Contemporary Mathematics

About finite dimensional Hopf algebras

Nicolás Andruskiewitsch

Dedicado a mis padres, Ana Bauchiero e Igor Andruskiewitsch.

Contents

1. Introduction

These Notes are the written suport to the Lectures I gave at the school "Quantum Symmetries in Theoretical Physics and Mathematics", held in Bariloche, January 2000. Both the Lectures and the Notes intend to survey the state of the art on the classification of finite dimensional Hopf algebras over a field. In despite of many interesting results of the last years, our knowledge of the structure of Hopf algebras is still in a primary stage. The impact of quantum groups in the area has not been realized yet in its full significance. I hope these Notes will convey the interest to a range of questions related to the classification of finite dimensional Hopf algebras.

This report is aimed to results on classification or structure of finite dimensional Hopf algebras. Applications to low dimensional topology and conformal field theory, and related topics like modular categories, operator algebras, various generalizations of the notion of Hopf algebra (face algebras, weak Hopf algebras, etc.), and many other aspects will not be touched.

1991 *Mathematics Subject Classification.* Primary 16W30, 17B37.

Key words and phrases. Hopf algebras, quantum groups.

Partially supported by CONICET, CONICOR, SeCYT (UNC) and FAMAF (República Argentina).

1.1. The first results on classification of Hopf algebras were obtained already by Hopf, Leray and Borel; their work was extended by Milnor and Moore [**MM**, Section 7], Cartier [**Ca**, Th. 2] and Kostant [**Sw**, Th. 8.1.5 and 13.0.1], [**Ko**, Th. 3.3]. The following result is known as the Cartier-Kostant-Milnor-Moore theorem.

THEOREM 1.1. *A cocommutative Hopf algebra over an algebraically closed field* $\mathbf{k}$ *of characteristic 0 is the semidirect product of a group algebra and the enveloping algebra of a Lie algebra. In particular, a finite dimensional cocommutative Hopf algebra over* $\mathbf{k}$ *is a group algebra.* □

It is also known that commutative Hopf algebra over $\mathbf{k}$ is the algebra of rational functions on a pro-algebraic group; see also [**Ga**], [**Se3**]. This Theorem is no longer true over algebraically closed fields of positive characteristic: restricted enveloping algebras of p-Lie algebras are finite dimensional cocommutative Hopf algebras but not group algebras. These finite dimensional Hopf algebras are Hopf kernels of Frobenius homorphism on algebraic groups. Indeed, the full classification is not known in this case; see however [**Ga**], [**FV**].

1.2. The ressemblance of the theory of Hopf algebras with group theory, almost a tautology at the level of cocommutative Hopf algebras, was boldly remarked by the discovery of quantum groups. Even this name was chosen by Drinfeld to emphasize the ideological bridge between the two theories. However, in despite of the fact that concepts of group theory served as inspiration and guide to recent research– an explicit example being Kaplansky's conjectures– many elementary facts about finite groups are hard to translate to finite dimensional Hopf algebras, or even false at least in the first naive approach. For instance, Nichols-Zoeller freeness theorem is a counterpart of Lagrange's theorem: a finite dimensional Hopf algebra is free over any Hopf subalgebra. However the known proof is not straightforward and relies on the Krull-Remak-Schmidt theorem. Sylow's theorems are no longer true (just look at the dual of a group algebra of a simple group). The class equation expressing the order of a finite group as the sum of the cardinals of its conjugacy classes can be somehow recovered, but without reference to isotropy subgroups.

On the other hand, our stock of examples of finite dimensional Hopf algebras is not as wide as one would like. We collect the main techniques of construction of Hopf algebras in Section 2.

1.3. The theory of Hopf algebras received a deep impact with the introduction of quantum groups [**Dr1**]. On one hand, a whole range of new techniques and concepts– the double, quasitriangular Hopf algebras, braided categories, twisting, . . . , just to mention the most used– came into use and form now part of the standard baggage of a Hopf algebraist. On the other hand, the fundamental examples of quantized enveloping algebras [**Dr1**], [**J**], their duals and twisted variations thereof, were intensively studied. In particular, a very important class of non-trivial Hopf algebras was discovered by Lusztig: these are called Frobenius-Lusztig kernels since they appear as Hopf kernels of a quantum Frobenius homomorphism. They can be thought as liftings to characteristic 0 of Frobenius kernels, and as such, they play an important role in representation theory [**AJS**].

1.4. The classification of finite dimensional Hopf algebras over an algebraically closed field $\mathbf{k}$ follows two definitely different tracks: the semisimple case and the non-semisimple case. Indeed, there are several equivalent characterizations of semisimple Hopf algebras when $\operatorname{char}\mathbf{k} = 0$; when $\operatorname{char}\mathbf{k} > 0$ the correct setting is that of semisimple and cosemisimple Hopf algebras. By a beautiful result of Etingof and Gelaki [**EG3**], this reduces to the characteristic 0 case. See Section 3. A nice survey on classification of semisimple Hopf algebras is [**Mo2**]; we will discuss in Section 4 some more recent results which are not included there.

1.5. Substantial results, though not definitive, on the classification of non-semisimple Hopf algebras are known only for the class of pointed Hopf algebras over an algebraically closed field of characteristic 0. In this case, the lifting principle, due to H. Schneider and the author [**AS2**], provides the adequate framework for this problem and allows Lie theory to enter into the picture through quantum groups. The goal of the series of papers [**AS2, AS3, AS4, AS5**] is to show that Frobelnius-Lusztig kernels, or Lusztig's small quantum groups, exhaust a natural class of finite dimensional Hopf algebras. See also [**AS7**] for the infinite dimensional case. An account is given in Section 5; we refer to the survey paper [**AS6**] for a more detailed exposition.

1.6. There are few results on classification of all Hopf algebras of a presecribed dimension; we collect them in Section 6. Section 7 contains some remarks on forms of Hopf algebras. Due to lack of space, some other interesting topics are not touched; this includes work of Etingof and Gelaki on classification of triangular Hopf algebras, see for instance [**EG2, G3**]. We touch Kaplansky's conjectures only in the course of the exposition; for a systematic overview of them, see [**Sr2**].

1.7. Acknowledgements. The development of the point of view on the material presented here benefited from uncountable conversations along the years with Hans Schneider and my students Sonia Natale and Matías Graña. I am very grateful to them for sharing with me their insights. I also profited from conversations with A. Abella, M. Beattie, S. Dăscălescu, W. Ferrer Santos, S. Gelaki, Y. Kashina, A. Masuoka, S. Montgomery, Y. Sommerhäuser, P. Schauenburg, Y. Zhu.

I also thank the Directors of the School, and Editors of this volume, R. Coquereaux and R. Trinchero, for the splendid organization of the School, and for the invitation to deliver the Lectures and write the Notes.

I have tried to give appropiate credit to all the papers I am aware of, but even with the help of the contemporary electronical techniques, some results or authors might have remained unrecognized in this paper; I only have to offer them my sincere apologies.

1.8. Conventions and notations. We shall work over a $\mathbf{k}$; suitable hypothesis on theory of Hopf algebras are [**Sw**], [**Mo1**], [**Sch3**], [**Ma3**]. The notation for Hopf algebras is standard: Δ, $\mathcal{S}$, ε, denote respectively the comultiplication, the antipode, the counit. We use Sweedler's notation but dropping almost always the summation symbol. That is, $\Delta(x) = \sum_{(x)} x_{(1)} \otimes x_{(2)} = x_{(1)} \otimes x_{(2)}$.

Similarly, if C is a coalgebra and V is a left comodule with structure map $\delta : V \to C \otimes V$, then $\delta(x) = \sum_{(x)} x_{(-1)} \otimes x_{(0)} = x_{(-1)} \otimes x_{(0)}$.

If A is a Hopf algebra, the well-known adjoint representation ad of A on itself is given by $\operatorname{ad} x(y) = x_{(1)} y \mathcal{S}(x_{(2)})$.

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 let $P_{g,h}(C) = \{x \in C \mid \Delta(x) = g \otimes x + x \otimes h\}$ be the space of all (g,h)-primitive elements. If A is a Hopf algebra and $\Gamma = G(A)$ is a finite abelian group, then Γ acts on each $P_{g,h}(A)$ by conjugation, and if χ is a character of Γ, then we define $P_{g,h}(A)^{\chi} = \{a \in P_{g,h}(A) \mid uau^{-1} = \chi(u)a, \text{ for all } u \in \Gamma\}$.

2. Examples

In this Section, we list several known ways to obtain finite dimensional Hopf algebras. Here $\mathbf{k}$ is an arbitrary field.

2.1. Duals. If H is a finite dimensional Hopf algebra, then its linear dual H^* is a again a Hopf algebra, by transposing all the maps (so that the multiplication of H^* is the transpose of the comultiplication of H and so on).

2.2. From groups. Let G be a finite group. The algebra $\mathbf{k}^G$ of functions from G to $\mathbf{k}$ is a semisimple Hopf algebra with pointwise product and comultiplication $\Delta(\phi)(g,h) = \phi(gh)$, $\phi \in \mathbf{k}^G$, $g,h \in G$, where we are identifying $\mathbf{k}^G \otimes \mathbf{k}^G \simeq \mathbf{k}^{G\times G}$. The antipode is $\mathcal{S}(\phi)(g) = \phi(g^{-1})$ and the counit is $\varepsilon(\phi) = \phi(1)$. For $g \in G$, let $\delta_g \in \mathbf{k}^G$ be the function which is 0 outside g and takes the value 1 in g. The dual Hopf algebra is the group algebra $\mathbf{k}G$; if $\{e_g\}$ is the dual basis of $\{\delta_g\}$, then $e_g e_h = e_{gh}$ and

$$\Delta(e_g) = e_g \otimes e_g. \tag{2.1}$$

An element of a Hopf algebra whose coproduct is given by (2.1) is called a group-like. The elements e_g can be thought as Dirac measures on the discrete topological space G. It is well-known that $\mathbf{k}^G$ is always semisimple, and that the group algebra $\mathbf{k}G$ is semisimple provided that the characteristic of $\mathbf{k}$ does not divide the order of G (Maschke's theorem).

2.3. By extension. It is natural to think on building Hopf algebras from smaller ones, just as in group theory. This was treated by many people in different settings: by G. I. Kac for his finite dimensional C^*-Hopf algebras [**Kc1**]; by Singer for connected Hopf algebras, in the so called abelian case [**Si**]; by Majid and Majid-Soibelman [**Ma1**], [**MS**]; by Hofstetter [**Ho**]; and also in [**By1**], [**By2**], [**Sch3**], [**Mk1**], [**AD**], [**A1**]. See also [**Mk8**]. Also, it is implicit in [**L3**]. Briefly, the situation is the following.

(a). A sequence of Hopf algebra maps $1 \to A \xrightarrow{\iota} C \xrightarrow{\pi} B \to 1$, where 1 denotes the Hopf algebra $\mathbf{k}$, is *exact* if

(1) ι is injective. Identify then A with its image.
(2) π is surjective.
(3) $\ker \pi = CA^+$. (A^+ is the augmentation ideal, i.e. the kernel of the counit).
(4) $A = \{x \in C : (\pi \otimes \mathrm{id})\Delta(x) = 1 \otimes x\}$.

Then the equality $\pi\iota = \varepsilon$ follows either from (3) or from (4). In such case, C is called an extension of the Hopf algebras A and B.

An injective morphism of Hopf algebras $A \xrightarrow{\iota} C$ is normal if $\iota(A^+)C = C\iota(A^+)$. In such case, the unique possible B completing the exact sequence is the "Hopf cokernel" C/CA^+. Now condition (5) above can be dropped if $A \xrightarrow{\iota} C$ is faithfully flat and A is stable by the adjoint action of C; and B does indeed complete the exact sequence. Examples of inclusions of Hopf algebras which are not faithfully flat were given by Schauenburg: they are related to the lack of bijectivity of the antipode [**Sbg2**]. In the finite dimensional case, any Hopf algebra is free over its Hopf subalgebras and this problem does not arise.

A similar analysis proceeds for a conormal, surjective, morphism of Hopf algebras $C \xrightarrow{\pi} B$; but the rôle of the "faithfully flat" requirement is played now by "faithfully coflat", see for instance [**AD**, Proposition 1.2.11].

In conclusion: if C is a finite dimensional Hopf algebra and A is a normal Hopf subalgebra of C, then the quotient coalgebra $B := C/CA^+$ is a quotient Hopf algebra of C and it fits in an exact sequence as above.

(b). If G is a group, A is a normal abelian subgroup and $N := G/A$, then N acts on A and G can be reconstructed from N, the N-module A and a 2-cocycle $\sigma : N \times N \to A$, unique up to its class in $H^2(N, A)$. Conversely, given a group N, an N-module A and a 2-cocycle $\sigma : N \times N \to A$ we can build a group G (whose underlying set is $A \times N$) with A as a normal subgroup and such that $N \simeq G/A$.

A similar, but much more involved, situation can be considered for Hopf algebras. Given Hopf algebras A and B, we can build a Hopf algebra structure on the vector space $A \otimes B$ from the following additional data: a "weak action" $\leftharpoonup: B \otimes A \to A$, a "2-cocycle" $\sigma : B \otimes B \to A$, a weak coaction $B \to A \otimes B$ and a "dual 2-cocycle" $A \to B \otimes B$, fulfilling a list of compatibility conditions. Conversely, given an extension as above, one can find a weak action, a weak coaction, a cocycle an a dual cocycle which are compatible and so that C can be reconstructed from A, B and these data, whenever the extension is *cleft*. Here cleft means that there exists an invertible comodule section of π. This section is somehow the analogue of the section of sets $N \to G$ at the group level, which always exists. But in some other settings, like algebraic groups the existence of such section in the category is not always true and similar considerations are carried out.

In any case, any extension of finite dimensional Hopf algebras is cleft [**Sch1**]. In conclusion: if C is a finite dimensional Hopf algebra and A is a normal Hopf subalgebra of C, then C can be reconstructed from A, the quotient Hopf algebra $B = C/CA^+$ and data as above.

(c). If A is commutative and B is cocommutative, the weak action and the weak coaction are a real action and a real coaction, respectively. Once they are fixed, the 2-cocycle and the dual 2-cocycle form have a cohomological meaning, forming a 2-cocycle in the total complex associated to a double complex. This is usually called the *abelian case*. To compute then how many extensions C (up to isomorphisms) can be constructed from A, B, a fixed action and a fixed coaction, amounts to comute the order of the second cohomology group $H^2(A, B)$. A very useful devise for this computation is the so-called Kac exact sequence, see for instance [**Mk8**].

(d). In several instances, properties of C can be deduced from similar properties of A and B, and viceversa. For example, C is semisimple if and only if both A and B are; use [**BM**].

(e). Let us say that a finite dimensional Hopf algebra is *simple* if it has no proper normal Hopf subalgebras. It is natural to ask for "genuine" examples of simple Hopf algebras. Clearly, if G is a simple group then both $\mathbf{k}G$ and $\mathbf{k}^G$ are simple Hopf algebras. For more examples, see the discussion in the next Subsection.

On the other hand, a rutinary dimension argument shows that any finite dimensional Hopf algebra can be obtained as an iterated extension of simple Hopf algebras. We can then attach to any finite dimensional Hopf algebra the sequence of its simple subfactors in *some* presentation as iterated extension. We do not know the answer to the following:

QUESTION 2.1. Does the Jordan-Hölder theorem hold for finite dimensional Hopf algebras? That is, is the sequence of simple subfactors alluded above unique up to permutation?

For some explicit computations of extensions, see [**AN2, Mk6, Mk7, Mk8, Mu2**].

2.4. By twisting. Let A be a Hopf algebra and $F \in A\otimes A$ be an invertible element. Let $\Delta_F := F\Delta F^{-1} : A \to A\otimes A$; it is again an algebra map. It is coassociative if and only if

$$(1\otimes F)(\mathrm{id}\otimes\Delta)(F) = (F\otimes 1)(\Delta\otimes\mathrm{id})(F)U, \tag{2.2}$$

where U is an element of $A\otimes A\otimes A$ that centralizes $\Delta^{\otimes 2}(A)$. It is counital if and only if

$$((\mathrm{id}\otimes\varepsilon)(F) = 1 = (\varepsilon\otimes\mathrm{id})(F). \tag{2.3}$$

If (2.2) and (2.3) hold, then A_F (the same algebra, but with comultiplication Δ_F) is again a Hopf algebra. We shall say in this case that F is a *pseudo-cocycle* and that A_F is obtained from A via twisting by F. When $U = 1$, F is a cocycle in a suitable sense. As the multiplication does not change, if A is semisimple then A_F is semisimple. This construction is originally due to Drinfeld and it was applied to group algebras in [**Nk**], [**Mv**], [**EG2**]. See also [**EV**]. In particular, examples of non-trivial twistings of group algebras of simple groups are given:

THEOREM 2.2. [**Nk**]. *There exists $F \in \mathbf{k}\mathbb{A}_5\otimes\mathbf{k}\mathbb{A}_5$ such that $(\mathbf{k}\mathbb{A}_5)_F$ is a simple non-commutative, non-cocommutative Hopf algebra.* □

Here $\mathbb{A}_5$ is the alternating group of dimension 60, the smallest non-abelian simple group. This Theorem was generalized to all non-abelian simple groups [**Hof**].

QUESTION 2.3. To our knowledge, the only known simple semisimple Hopf algebras are group algebras, their twistings and duals of them. Are there more?

One could begin by the following:

QUESTION 2.4. What are all the simple semisimple Hopf algebras of dimension 60?

One says that a finite dimensional Hopf algebra is *trivial* if it is isomorphic group algebra or a dual group algebra. Further, one has the following natural definition.

DEFINITION 2.5. [**MoW**] A finite dimensional Hopf algebra is *semi-solvable* if it can be obtained by sucesive extensions from group algebras or duals of group algebras.

Question 2.3 is very close to the following.

QUESTION 2.6. Does there exist a semisimple Hopf algebra which is *not* a twisting of a semi-solvable Hopf algebra?

2.5. Twisting the multiplication. There is a dual version of the twisting operation, which amounts to twist the multiplication. Let A be a Hopf algebra and let $\sigma : A \times A \to \mathbf{k}$ be an invertible 2-cocycle, that is

$$\sigma(x_{(1)}, y_{(1)})\sigma(x_{(2)}y_{(2)}, z) = \sigma(y_{(1)}, z_{(1)})\sigma(x, y_{(2)}z_{(2)}),$$
$$\sigma(1,1) = 1,$$

for all $x, y, z \in A$. Then A_σ– the same A but with the multiplication $._\sigma$ below– is again a Hopf algebra, where

$$x._\sigma y = \sigma(x_{(1)}, y_{(1)})x_{(2)}y_{(2)}\sigma^{-1}(x_{(3)}, y_{(3)}).$$

REMARK 2.7. There is a very convenient setting where this last construction can be performed. Let U, H be Hopf algebras. Let $\tau : U \otimes H \to \mathbf{k}$ be a bilinear map such that for all $u, v \in U$, $a, b \in H$

- $\tau(uv, a) = \tau(u, a_{(1)})\tau(v, a_{(2)})$,
- $\tau(u, ab) = \tau(u_{(1)}, b)\tau(u_{(2)}, a)$,
- $\tau(1, a) = \varepsilon(a)$,
- $\tau(u, 1) = \varepsilon(u)$.

Let A be the tensor product Hopf algebra $A = U \otimes H$ and let $\sigma : A \otimes A \to \mathbf{k}$ be the bilinear map

$$\sigma(u \otimes a, v \otimes b) = \varepsilon(u)\tau(v, a)\varepsilon(b), \qquad u, v \in U, \quad a, b \in H.$$

Then τ is convolution invertible with inverse given by $\tau^{-1}(v, a) = \varphi(\mathcal{S}\, v)(a) = \varphi(v)(\mathcal{S}^{-1}\, a)$; σ is an invertible 2-cocycle– with inverse

$$\sigma^{-1}(u \otimes a, v \otimes b) = \varepsilon(u)\tau^{-1}(v, a)\varepsilon(b), \qquad u, v \in U, \quad a, b \in H;$$

and consequently A_σ is a Hopf algebra. Note that U and H are naturally identified with Hopf subalgebras of A_σ; and the multiplication induces a linear isomorphism $U \otimes H \simeq A_\sigma$. This means that U and H form a *matched pair* and that A_σ is the *double crossproduct* of U and H. See [**Ma3**, Chapter 7] for a detailed exposition and examples.

REMARK 2.8. In the notation of Remark 2.7, assume that H is finite dimensional and let $\varphi : U \to (H^*)^{\rm cop}$ be a Hopf algebra homomorphism. Then $\tau : U \otimes H \to \mathbf{k}$, $\tau(v, a) = \varphi(v)(a)$, is invertible– with inverse given by $\tau^{-1}(v, a) = \varphi(\mathcal{S}\, v)(a) = \varphi(v)(\mathcal{S}^{-1}\, a)$, and satisfies the requirements above. Reciprocally, given such τ there is a unique such φ.

