 0.2 (iii). We set $g = g_1$ and $q = \chi_1(g) \in \mathbb{G}_p$. There are integers m, n such that $g_2 = g^m$ and $\chi_2(g) = q^n$. But $\chi_1(g_2)\chi_2(g_1) = 1$ forces $n = -m$.

Relations (0.7) turn to $a_i^p = 0$. If $\lambda = 0$ in (0.9), then A is isomorphic to a book algebra and is of type (f). If $\lambda \neq 0$, then $\chi_1 \chi_2 = 1$ implies $m = 1$. It is now clear that A is isomorphic to the Frobenius–Lusztig kernel; that is, it is of type (e).

REFERENCES

[A] N. Andruskiewitsch, Notes on extensions of Hopf algebras, *Canad. J. Math.* **48** (1996), 3–42.

[AS1] N. Andruskiewitsch and H.-J. Schneider, Simplicity of some pointed Hopf algebras, Appendix. *Canad. J. Math.* **48** (1996), 3–42.

[AS2] N. Andruskiewitsch and H.-J. Schneider, Hopf Algebras of order p^2 and braided Hopf algebras of order p, *J. Algebra* **199** (1998), 430–454.

[AS3] N. Andruskiewitsch and H.-J. Schneider, On Hopf Algebras whose coradical is a Hopf subalgebra, in preparation.

[Be] G. Bergman, The diamond lemma for ring theory, *Adv. Math.* **29** (1978), 178–218.

[BDG] M. Beattie, S. Dascalescu and L. Grünenfelder, On the number of types of finite-dimensional Hopf algebras, *Inventiones Math.* to appear.

[B] N. Bourbaki, "Algébre commutative. Charitre III," Hermann, 1961.

[CD] S. Caenepeel and S. Dascalescu, Pointed Hopf algebras of dimension p^3, *J. Algebra*, to appear.

[CM] W. Chin and I. Musson, The coradical filtration for quantized universal enveloping algebras, *J. London Math. Soc.* **53** (1996), no. 2, 50–67.

[G] S. Gelaki, On pointed Hopf algebras and Kaplansky's tenth conjecture, *J. Algebra*, to appear.

[K] I. Kaplansky, "Bialgebras," University of Chicago, Chicago, 1975.

[LR] R. G. Larson and D. E. Radford, Finite dimensional cosemisimple Hopf algebras in characteristic 0 are semisimple, *J. Algebra* **117** (1988), 267–289.

[L1] G. Lusztig, Finite dimensional Hopf algebras arising from quantized universal enveloping algebras, *J. Amer. Math. Soc.* **3** (1990), 257–296.

[L2] G. Lusztig, Quantum groups at roots of 1, *Geom. Dedicata* **35** (1990), 89–114.

[Mj] S. Majid, Crossed products by braided groups and bosonization, *J. Algebra* **163** (1994), 165–190.

[Ma1] A. Masuoka, Self dual Hopf algebras of dimension p^3 obtained by extension, *J. Algebra* **178** (1995), 791–806.

[Ma2] A. Masuoka, The p^n theorem for semisimple Hopf algebras, *Proc. Amer. Math. Soc.* **124**, No. 3 (1996), 735–737.

[M] S. Montgomery, "Hopf Algebras and Their Actions on Rings," Am. Math. Soc., Providence, 1993.

[N] W. D. Nichols, Bialgebras of type one, *Commun. Alg.* **6** (1978), 1521–1552.

[NZ] W. D. Nichols and M. B. Zoeller, A Hopf algebra freeness theorem, *Amer. J. Math.* **111** (1989), 381–385.

[OS] U. Oberst and H. -J. Schneider, Über Untergruppen endlicher algebraischer Gruppen, *Manuscripta Math.* **8** (1973), 217–241.

[R1] D. Radford, On the coradical of a finite dimensional Hopf algebra, *Proc. Amer. Math. Soc.* **53** (1975), 9–15.

[R2] D. Radford, The order of the antipode of a finite dimensional Hopf algebra is finite, *Amer. J. Math.* **98** (1976). 333–355.

[R3] D. Radford, Hopf algebras with projection, *J. Algebra* **92** (1985), 322–347.

[S] H.-J. Schneider, Finiteness results for semisimple Hopf algebras, manuscript.

[St] D. Stefan, The set of types of n-dimensional semisimple and cosemisimple Hopf algebras is finite, *J. Algebra* **193** (1997), 571-580.

[SvO] D. Stefan and F. van Oystaeyen, Hochschild cohomology and coradical filtration of pointed Hopf algebras, preprint (1997).

[Sw] Sweedler, M., "Hopf Algebras," Benjamin, New York, 1969.

[TW] E. Taft and R. L. Wilson, On antipodes in pointed Hopf algebras, *J. Algebra* **29** (1974), 27–32.

[T] M. Takeuchi, Some topics on $GL_q(n)$, *J. Algebra* **147** (1992), 379–410.

[Z] Y. Zhu, Hopf algebras of prime dimension, *Int. Math. Res. Notes* **1** (1994), 53–59.