2.6. The double. Let H be a finite dimensional Hopf algebra. Let $U = (H^*)^{\mathrm{cop}}$; by Remark 2.8 applied to $\varphi = \mathrm{id}$, we obtain a linear map τ which gives rise in turn to a cocycle σ, as explained in Remark 2.7. The Hopf algebra $((H^*)^{\mathrm{cop}} \otimes H)_\sigma$ is called the *Drinfeld double*, or simply the double of H, and is denoted by $D(H)$. Introduced by Drinfeld in the seminal paper [**Dr1**], it is one of the most important constructions in Hopf algebra theory. We refer to [**Mo1**], [**Ma3**], for detailed expositions. We content ourselves by listing some of the fundamental properties of the double:

- [**Dr1**]. $(D(H), \mathcal{R})$ is a quasitriangular Hopf algebra, where $\mathcal{R} \in H \otimes H^* \subset D(H) \otimes D(H)$ is the canonical element.
- [**Dr1**]. If (H, R) is quasitriangular, then R induces a Hopf algebra projection $D(H) \to H$, with kernel $(H^*)^{\mathrm{cop}}$.
- [**Dr2**]. If (H, R) is quasitriangular, and $R = \sum_i R_i \otimes R^i$, then the element $u = \sum_i \mathcal{S}(R^i) R_i$ is invertible and satisfies
$$\mathcal{S}^2(x) = uxu^{-1}, \quad x \in H, \qquad \Delta(u) = (u \otimes u)(R_{21}R)^{-1}.$$
Here $R_{21} = \sum_i R^i \otimes R_i$. u is called the *Drinfeld element* of H.
- [**RS**]. The double of the double $D(D(H))$ is isomorphic to $(D(H) \otimes D(H))_\sigma$, for a suitable cocycle σ.

The following Proposition is useful in classification problems. We identify $D(H)^*$ with $H \otimes H^*$ as vector spaces.

Proposition 2.9. [**R3**]. *(i). The group $G(D(H))$, is isomorphic to $G(H^*) \times G(H)$, via multiplication.*

(ii). The elements of group $G(D(H)^*)$ are of the form $g \times \eta$, where $\eta \in G(H^*)$ and $g \in G(H)$, and $\eta \times g$ is in the center of $D(H)$. □

2.7. By bosonization. This is a more sophisticated kind of extension. It was discovered by Radford and interpreted in braided-categorical terms by Majid, see [**Ma2**], [**R2**]. It is a distinguished feature of Hopf algebra theory with no analogue in group theory; it is a very useful tool in classification problems, specially in the pointed case.

Let A and H be Hopf algebras with bijective antipode, and assume there are Hopf algebra maps $\pi : A \to H$ and $\iota : H \to A$ such that $\pi\iota = \mathrm{id}_H$; so that π is surjective and ι is injective. By analogy with elementary group theory, one seeks to reconstruct A from H and the kernel of π as a semidirect product. The role of the kernel of π is played in this situation by the algebra of coinvariants

$$R := A^{\mathrm{co}\,\pi} = \{a \in A : (\mathrm{id} \otimes \pi)\Delta(a) = a \otimes 1\}. \tag{2.4}$$

In contrast with the group case, this is not a usual Hopf algebra; but it is a *braided* Hopf algebra.

To explain what this means, let us first recall some definitions. Given a Hopf algebra H, a Yetter-Drinfeld module over H is a vector space V provided with

- A structure of left H-module: $H \otimes V \to V$;

- and a structure of left H-comodule: $V \to H \otimes V$, such that
- the following compatibility condition is satisfied:

$$\delta(h.v) = h_{(1)}v_{(-1)}\mathcal{S}(h_{(3)}) \otimes h_{(2)}.v_{(0)}. \tag{2.5}$$

The category of all Yetter-Drinfeld modules, with morphisms the maps of modules and comodules, is denoted by ${}^H_H\mathcal{YD}$. (If $H = \mathbf{k}\Gamma$, we simply write ${}^\Gamma_\Gamma\mathcal{YD}$). It is a braided category; that is, if $M, N \in {}^H_H\mathcal{YD}$, then:

- The tensor product $M \otimes N$ and the dual M^*, with the natural module and comodule structures, are again Yetter-Drinfeld modules.
- There exists a natural isomorphism $c : M \otimes N \to N \otimes M$ given explicitly by

$$c(m \otimes n) = m_{(-1)}.n \otimes m_{(0)} \tag{2.6}$$

which satisfies appropiate axioms, see for instance [**Mo1**]. When H is finite dimensional, a Yetter-Drinfeld module over H is nothing but a left module over the Drinfeld double $D(H)$ of H; and the braiding is just the one defined by the universal R-matrix of $D(H)$.

Remark 2.10. A natural way to introduce Yetter-Drinfeld modules is through Hopf bimodules. A *Hopf bimodule* is simultaneously a bimodule and a bicomodule (so it has left and right actions, and left and right coactions); all this structure is required to satisfy natural compatibility conditions. Given a Hopf bimodule M, the space of right coinvariants $M^{\mathrm{co}} = \{m \in M : \delta_r(m) = 1 \otimes m\}$ bears a natural structure of Yetter-Drinfeld module. One gets in this way an equivalence between the two categories. See [**N, W2**].

We can then consider braided Hopf algebras in the braided category ${}^H_H\mathcal{YD}$. We recall that R is a braided Hopf algebra in R if:

- R is an algebra; the product and unit are morphisms in ${}^H_H\mathcal{YD}$.
- R is a coalgebra; the coproduct and counit are morphisms in ${}^H_H\mathcal{YD}$.
- The coproduct Δ_R is an algebra map; but here we consider in $R \otimes R$ not the usual product but the one defined by

  $$m_{R\otimes R} = (m_R \otimes m_R)(\mathrm{id} \otimes c \otimes \mathrm{id}) : R \otimes R \otimes R \otimes R \to R \otimes R.$$

  (this multiplication differs from the usual tensor product multiplication in the appearance of c instead of the usual flip).
- The identity $\mathrm{id} : R \to R$ has a convolution-inverse $\mathcal{S}_R$ in $\operatorname{End} R$, the antipode.

The archetypical example of a braided Hopf algebra in ${}^H_H\mathcal{YD}$ is the algebra of coinvariants R as in (2.4). Namely, R is a subalgebra and it is also stable under the adjoint action of H; the coaction and the comultiplication are given by

$$\delta = (\pi \otimes \mathrm{id})\Delta, \qquad \Delta_R(r) = r_{(1)}\iota\pi\mathcal{S}(r_{(2)}) \otimes r_{(3)}.$$

Conversely, let R be a braided Hopf algebra in ${}^H_H\mathcal{YD}$. Then the *bosonization* or biproduct of R by H is a usual Hopf algebra $A = R\#H$, with underlying vector space $R \otimes H$, whose multiplication and comultiplication are given by

$$(r\#h)(s\#f) = r(h_{(1)}.s)\#h_{(2)}f, \tag{2.7}$$

$$\Delta(r\#h) = r^{(1)}\#(r^{(2)})_{(-1)}h_{(1)} \otimes (r^{(2)})_{(0)}\#h_{(2)}. \tag{2.8}$$

The maps $\pi : A \to H$ and $\iota : H \to A$, $\pi(r\#h) = \epsilon(r)h$, $\iota(h) = 1\#h$, are Hopf algebra homomorphisms; we have $R = \{a \in A : (\mathrm{id} \otimes \pi)\Delta(a) = a \otimes 1\}$. So that these constructions are inverse to each other.

We would like to have new examples of Hopf algebras constructed by bosonization. Let R be a braided Hopf algebra in ${}^H_H\mathcal{YD}$ and let $A = R\#H$. First, A is semisimple if and only if both R and H are (again by [**BM**]). There are some non-trivial examples of semisimple Hopf algebras which can be constructed as bosonization [**G1, AN2, Sr1**]. Unfortunately, all these examples can also be described as extensions.

Definition 2.11. [**AS2**]. A Hopf algebra H is *very simple* if it is simple, and it can not be presented as a bosonization in a non-trivial way.

Question 2.12. Does there exist a semisimple Hopf algebra which is simple but not very simple? That is, a non-trivial bosonization but not an extension.

A positive answer to this Question would also answer Question 2.3, by the negative.

Example 2.13. Let $N > 1$ be a natural number and let $R = \mathbf{k}[x]/(x^N)$. Since $\operatorname{char} \mathbf{k} = 0$, there is no algebra map from R to $R \otimes R$ (with the usual tensor product multiplication) sending x to $x \otimes 1 + 1 \otimes x$.

Now, let Γ be a group, $g \in Z(\Gamma)$ and χ a one-dimensional representation of Γ such that $\chi(g) =: q$ is a root of 1 of order N. We consider $R \in {}^\Gamma_\Gamma\mathcal{YD}$ by $h.x^j = \chi(h)^j x^j$, $\delta(x^j) = g^j \otimes x^j$. Then $c(x^j \otimes x^t) = q^{jt} x^t \otimes x^j$. Using the quantum binomial formula, one can see without effort that there is an algebra map $\Delta_R : R \to R \otimes R$ (with the "braided" tensor product multiplication) sending x to $x \otimes 1 + 1 \otimes x$; and that this is indeed a braided Hopf algebra.

If g has order N and Γ is generated by g, then the bosonization $T_q = R\#\mathbf{k}\Gamma$ is called a Taft algebra; one has $T_q \simeq \mathbf{k}\langle g, x | q^N = 1, x^N = 0, gx = qxg\rangle$ with g group-like and $\Delta(x) = x \otimes 1 + g \otimes x$. It is also not difficult to see that $T_q \simeq T_q^*$ as Hopf algebras, and that the proper Hopf subalgebras of T_q are contained in $\mathbf{k}\langle g\rangle$. It follows at once that T_q is simple (but not very simple). For a general criteria of simplicity of pointed Hopf algebras, see [**AS0**].

If R is a braided Hopf algebra in ${}^H_H\mathcal{YD}$ then there is also a braided adjoint representation ad_c of R on itself given by

$$\mathrm{ad}_c\, x(y) = \mu(\mu \otimes \mathcal{S})(\mathrm{id} \otimes c)(\Delta \otimes \mathrm{id})(x \otimes y),$$

where μ is the multiplication and $c \in \operatorname{End}(R \otimes R)$ is the braiding. Note that if $x \in \mathcal{P}(R)$ then the braided adjoint representation of x is just

$$\mathrm{ad}_c\, x(y) = \mu(\mathrm{id} - c)(x \otimes y) =: [x, y]_c. \tag{2.9}$$

The element $[x,y]_c$ defined by the second equality for any x and y, regardless of whether x is primitive, will be called a braided commutator.

When $A = R\#H$, then for all $b, d \in R$,

$$\operatorname{ad}_{(b\#1)}(d\#1) = (\operatorname{ad}_c b(d))\#1. \tag{2.10}$$

3. General results

In this Section, we review some basic fundamental results that allow to organize the study of classification problems of finite dimensional Hopf algebras. The field $\mathbf{k}$ is general, except when explicitly stated.

3.1. Freeness results. Let H be a Hopf algebra. Let $R \subseteq H$ be a subalgebra such that $\Delta(R) \subseteq H \otimes R$; that is, R is la left coideal subalgebra. A (left) relative (H,R)-module is a left R-module M provided with a left comodule structure $\delta : M \to H \otimes M$ such that

$$\delta(r.m) = r_{(1)}m_{(-1)} \otimes r_{(2)}.m_{(0)},$$

for all $m \in M$, $r \in R$. The category of left relative (H,R)-modules is denoted by ${}^H_R\mathcal{M}$. Here is one of the fundamental results that opened the recent theory of finite dimensional Hopf algebras.

Theorem 3.1. [**NZ**]. *If B is a Hopf subalgebra of a finite dimensional Hopf algebra A then any left relative (A,B)-module is a free left B-module.* □

An example of relative (A,B)-module is A itself, with left multiplication of B and the comultiplication of A. Clearly, a subspace C of A is a relative (A,B)-submodule if $BC \subseteq C$ and $\Delta(C) \subseteq A \otimes C$. The following applications of Theorem 3.1 illustrate better its importance.

Corollary 3.2. [**NZ**]. *Let A be a finite dimensional Hopf algebra.*

(1) *If B is a left coideal subalgebra, in particular if it is a Hopf subalgebra, of A, then A is free as B-module with left multiplication. In particular,* $\dim B$ *divides* $\dim A$.

(2) *If C is a subcoalgebra of A and S is a subgroup of $G(A)$ such that $gC \subseteq C$ for all $g \in S$, then $|S|$ divides* $\dim C$.

(3) *If $\pi : A \to H$ is a Hopf algebra epimorphism and B is a Hopf subalgebra of A such that $B \subseteq A^{\operatorname{co}\pi}$, then* $\dim B$ *divides* $\dim A^{\operatorname{co}\pi}$*; cf.* (2.4).

□

In the case of group algebras, part (i) of the Corollary amounts to Lagrange's theorem. For infinite dimension the preceding is false; a counterexample is given in [**OS2**]. A substitute would be the following statement: "any inclusion of Hopf algebras is faithfully flat"; but this is also false as shown by Schauenburg [**Sbg2**].

For a left coideal subalgebra B of a finite dimensional Hopf algebra A, the integer

$$[A:B] := \frac{\dim A}{\dim B}$$

will be called the *index* of B in A. If $B = \mathbf{k}G$ is a group algebra, we just write $[A:G] := [A:B]$.

Recently, the Nichols-Zöller theorem was generalized to the braided case.

THEOREM 3.3. [**Sf, T1**]. *Let H be a Hopf algebra with bijective antipode and let A be a finite dimensional braided Hopf algebra in ${}^H_H\mathcal{YD}$. If B is a braided Hopf subalgebra of A, then A is free as B-module with left multiplication. In particular,* $\dim B$ *divides* $\dim A$. □

Notice that Theorem 3.3 follows directly from Corollary 3.2 in the case when H is also finite dimensional [**AS1**]. A variation of this result will be discussed later, see Theorem 5.42.

3.2. Integrals and applications. Let A be a Hopf algebra. We say that $\lambda \in A^*$ is a *right integral on* A if

$$\lambda\beta = \lambda\langle\beta, 1\rangle,$$

for all $\beta \in A^*$; or equivalently if $\langle\lambda, x\rangle 1 = \langle\lambda, x_{(1)}\rangle x_{(2)}$, for all $x \in A$. Similarly left integrals on A are defined. Furthermore, we say that $\Lambda \in A$ is a *left integral in* A if

$$x\Lambda = \langle\varepsilon, x\rangle\Lambda,$$

for all $x \in A$. We collect several facts about integrals:

THEOREM 3.4. *Let A be a Hopf algebra.*

(1) [**LS**]. *If A is finite dimensional Hopf algebra, then the space of left integrals in A is one-dimensional.*

(2) *If the space of left integrals in A is non-zero, then A is finite dimensional. This implies:*

(3) [**Sw**, Ex. 1-4, pp. 107]. *If A is semisimple*[1]*, then it is finite dimensional.*

(4) [**Sul**]. *The space of left integrals on A has dimension ≤ 1.*

□

If A is a Hopf algebra with a non-zero integral on it, then A is called *co-Frobenius*. For instance, cosemisimple Hopf algebras (like compact quantum groups) are co-Frobenius. Co-Frobenius Hopf algebras are matter of current interest. See [**DNT**] and references therein.

We fix now a finite dimensional Hopf algebra A, a non-zero right integral $\lambda \in A^*$ and a a non-zero left integral $\Lambda \in A$. Notice that neither λ is necessarily a left integral in A^*, nor Λ is necessarily a right integral in A. The failures are respectively measured by the so-called modular (or distinguished) group-like elements $a \in A$, $\alpha \in A^*$. They are determined by

$$\beta\lambda = \lambda\langle\beta, a\rangle, \qquad \Lambda x = \langle\alpha, x\rangle\Lambda.$$

We say that A is unimodular if Λ is a right integral in A; that is, if $\alpha = \varepsilon$. It is known that:

(1) Semisimple Hopf algebras are unimodular;

[1] In this paper, we understand by "semisimple ring" one whose category of modules is semisimple. Some authors use "artinian semisimple", and reserve "semisimple" for a ring whose Jacobson radical is zero.

(2) quasitriangular (finite dimensional) Hopf algebras are unimodular. In particular, a Drinfeld double is unimodular, and hence any finite dimensional Hopf algebra can be embedded in a unimodular one.

The modular elements are related to the antipode by the following important formula discovered by Radford:

THEOREM 3.5. [**R1**]. $\mathcal{S}^4(x) = \operatorname{ad}\alpha(\operatorname{ad}a(x)) = \operatorname{ad}a(\operatorname{ad}\alpha(x))$. □

See [**Sch3**] for an elegant conceptual proof of Radford's formula.

If $A = \mathbf{k}G$ is the group algebra of a finite group G, then $\Lambda = \sum_{g\in G} g$ is a (right and left) integral. Note that this a Haar measure on the finite group G; this justifies the name of *integral* given above. The well known Maschke theorem asserts that $\mathbf{k}G$ is semisimple iff the characteristic of $\mathbf{k}$ does not divide the order $|G|$ of G. As $|G| = \sum_{g\in G} < \epsilon, g > = < \epsilon, \sum_{g\in G} g >$, Maschke theorem is equivalent to the statement " $\mathbf{k}G$ is semisimple iff $< \epsilon, \Lambda > \neq 0$". It can be generalized in this way to finite dimensional Hopf algebras:

THEOREM 3.6. **(Maschke Theorem for Hopf algebras).** *The following statements are equivalent.*

(1) *A is semisimple.*
(2) $< \epsilon, \Lambda > \neq 0$.

□

The square of the antipode $\mathcal{S}$ is intimately related to the semisimplicity of A:

THEOREM 3.7. [**OS1**]. *Let $\lambda \in A^*$ (resp. $\Lambda \in A$) be integrals as above. We normalize them by $\lambda(\Lambda) = 1$. Then $\operatorname{tr}\mathcal{S}^2 = \varepsilon(\Lambda)\lambda(1)$. Therefore the following are equivalent:*

(1) $\operatorname{tr}\mathcal{S}^2 \neq 0$.
(2) *A and A^* are semisimple.*

□

Here is a useful consequence of the preceding ideas.

LEMMA 3.8. [**Z1**] *Let H be a Hopf algebra of odd dimension. If both H and H^* are unimodular, then H is semisimple. In particular, if both $G(H)$ and $G(H^*)$ are trivial, then H is semisimple.*

PROOF. By Radford's formula 3.5, $\mathcal{S}^4 = \operatorname{id}$. If H would not be semisimple, then $\operatorname{tr}\mathcal{S}^2 = 0$ by Theorem 3.7. Let $H_\pm$ be the eigenspace of $\mathcal{S}^2$ of eigenvalue ± 1. Then $\dim H_+ + \dim H_- = \dim H$, $\dim H_+ - \dim H_- = 0$; hence $\dim H$ is even, a contradiction. □

THEOREM 3.9. [**LR1, LR2**]. *If the characteristic of $\mathbf{k}$ is zero, the following conditions on a finite dimensional Hopf algebra A are equivalent:*

(1) *A is semisimple.*
(2) *A is cosemisimple, that is, A^* is semisimple.*
(3) *A is involutory, i.e. $\mathcal{S}^2 = \operatorname{id}$.*

□

It follows at once from Theorem 3.9 that Hopf subalgebras and quotient Hopf algebras of a semisimple Hopf algebra, are also semisimple.

In positive characteristic, the preceding Theorem is false: group algebras are involutory, but not always semisimple. Conditions i) and ii) imply that the characteristic of $\mathbf{k}$ does not divide the dimension of A [**LR2**, Th. 2]; also, if we suppose that $\dim A \neq 0$, then condition iii) implies i) and ii). It seems that the right analogue is that of semisimple and cosemisimple Hopf algebras. This is enhanced by the following beautiful result. For the rest of this Section, $\mathbf{k}$ is an algebraically closed field of characteristic $p > 0$.

We need some notation. The idea of the Theorem 3.10 below is that one can lift the category of semisimple and cosemisimple Hopf algebras over $\mathbf{k}$ to some analogous category but in characteristic 0. We need a field of characteristic 0; for this, one considers the ring $\mathcal{O}$ of Witt vectors of $\mathbf{k}$ and its field of fractions K. It is known that char $K = 0$, $\mathcal{O}$ is a discrete valuation ring, say with maximal ideal $\mathfrak{M}$, and $\mathfrak{M}/\mathfrak{M}^2 \simeq \mathbf{k}$.

Theorem 3.10. [**EG3**, Section 2] *Let A be a semisimple and cosemisimple Hopf algebra over $\mathbf{k}$ of dimension N. Then there exists a unique, up to isomorphism, Hopf algebra $\overline{A}$ over $\mathcal{O}$, free of rank N, such that $\overline{A}/p\overline{A} \simeq A$ as Hopf algebras. The Hopf algebra $A_0 := \overline{A} \otimes_{\mathcal{O}} K$ satisfies the following properties:*

- *It is semisimple and cosemisimple.*
- *The dimensions of its irreducible modules and comodules are the same as those of A.*
- *If A is quasitriangular, then the universal R-matrix also lifts to an universal R-matrix for A_0, which is then also quasitriangular. If A is triangular, then A_0 also is.*

□

This Lifing Theorem allows to deduce many results in the positive characteristic case, from the characteristic 0 case. Notably, here is an answer to another conjecture of Kaplansky.

Theorem 3.11. [**EG3**]. *The following conditions on a finite dimensional Hopf algebra A are equivalent:*

(1) *A is semisimple and cosemisimple.*
(2) *$\dim A \neq 0$ and $\mathcal{S}^2 = \mathrm{id}$.*

□

It is worth mentioning that there exists only a finite number of isomorphism classes of semisimple and cosemisimple Hopf algebras of fixed dimension n. This was conjectured by Kaplansky and proved by Stefan [**St2**]. An alternative proof was independiently found in [**Sch4, EG3**].

3.3. The exponent. In this subsection, $\mathbf{k}$ is any field. In analogy with elementary group theory, one could consider the following notion.

Definition 3.12. [**EG5, Ka1**] The *exponent* of a Hopf algebra H is

$$\exp H := \min\{N \in \mathbb{N} : \mu_N \circ (\mathrm{id} \otimes \mathcal{S}^{-2} \otimes \cdots \otimes \mathcal{S}^{-2n+2})\Delta_N = \varepsilon.1\} \in \mathbb{N} \cup \infty.$$

In [**EG5**] several properties and alternative characterizations of the exponent are proved. Notably, they use Vafa's formula from Conformal field theory to show:

THEOREM 3.13. [**EG5**] *If H is a semisimple and cosemisimple Hopf algebra over* $\mathbf{k}$*, then* $\exp H$ *divides* $(\dim H)^3$. □

This gives support to the following natural conjecture.

CONJECTURE 3.14. [**Ka1**] *If H is a semisimple and cosemisimple Hopf algebra over* $\mathbf{k}$*, then* $\exp H$ *divides* $\dim H$.

The validity of the Conjecture was verified by Kashina in most of the known cases. A further motivation for this conjecture is given by

PROPOSITION 3.15. [**Ka1**] *If H is a semisimple and cosemisimple Hopf algebra over* $\mathbf{k}$*, and R is a a semisimple and cosemisimple Hopf algebra in* ${}^H_H\mathcal{YD}$*, then the order of the square of the antipode of R divides* $\exp H$. □

More questions about the exponent can be found in [**EG5**].

4. The semisimple case

In this Section we survey known results on classification of semisimple Hopf algebras. The base field $\mathbf{k}$ is now algebraically closed; it has characteristic 0, except where is stated otherwise.

4.1. The Class Equation. A first fundamental result is the so-called Class Equation, found by G. I. Kac in 1972 [**Kc2**] and rediscovered by Y. Zhu 20 years later [**Z1**]. To state it, we need some preliminaries that have interest in their own.

Let H be a finite dimensional Hopf algebra and let V be a finite dimensional left H-module, corresponding to a representation $\rho : H \to \operatorname{End} V$. We define the *character* of V as the functional $\chi_V \in H^*$ given by

$$\chi_V(h) = \operatorname{tr}_V(\rho(h)), \qquad h \in H.$$

Here are some elementary properties of the characters: if V and W are finite dimensional H-modules, then

- $\chi_U = \chi_V + \chi_W$ for any extension U of V by W, in particular $\chi_{V\oplus W} = \chi_V + \chi_W$;
- $\chi_{V\otimes W} = \chi_V \cdot \chi_W$;
- $\chi_{V^*} = \mathcal{S}(\chi_V)$.

Hence, the abelian subgroup of H^* generated by the characters of the finite dimensional modules of H is finitely generated, and is a subring of H^*. It will be denoted by $R_{\mathbb{Z}}(H)$; If T is any ring, we set $R_T(H) := R_{\mathbb{Z}}(H) \otimes T$.

Now assume that the Hopf algebra H is actually semisimple. It can be shown that

- $R_{\mathbb{Z}}(H)$ is a free abelian group of finite rank; and if $V_1, \dots, V_s$ form a set of representatives of isomorphism classes of ireducible modules, then $\chi_{V_1}, \dots, \chi_{V_s}$ form a $\mathbb{Z}$-basis of $R_{\mathbb{Z}}(H)$.

- $R_{\mathbf{k}}(H)$ is isomorphic to the $\mathbf{k}$-subalgebra of H^* spanned by the characters. In particular, $\chi_{V_1}, \dots, \chi_{V_s}$ form a $\mathbf{k}$-basis of $R_{\mathbf{k}}(H)$.

- $R_{\mathbf{k}}(H)$ is a semisimple subalgebra of H^*.

More information about the character ring of a Hopf algebra can be found in [**Lo2**, **Wi2**].

THEOREM 4.1. [**Kc2**, **Z1**] *(The Class Equation for semisimple Hopf algebras). Let H be a semisimple Hopf algebra. Let $\lambda \in H^*$ be an integral, such that $< \lambda, 1 >= 1$, and let $\lambda = e_1, e_2, \dots, e_n$, be a complete set of orthogonal primitive idempotents in $R_{\mathbf{k}}(H)$. Then*

$$\dim H = \sum_{i=1}^{n} \dim(e_i H^*),$$

with $\dim(e_1 H^*) = 1$, *and* $\dim(e_i H^*) \,/ \dim H$, $\forall 1 \leq i \leq n$. □

The original proof of Kac and Zhu used some algebraic number theory. A shorter proof was given in [**Lo1**].

EXAMPLE 4.2. Let $H = \mathbf{k}G$ be a group algebra. Then the algebra of characters $R(G) \subset \mathbf{k}^G$ is the algebra of class functions, whose idempotents are the characteristic functions of the conjugacy classes. In this case, the Class Equation expresses the elementary fact that the cardinals of the conjugacy classes divide the order of G. So the name of Theorem 4.1.

EXAMPLE 4.3. Let $H = \mathbf{k}^G$ be a the dual group algebra. Now the algebra of characters $R(G)$ is all the dual $\mathbf{k}G$. The orthogonal primitive idempotents in $R(\mathbf{k}^G)$ are the orthogonal primitive idempotents in $\mathbf{k}G$. In this case, the Class Equation says that the dimensions of the irreducible G-modules divide the order of G (Frobenius theorem).

Let us now state some applications of the Class Equation. The following Theorem was obtained by Masuoka, finding the right setting for previous results of Kac and Zhu.

THEOREM 4.4. [**Mk3**]. *Let H be a semisimple Hopf algebra such that* $\dim H = p^m$, *with p a prime, and $m \geq 1$. Then H contains a central grouplike $g \neq 1$.*

PROOF. (Sketch). The Class Equation implies the existence of a *non-trivial* orthogonal primitive idempotent e in $R_{\mathbf{k}}(H)$ such that $\dim(eH^*) = 1$. But e correspond to a central group-like in H, as desired; see for instance [**Sch3**, 4.14]. □

The following result was conjectured by Kaplansky in 1975 and proved by Zhu; similar ideas were used by G. I. Kac to obtain an analogous result in the framework of C^*-algebras [**Kc2**].

THEOREM 4.5. [**Z1**]. *Let p be a prime number. Assume that the characteristic of $\mathbf{k}$ is 0. A Hopf algebra of dimension p is necessarily semisimple and isomorphic to the group algebra of $\mathbb{Z}/(p)$.*

PROOF. We can assume that $p > 2$, the case $p = 2$ being not difficult. By Theorem 4.4, it is enough to show that H is semisimple. Assume that H is not semisimple. By Lemma 3.8, then either $G(H)$ or $G(H^*)$ has to be non-trivial. But this would imply, by Corollary 3.2, that H itself is a group algebra, contradicting the assumption. □

Theorem 3.10 allows to extend Theorem 4.5 to characteristic $q \neq p$.

THEOREM 4.6. *Let p be a prime number and assume that char $\mathbf{k} = q$. Let H be a Hopf algebra of dimension p.*

(i).[**EG3**, Theorem 3.4]. *If H is semisimple and cosemisimple, then $q \neq p$ and H is isomorphic to the group algebra of $\mathbb{Z}/(p)$.*

(ii). [**EG3**, Corollary 3.4]. *If $q > p$, then H is necessarily semisimple and cosemisimple.* □

QUESTION 4.7. What are all the Hopf algebras of dimension p, say in char p?

Here is another application of Theorem 4.4.

COROLLARY 4.8. [**Mk3**]. *Let p be a prime number. Semisimple Hopf algebras of order p^2 are group algebras, in particular, commutative and cocommutative.* □

This follows from Theorem 4.4 by an argument on extensions. A harder analysis of extensions gives the classification also for p^3, p an odd prime. (For $p = 2$, this was also done by Masuoka, and the list is slightly different).

THEOREM 4.9. [**Mk2**]. *There are $p + 8$ semisimple Hopf algebras of order p^3:*

(1) *Three group algebras of abelian groups.*
(2) *Two group algebras of non-abelian groups, and their duals.*
(3) *Finally, $p + 1$ Hopf algebras which are neither commutative nor cocommutative. They are extensions of the group algebra $\mathbf{k}(\mathbb{Z}/(p) \times \mathbb{Z}/(p))$ by $\mathbf{k}(\mathbb{Z}/(p))$.*

□

In principle, one could go further by classifying extensions. In this direction, Kashina classified all semisimple Hopf algebras of order 16 [**Ka2**]. As in the group case, the computations become harder and harder; Kashina's paper witness this. To deal with other dimensions, one needs more sophisticated tools. We will see some of them in the following Subsection. Let us state before another nice application of the Class Equation.

THEOREM 4.10. *Let K be a Hopf subalgebra of a semisimple Hopf algebra H. Assume that there exists a prime number r such that the index $[H : K] = r^n$, $n \geq 1$, and $r^n < s$, for all prime number s dividing the dimension of H, $s \neq r$. Then K is normal in H.* □

For $r = 2$, $n = 1$, this was obtained by Masuoka, see *e. g.* [**Mk4**]. A statement very close to this is [**Na1**, Th. 2.2.1]; a small change in the proof of *loc. cit.* is required to obtain the result as stated here. For $n = 1$, it appeared without proof already in [**KM**] (I am grateful to Y. Kashina for communicating me this). An alternative proof, using Theorem 4.12 below, was independiently found by Bakhturin, Montgomery and Gelaki.

4.2. The Frobenius property. The validity of the following Conjecture will have deep consequences in the classification of semisimple Hopf algebras.

CONJECTURE 4.11. *(Kaplansky). If H is a semisimple Hopf algebra, then the sizes of the matrices occuring in any full matrix constituent of H divide the dimension of H.*

In general, the conjecture is still open. A semisimple Hopf algebra satisfying the conclusion of the Conjecture will be said to have *the Frobenius property*. A semisimple Hopf algebra H is known to have the Frobenius property in the following cases:

- If H is a group algebra. This is a classical result by Frobenius; here is where the name comes from.
- If H has a form over a ring of algebraic integers. This was proved by Larson in 1971 [**L**]. Another proof was offered in [**AN1**].
- If $R(H)$ is central in H^* [**ZS**, Theorem 8]. (The result is more specific).
- If H is semi-solvable [**MoW**], *cf.* Definition 2.5.

But the most striking instance of Hopf algebras with the Frobenius property is given by the following result of Etingof and Gelaki.

THEOREM 4.12. [**EG1**]. *If H is a semisimple Hopf algebra and V is an irreducible module over the Drinfeld double $D(H)$, then the dimension of V divides the dimension of H.* □

COROLLARY 4.13. [**EG1**]. *If H is a quasitriangular semisimple Hopf algebra then it has the Frobenius property.*

PROOF. The universal R matrix provides a surjective Hopf algebra map from $D(H)$ to H; so that any irreducible representation of H is also an irreducible representation of $D(H)$. □

The original proof of Theorem 4.12 used the Verlinde formula from modular categories. A second proof was shortly after offered in [**TZ**], based on [**Z2**] which uses in turn the Class Equation. A third proof of Theorem 4.12 appears in [**Sch5**]; it also uses the Class Equation, combined with a nice generalization of a result of Drinfeld [**Dr2**]. In addition, it is shown in [**Sch5**] that the Verlinde formula in the case of Hopf algebras can be derived from the Class Equation. All in all, it seems that the Class Equation and the Verlinde formula are deeply intertwined.

4.3. Semisimple Hopf algebras of low dimension. A first application of Theorem 4.12 to classification results is the following.

THEOREM 4.14. [**EG4, GW, Mk4**]. *Let $p \neq q$ be prime numbers. A semisimple Hopf algebra of dimension pq is necessarily commutative or cocommutative.* □

This was proved in the case $2p$ in [**Mk4**] without Theorem 4.12; in [**GW**], it was shown for Hopf algebras of Frobenius type. The general case was derived in [**EG4**] from [**GW**] and Theorem 4.12; but the derivation is not straightforward and needs extra arguments. Alternative proofs of Theorem 4.14 were offered in [**Sr1, Na1**]; both use Theorem 4.12. The proof in [**Na1**] is based in the following result, inspired in turn by the proof of [**EG4**, Lemma 2].

THEOREM 4.15. [**Na1**]. *Let $p \neq q$ be prime numbers, n, m, non-negative integers. Let H be a semisimple Hopf algebra of dimension $p^n q^m$. Assume H is of Frobenius type. If $p > q^b$, where*

$$b := \max\{j : \exists \text{ an irreducible character of } H \text{ of degree } q^j\},$$

then H has a non-trivial one-dimensional representation. □

COROLLARY 4.16. [**Na1**]. *Suppose H is any semisimple Hopf algebra of dimension $p^a q^b$. If $p > q^b$, then $G(D(H)^*)$ is non-trivial.* □

The meaning of the Corollary is clarified by Proposition 2.9; one has indeed a short exact sequence

$$1 \to \mathbf{k}G(D(H)^*) \xrightarrow{\iota} D(H) \xrightarrow{\pi} K \to 1, \tag{4.1}$$

for *any* finite dimensional Hopf algebra H (not necessarily semisimple). This sequence was considered with profit in [**Na1, Na4**]. Note that K is of Frobenius type, when H is semisimple.

The following question was raised by S. Montgomery, in a slightly different formulation.

QUESTION 4.17. What is the analogue of Burnside's $p^a q^b$-Theorem for semisimple Hopf algebras?

The only known results in this direction are in the case of dimension pq^2, besides those already reviewed.

THEOREM 4.18. *Let $p \neq q$ be prime numbers. Let H be a semisimple Hopf algebra of dimension pq^2.*

(i). [**Na1**]. *If H is not simple, then H is known. Specifically, either H is trivial or belongs to one of three families of extensions: $\mathcal{A}_l$, $0 \leq l \leq q-1$, $p = 1 \mod q$ (constructed in* [**G1**]*); $\mathcal{B}_{\lambda_j}$, $0 \leq j \leq \frac{p-1}{2}$ $q = 1 \mod p$; or $\mathcal{B}^*_{\lambda_j}$ (constructed in* [**Mk5**] *for $p = 2$). See* [**Na1**] *for details.*

(ii). [**Na1**]. *Either H or H^* has a non-trivial central group-like under the following restrictions:*

- *$p = 2, 3$ or $p^2 < q$; or*
- *$p > q^4$ and $p \neq 1 \mod q$.*

Therefore, for these p and q, H is known. Also, either H or H^* has a non-trivial central group-like under extra assumptions on H, for instance:

- *$p < q$ and A or A^* of Frobenius type.*

(iii). [**Na2**]. *Suppose that both H and H^* are of Frobenius type, and that $p > q$. Then either H or H^* has a non-trivial central group-like in the following cases.*

- *$p \neq 1 \mod q^2$; or*
- *$p = 1 \mod q^2$ and $G(A)$ is cyclic.*

□

The proof uses most of the machinery already explained; one of the main new tools is a systematic consideration of the exact sequence (4.1).

REMARK 4.19. We would like to stress the case where pq^2 is open, assuming that Conjecture 4.11 is true: If A is a semisimple Hopf algebra of dimension pq^2, and A is not an extension, then $p = 1 \mod q^2$, $G(A) \simeq \mathbb{Z}/(q) \times \mathbb{Z}/(q)$, and in fact A is a bosonization $A \simeq R\#\mathbf{k}(\mathbb{Z}/(q) \times \mathbb{Z}/(q))$, where R is a braided Hopf algebra of dimension p. Moreover, there is an algebra isomorphism $R \simeq \mathbf{k} \times M(q, \mathbf{k})^M$, for some M; and a coalgebra isomorphism $R \simeq \mathbf{k} \times C(q, \mathbf{k})^M$, where $C(q, \mathbf{k}) = M(q, \mathbf{k})^*$. See [**Na2**]. Whether such an R exists is open; the lowest possible dimension is 20.

The following question was raised by S. Montgomery.

QUESTION 4.20. Classify all semisimple Hopf algebras H such that $\dim H < 60$.

The actual status of this Problem is the following:

- It is open for dimensions 20, 24, 30, 32, 36, 40, 42, 48, 52, 54, 56, and known for the rest of the dimensions.

- For the dimensions where the classification is known, there are non-trivial examples in some of the dimensions; all of them are extensions.

- For the dimensions where the classification is *not* known, there are non-trivial examples in all the dimensions but 30; all of them are extensions.

The proof, for the cases where the answer is known, follows from Theorems 4.5, 4.9 4.14, 4.18 and the main result of [**Ka2**]. We should notice that some low cases were previously known, *e.g.* 12 was done in [**F**], 18 [**Mk5**]; and that to apply Theorem 4.18 one needs in some cases to check that a Hopf algebra of the desired dimension is of Frobenius type, but this follows from a counting argument in low dimension.

It is the personal opinion of this author, that one should concentrate efforts in determining whether the Hopf algebras with the remaining dimensions are semi-solvable, rather than in computing explicitly all the extensions. For, it is enough for many applications to know that a Hopf algebra is semi-solvable, in analogy with the similar situation for finite groups. And on the contrary, if it is discovered that there examples of those dimensions which are not semi-solvable, then these examples would be really new.

5. The pointed case

We have seen that the semisimple case is essentially different to the non-semisimple case, *cf.* Theorems 3.7, 3.9. We can replace "semisimple" by "cosemisimple" in the preceding sentence, by Theorem 3.9; this fits better in the following framework.

Let us say that a coalgebra C is *simple* if any non-zero subcoalgebra D is equal to C. If C is simple then it is finite dimensional and indeed, it is dual to a matrix algebra.

Given any coalgebra C, we can consider the sum of all its simple subcoalgebras:

$$C_0 := \sum_{D \subseteq C,\, D \text{ simple}} D.$$

Then C_0, itself a subcoalgebra of C, is a direct sum of simple subcoalgebras; it is called the *coradical* of C. Furthermore, we can define recursively a filtration of C by

$$C_{n+1} := \{x \in C : \Delta(x) \in C_n \otimes C + C \otimes C_n\}.$$

Then all the C_n's are subcoalgebras of C, so that $C_0 \subseteq C_1 \subseteq \dots C_n \subseteq C_{n+1} \dots$; and the filtration is exhaustive, *i. e.* $C = \bigcup_{n \geq 0} C_n$. It is called the *coradical filtration* of C.

When C is finite dimensional, so that it is the dual coalgebra of an algebra A, then $C_n = (\operatorname{Jac} A^{n+1})^{\perp}$, where Jac denotes the Jacobson radical.

It is natural to separate the investigation of finite dimensional Hopf algebras according to the shape of its coradical, and the relative position in the full Hopf algebra. One extreme case is when the Hopf algebras coincide with their coradical; this is the cosemisimple case. The opposite case is when the coradical is as simple as possible, but not the full Hopf algebra.

DEFINITION 5.1. A coalgebra (not necessarily finite dimensional) C is called *pointed* if any simple subcoalgebra of C has dimension one.

This can be phrased alternatively as "any simple comodule has dimension one" or as "the coradical is cocommutative" (since $\mathbf{k}$ is algebraically closed). If H is a pointed Hopf algebra, then H_0 is the group algebra of $G(H)$.

A first information about the coradical filtration of a pointed coalgebra is given by the Theorem of Taft and Wilson.

THEOREM 5.2. [**TW**]*; see* [**Mo1**, Theorem 5.4.1]. *Let* C *be a pointed coalgebra. Then:*

- *If* $n \geq 1$*, the* n*-th term of the coradical filtration can be decomposed as*
$$C_n = \sum_{g,h \in G(C)} C_n(g,h), \ \ \textit{where}$$
$$C_n(g,h) = \{x \in C : \Delta(x) = x \otimes h + g \otimes x + u, \ \textit{for some} \ u \in C_{n-1} \otimes C_{n-1}\}.$$
- *The first term of the coradical filtration can be expressed as*
$$C_1 = kG(C) + (\oplus_{g,h \in G(C)} P_{g,h}).$$

□

This Section is devoted to finite dimensional pointed Hopf algebras. For shortness, we shall say "pointed" for pointed non-cosemisimple. From now on, the field $\mathbf{k}$ is supposed algebraically closed and of characteristic 0.

5.1. Summary. We now give an account of results on classification of pointed Hopf algebras. Let p be a prime number.

Assume first that $p = 2$. All pointed Hopf algebras with coradical $\mathbb{Z}/(2)$ were classified in [**N**]; there is exactly one isomorphism class in each dimension 2^n. By a different method, the same result was obtained later in [**CD2**]. Pointed Hopf algebras of dimension 16, resp. 32, were classified in [**CDR**]; respectively in [**Gñ1**].

Assume now that $p > 2$. The only pointed Hopf algebras of dimension p^2 are the Taft algebras. This follows at once from a Theorem of Taft and Wilson on the coradical filtration and corollary 3.2 (i). This was known to Nichols [**N**] and was rediscovered independiently by Chin, Stefan and the present author.

Pointed Hopf algebras of dimension p^3 were classified in [**CD1**], [**AS2**], [**SvO**] by different methods. Pointed Hopf algebras of dimension p^4 were classified in [**AS3**], using results of [**AS2**]. As a matter of fact, there exist infinitely many isomorphism classes of pointed Hopf algebras of dimension p^4; hence, one of the ten conjectures of Kaplansky is not true. This was shown independiently in [**AS2, BDG, G2**]. The classification of pointed Hopf algebras of dimension p^5 follows from [**Gñ2**] combined with [**AS5**]. The Lifting Method allows to obtain many other classification results; with these ideas, for instance it is also possible to classify pointed Hopf algebras of dimension pq^2, q another prime [**AN3**].

An important classifcation result is given in [**AS5**], where the list of all finite dimensional pointed Hopf algebras with coradical of dimension p is presented. See Theorem 5.38.

There are classifications of Hopf algebras with special properties. Minimal triangular pointed Hopf algebras were classified in [**G3**]. Finite dimensional pointed Hopf algebras H such that the index $[H : \mathbf{k}G(H)]$ is either p, p^2 or p^3 are classified in [**Gñ3**] (this result has antecedents in [**AS2**, Th. 0.2], [**AS3**, Prop. 7.4], [**D**]). Finite dimensional pointed Hopf algebras H with $[H : \mathbf{k}G(H)] \leq 32$ are classified in [**Gñ4**]. Many other interesting results can be found in [**AS2, AS3, AS4, AS6, AS5, Gñ3, Gñ4**]; their formulation is too technical to be included here. Some of them will be evoked below.

5.2. Methods. We shall devote the next Subsection to the "Lifting method" [**AS2**]; here we review another methods.

The Theorem of Taft and Wilson has been a very valuable tool in the study of pointed Hopf algebras; it is applied combined with variations of the Proposition 5.3 below; the proposition appears in [**AN3**] but the idea of the proof goes back to [**N**], [**AS1**], [**St1**]. We need first some notation.

Let M and N be non-negative integers such that M divides N and let $\xi \in \mathbf{k}^\times$ be a primitive M-th. root of unity. Consider the algebra $K_\mu(N,\xi)$, generated by elements x and g with relations

$$x^M = \mu(1-g^M), \quad g^N = 1, \quad gx = \xi xg,$$

where $\mu = 0$, if $M = N$, and $\mu \in \{0,1\}$, if $M \neq N$. The formulas

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

determine a Hopf algebra structure in $K_\mu(N,\xi)$. It follows from [**AS2**, Theorem 5.5] that the dimension of $K_\mu(N,\xi)$ is MN. If $M = N$, then $K_\mu(N,\xi) \simeq T(\xi)$, where $T(\xi)$ is the Taft algebra corresponding to ξ.

PROPOSITION 5.3. *Let H be a finite dimensional Hopf algebra. Suppose that $\mathbf{k}(g-h) \neq P_{g,h}$, for some $g,h \in G(H)$. Then H contains a Hopf subalgebra K isomorphic to $K_\mu(N,\xi)$, for some root of unity $\xi \in \mathbf{k}$, and some $\mu \in \{0,1\}$. In particular, if $\dim H$ is free of squares, then H does not contain non-trivial skew primitive elements.* □

Note that $\mathbf{k}(g-h) \neq P_{g,h}$ implies that H is not cosemisimple.

In the pioneering paper [**N**], the author introduces many interesting concepts, including the "bialgebras of type one" and the now called "Nichols algebras" (see Subsection 5.3 below). He approaches a general pointed Hopf algebra by a limit procedure from bialgebras of type one. He discusses several examples; most of them were recently interpreted in [**Gñ4**].

In the papers [**BDG, CD1, CD2, CDR, D**] the authors construct pointed Hopf algebras as iterated Ore extensions; then they determine the isomorphism classes and, in suitable situations, obtain classification results. This is a very simple and elegant method but it does not seem to be applicable to complicated situations.

In the paper [**SvO**], the authors study a projection $H_1 \to H_0$ and interpret it in terms of coalgebra cohomology. This idea is related to the problem of lifting discussed below. They are able to obtain the classification of pointed Hopf algebras of dimension p^3, as said above.

5.3. The lifting method.

5.3.1. *Overview.* The lifting method [**AS2, AS3**] seems to be the most powerful method to understand pointed Hopf algebras up to now. Let us first roughly overview the method in words. We shall then discuss the main tools of the method and illustrate it with some examples. For more details, see [**AS2, AS3, AS4, AS6, AS5, Gñ3, Gñ4**]. The method works in principle for more general Hopf algebras than pointed; it is enough to assume that the coradical is a Hopf subalgebra.

Let A be a Hopf algebra whose coradical $H = A_0$ is a Hopf subalgebra. We attach to A several invariants; a very sensible one is an algebra R which is not a usual Hopf algebra, but a braided Hopf algebra in the braided category ${}^H_H\mathcal{YD}$. If A is finite dimensional, then R also is; in many cases (and conjecturally, always), one is able to classify such R in combinatorial terms. The last step is to recover A from R and H; this is the so-called lifting step. The outcome is, loosely speaking, that finite dimensional pointed Hopf algebras are variations of Frobenius-Lusztig kernels, the finite quantum groups constructed by Lusztig.

Let us describe the invariants of A that we shall consider. Let

$$\operatorname{gr} A = \oplus_{n\geq 0} \operatorname{gr} A(n) \tag{5.1}$$

be the graded vector space associated to the coradical filtration, where $\operatorname{gr} A(n) = A_n/A_{n-1}$, $n > 0$, and $\operatorname{gr} A(0) = A_0 = H$. In general, $\operatorname{gr} A$ is a graded coalgebra [**Sw**, Chapter 11]; but in this situation, it is a graded Hopf algebra because the coradical is a Hopf subalgebra [**Mo1**, 5.2.8]. The graded projection $\pi : \operatorname{gr} A \to \operatorname{gr} A(0) = H$ is a Hopf algebra map and a retraction of the inclusion $\iota : \operatorname{gr} A(0) \to \operatorname{gr} A$. We can then apply the general remarks of Subsection 2.7. Let

$$R = \{a \in \operatorname{gr} A : (\operatorname{id} \otimes \pi)\Delta(a) = a \otimes 1\}$$

be the algebra of coinvariants of π; R is a braided Hopf algebra in the category ${}^H_H\mathcal{YD}$ of Yetter-Drinfeld modules over H and $\operatorname{gr} A$ can be reconstructed from R and H as a bosonization: $\operatorname{gr} A \simeq R\#H$.

In the present case, the braided Hopf algebra has some extra properties. First, R inherits the gradation from $\operatorname{gr} A$: $R = \oplus_{n\geq 0} R(n)$, where $R(n) = \operatorname{gr} A(n) \cap R$, and R is a *graded* braided Hopf algebra; also, $R(0) = \mathbf{k}1$. Second, since we began from the coradical filtration of A, we can conclude that the coradical filtration of R coincides with the filtration given by the gradation:

$$R_n = \oplus_{m\leq n} R(n).$$

The important consequence of this is that $R(1) = P(R)$, the space of primitive elements of R. The reason will be explained in the next Subsection.

5.3.2. *Nichols algebras.* One of the important tools in the Lifting Method is the notion of Nichols algebras. Nichols algebras can be presented in several different ways, all of them relatively technical. We choose one of these ways and then state the main property of Nichols algebras relating them to the Lifting Method.

DEFINITION 5.4. A braided vector space (V, c) is a finite dimensional vector space provided with an isomorphism $c : V \otimes V \to V \otimes V$ which is a solution of the braid equation, that is

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

A Yetter-Drinfeld module is always a braided vector space; however, a braided vector space could be realized as a Yetter-Drinfeld module only when the braiding is *rigid*, see for instance [**T2**]; and if so, it can be realized in many different ways.

Let (V, c) be a braided vector space. The braiding $c : V \otimes V \to V \to \otimes V$ induces representations of the braid groups $\mathbb{B}_n \to \mathrm{Aut}(V^{\otimes n})$. On the other hand, there is a well-known set-theoretical section s from the symmetric group $\mathbb{S}_n$ to $\mathbb{B}_n$. We consider the quantum antisymmetrizer

$$\mathfrak{S}_n := \sum_{\sigma \in \mathbb{S}_n} s(\sigma)$$

as an element of the group algebra $\mathbf{k}\mathbb{B}_n$, and by abuse of notation, as an endomorphism of $V^{\otimes n} = T^n(V)$.

DEFINITION 5.5. The *quantum symmetric algebra* of braided vector space (V, c) is the quotient $\mathfrak{B}(V) := T(V)/\mathcal{J}$, where $\mathcal{J} = \oplus_{n \geq 0} \ker \mathfrak{S}_n$.

If $V \in {}^H_H\mathcal{YD}$, H a Hopf algebra with bijective antipode, then $\mathfrak{B}(V)$ is actually a braided Hopf algebra in ${}^H_H\mathcal{YD}$ called the *Nichols algebra* of V over H.

REMARK 5.6. Nichols algebras apeared first in [**N**], as the invariant part of "bialgebras of type one". Woronowicz rediscovered them in his approach to "quantum differential calculus" [**W2**]. Lusztig used them, in a different language, to present quantum groups in an invariant way: indeed, the algebras $\mathfrak{f}$ in [**L3**] (defined by the non-degeneracy of certain invariant bilinear form) are Nichols algebras of Yetter-Drinfeld modules arising from generalized Cartan matrices. See also [**Ro1, Ro2, Sbg1, Rz, BD**]. Also, the positive parts of the "small quantum groups" of [**L1**], [**L2**]- which we shall call *Frobenius-Lusztig kernels*- are also Nichols algebras [**Mu1, Ro1**]. The presentation via non-degeneracy of the invariant bilinear form always holds [**AG**].

THEOREM 5.7. *(Nichols). Let $V \in {}^H_H\mathcal{YD}$. A braided graded Hopf algebra $T = \oplus_{n\geq 0} T(n)$ with $T(0) = \mathbf{k}1$ is isomorphic to the Nichols algebra of V if and only if $V \simeq T(1)$ in ${}^H_H\mathcal{YD}$ and*

(1) *$P(T) = T(1)$,*
(2) *T is generated as an algebra by $T(1)$.*

PROOF. See [**AG**, Prop. 3.2.12 or Th. 3.2.29]. □

Let us return to the situation of the preceding Subsection, and the corresponding notation A, H, $\operatorname{gr} A$, R. It follows from Theorem 5.7 that the subalgebra R' of R generated by $R(1)$ is isomorphic to the Nichols algebra of V: $R' \simeq \mathfrak{B}(V)$. To summarize, we give a list of invariants of our initial Hopf algebra A:

- The graded braided Hopf algebra R; it is called the *diagram* of H.
- The braided vector space (V, c), where $V := R(1) = P(R)$ and $c : V \otimes V \to V \otimes V$ is the braiding in ${}^H_H\mathcal{YD}$. It will be called the *infinitesimal braiding* of H.
- The dimension of $V = P(R)$, called the *rank* of H, or of R.
- The subalgebra R' of R generated by $R(1)$: $R' \simeq \mathfrak{B}(V)$.

5.3.3. *Description of the method.* Now we can describe the *lifting method* to deal with Hopf algebras whose coradical is a Hopf subalgebra. This method can be used to solve different problems, but we shall restrict our attention to questions of finite dimensionality. Let us fix a finite dimensional Hopf algebra H. To determine all finite dimensional Hopf algebras A with $A_0 \simeq H$ as Hopf algebras, then we have to address the following steps.

(a). Determine when $\mathfrak{B}(V)$ is finite dimensional, for all braided vector spaces (V, c) in a suitable class.

(b). For those V as in (a), find in how many ways, if any, they can be realized as Yetter-Drinfeld modules over H.

For instance, if $R = \mathbf{k}[x]/(x^N)$ as in Example 2.13 with a fixed q determining the braiding, then it can be realized over $H = \mathbf{k}\Gamma$ whenever there exist $g \in Z(\Gamma)$ and χ a one-dimensional representation of Γ such that $\chi(g) =: q$.

(c). For $\mathfrak{B}(V)$ as in (a), compute all Hopf algebras A such that $\operatorname{gr} A \simeq \mathfrak{B}(V)\#H$ ("lifting").

(d). Investigate whether any *finite dimensional* graded braided Hopf algebra $R = \oplus_{n\geq 0} R(n)$ in ${}^H_H\mathcal{YD}$ satisfying $R(0) = \mathbf{k}1$ and $P(R) = R(1)$, is generated by its primitive elements, *i. e.* is a Nichols algebra.

In the next Subsections, we shall discuss the meaning and difficulty of these steps.

5.3.4. *The pointed case.* We shall assume in the rest of this Section that $H = \mathbf{k}\Gamma$ is a group algebra. We shall consider suitable clases of braided vector spaces; to justify this, let us recall the classification of all finite dimensional Yetter-Drinfeld modules over a finite group.

Let us first treat the case of a finite abelian group Γ. If $V \in {}^\Gamma_\Gamma\mathcal{YD}$ is finite dimensional, then the action of Γ is diagonalizable. Therefore,

$$V = \oplus_{g\in\Gamma, \chi\in\widehat{\Gamma}} V_g^\chi, \tag{5.2}$$

where $V^\chi = \{v \in V : g.v = \chi(g)v\}$, $V_g = \{v \in V : \delta(v) = g \otimes v\}$ and $V_g^\chi = V^\chi \cap V_g$. Conversely, any vector space with a decomposition (5.2) is a Yetter-Drinfeld module over Γ. The braiding is given by $c(v \otimes w) = \chi(g)w \otimes v$, $v \in V_g$, $w \in V^\chi$. In other words, there exists a basis $x_1, \dots, x_\theta$ of V and $g(1), \dots, g(\theta) \in \Gamma$, $\chi(1), \dots, \chi(\theta) \in \widehat{\Gamma}$ such that $x_i \in V_{g_i}^{\chi_i}$, $1 \leq i \leq \theta$; and then $c(x_i \otimes x_j) = \chi_i(g_i)x_j \otimes x_i$, $1 \leq i, j \leq \theta$.

Let us now treat the case of a finite non-abelian group Γ. The irreducible Hopf bimodules over Γ were classified in [**DPR, Ci**]. By Remark 2.10, the classification of irreducible Yetter-Drinfeld modules follows; this was also done in [**Wi1**]. In the notation of [**AG**], we have:

Let $g \in \Gamma$ and let $\rho : \Gamma^g \to \operatorname{End} V$ be an irreducible representation of the isotropy subgroup Γ^g, that is, the centralizer of g in Γ. Let W be the space of the induced representation of ρ. If one fixes a set of elements $h_1, \dots, h_s$ such that $(h_i g h_i^{-1})_{1 \le i \le s}$ is a numeration of the conjugacy class $\mathcal{O}_g$, then as a vector space

$$W = \oplus_{1 \le i \le s} h_i \otimes V.$$

There is a Yetter-Drinfeld module structure on W given by

$$\delta(h_i \otimes v) = h_i g h_i^{-1} \otimes h_i \otimes v, \tag{5.3}$$

$$x.(h_i \otimes v) = h_j \otimes \rho(t)(v), \qquad \text{if } xh_i = h_j t, t \in \Gamma^g. \tag{5.4}$$

Indeed, $xh_i g h_i^{-1} x^{-1}$ is of the form $h_j g h_j^{-1}$ for a unique j in $\{1, \dots, s\}$, and then there exists a unique $t \in \Gamma^g$ such that $xh_i = h_j t$.

This Yetter-Drinfeld module will be denoted $M(g, \rho)$; it is not difficult to see that it is irreducible.

If we fix a class $(g)_{g \in \mathcal{C}}$ of representants of conjugacy classes of Γ, and for each of them a class of representants $\widehat{\Gamma^g}$ of irreducible representations, then the Yetter-Drinfeld modules $M(g, \rho)$, $g \in \mathcal{C}$, $\rho \in \widehat{\Gamma^g}$, are pairwise non-isomorphic; and these are all the irreducible Yetter-Drinfeld modules over Γ.

Definition 5.8. We shall say that a braided vector space (V, c) is of *group type* if there exists a basis $x_1, \dots, x_\theta$ of V such that

$$c(x_i \otimes x_j) = g_i(x_j) \otimes x_i; \tag{5.5}$$

necessarily $g_i \in GL(V)$. Notice that $V \in {}^G_G\mathcal{YD}$, where G is the subgroup of $GL(V)$ generated by $g_1, \dots, g_\theta$.

Furthermore, we shall say that (V, c) is of *finite group type* (resp., of *abelian group type*) if G is finite (resp. abelian).

We shall say that (V, c) is of *diagonal type* if V has a basis $x_1, \dots, x_\theta$ such that

$$c(x_i \otimes x_j) = q_{ij}(x_j \otimes x_i), \tag{5.6}$$

for some q_{ij} in $\mathbf{k}$.

The suitable class related to pointed Hopf algebras is that of braided vector spaces of group type. Let us first concentrate in the case when Γ is a finite abelian group; so, we focus on braided vector spaces of finite abelian group type; clearly, they are of diagonal type. The first fundamental question in the classification program of finite dimensional pointed Hopf algebras with abelian coradical is then the following:

Question 5.9. Given a matrix $(q_{ij})_{1 \le i,j \le \theta}$ whose entries are roots of 1, when $\mathfrak{B}(V)$ is finite dimensional, where V is a vector space with basis $x_1, \dots, x_\theta$ and braiding (5.6)? If so, compute $\dim \mathfrak{B}(V)$, and give a "nice" presentation by generators and relations.

The meaning of "nice" will be clarified later. We shall give several criteria answering partially Question 5.9.

Let us keep the notation q_{ij}, V as above. We shall denote $N_i = \operatorname{ord} q_{ii}$. If W is a vector subspace of V spanned by some subset of $x_1, \dots, x_\theta$, then W is a braided vector space itself, and $\mathfrak{B}(W)$ can be identified with the subalgebra of $\mathfrak{B}(V)$ generated by W (use Theorem 5.7). Moreover, $\dim \mathfrak{B}(W)$ divides $\dim \mathfrak{B}(V)$ by Theorem 3.3.

If $V = \mathbf{k}x$ is a one-dimensional braided vector space, say with $c(x \otimes x) = qx$, then $\mathfrak{B}(V) \simeq \mathbf{k}[X]$, the polynomial algebra in one variable, when $q = 1$; or else $\mathfrak{B}(V) \simeq \mathbf{k}[X]/(X^N)$ where N is the order of q, when $N > 1$. The first criteria follows easily:

Remark 5.10. If $\dim \mathfrak{B}(V)$ is finite, then

$$q_{ii} \neq 1, \quad 1 \leq i \leq \theta. \tag{5.7}$$

The analysis of the following family of examples gives already several interesting consequences.

Definition 5.11. Assume that 5.7 holds. We shall say that $\mathfrak{B}(V)$ is a *quantum linear space* if

$$q_{ij} q_{ji} = 1, \quad 1 \leq i \neq j \leq \theta. \tag{5.8}$$

Let us see how the Lifting Method works in the case of quantum linear spaces.

Lemma 5.12. [**AS2**] *Let V be a braided vector space of diagonal type, with braiding given by a matrix $(q_{ij})_{1 \leq i,j \leq \theta}$ whose entries are roots of 1. Assume that 5.7 holds.*

(a). $\dim \mathfrak{B}(V) \geq \prod_{1 \leq i \leq \theta} N_i$; the equality holds if and only if $\mathfrak{B}(V)$ is a quantum linear space.

(b). If $\mathfrak{B}(V)$ is a quantum linear space, then it is isomorphic to the algebra presented by generators $x_1, \dots, x_\theta$ with relations

$$x_i^{N_i} = 0, \quad 1 \leq i \leq \theta, \tag{5.9}$$

$$x_i x_j = q_{ij} x_j x_i, \quad 1 \leq i < j \leq \theta. \tag{5.10}$$

□

We now illustrate step (b) of the lifting Method in the setting of quantum linear spaces. Let Γ be a finite abelian group. Let $\theta(\Gamma)$ be the greatest integer θ such that Γ admits a quantum linear space of rank θ. To compute $\theta(\Gamma)$ and the classification quantum linear spaces over Γ, are subtle combinatorial questions. For instance, $\theta(\Gamma) = 2$ if Γ is a cyclic p-group, where p is an odd prime; and $\theta(\Gamma \times \widetilde{\Gamma}) = \theta(\Gamma) + \theta(\widetilde{\Gamma})$ if the orders of Γ and $\widetilde{\Gamma}$ are relatively prime. See [**AS2**]. However, $\theta(\mathbb{Z}/2) = \infty$.

We shall describe now all possible finite dimensional pointed Hopf algebras with abelian coradical whose diagram is a quantum linear space.

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, $1 \leq \ell \leq \sigma$.

A compatible datum of quantum linear space $\mathcal{D}$ for Γ consists of families $g_1, \dots, g_\theta \in \Gamma$, $\chi_1, \dots, \chi_\theta \in \widehat{\Gamma}$, $\mu_1, \dots, \mu_\theta \in \{0, 1\}$, $\lambda_{ij} \in \mathbf{k}$, $1 \le i < j \le \theta$ such that (5.7), (5.8) hold for $q_{ij} := \chi_j(g_i)$ and

(5.11) μ_i is arbitrary if $g_i^{N_i} \neq 1$ and $\chi_i^{N_i} = 1$ but 0 otherwise;

(5.12) λ_{ij} is arbitrary if $g_i g_j \neq 1$ and $\chi_i \chi_j = 1$ but 0 otherwise.

THEOREM 5.13. [**AS2**, Th. 5.5]. *Let A be a pointed finite dimensional Hopf algebra with coradical $H = k(\Gamma)$, where Γ is an abelian group as above. We assume that the diagram of A is a quantum linear space.*

Then there exists a compatible datum of quantum linear space $\mathcal{D}$ such that A is isomorphic to as Hopf algebra to the algebra presented by generators h_ℓ, $1 \le \ell \le \sigma$, and a_i, $1 \le i \le \theta$ with defining relations

(5.13) $h_\ell^{M_\ell} = 1, \quad 1 \le \ell \le \sigma;$

(5.14) $h_\ell h_t = h_t h_\ell, \quad 1 \le t < \ell \le \sigma;$

(5.15) $a_i h_\ell = \chi_i^{-1}(y_\ell) h_\ell a_i, \quad 1 \le \ell \le \sigma, \quad 1 \le i \le \theta;$

(5.16) $a_i^{N_i} = \mu_i \left(1 - g_i^{N_i}\right), \quad 1 \le i \le \theta;$

(5.17) $a_j a_i = \chi_i(g_j) a_i a_j + \lambda_{ij}(1 - g_i g_j), \quad 1 \le i < j \le \theta;$

and where the Hopf algebra structure is determined by

(5.18) $\Delta(h_\ell) = h_\ell \otimes h_\ell, \quad 1 \le \ell \le \sigma;$

(5.19) $\Delta(a_i) = a_i \otimes 1 + g_i \otimes a_i, \quad 1 \le i \le \theta.$

Conversely, given a compatible datum of quantum linear space $\mathcal{D}$, the algebra $\mathcal{A}(\mathcal{D})$ presented by generators h_ℓ, $1 \le \ell \le \sigma$, and a_i, $1 \le i \le \theta$ with defining relations (5.13), (5.14), (5.15), (5.16) *and* (5.17) *has a unique Hopf algebra structure determined by* (5.18) *and* (5.19). *It is pointed; $G(\mathcal{A}(\mathcal{D})) \simeq \Gamma$ and*

$$\dim \mathcal{A}(\mathcal{D}) = |\Gamma| \prod_{1 \le i \le \theta} N_i.$$

□

REMARK 5.14. The meaning of this formulas is as follows: (5.13), (5.14) and (5.18) are responsible of the group Γ. The families $g_1, \dots, g_\theta \in \Gamma$, $\chi_1, \dots, \chi_\theta \in \widehat{\Gamma}$ define a Yetter-Drinfeld module structure over Γ on the braided vector space (V, c) with basis $x_1, \dots, x_\theta$, by

$$\delta(x_i) = g_i \otimes x_i, \qquad h.x_i = \chi_i(h) x_i.$$

Then (5.15) and (5.19) reflect (2.7) and (2.8). Finally, (5.16) and (5.17) are the "lifting" of the formulas (5.9) and (5.10). This illustrates what we mean by "nice" relations; (5.9) and (5.10) are nice because we can lift them.

REMARK 5.15. The definition of compatible datum of quantum linear space and the preceding Theorem can be extended to non-abelian finite groups by requiring the elements $g_1, \dots, g_\theta$ to be central.

REMARK 5.16. Given two compatible data $\mathcal{D}$ and $\mathcal{D}'$ for groups Γ and Γ' respectively, a Hopf algebra isomorphism $A(\mathcal{D}) \to A(\mathcal{D}')$ induces, first, an isomorphism of the groups Γ and Γ'; and second, sends skew-primitive elements to skew-primitive elements. The presence of the relations (5.16) and (5.17) imposes further conditions; this gives rise to constructions of infinite families of non-isomorphic pointed Hopf algebras of the same dimension, in particular of dimension p^4 [**AS2**]. For more on the isomorphism problem, see [**AS3, AS4, Be**].

REMARK 5.17. The basic hypothesis of Theorem 5.13 is that the diagram of A is a quantum linear space. This hypothesis is very restricted and contains the fact that R is generated in degree 1; with tricky but elementary arguments we can also show that R is generated in degree one in some restricted situations, *e. g.* when $\dim R(1) = 1$. To go on, we need more powerful ideas, that will be explained in the next Subsection.

5.3.5. *Braidings of Cartan type.* Let (V, c) be a braided vector space of diagonal type, with a basis $x_1, \dots, x_\theta$ such that (5.6) holds, where the q_{ij}'s are roots of 1. Clearly, the matrix (q_{ij}) determines such a braided vector space (up to a permutation of the index set).

DEFINITION 5.18. We shall say that (V, c) is *of Cartan type* if for all i, j, $q_{ii} \neq 1$ and there exists $a_{ij} \in \mathbb{Z}$ such that

$$q_{ij} q_{ji} = q_{ii}^{a_{ij}}. \tag{5.20}$$

The integers a_{ij} are uniquely determined when chosen in the following way:

(5.21) $a_{ii} = 2$;

(5.22) $-\operatorname{ord} q_{ii} < a_{ij} \leq 0, \quad i \neq j.$

It follows that (a_{ij}) is a generalized Cartan matrix (GCM) in the sense of the book [**K**]. We shall adapt the terminology from generalized Cartan matrices and Dynkin diagrams to braidings of Cartan type. For instance, we shall say that (V, c) is of *finite Cartan type* if it is of Cartan type and the corresponding GCM is actually of finite type, *i. e.* a Cartan matrix associated to a finite dimensional semisimple Lie algebra. We shall say that a Yetter-Drinfeld module V is *of Cartan type* (resp., connected, ...) if the matrix (q_{ij}) as above is of Cartan type (resp., connected, ...).

Let (a_{ij}) be a Cartan matrix. Let $\mathcal{X}$ be the set of connected components of the Dynkin diagram corresponding to it. For each $I \in \mathcal{X}$, we let $\mathfrak{g}_I$ be the Kac-Moody Lie algebra corresponding to the generalized Cartan matrix $(a_{ij})_{i,j\in I}$ and $\mathfrak{n}_I$ be the Lie subalgebra of $\mathfrak{g}_I$ spanned by all its positive roots. We omit the subindex I when $I = \{1, \dots, \theta\}$.

The fundamental examples of braidings of Cartan type are given as follows. Let $(a_{ij})_{1\leq i,j\leq \theta}$ be a generalized Cartan matrix; assume that it is *symmetrizable*, *i. e.* that there exists positive integers $d_1, \dots, d_\theta$ such that $d_i a_{ij} = d_j a_{ji}$ for all i, j. Let $q \neq 1$ be a root of unity of order N and let $q_{ij} := q^{d_i a_{ij}}$, $1 \leq i, j \leq \theta$. Let $(\mathbb{V}, c)$ denote the corresponding braided vector space with a basis $X_1, \dots, X_\theta$.

To state the following important Theorem, we need first to discuss a delicate notion. Recall the definition of braided commutator (2.9). Lusztig defined root vectors $X_\alpha \in \mathfrak{B}(\mathbb{V})$, $\alpha \in \Phi^+$ [**L2**]. One can see from [**L3**] that, up to a non-zero scalar, each root vector can be written as an iterated braided commutator in some sequence $X_{\ell_1}, \dots, X_{\ell_a}$ of simple root vectors such as $[[X_{\ell_1}, [X_{\ell_2}, X_{\ell_3}]_c]_c, [X_{\ell_4}, X_{\ell_5}]_c]_c$. See also [**Ri**]. We now fix for each $\alpha \in \Phi^+$ such a representation of X_α as an iterated braided commutator. For a general braided vector space (V, c) of finite Cartan type, we define root vectors x_α in the tensor algebra $T(V)$, $\alpha \in \Phi^+$, as the same formal iteration of braided commutators in the elements $x_1, \dots, x_\theta$ instead of $X_1, \dots, X_\theta$ but with respect to the braiding c given by the general matrix (q_{ij}).

THEOREM 5.19. [**L1, L2, L3, Ro1, Mu1**]. *The algebra $\mathfrak{B}(\mathbb{V})$ is finite dimensional if and only if (a_{ij}) is a finite Cartan matrix.*

If this happens, then $\mathfrak{B}(\mathbb{V})$ can be presented by generators X_i, $1 \le i \le \theta$, and relations

$$\mathrm{ad}_c(X_i)^{1-a_{ij}}(X_j) = 0, \qquad i \ne j, \tag{5.23}$$

$$X_\alpha^N = 0, \qquad \alpha \in \Phi^+. \tag{5.24}$$

Moreover, the following elements constitute a basis of $\mathfrak{B}(\mathbb{V})$:

$$X_{\beta_1}^{h_1} X_{\beta_2}^{h_2} \dots X_{\beta_P}^{h_P}, \qquad 0 \le h_j \le N-1, \quad 1 \le j \le P.$$

In particular,

$$\dim \mathfrak{B}(\mathbb{V}) = N^{\dim \mathfrak{n}}.$$

□

The basis and dimension statements of this Theorem are due to Lusztig, in the setting of the now called Frobenius-Lusztig kernels. Rosso and Müller showed that Frobenius-Lusztig kernels are Nichols algebras.

REMARK 5.20. The definition of braided vector space of Cartan type is also valid for braided vector spaces of diagonal type with general q_{ij} (not necessarily roots of 1). Also, there is a braided vector space $(\mathbb{V}, c)$ attached to q general, (not necessarily a root of 1); when q is not a root of 1, $\mathfrak{B}(\mathbb{V})$ is the $+$-part of the quantized enveloping algebra of the Lie algebra $\mathfrak{g}$ [**L3, Ro1, Ro2**].

Theorem 5.19 motivates the following definition.

DEFINITION 5.21. Let (V, c) be a braided vector space of Cartan type with associated Cartan matrix (a_{ij}) as in (5.21), (5.22). We say that (V, c) is of *FL-type* if there exists positive integers $d_1, \dots, d_\theta$ such that for all i, j,

(5.25) $d_i a_{ij} = d_j a_{ji}$hence (a_{ij}) is symmetrizable;

(5.26) There exists $q \in \mathbf{k}$ such that $q_{ij} = q^{d_i a_{ij}}$.

Furthermore, we shall say that (V, c) is *locally of FL-type* if for any subset $I \subset \{1, \dots, \theta\}$ of cardinal 2, the submatrix $(q_{ij})_{i,j \in I}$ gives a braiding of FL-type.

The following result follows from Theorem 5.19 in combination with the twisting operation, see Subsection 2.4.

THEOREM 5.22. [**AS3, AS5**]. *Let (V, c) be a braided vector space of Cartan type. We also assume that q_{ij} has odd order for all i, j.*

(i). Assume that (V, c) is locally of FL-type and that, for all i, the order of q_{ii} is relatively prime to 3 whenever $a_{ij} = -3$ for some j, and is different from 3, 5, 7, 11, 13, 17. If $\mathfrak{B}(V)$ is finite dimensional, then (V, c) is of finite Cartan type.

(ii). If (V, c) is of finite Cartan type, then $\mathfrak{B}(V)$ is finite dimensional, and if moreover 3 does not divide the order of q_{ii} for all i in a connected component of the Dynkin diagram of type G_2, then

$$\dim \mathfrak{B}(V) = \prod_{I \in \mathcal{X}} N_I^{\dim \mathfrak{n}_I},$$

where $N_I = \operatorname{ord}(q_{ii})$ for all $i \in I$ and $I \in \mathcal{X}$. The Nichols algebra $\mathfrak{B}(V)$ is presented by generators x_i, $1 \leq i \leq \theta$, and relations

$$\operatorname{ad}_c(x_i)^{1-a_{ij}}(x_j) = 0, \qquad i \neq j, \tag{5.27}$$

$$x_\alpha^{N_I} = 0, \qquad \alpha \in \Phi_I^+, I \in \mathcal{X}. \tag{5.28}$$

Moreover, the following elements constitute a basis of $\mathfrak{B}(V)$:

$$x_{\beta_1}^{h_1} x_{\beta_2}^{h_2} \dots x_{\beta_P}^{h_P}, \qquad 0 \leq h_j \leq N_I - 1, \text{ if } \beta_j \in I, \quad 1 \leq j \leq P.$$

□

There is a large class of finite abelian groups where the preceding result allows to answer completely step (a).

COROLLARY 5.23. [**AS3**]. *Let p be an odd prime number, Γ a finite direct sum of copies of $\mathbb{Z}/(p)$ and V a finite dimensional Yetter-Drinfeld module over Γ. We assume that $q_{ii} \neq 1$ for all i. Then (V, c) is of Cartan type and*

(i). If V is of finite Cartan type, then $\mathfrak{B}(V)$ is finite dimensional, and

$$\dim \mathfrak{B}(V) = p^M,$$

where $M = \sum_{I \in \mathcal{X}} \dim \mathfrak{n}_I$ is the number of positive roots of the root system of (a_{ij}).

(ii). If $\mathfrak{B}(V)$ is finite dimensional and $p > 17$, then V is of finite type. □

5.3.6. *Yetter-Drinfeld modules of Cartan type over a fixed abelian group.* Let us now address step (b) of the lifting method in the setting of Theorem 5.22. This means, to determine which braidings of finite Cartan type actually appear over a general finite abelian group Γ. This reduces, for each fixed finite Cartan matrix $(a_{ij}) \in \mathbb{Z}^{\theta \times \theta}$, to find all the sequences $g(1), \dots, g(\theta) \in \Gamma$, $\chi(1), \dots, \chi(\theta) \in \widehat{\Gamma}$ such that

(5.29) $\langle \chi(i), g(i) \rangle \neq 1, \quad$ for all i;

(5.30) $\langle \chi(j), g(i) \rangle \langle \chi(i), g(j) \rangle = \langle \chi(i), g(i) \rangle^{a_{ij}}, \quad$ for all i, j.

This can be interpreted as a problem of computational number theory: to compute all the solutions of a system of quadratic congruences. See [**AS3**, Section 8] for a discussion. This author feels that a compact answer to such question is out of reach; however, for each fixed finite abelian group, the computation could be performed. In this sense, it is worth mentioning the following consequence of Theorem 5.19, due to M. Graña.

PROPOSITION 5.24. [**Gñ4**] *Let Γ be a finite group of odd order. Then there are only finitely many isomorphisms classes of Yetter-Drinfeld modules V such that $\mathfrak{B}(V)$ has finite dimension.*

PROOF. Let us assume for simplicity that Γ is abelian. Assume that 3 is relatively prime to the order of Γ. Let V be a Yetter-Drinfeld module with a basis $x_1, \dots, x_\theta$ with $x_i \in V_{g_i}^{\chi_i}$ for all i. Suppose that $\mathfrak{B}(V)$ has finite dimension. We claim the following more specific result:

There is no $i \neq j$ such that $g_i = g_j$ and $\chi_i = \chi_j$.

For, if such i and j, the Yetter-Drinfeld submodule W generated by x_i and x_j has diagonal braiding with matrix

$$\begin{pmatrix} q & q \\ q & q \end{pmatrix},$$

where $q = \chi_i(g_i)$. But this braiding is of Cartan type, with generalized Cartan matrix

$$\begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix},$$

i. e. of type $A_1^{(1)}$; thus $\mathfrak{B}(W)$ has infinite dimension. If 3 divides the order of Γ, then one proves similarly that there is no i, j, k all different such that $g_i = g_j = g_k$ and $\chi_i = \chi_j = \chi_k$. The argument for Γ non-abelian uses also the same idea. $\square$

Let $\Gamma \simeq \mathbb{Z}/(p)$, where p is an odd prime number. Then the determination of all Yetter-Drinfeld modules over Γ with braiding of finite Cartan type is given in [**AS3**, Theorem 1.3]. We shall not repeat the list here, but instead we discuss the following case.

LEMMA 5.25. *There exists a Nichols algebra with Dynkin diagram G_2 if and only if $p \equiv 1 \mod 3$.*

PROOF. If V is a Yetter-Drinfeld module of dimension 2 with a braiding of Cartan type G_2, then there exists a generator u of Γ, $q \in k^\times$ of order p and integers b, d such that

$$g(1) = u, \quad g(2) = u^b, \quad \langle \chi(1), u \rangle = q, \quad \langle \chi(2), u \rangle = q^d.$$

So $b_{11} = q, \quad b_{22} = q^{bd}$. By definition of the Cartan matrix associated to a braiding, we have $p > 3$. We should have

$$\langle \chi(1), g(2) \rangle \langle \chi(2), g(1) \rangle = b_{11}^{-1} = b_{22}^{-3}.$$

This means $b + d \equiv -1 \equiv -3bd \mod p$. Thus $3b^2 + 3b + 1 \equiv 0 \mod p$ and looking at the discriminant of this equation we see that it has a solution if and only if -3 is a square $\mod p$. By the quadratic reciprocity law, this happens exactly when $p \equiv 1 \mod 3$. $\square$

5.3.7. *Liftings.* We now discuss the step (c) of the lifting method for pointed Hopf algebras whose diagram is a Nichols algebra of Cartan type.

Let $\Gamma = \langle y_1 \rangle \oplus \cdots \oplus \langle y_\sigma \rangle$ be a finite abelian group; we denote by M_ℓ the order of y_ℓ, $1 \le \ell \le \sigma$. Let A be a pointed Hopf algebra with $G(A) \simeq \Gamma$ and whose diagram $R \simeq \mathfrak{B}V$, with V of finite Cartan type; say as usual with a basis $x_1, \dots, x_\theta$, $x_i \in V_{g_i}^{\chi_i}$ for all i, and with Cartan matrix (a_{ij}). Then Theorem 5.22 and formulas (2.7) imply that $\operatorname{gr} A$ can be presented by generators h_ℓ, $1 \le \ell \le \sigma$, and x_i, $1 \le i \le \theta$ with defining relations (5.13), (5.14), (5.15) (with x_i instead of a_i), (5.27) and (5.28). We can then lift the generators h_ℓ to group-like elements with the same name (by abuse of notation), and the generators x_i to elements $a_i \in \mathcal{P}_{g_i,1}^{\chi_i}$; this choice guarantees that relations (5.13), (5.14) and (5.15) hold now in A. It is not difficult to see that the elements h_ℓ, $1 \le \ell \le \sigma$, and a_i, $1 \le i \le \theta$ are now generators of the algebra A. It remains to see what happens with the relations (5.27) and (5.28). We split this in three cases:

- lifting of the "quantum Serre relations" $x_j x_i - \chi_i(g_j) x_i x_j = 0$, when $i \neq j$ live in different components of the Dynkin diagram;
- lifting of the "quantum Serre relations" $\operatorname{ad}_c(x_i)^{1-a_{ij}}(x_j) = 0$, when $i \neq j$ live in the same component of the Dynkin diagram;
- lifting of the "power of root vectors relations" $x_\alpha^{N_I} = 0$, α a root.

In the first case, a straightforward computation shows that $a_j a_i - \chi_i(g_j) a_i a_j$ is again a skew-primitive. It can be then shown that

$$a_j a_i = \chi_i(g_j) a_i a_j + \lambda_{ij}(1 - g_i g_j),$$

where λ_{ij} satisfies (5.12). To deal with this, we introduce the following notion.

DEFINITION 5.26. We say that two vertices i and j *are linkable* (or that i *is linkable to* j) if

(5.31) $i \not\sim j$,

(5.32) $g_i g_j \neq 1$ and

(5.33) $\chi_i \chi_j = 1$.

These are the first elementary properties related to this notion.

(5.34) If i is linkable to j, then $\chi_i(g_j)\chi_j(g_i) = 1, \quad \chi_j(g_j) = \chi_i(g_i)^{-1}$

(5.35) If i and k, resp. j and ℓ, are linkable. Then $a_{ij} = a_{k\ell}$, $a_{ji} = a_{\ell k}$.

(5.36) A vertex i can not be linkable to two different vertices j and h.

A *linking datum* is a collection $(\lambda_{ij})_{1 \le i < j \le \theta, i \not\sim j}$ of elements in $\mathbf{k}$ such that λ_{ij} is arbitrary if i and j are linkable but 0 otherwise. Given a linking datum, we say that two vertices i and j *are linked* if $\lambda_{ij} \neq 0$.

We shall use this Definition in Theorem 5.38 below. For the second case, we can offer the following:

THEOREM 5.27. [**AS5**, Theorem 6.8]. *Let $I \in \mathcal{X}$. Assume that $N_I \neq 3$. If I is of type B_n, C_n or F_4, resp. G_2, assume further that $N_I \neq 5$, resp. $N_I \neq 7$. Then the quantum Serre relations hold for all $i \neq j \in I$.* □

QUESTION 5.28. What happens in the low cases excluded in the hypothesis of Theorem 5.27?

The third case is the most complicated. First, if the root α is simple, say corresponding to a vertex i, then an easy computation shows that $a_i^{N_i}$ is again a skew-primitive. It can be then shown that

$$a_i^{N_i} = \mu_i \left(1 - g_i^{N_i}\right), \tag{5.37}$$

where μ_i satisfies (5.11). Now, if the root α is *not* simple then $a_i^{N_i}$ is not necessarily a skew-primitive, but a skew-primitive "modulo root vectors of shorter lenght".

EXAMPLE 5.29. We consider the case when the Dynkin diagram has type A_2. That is, let $g_1, g_2 \in \Gamma$, $\chi_1, \chi_2 \in \widehat{\Gamma}$ such that

$$q = \chi_1(g_1) = \chi_2(g_2), \quad \chi_1(g_2)\chi_2(g_1) = q^{-1}, \tag{5.38}$$

where $q \in \mathbf{k}$ is a primitive p-th root of unity, $p > 1$ an odd integer. Let $V := \mathbf{k}x_1 + \mathbf{k}x_2$ be a Yetter-Drinfeld module over Γ with $x_i \in V_{g_i}^{\chi_i}$, $i = 1, 2$. In $\mathfrak{B}(V)$, we define a non-simple root vector by

$$x_{1,2} = x_1 x_2 - \chi_2(g_1) x_2 x_1.$$

Then $\Delta(x_{1,2}) = g_1 g_2 \otimes x_{1,2} + x_{1,2} \otimes 1 + (1 - q^{-1}) x_1 g_2 \otimes x_2$, and using the quantum Serre relations, one can prove that

$$\Delta(x_{1,2}^p) = g_1^p g_2^p \otimes x_{1,2}^p + x_{1,2}^p \otimes 1 + (q-1)^p \chi_1(g_2)^{\frac{p(p-1)}{2}} x_1^p g_2^p \otimes x_2^p.$$

Let A be a pointed Hopf algebra such that $G(A) \simeq \Gamma$ and the diagram R of A is isomorphic to $\mathfrak{B}(V)$. As before, we lift $x_1, x_2 \in \operatorname{gr} A$ to $a_1, a_2 \in A$ such that $x_i \in \mathcal{P}(A)_{g_i}^{\chi_i}$, $i = 1, 2$. As we said, there exist $\mu_1, \mu_2 \in \{0, 1\}$ satisfying (5.11) (with $N_1 = N_2 = p$) such that (5.37) holds.

Let $a_{1,2} = a_1 a_2 - \chi_2(g_1) a_2 a_1$. It is possible to show that there exists $\lambda \in \mathbf{k}$ such that

$$a_{1,2}^p - \mu_1 \mu_2 (q-1)^p (1 - g_2^p) + \lambda (1 - g_1^p g_2^p), \tag{5.39}$$

where λ can be chosen in the following way:

$$\lambda = 0, \text{ if } g_1^p g_2^p = 1 \quad \text{or} \quad \chi_1^p \chi_2^p \neq \varepsilon. \tag{5.40}$$

THEOREM 5.30. [**AS4**]. *Let A be a pointed Hopf algebra such that $G(A) \simeq \Gamma$ and the diagram R of A is isomorphic to $\mathfrak{B}(V)$ with V as above of type A_2. Then A can be presented by generators h_ℓ, $1 \leq \ell \leq \sigma$, and a_i, $1 \leq i \leq 2$ and relations* (5.13), (5.14), (5.15) (5.37) *and* (5.39)*;*

An algebra presented by generators h_ℓ, $1 \leq \ell \leq \sigma$, and a_i, $1 \leq i \leq 2$ and relations (5.13), (5.14), (5.15) (5.37) *and* (5.39)*, where $\mu_1, \mu_2 \in \{0, 1\}$ satisfy* (5.11) *and $\lambda \in \mathbf{k}$ satisfy* (5.40)*, is a pointed Hopf algebra of dimension* $\operatorname{ord}\Gamma\, p^3$. □

That is, we have a complete answer when the type is A_2. The general case presents a delicate combinatorial question. See also [**AS6**].

5.3.8. *Generation in degree one.* Let us now discuss step (d) of the Lifting method. More generally, let H be any Hopf algebra with bijective antipode and let $R = \oplus_{n \geq 0} R(n)$ be a graded braided Hopf algebra in ${}^H_H\mathcal{YD}$ such that

- $R(0) = \mathbf{k}1$ and

- $P(R) = R(1)$.

QUESTION 5.31. When R is generated as an algebra by its primitive elements, *i. e.* is a Nichols algebra?

There is a dual version of this problem. Let $S = \oplus_{n\geq 0} S(n)$ be a graded braided Hopf algebra in ${}^H_H\mathcal{YD}$ such that

- $S(0) = \mathbf{k}1$ and
- S is generated as an algebra by $S(1)$.

QUESTION 5.32. When $P(S) = S(1)$, *i. e.* S is a Nichols algebra?

Both questions are equivalent in the category of graded braided Hopf algebras, whose homogeneous components are finite dimensional. Indeed, if $R = \oplus_{n\geq 0} R(n)$ is such a Hopf algebra and $S = \oplus_{n\geq 0} S(n)$ is its graded dual, that is $S(n) = R(n)^*$ for all n, then the answer to Question 5.31 for R is yes if and only if the answer to Question 5.32 for S is yes. See *e. g.* [**AS3**, Lemma 5.5].

EXAMPLE 5.33. Question 5.32 has a negative answer over a field $\mathbf{F}$ of positive characteristic p. For, let $S = \mathbf{F}[X]$; this a (usual) Hopf algebra when X is required to be primitive. But X^{p^j} are also primitive for all j. Finite dimensional counterexamples are the quotients $\mathbf{F}[X]/(X^{p^j})$, $j \geq 2$.

More general counterexamples arise by considering the infinitesimal or Frobenius kernels of powers of the Frobenius homomorphism of an algebraic group; the preceding are just those related to the affine group of dimension one.

EXAMPLE 5.34. Question 5.32 has a negative answer over $\mathbf{k}$, but the counterexamples are infinite dimensional. For, let q be a primitive root of unity of odd order p. Let $H = \mathbf{k}\mathbb{Z}$; say g is a generator of $\mathbb{Z}$. Let $S = \mathbf{k}[X]$; this a braided Hopf algebra in ${}^H_H\mathcal{YD}$ with $\delta(X) = g \otimes X$, $g.X = qX$, and X is required to be primitive. But using the quantum binomial formula, X^p is also primitive.

More general counterexamples arise by considering the "positive" parts of quantized enveloping algebras at roots of one [**L1, L2**].

We are not aware of any counterexample to Question 5.31 over $\mathbf{k}$, when both H and R are finite dimensional. In the case when H is a group algebra, a positive answer to Question 5.31, or to Question 5.32, in this setting is equivalent to a positive answer to the following:

CONJECTURE 5.35. [**AS3**]. *Any pointed finite dimensional Hopf algebra over* $\mathbf{k}$ *is generated by group-like and skew-primitive elements.*

A strong indication that the conjecture is true is given by:

THEOREM 5.36. [**AS5**]. *Let A be a finite-dimensional pointed Hopf algebra with coradical* $\mathbf{k}\Gamma$, *and let R be the diagram of A, that is*

$$\operatorname{gr} \mathcal{A} \simeq R\#\mathbf{k}\Gamma,$$

and $R = \oplus_{n\geq 0} R(n)$ *is a graded braided Hopf algebra in* ${}^\Gamma_\Gamma\mathcal{YD}$ *with* $R(0) = \mathbf{k}1$, $R(1) = \mathcal{P}(R)$.

Assume that $R(1)$ is a Yetter-Drinfeld module of finite Cartan type with braiding $(b_{ij})_{1\le i,j\le\theta}$. For all i, let $q_i = b_{ii}$, $N_i = ord(q_i)$. Assume that $ord(b_{ij})$ is odd and N_i is not divisible by 3 and > 7 for all $1 \le i, j \le \theta$.

1. *For any $1 \le i \le \theta$ contained in a connected component of type B_n, C_n or F_4 resp. G_2, assume that N_i is not divisible by 5 resp. by 5 or 7.*
2. *If i and j belong to different components, assume $q_iq_j = 1$ or $\operatorname{ord}(q_iq_j) = N_i$.*

Then R is generated as an algebra by $R(1)$, that is A is generated by skew-primitive and group-like elements. □

Let us discuss the idea of the proof of Theorem 5.36. As mentioned, one could focus the attention on the graded dual S of R; then one has a surjection of graded braided Hopf algebras $S \to \mathfrak{B}(V)$, where $V = S(1)$. But we know the defining relations of $\mathfrak{B}(V)$, since it is of finite Cartan type. So that we are reduced to show that these relations also hold in S. For instance, take a quantum Serre relation $\operatorname{ad}_c(x_i)^{1-a_{ij}}(x_j) = 0$, $i \ne j$; and consider the Yetter-Drinfeld submodule W of S generated by x_i and $\operatorname{ad}_c(x_i)^{1-a_{ij}}(x_j)$. The assumptions (1) and (2) of the Theorem guarantee that W also is of Cartan type, but not finite. Thus $\operatorname{ad}_c(x_i)^{1-a_{ij}}(x_j) = 0$ in S.

Remark 5.37. We see that the main point in the proof of Theorem is to have control on Nichols algebras of rank 2. When this is granted, the proof can be extended to other settings; see [**Gñ1, Gñ4**]. There also versions of this Theorem in the infinite dimensional case, over $\mathbb{C}$ and for "positive" braidings; see [**AS7**].

Putting together the previous results, we get a complete answer in a significant case. Let p be an odd prime number. Let s be a natural number and let $\Gamma(s) = (\mathbb{Z}/(p))^s$.

Theorem 5.38. [**AS5**]. *(a). Let $p > 17$. Let $\mathcal{A}$ be a pointed finite-dimensional Hopf algebra such that $G(\mathcal{A}) \simeq \Gamma(s)$. Then there exist*

- *a finite Cartan matrix $(a_{ij}) \in \mathbf{k}^{\theta\times\theta}$ [**K**];*
- *elements $g_1, \dots, g_\theta \in \Gamma(s)$, $\chi_1, \dots, \chi_\theta \in \widehat{\Gamma(s)}$ such that*

$$\langle\chi_i, g_i\rangle \ne 1, \qquad \text{for all } 1 \le i \le \theta, \tag{5.41}$$

$$\langle\chi_j, g_i\rangle\langle\chi_i, g_j\rangle = \langle\chi_i, g_i\rangle^{a_{ij}}, \qquad \text{for all } 1 \le i, j \le \theta; \tag{5.42}$$

- *and a linking datum $(\lambda_{ij})_{1\le i<j\le\theta, i\not\sim j}$, cf. Definition 5.26;*

such that $\mathcal{A}$ can be presented as algebra by generators $a_1, \dots, a_\theta$, $y_1, \dots, y_s$ and relations

$$y_h^p = 1, \qquad y_my_h = y_hy_m, \qquad 1 \le m, h \le s, \tag{5.43}$$

$$y_ha_j = \chi_j(y_h)a_jy_h, \qquad 1 \le h \le s, 1 \le j \le \theta, \tag{5.44}$$

$$(\operatorname{ad} a_i)^{1-a_{ij}} a_j = 0, \qquad 1 \le i \ne j \le \theta, \quad i \sim j, \tag{5.45}$$

$$a_ia_j - \chi_j(g_i)a_ja_i = \lambda_{ij}(1 - g_ig_j), \qquad 1 \le i < j \le \theta, \quad i \not\sim j; \tag{5.46}$$

$$a_\alpha^p = 0, \qquad \alpha \in \Phi^+; \tag{5.47}$$

and where the Hopf algebra structure is determined by

$$\Delta y_h = y_h \otimes y_h, \qquad \Delta a_i = a_i \otimes 1 + g_i \otimes a_i, \qquad 1 \le h \le s, 1 \le i \le \theta. \tag{5.48}$$

(b). Conversely, let $(a_{ij}) \in \mathbb{Z}^{\theta\times\theta}$ *be a finite Cartan matrix,* $g_1, \dots, g_\theta \in \Gamma(s)$, $\chi_1, \dots, \chi_\theta \in \widehat{\Gamma(s)}$ *such that* (5.41), (5.42) *hold and* (λ_{ij}) *a "linking datum" for* (a_{ij}), $g_1, \dots, g_\theta$ *and* $\chi_1, \dots, \chi_\theta$. *Assume that* $p > 3$ *if the Cartan matrix* (a_{ij}) *has a connected component of type* G_2. *Then the algebra* $\mathcal{A}$ *presented by generators* $a_1, \dots, a_\theta$, $y_1, \dots, y_s$ *and relations* (5.43), (5.44), (5.45), (5.46), (5.47) *has a unique Hopf algebra structure determined by* (5.48). $\mathcal{A}$ *is pointed,* $G(\mathcal{A}) \simeq \Gamma(s)$ *and* $\dim \mathcal{A} = p^{s+|\Phi^+|}$. □

Remark 5.39. As a corollary of the Theorem and its proof, we get the complete clasification of all finite dimensional pointed Hopf algebras with coradical of prime dimension p, $p \neq 5, 7$. The same result was obtained by Musson, using the Lifting method [**Mus**].

5.3.9. *Low dimension.* To proceed with the lifting method out of the Cartan case, and also because of the reason explained in Remark 5.37, we need to answer the following particular case of Question 5.9.

Question 5.40. Given a braided vector space V of diagonal type and dimension 2, decide when $\mathfrak{B}(V)$ is finite dimensional. If so, compute $\dim \mathfrak{B}(V)$, and give a "nice" presentation by generators and relations.

Examples of finite dimensional Nichols algebras $\mathfrak{B}(V)$ of rank 2 over cyclic groups of even order which are *not* of Cartan type were known already to Nichols [**N**, pp. 1540 ff.]. All of them are encompassed by the following Proposition, which gives a partial answer to Question 5.40.

We recall first the following computation in a Nichols algebra, see [**Ro2**]. If $i \neq j$, then

$$\operatorname{ad}_c(x_i)^r(x_j) = (r)!_{b_{ii}} \prod_{0\le k\le r} \left(1 - b_{ii}^k b_{ij} b_{ji}\right) x_i^r x_j.$$

Proposition 5.41. [**Gñ4**] *Let* (V, c) *be a 2 dimensional BP of finite GT (and thus of diagonal GT), with basis* $\{x_1, x_2\}$ *and matrix* (q_{ij}), *and let* $N_j = N(q_{jj})$ *for* $j = 1, 2.$ *, let* $r + 1$ *be nilpotency order of* ad_{x_2} *on* x_1. *For* $1 \le i \le r$ *let* $M_i = N(q_{11}(q_{12}q_{21})^i q_{22}^{i^2})$. *Then*

$$\dim \mathfrak{B}V \ge N_1 N_2 \prod_{1\le i\le r} M_i.$$

Furthermore, suppose that the nilpotency order of ad_{x_1} *on* x_2 *is* 2. *We have:*

1. *If* $r = 1$ *then the equality holds.*
2. *If* $r = 2$, *and* $N(q_{11}) \neq 2$ *or* $N(q_{22}) \neq 3$ *then the equality holds.*
3. *If* $r = 2$, $N(q_{11}) = 2$ *and* $N(q_{22}) = 3$ *then the equality holds if and only if* $q_{12}q_{21} = -1$, *or* $q_{12}q_{21} = q_{22}$, *or* $q_{12}q_{21} = -q_{22}$.

□

An useful tool to deal with low index problems is the next Theorem. Let Γ be an arbitrary group. We denote by $P_V(t)$ the Hilbert polynomial of a graded vector space V.

Theorem 5.42. [**Gñ3**]. *Let* $V \in {}^{\Gamma}_{\Gamma}\mathcal{YD}$ *be finite dimensional and let* $W \subset V$ *be* $\mathbf{k}\Gamma$*-subcomodule. Let* $\Gamma' \subset \Gamma$ *be the smallest subgroup such that* $\delta(W) \subseteq \mathbf{k}\Gamma' \otimes W$. *We make the following assumptions:*

- W *is stable under the action of* Γ'. *Thus* $c(W \otimes W) = W \otimes W$, *and we can consider* $\mathfrak{B}(W)$.

- *$V = W \oplus W'$, where W' is a $\mathbf{k}\Gamma$-subcomodule and a $\mathbf{k}\Gamma'$-submodule.*
- *$\mathfrak{B}(W)$ is finite dimensional.*

Then there exists a graded subalgebra K of $\mathfrak{B}(V)$ such that $\mathfrak{B}(V) \simeq K \otimes \mathfrak{B}(W)$ as right $\mathfrak{B}W$-modules and left K-modules. In particular, $P_{\mathfrak{B}V}(t) = P_K(t)P_{\mathfrak{B}W}(t)$; hence $\dim \mathfrak{B}W$ divides $\dim \mathfrak{B}V$.

The proof of Theorem 5.42 uses "quantum differential operators"; the subalgebra K can be presented as the algebra of invariant elements of the quantum differential operators generated by W. An alternative proof of Theorem 5.42 is given in [**MiS**], dropping the finiteness assumption on $\mathfrak{B}(W)$.

Corollary 5.43. [**Gñ3**]. *Let A be a finite dimensional pointed Hopf algebra. Let p be a prime number.*

(1) *If the index $[A : G(A)] = p$, then A is a lifting of a quantum line.*

(2) *If the index $[A : G(A)] = p^2$, then A is a lifting of a quantum line or a quantum plane.*

(3) *If the index $[A : G(A)] = p^3$, then A is a lifting of a quantum line, a quantum plane, or a Nichols algebra of type A_2.*

In particular, A is generated by group-like and skew primitive elements. □

Parts (1) and (2) of Theorem 5.43 were proved in [**AS2**] under the assumption $G(A)$ abelian; part (1) was proved in [**AS3, D**] under the assumption that p is the lowest prime dividing the order of $G(A)$.

Combining Corollary 5.43 with *ad-hoc* techniques, it is possible to show:

Theorem 5.44. [**Gñ4**]. *Let A be a finite dimensional pointed Hopf algebra. If the index $[A : G(A)] < 32$, then A is a lifting of a quantum line, a quantum plane, or a Nichols algebra of generalized type A_2 or B_2. In particular, A is generated by group-like and skew primitive elements.* □

Corollary 5.45. *Let A be a finite dimensional pointed Hopf algebra. If $\dim A < 32$, then A is a lifting of a quantum line, a quantum plane, or a Nichols algebra of generalized type A_2 or B_2. In particular, A is generated by group-like and skew primitive elements.*

Proof. (Sketch). The only cases not covered by Theorem 5.44 are $64 = 2.32$ and $96 = 3.32$; but in these cases, $G(A)$ should have order 2, resp. 3; and we know the answer anyway by [**N**], resp. Theorem 5.38. □

All these Hopf algebras can be explicitly presented, and their isomorphism can be explicitly given. The computation of the liftings can be actually done; the most involved case should be 64 again.

5.3.10. *Nichols algebras over non-abelian finite groups.* To classify pointed Hopf algebras with non-abelian group of group-likes by the Lifting Method, we need to deal first of all with step (a). This means, given a braided vector space V of group type, *cf.* Definition 5.8, to decide when V is finite dimensional and compute it explicitly. It is convenient to consider the following definition, for general braided vector spaces.

Definition 5.46. Let (V, c) be a braided vector space. We say that (V, c) is *decomposable* if there exist proper vector subspaces V_1, V_2, of V such that $V = V_1 \oplus V_2$ and $c(V_i \otimes V_j)) \subseteq V_j \otimes V_i$, $1 \le i, j \le 2$. Otherwise, we say that (V, c) is *indecomposable* or a *fat point*.

In the same spirit, a *decomposition* of a braided vector space (V, c) is a direct sum $V = \oplus_{1 \le i \le r} V_i$, with $0 \ne V_i \ne V$, and $c(V_i \otimes V_j)) \subseteq V_j \otimes V_i$, $1 \le i, j \le r$. We shall denote $c_{ij} := c|_{V_i \otimes V_j} : V_i \otimes V_j \to V_j \otimes V_i$.

A decomposition $V = \oplus_{1 \le i \le r} V_i$ shall be called *irreducible* if (V_i, c_{ii}) is indecomposable, $1 \le i \le r$.

A braided vector space (V, c) of diagonal type is indecomposable if and only if $\dim V = 1$. This justifies the name of fat point.

We propose to split our problem in two parts:

- First, deal with fat points of group type.
- Next, deal with decomposable braided vector spaces of group type.

We would be happy if the second case can be interpreted as a diagram with fat points. Here is a first clue that this approach could be correct.

Theorem 5.47. [**Gñ3**]. *Let $V = \oplus_{1 \le i \le r} V_i$ be a decomposition of a braided vector space (V, c). Assume that $\mathfrak{B}V_i$ is finite dimensional $\forall i$. Then $\dim \mathfrak{B}V \ge \prod_{i=1}^{n} \dim \mathfrak{B}V_i$. Furthermore, the equality holds if and only if $c_{ij} = c_{ji}^{-1}$ $\forall i \ne j$.* □

Remark 5.48. [**Gñ3**]. Let (V, c) be a braided vector space of group type. Assume that $\mathfrak{B}(V)$ is finite dimensional and let $V = \oplus_{1 \le i \le r} V_i$ be a decomposition of (V, c). For each $1 \le i \le r$, let $W_i \subseteq V_i$ be a (possibly zero) subspace of V_i satisfying the same hypothesis as in Theorem 5.42, with respect to V. Then $\prod_{i=1}^{r} P_{\mathfrak{B}(W_i)}(t)$ divides $P_{\mathfrak{B}(V)}(t)$ and the quotient lies in $\mathbb{Z}[t]$. In particular, $\prod_{i=1}^{r} \dim \mathfrak{B}(W_i)$ divides $\dim \mathfrak{B}(V)$.

An irreducible decomposition with $c_{ij} = c_{ji}^{-1}$, for all $i \ne j$ might be called a "quantum linear space of fat points". Observe the perfect analogy with Lemma 5.12. In general, one would consider first irreducible decompositions with $c_{ij} c_{ji} = c_{ii}^{a_{ij}}$, for all $i \ne j$ ... but before even daring of doing this, we should solve the problem for fat points, which is still far from our knowledge as we explain now.

Let Γ be a finite group. Let $V = M(g, \rho)$, for some $g \in \Gamma$ and $\rho : \Gamma^g \to \operatorname{End} W$ an irreducible representation of the isotropy subgroup Γ^g. Then $\rho(g)$ acts by a scalar, by Schur's lemma, say q. Consider $W \hookrightarrow V$, via $x \mapsto 1 \otimes x$. If $x, y \in W$, then

$$c(x \otimes y) = q y \otimes x.$$

A first immediate consequence is that $q \ne 1$ if $\mathfrak{B}(V)$ has finite dimension. But, arguing as in Proposition 5.24, Theorem 5.19 implies the following restrictions.

Proposition 5.49. [**Gñ4**] *If $\dim \mathfrak{B}(V)$ is finite, then*

- *if $\dim W \ge 3$ then $q = -1$;*
- *if $\dim W = 2$ then $q = -1$ or it is a third root of unity.*

□

When $\dim W > 1$ and $q = -1$ or a a third root of unity, very few is known. For instance, if $\Gamma = \Gamma^g$, then $V = M(g, \rho)$ is not a fat point but a quantum linear space (if $q = -1$), or has type A_2 (if q is a third root of unity).

Let us now consider the case when $\dim W = 1$, *i. e.* when ρ is a character. We first describe, following **[Gñ4]**, a relation between braided vector spaces of group type, whose indecomposable components can be realized as $M(g, \rho)$ with ρ a character, and set-theoretical solutions of the braid equation.

DEFINITION 5.50. A *crossed set* is a pair $(X, \triangleright)$, where X is a finite set and $\triangleright : X \times X \to X$ is a function, such that

- for each $i \in X$, the function $e^{\triangleright}(i) : X \to X$, $e^{\triangleright}(i)(j) = i \triangleright j$, is a bijection,
- $i \triangleright i = i \ \forall i \in X$,
- $j \triangleright i = i$ whenever $i \triangleright j = j$, and
- $i \triangleright (j \triangleright k) = (i \triangleright j) \triangleright (i \triangleright k) \ \forall i, j, k \in X$.

The archetypical example is a subset X of a finite group Γ stable under the conjugation, with $i \triangleright j = iji^{-1}$. A crossed set provides a set-theoretical solution of the Braid Equation by

$$c : X \times X \to X \times X, \quad c(i, j) = (i \triangleright j, i). \tag{5.49}$$

There is a large class of set-theoretical solutions of the Braid Equation which are equivalent, in a suitable sense, to solutions of this form **[So, LYZ]**.

Let A be an abelian group, denoted multiplicatively. Let $(C^{\bullet}(X, A), \delta)$ be the cochain complex defined by

- $C^n(X) = \{f : X^n \to A\}$, $n \geq 0$.
- $\delta^0 = 0$,
- $\delta^n(f)(x_0, \dots, x_n) = \prod_{i=0}^{n-1} f(x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n)^{(-1)^i}$
  $\times f(x_0, \dots, x_{i-1}, x_i \triangleright x_{i+1}, \dots, x_i \triangleright x_n)^{(-1)^{i+1}}$.

The cohomology groups $H^n(X, A) = H^n(C^{\bullet}(X, A), \delta)$ have interesting interpretations for low n. First, $H^1(X, \mathbf{k}^{\times}) = \mathbf{k}^{\pi_0(X)}$, where $\pi_0(X)$ is the set of equivalence classes of the relation generated by $j \sim i \triangleright j$.

Second, let $\mathbf{k}X$ denote the vector space with basis X. If $f \in C^2(X, \mathbf{k}^{\times})$, we define a map $c^f : \mathbf{k}X \otimes \mathbf{k}X \to \mathbf{k}X \otimes \mathbf{k}X$ by

$$c^f(i \otimes j) = f(i, j) i \triangleright j \otimes i.$$

We then have

$$H^2(X,\mathbf{k}^\times) = \{f \in C^2(X,\mathbf{k}^\times) \mid c^f \text{ verifies the Braid Equation}\}/\sim;$$

where $\sim$ amounts for a change of basis of the form $i \mapsto \lambda_i i$, $\lambda_i \in \mathbf{k}^\times$ for all $i \in X$. We can then refer to a braiding c^f, for $f \in H^2(X,\mathbf{k}^\times)$. Similarly, we consider $H^2(X,\mathbb{G}_\infty)$, where $\mathbb{G}_\infty$ is the group of all roots of 1 in $\mathbf{k}$.

LEMMA 5.51. **[Gñ4]** *If $f \in H^2(X,\mathbb{G}_\infty)$ then $(\mathbf{k}X, c^f)$ is of finite group type. Conversely, a braided vector space of finite group type arising from a Yetter-Drinfeld module $\oplus_{1\le i\le s} M(g_i,\rho_i)$ with ρ_i characters, is of the form $(\mathbf{k}X, c^f)$ for some $(X,\triangleright)$, $f \in H^2(X,\mathbb{G}_\infty)$.* □

In other words, the class of braided vector spaces $(\mathbf{k}X, c^f)$, $(X,\triangleright)$ a crossed set, $f \in H^2(X,\mathbb{G}_\infty)$, is one of the "suitable classes" we are looking for.

QUESTION 5.52. Given $(\mathbf{k}X, c^f)$, $(X,\triangleright)$ a crossed set, $f \in H^2(X,\mathbb{G}_\infty)$ compute the dimension of the associated $\mathfrak{B}(\mathbf{k}X)$. If finite, give a nice presentation of $\mathfrak{B}(\mathbf{k}X)$.

We are naturally led to the problems of, first, classifying all the crossed sets $(X,\triangleright)$, and second, computing $H^2(X,\mathbb{G}_\infty)$ for each of them. The answer is known only for crossed sets of cardinal 3 or 4 **[Gñ4]**. A first reduction is to determine the pairs $(\mathbf{k}X, c^f)$ which are fat points, or indecomposable. In this sense, it is natural to say that a crossed set $(X,\triangleright)$ is *indecomposable* if for any $Y \subseteq X$ such that $Y \triangleright Y = Y$, $(X-Y)\triangleright(X-Y) = (X-Y)$, then necessarily $Y = X$ or $X - Y = X$. If the braided vector space $(\mathbf{k}X, c^f)$ is indecomposable, then the crossed set $(X,\triangleright)$ is indecomposable. However, the converse is not true; see **[Gñ4**, Section 5.2].

Let us show now some explicit examples of braided vector spaces $(V,c) = (\mathbf{k}X, c^f)$. We assume that $\dim V \ge 3$, otherwise V is of diagonal type **[AG]**. Notice that we always have a map $\mathbb{G}_\infty \to H^2(X,\mathbb{G}_\infty)$ by $q \mapsto f_q$, $f(i,j) = q$; we denote the corresponding cocycle by c^q.

EXAMPLE 5.53. **[MiS]**. Let (W,S) be a finite Coxeter group and let X be the union of the orbits of all elements of S; let $\triangleright$ be the restriction of the conjugation. The authors consider the braided vector space $(V,c) = (\mathbf{k}X, c^q)$. They compute the dimension of $\mathfrak{B}(V)$ in the following cases:

- If $W = \mathbb{S}_3$, then $\dim \mathfrak{B}(V) = 12$.
- If $W = \mathbb{S}_4$, then $\dim \mathfrak{B}(V) = 24^2$.
- If $W = \mathbb{D}_4$, then $\dim \mathfrak{B}(V) = 48$.
- If $W = \mathbb{S}_5$, then $\dim \mathfrak{B}(V) < \infty$ by **[FK]**.

EXAMPLE 5.54. **[Gñ4**, Section 5.2]. Let $X = \{1,2,3,4\}$. Then there exists a structure of crossed set $\triangleright$ on X, such that the corresponding map $e^\triangleright$ is given by

$$e^\triangleright(1) = (2\,3\,4), \quad e^\triangleright(2) = (1\,4\,3), \quad e^\triangleright(3) = (1\,2\,4), \quad e^\triangleright(4) = (1\,3\,2).$$

Then there is a cocycle f such that $\mathfrak{B}(\mathbf{k}X)$ has dimension 72; a nice presentation by generators and relations is also given in **[Gñ4]**.

These are the only examples were we know that the dimension is finite.

In the spirit of step (b), we also may ask whether, for a fixed finite group Γ, there exist "genuine" examples of finite dimensional pointed Hopf algebras H with $G(H) \simeq \Gamma$. The best way to state precisely what "genuine" means, is as follows.

DEFINITION 5.55. [**MiS**]. A Yetter-Drinfeld module $V \in {}^{\Gamma}_{\Gamma}\mathcal{YD}$ is *link-indecomposable* if Γ is generated by the elements g such that $V_g \neq 0$.

QUESTION 5.56. Determine all finite groups Γ having a link-indecomposable Yetter-Drinfeld module V such that $\mathfrak{B}(V)$ is finite dimensional.

5.3.11. *Nichols algebras over semisimple Hopf algebras.* We know almost nothing about finite dimensional Hopf algebras whose coradical is a Hopf subalgebra, but are not pointed. In order to restrict our attention to "genuine" examples, we propose the following definition.

DEFINITION 5.57. Let H be a semisimple Hopf algebra and let $V \in {}^{H}_{H}\mathcal{YD}$. Let C_V be the subcoalgebra of H generated by the matrix coeficients of V. We say that V is *link-indecomposable* if H is generated as an algebra by $C_V + C_{V^*}$.

QUESTION 5.58. Determine all semisimple Hopf algebras H having a link-indecomposable Yetter-Drinfeld module V such that $\mathfrak{B}(V)$ is finite dimensional.

6. The general case

We assume in this Section that $\mathbf{k}$ is algebraically closed.

In this Section we are concerned with the following question: what is the classification of all Hopf algebras of a fixed dimension? Of course, this is a very difficult problem (it contains the classification of all groups of a fixed order). One should probably be happy to answer the following partial questions:

QUESTION 6.1. Classify all Hopf algebras of dimension d, where d is small; say, $d \leq 100$.

QUESTION 6.2. Classify all Hopf algebras of dimension d, where d factorizes in a simple way; say, $d = p^2, pq, pqr, pq^2, p^3, p^a q^b, \dots$, where p, q, r are distinct prime numbers.

The purpose of addressing these Questions is, naturally, to gain insight into the structure of general Hopf algebras, before even daring to state general conjectures or questions about them.

About Question 6.2, the only general known result is Theorem 4.5, classifying Hopf algebras of prime dimension. I am aware of the following two partial results.

THEOREM 6.3. [**AS1**]. *Assume that char* $\mathbf{k} = 0$. *Let H be a Hopf algebra of simension p^2. Assume that $\mathcal{S}$ has order $2p$. Then H is either semisimple (hence, a group algebra) or pointed (hence a Taft algebra).* □

Recall that by Radford's formula 3.5 and Nichols-Zöller theorem 3.2, $\mathcal{S}^{4p} = \mathrm{id}$; so that the only remaining case is when the order of $\mathcal{S}$ is $4p$.

THEOREM 6.4. [**Na4**]. *Assume that char* $\mathbf{k} = 0$. *Let H be a Hopf algebra of dimension p^2 or pq, where p and q are odd. Assume that H is quasitriangular. Then H is semisimple; hence, a group algebra, or the dual of an abelian group algebra.* □

In general, Proposition 5.3 motivates the following Question:

QUESTION 6.5. Let N be a positive integer which is free of squares. Is any Hopf algebra of dimension N semisimple?

Here is what we know about Question 6.1.

THEOREM 6.6. *Assume that char* $\mathbf{k} = 0$. *All Hopf algebras of dimension d are known for $d \le 12$, or $d = 15, 21, 25, 35, 49$. They are either semisimple, or pointed, or dual to a pointed.* □

For $d \le 11$, this was proved in [**Wl**] and an alternative, more conceptual, proof was offered in [**St3**]; For $d = 12$, this was proved in [**Na3**]; the rest of the cases are in [**AN3**].

REMARK 6.7. It is natural to ask whether there exist Hopf algebras H which are neither semisimple, neither pointed, nor H^* is pointed. Infinite families of such examples are constructed in the very interesting paper [**Mu2**], as a byproduct of his study of the "finite quantum subgroups of $GL(N)$", that is, finite dimensional Hopf algebra quotients of $\mathbf{k}_q[GL(N)]$.

6.1. On the coradical filtration. The purpose of this Subsection is to state a description of the coradical filtration due to Nichols and some consequences, useful for problems in low dimension.

Let C be a coalgebra over $\mathbf{k}$. We denote by $\widehat{C}$ the set of isomorphism types of simple left C-comodules; and by V_τ (resp., V_τ^*) the simple left (resp. right) C-comodule corresponding to $\tau \in \widehat{C}$. We have $C_0 \simeq \oplus_{\tau \in \widehat{C}} C_\tau$, where C_τ is a simple subcoalgebra of dimension d_τ^2, $d_\tau \in \mathbb{Z}$. We also set $C_{0,d} := \oplus_{\tau \in \widehat{C} : d_\tau = d} C_\tau$.

A C_0-bicomodule is a vector space M with left and right C_0-coactions $\rho_L : M \to C_0 \otimes M$ and $\rho_R : M \to M \otimes C_0$ such that $(\rho_L \otimes \mathrm{id})\rho_R = (\mathrm{id} \otimes \rho_R)\rho_L$. Any C_0-bicomodule is a direct sum of simple C_0-sub-bicomodules and a simple C_0-bicomodule is of the form $V_\tau \otimes V_\mu^*$ and has dimension $d_\tau d_\mu$ for some $\tau, \mu \in \widehat{C}$. If M is a C_0-bicomodule, we set $M^{\tau,\mu}$ for the isotypic component of type $V_\tau \otimes V_\mu^*$.

There exists a coalgebra projection π of C onto C_0 [**Mo1**, 5.4.2]; let $I := \ker \pi$. Then C is a C_0-bicomodule via $\rho_L := (\pi \otimes \mathrm{id})\Delta : C \to C_0 \otimes C$, $\rho_R := (\mathrm{id} \otimes \pi)\Delta : C \to C \otimes C_0$; I and C_n, $n \ge 0$, are sub-bicomodules of C. Let $P_0 = 0$,

$$P_1 = \{x \in C : \Delta(x) = \rho_L(x) + \rho_R(x)\} = \Delta^{-1}(C_0 \otimes I + I \otimes C_0),$$

$$P_n = \{x \in C : \Delta(x) - \rho_L(x) - \rho_R(x) \in \sum_{1 \le i \le n-1} P_i \otimes P_{n-i}\}, \quad n \ge 2.$$

In particular the P_n's are C_0-sub-bicomodules of I, $n \ge 0$; but they are not intrinsic since they depend on the projection π. The following Lemma can be thought as a substitute of Theorem 5.2.

LEMMA 6.8. *(W. Nichols) (i). $P_n = C_n \cap I$.*
(ii). $C_1 = \sum_{\tau,\mu \in \widehat{C}} C_\tau \wedge C_\mu$.
(iii). $C_\tau \wedge C_\tau = C_\tau \oplus P_1^{\tau,\mu}$ and $C_\tau \wedge C_\mu = C_\tau \oplus C_\mu \oplus P_1^{\tau,\mu}$, if $\tau \ne \mu$. □

Assume in what follows that $C = H$ is a finite dimensional Hopf algebra. If $\tau \in \widehat{C}$ and $g \in G(H)$, we denote $C_{\tau^d} := \mathcal{S}(C_\tau)$, $g.C_\tau := C_{g.\tau}$, $C_\tau.g := C_{\tau.g}$; they are simple subcoalgebras of C.

COROLLARY 6.9. [**AN3**]. *(i). For any $g \in G(H)$,*

$$\dim P_1^{\tau,\mu} = \dim P_1^{\mu^d,\tau^d} = \dim P_1^{g\cdot\tau,g\cdot\mu} = \dim P_1^{\tau\cdot g,\mu\cdot g}.$$

(ii). If I is a direct sum of one-dimensional H_0-sub-bicomodules then $H_1 = H_0 + \sum_{g,h\in G(H)} P_{g,h}(H)$. $\square$

Consider the right action $\leftharpoonup$: $H^* \otimes H \to H^*$ given by $\alpha \leftharpoonup h = \langle \alpha_1, h\rangle \alpha_2$, $\forall h \in H$, $\alpha \in H^*$. Let $\int \in H^*$ be a non-zero left integral and let $g_0 \in G(H)$ be the distinguished group-like element, so that

$$\alpha \textstyle\int = \langle \alpha, 1\rangle \int \quad \text{and} \quad \int \alpha = \langle \alpha, g_0\rangle \int, \qquad \forall \alpha \in H^*.$$

We shall assume in what follows that H is not cosemisimple, or equivalently, that $\langle \int, 1\rangle = 0$; in particular $\int^2 = 0$ and if $g \in G(H)$, also $(\int \leftharpoonup g)^2 = \int^2 \leftharpoonup g = 0$. Observe that if $C \neq \mathbf{k}1$ is a simple subcoalgebra of H, and if $c \in C$, then

$$\langle \textstyle\int, c\rangle 1 = \langle \int, c_2\rangle c_1 \quad \in C \cap \mathbf{k}1,$$

whence $\int|_C = 0$, *i.e.*, $\int$ belongs to the anihilator of H_0, $H_0^\perp = \operatorname{Jac} H^*$. Let $g \in G(H)$. Since the left (and right) multiplication by g is a coalgebra automorphism of H, it preserves H_0. This implies that also $\int \leftharpoonup g$ belongs to $\operatorname{Jac} H^*$. Also, for all $\alpha \in H^*$, we have

$$\alpha(\textstyle\int \leftharpoonup g) = \langle \alpha, g^{-1}\rangle \int \leftharpoonup g, \quad \text{and} \quad (\int \leftharpoonup g)\alpha = \langle \alpha, g^{-1}g_0\rangle \int \leftharpoonup g.$$

Hence $\mathbf{k}(\int \leftharpoonup g)$ is a two-sided ideal of H^* and $\mathbf{k}(\int \leftharpoonup g) \subseteq \operatorname{Jac} H^*$. Moreover, since distinct group-like elements are linearly independent and the map $H \to H^*$, $h \mapsto \int \leftharpoonup h$, is injective, the ideals $\mathbf{k}(\int \leftharpoonup g)$ and $\mathbf{k}(\int \leftharpoonup g')$ are distinct if $g \neq g'$.

LEMMA 6.10. [**AN3**] *Let H be a non-cosemisimple finite dimensional Hopf algebra. Let $L = (\int \leftharpoonup \mathbf{k}G(H))^\perp$, $s = |G(H)|$. Then $L \subseteq H$ is a subcoalgebra of H containing H_0 and there is an H_0-bicomodule decomposition*

$$H = L \oplus \bigoplus_{j=1}^{s} I_j,$$

where I_j are one-dimensional H_0-sub-bicomodules of I, $\forall j = 1, \dots, s$. $\square$

PROPOSITION 6.11. [**AN3**] *Let H be a non-cosemisimple finite dimensional Hopf algebra.*

(i). If $\dim H - \dim H_0 = |G(H)|$, then $\mathcal{P}_{g,h} \neq \mathbf{k}(g-h)$, for some $g, h \in G(H)$.

(ii). Suppose that $\mathcal{P}_{g,h} = \mathbf{k}(g-h)$, for all $g, h \in G(H)$. Then $\int \leftharpoonup \mathbf{k}G(H) \subseteq (\operatorname{Jac} H^*)^2$. In particular, $|G(H)| \leq \dim H - \dim H_1$.

(iii). If $H_1 = H$ then H has a non-trivial skew primitive element. In particular, if char $\mathbf{k} = 0$, then $G(H)$ is non-trivial. $\square$

6.2. Relation with quantum $s\ell(2)$. We briefly discuss a very interesting result from [**St3**] and some consequences.

THEOREM 6.12. [**St3**, Th. 1.5] *Let A be a Hopf algebra containing a simple subcoalgebra C of dimension 4 stable by $\mathcal{S}$. Assume that $1 < \operatorname{ord}(\mathcal{S}^2|_C) = n < \infty$. Then there exists a root of unity ω, such that the order of ω^2 is n, and a surjective homomorphism of Hopf algebras $\mathcal{O}_{\sqrt{-\omega}}(SL_2(\mathbf{k})) \to B := \mathbf{k}C$.* $\square$

Here, $\mathbf{k}C$ denotes the subalgebra of A generated by C, which is a Hopf subalgebra of A. Notice that the hypothesis on the order of the antipode always holds whenever A is finite dimensional and non-semisimple.

Let $q := \sqrt{-\omega}$. Let N be the order of q. There is a central inclusion of Hopf algebras $\mathcal{O}(SL_2(\mathbf{k})) \to \mathcal{O}_q(SL_2(\mathbf{k}))$, $X_{ij} \mapsto x_{ij}^N$, where X_{ij} are the usual coordinates in $\mathcal{O}(SL_2(\mathbf{k}))$.

COROLLARY 6.13. [**Na4**] *Let A be a finite dimensional non-semisimple Hopf algebra. Suppose that A is generated by a simple subcoalgebra C of dimension 4 which is stable by the antipode. Then A fits into an extension $1 \to \mathbf{k}^G \to A \to H \to 1$, where G is a finite group and H^* is a pointed non-semisimple Hopf algebra.* $\square$

It would be really interesting to generalize this result, and to understant the reasons behind it.

7. Forms

7.1. Forms of Hopf algebras. The passage from the algebraically closed case to the general case follows in principle the general guidelines of Galois descent [**Se2**]. Let $\mathbf{k}$ be a field with algebraic closure $\overline{\mathbf{k}}$ and suppose we have classified all Hopf algebras of certain type over $\overline{\mathbf{k}}$, say all the Hopf algebras of a fixed dimension d. For each Hopf algebra H over $\overline{\mathbf{k}}$ in the obtained list, one seeks to describe all Hopf algebras H_0 over $\mathbf{k}$ such that $H_0 \otimes_{\mathbf{k}} \overline{\mathbf{k}} \simeq H$; briefly, the $\mathbf{k}$-forms of H. This problem splits into two parts: first one needs to show the existence of at least one form, second the set of all forms is described as a non-abelian H^1. The first part, which is trivial in the case of group algebras, is not all evident for general Hopf algebras. The literature on these Questions is not very abundant: [**TO**] is concerned with commutative Hopf algebras of prime dimension, [**HaP**], [**P**] treat the case of finite group algebras; recently, forms of Frobenius-Lusztig kernels were discussed in [**CDB**] (over fields where the existence of a form is granted).

QUESTION 7.1. Do there exist forms of the Frobenius-Lusztig kernels over $\mathbb{Q}$?

7.2. Finite compact quantum groups. There is another version of the notion of "form", with a more "quantum" flavor since it has origins in the theory of operator algebras. We shall work over $\mathbb{C}$, regarding $\mathbb{R}$-forms; the first general definitions and notions can be adapted *mutatis mutandis* to quadratic extensions. I do not know a formulation for more general field extensions, if any.

DEFINITION 7.2. A $*$-Hopf algebra is a pair $(H, *)$, where H is a Hopf algebra and $* : H \to H$ is a conjugate-linear map (that is, $(\lambda x)^* = \overline{\lambda} x^*$ for $\lambda \in \mathbb{C}$, $x \in H$) such that:

- $(xy)^* = y^* x^*$, *i. e.* $*$ is an anti-algebra map;
- $\Delta(x^*) = \sum_{(x)} {x_{(1)}}^* \otimes {x_{(2)}}^*$, *i. e.* $*$ is a coalgebra map.

It follows easily that $(\mathcal{S}*)^2 = \mathrm{id}$. Also, one could consider "$\circ$-Hopf algebra", where $\circ : H \to H$ is a conjugate-linear, algebra and anti-coalgebra, map. However, the two notions are equivalent by the equality $x^\circ = (\mathcal{S}(x))^*$.

For simplicity, assume now that $(H, *)$ is a finite dimensional $*$-Hopf algebra. The transpose of the $*$-operation is a $\circ$-operation in the dual Hopf algebra H^*; by the preceding H^* is a $*$-Hopf algebra in a natural way.

Let $\int : H \to \mathbb{C}$ be a right integral and let $(\,|\,) : H \times H \to \mathbb{C}$ be the sesquilinear form given by

$$(x|y) := \langle \int, y^* x \rangle.$$

It is easy to see that

$$(xy|z) = (y|x^* z), \qquad (p \rightharpoonup x|y) = (x|p^* \rightharpoonup y), \qquad x, y, z \in H, p \in H^*.$$

Here $\rightharpoonup$ is the action of H^* on H transpose to right multiplication. Assume further that H is semisimple; then we normalize $\int$ by $\langle \int, 1 \rangle = 1$. The corresponding $(\,|\,)$ is hermitian, since $\int$ is also a left integral.

Definition 7.3. A *finite compact quantum group* is a $*$-Hopf algebra $(H, *)$ with H semisimple and $\int$ normalized by $\langle \int, 1 \rangle = 1$, such that $(\,|\,)$ is positive definite. We say that $*$ is a *compact involution.*

This definition is equivalent to the original definition of Woronowicz [**W1**], as shown in [**A2**, 2.4]. Finite compact quantum group are also called Kac algebras in honor of G. I. Kac [**Kc1, Kc2, KP**].

Theorem 7.4. [**A2**, 2.4]. *Let $(H, *)$ be a finite compact quantum group and let $\# : H \to H$ be another structure of $*$-Hopf algebra. Then there exists a Hopf algebra automorphism $T : H \to H$ such that $\#$ and $T * T^{-1}$ commute.*

If $\#$ is another compact involution, then there exists a Hopf algebra automorphism $T : H \to H$ such that $\# = T * T^{-1}$. □

The proof of Theorem 7.4 is inspired in an analogous proof for semisimple Hopf algebras due to Mostow; it actually applies also in the infinite dimensional case [**A2**]. In presence of this Theorem, the classification of finite compact quantum groups is equivalent to the following problem:

Question 7.5. Given a semisimple Hopf algebra H, does it admit a compact involution?

8. Appendix. Questions

For convenience of the reader, we collect here the Questions discussed in the text.

Question 2.1. Jordan-Hölder theorem for finite dimensional Hopf algebras.

Question 2.3. Simple semisimple Hopf algebras are twistings of group algebras of simple groups, or their duals?

Question 2.4. Classify simple semisimple Hopf algebras of dimension 60.

Question 2.6. Does there exist a semisimple Hopf algebra which is *not* a twisting of a semi-solvable Hopf algebra?

Question 2.12. Find a semisimple Hopf algebra which is a bosonization but not an extension.

Conjecture 4.11. (Kaplansky). If H is a (semisimple) Hopf algebra over the algebraically closed field $\mathbf{k}$, then the sizes of the matrices occuring in any full matrix constituent of H divide the dimension of H.

Question 4.7. (Kaplansky). Classify all Hopf algebras of dimension p, in char p.

Question 4.17. (S. Montgomery). What is the analogue of Burnside's $p^a q^b$-Theorem for semisimple Hopf algebras?

Question 4.20. (S. Montgomery). Classify all semisimple Hopf algebras H such that $\dim H < 60$; that is, those of dimension 20, 24, 30, 32, 36, 40, 42, 48, 52, 54, 56.

Question 5.9. Given a matrix whose entries are roots of 1, compute the dimension of the associated $\mathfrak{B}(V)$. If finite, give a nice presentation of $\mathfrak{B}(V)$.

Question 5.28. Compute liftings of the quantum Serre relations for vertices in the same connected component, in the low order cases.

Question 5.31. If $R = \oplus_{n\geq 0} R(n)$ is a graded braided Hopf algebra with $R(0) = \mathbf{k}1$ and $P(R) = R(1)$, when R is generated in degree one, *i. e.* is a Nichols algebra?

Question 5.32. If $S = \oplus_{n\geq 0} S(n)$ is a graded braided Hopf algebra with $S(0) = \mathbf{k}1$ which is generated in degree one, when $P(R) = R(1)$, *i. e.* when S is a Nichols algebra?

Conjecture 5.35. [**AS3**]. Any pointed finite dimensional Hopf algebra over $\mathbf{k}$ is generated by group-like and skew-primitive elements.

Question 5.40. Same as 5.9 but in the particular case of rank 2.

Question 5.52. Given $(\mathbf{k}X, c^f)$, $(X, \triangleright)$ a crossed set, $f \in H^2(X, \mathbb{G}_\infty)$ compute the dimension of the associated $\mathfrak{B}(\mathbf{k}X)$. If finite, give a nice presentation of $\mathfrak{B}(V)$.

Question 5.56. Determine all finite groups Γ having a link-indecomposable Yetter-Drinfeld module V such that $\mathfrak{B}(V)$ is finite dimensional.

Question 5.58. Same for semisimple Hopf algebras.

Question 6.1. Classify all Hopf algebras of dimension $d \leq 100$.

Question 6.2. Classify all Hopf algebras of dimension d, where d factorizes in a simple way.

Question 6.5. Let N be a free of squares positive integer. Is any Hopf algebra whose dimension is free of squares, necessarily semisimple?

Question 7.1. Do there exist forms of the Frobenius-Lusztig kernels over $\mathbb{Q}$?

Question 7.5. Given a semisimple Hopf algebra H, does it admit a compact involution?

References

[AJS] H. H. Andersen, J. Jantzen and W. Soergel, *Representations of quantum groups at a p-th root of unity and of semisimple groups in characteristic p: Independence of p* Astérisque **220**, 1994.

[A1] N. Andruskiewitsch, *Notes on extensions of Hopf algebras*, Canad. J. Math. **48** (1996), pp. 3–42.

[A2] ______, *Compact involutions on semisimple quantum groups*, Czechoslovak J. Phys. **44** (1994), pp. 963–972.

[AD] N. Andruskiewitsch and J. Devoto, *Extensions of Hopf algebras*, Algebra i Analiz **7** (1995), pp. 17–52.

[AG] N. Andruskiewitsch and M. Graña, *Braided Hopf algebras over non abelian groups*, Bol. Acad. Ciencias (Córdoba) **63** (1999), 45-78.

[AN1] N. Andruskiewitsch and S. Natale, *Plancherel identity for semisimple Hopf algebras*, Commun. Alg. **25** (1997), pp. 3239-3254.

[AN2] ———, *Examples of self-dual Hopf algebras*, J. Math. Sci. Univ. Tokyo **6** (1999), pp. 181-215.

[AN3] ———, *Counting arguments for low dimensional Hopf algebras*, Tsukuba Math. J., to appear.

[AS0] N. Andruskiewitsch and H-J. Schneider, *Appendix to* [**A1**].

[AS1] ———, *Hopf algebras of order p^2 and braided Hopf algebras of order p*, J. Algebra, **199** (1998), pp.430–454.

[AS2] ———, *Lifting of quantum linear spaces and pointed Hopf algebras of order p^3*, J. Algebra **209** (1998), pp. 659–691.

[AS3] ———, *Finite quantum groups and Cartan matrices*, to appear in Adv. in Math.

[AS4] ———, *Lifting of Nichols algebras of type A_2 and Pointed Hopf Algebras of order p^4*, in "Hopf algebras and quantum groups", ed. S. Caeneppel and F. van Oystaeyen, M. Dekker, 1–16.

[AS5] ———, *Finite quantum groups over abelian groups of prime exponent*, preprint (1999).

[AS6] ———, *Pointed Hopf Algebras*, in "Recent developments in Hopf algebras", Cambridge Univ. Press, to appear.

[AS7] ———, *A characterization of quantum groups*, in preparation.

[Be] M. Beattie, *An isomorphism theorem for Ore extension Hopf algebras* Comm. Algebra **28** (2000), 569–584.

[BDG] M. Beattie, S. Dăscălescu, and L. Grünenfelder, *On the number of types of finite-dimensional Hopf algebras*, Inventiones Math. **136** (1999), 1-7.

[BD] Yu. Bespalov and B. Drabant, *Hopf (bi-)modules and crossed modules in braided monoidal categories*, J. Pure Appl Alg. **123** (1998), pp. 105–129.

[BM] R. J. Blattner and S. Montgomery, *Crossed products and Galois extensions of Hopf algebras*, Pacific J. of Math. **137** (1989), pp. 37–54.

[By1] N. P. Byott, *Cleft extensions of Hopf algebras*, J. Algebra **157** (1993), 405–429.

[By2] ———, *Cleft extensions of Hopf algebras, II*, Proc. London Math. Soc. (3) **67** (1993), 277–304.

[CD1] S. Caenepeel and S. Dăscălescu, *Pointed Hopf algebras of dimension p^3*, J. Algebra **209** (1998), 622–634.

[CD2] ———, *On pointed Hopf algebras of dimension 2^n*, Bull. London Math. Soc. **31** (1999), 17–24.

[CDB] S. Caenepeel, S. Dăscălescu and L. Le Bruyn, *Forms of pointed Hopf algebras*, Manuscripta Math. **100** (1999), pp. 35–53.

[CDR] S. Caenepeel, S. Dăscălescu and S. Raianu, *Classifying Pointed Hopf algebras of dimension* 16, Commun. Alg. **28** (2000), 541–568.

[Ca] P. Cartier, *Groupes algebriques et groupes formels* in "Colloq. Théorie des Groupes Algébriques (Bruxelles, 1962)", pp. 87–111, Librairie Universitaire, Louvain; Gauthier Villars, Paris.

[Ci] C. Cibils, *Tensor products of Hopf bimodules over a group algebra*, Proc. A.M.S. **125** (1997), pp. 1315–1321.

[D] S. Dăscălescu, *Pointed Hopf algebras with large coradical*, Commun. Alg. **27** (1999), pp. 4821–4826.

[DNT] S. Dăscălescu, C. Nastasescu and B. Torrecillas, *Co-Frobenius Hopf algebras: Integrals, Doi-Koppinen Modules and Injective objects*, J. Algebra **220** (1999), pp. 542–560.

[DPR] R. Dijkgraaf, V. Pasquier and P. Roche, *Quasi Hopf algebras, group cohomology and orbifold models*, Nuclear Phys. B Proc. Suppl. **18B** (1991), pp. 60–72.

[Dr1] V. Drinfeld, *Quantum groups*, Proceedings of the ICM Berkeley 1986, A.M.S.

[Dr2] ———, *On almost cocommutative Hopf algebras*, Leningrad Math. J. **1** (1990), pp. 321–342.

[EG1] P. Etingof and S. Gelaki, *Some properties of finite-dimensional semisimple Hopf algebras*, Math. Res. Lett. **5** (1998), 191–197.

[EG2] ———, *A method of construction of finite-dimensional triangular semisimple Hopf algebras* , Math. Res. Lett. **5** (1998), 551–561.

[EG3] ———, *On finite-dimensional semisimple and cosemisimple Hopf algebras in positive characteristic*, Internat. Math. Res. Notices **1998**, no. 16, 851–864.

[EG4] ______, *Semisimple Hopf algebras of dimension pq are trivial*, J. Algebra **210** (1998), 664-669.
[EG5] ______, *On the exponent of finite-dimensional Hopf algebras*, Math. Res. Lett. **6** (1999), 131–140.
[EV] M. Enock and L. Vainerman, *Deformation of a Kac algebra by an abelian subgroup*, Commun. Math. Phys. **178** (1996), 571-596.
[FK] S. Fomin and K. N. Kirillov, *Quadratic algebras, Dunkl elements, and Schubert calculus*, Progr. Math. **172**, Birkhauser, (1999), 146–182.
[F] N. Fukuda, *Semisimple Hopf algebras of dimension 12*, Tsukuba J. Math. **21** (1997), pp. 43–54.
[FV] R. Farnsteiner and D. Voigt, *Modules of solvable infinitesimal groups and the structure of representation-finite cocommutative Hopf algebras*, Math. Proc. Cambridge Philos. Soc. **127** (1999), pp. 441–459.
[Ga] P. Gabriel, *Étude infinitésimale des schémas en groupe et groupes formels* and *Groupes formels*,in Schémas en groupes. I: Propriétés générales des schémas en groupes. (French) Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics **151** (1970), Springer-Verlag, Berlin-New York.
[G1] S. Gelaki,*Quantum Groups of Dimension* pq^2, Israel J. Math. **102** (1997), 227-267.
[G2] ______, *On pointed Hopf algebras and Kaplansky's tenth conjecture*, J. Algebra **209** (1998), 635-657.
[G3] ______, *Some properties and examples of triangular pointed Hopf algebra*, Math. Res. Lett. **6** (1999), 563–572.
[GW] S. Gelaki and S. Westreich,*On semisimple Hopf algebras of dimension pq*, Proc. Amer. Math. Soc. **128** (2000), 39–47.
[Gñ1] M. Graña, *Pointed Hopf algebras of dimension* 32, Commun. Algebra, to appear.
[Gñ2] ______, *On Pointed Hopf algebras of dimension* p^5, Glasgow Math. J., to appear.
[Gñ3] ______, *A freeness theorem for Nichols algebras*, J. Algebra, to appear.
[Gñ4] ______, *On Nichols algebras of low dimension*, Contemp. Math., to appear.
[HaP] R. Haggenmüller and B. Pareigis, *Hopf algebra forms of the multiplicative group and other groups*, Manuscripta Math. **55** (1986), pp. 121–136.
[Hof] C. Hoffman, *On some examples of simple quantum groups*, preprint (1997).
[Ho] I. Hofstetter, *Extensions of Hopf algebras and their cohomological description*, J. Algebra **164** (1994), 264–298.
[J] M. Jimbo, *A q-difference analogue of* $U(\mathfrak{g})$ *and the Yang-Baxter equation*, Lett. Math. Phys. **10** (1985), 63–69.
[K] V. Kac, *Infinite dimensional Lie algebras*, Cambridge Univ. Press (1995), Third edition.
[Kc1] G. I. Kac, *Extensions of groups to ring groups*, Math. USSR Sbornik **5** (1968), pp. 451–474.
[Kc2] ______, *Certain arithmetic properties of ring groups*, Funct. Anal. Appl. **6** (1972), pp. 158–160.
[KP] G. I. Kac and V. G. Paljutkin, *Finite group rings*, Trans. Moscow. Math. Soc. **15** (1966),pp. 251–294.
[Ka1] Y. Kashina, *On the order of the antipode of Hopf algebras in* ${}^H_H\mathcal{YD}$, Commun. Alg. **27** (1999), pp. 1261-1273.
[Ka2] ______, *Semisimple Hopf algebras of dimension 16*, preprint (2000).
[KM] T. Kobayashi and A. Masuoka, *A result extended from groups to Hopf algebras*, Tsukuba J. Math. **21** (1997), pp. 55–58.
[Ko] B. Kostant, *Graded manifolds, graded Lie theory, and prequantization.* Lect. Notes Math. **570** (1975), pp. 177–306.
[L] R. Larson, *Characters of Hopf algebras*, J. Algebra, **17** (1971), pp. 352-368.
[LR1] R. Larson and D. Radford, *Finite dimensional cosemisimple Hopf algebras in characteristic 0 are semisimple*, J. Algebra, **117** (1988), pp. 267–289.
[LR2] ______, *Semisimple Cosemisimple Hopf Algebras*, Amer. J. of Math. **110** (1988), pp. 187–195.
[LS] R. Larson and M. Sweedler, *An associative orthogonal bilinear form for Hopf algebras*, Amer. J. of Math. **91** (1969), pp. 75–94.
[Lo1] M. Lorenz, *On the class equation for Hopf algebras*, Proc. Amer. Math. Soc. **126** (1998), 2841–2844.

[Lo2] ______, *Representations of finite-dimensional Hopf algebras*, J. Algebra **188** (1997), 476-505.

[LYZ] Jiang-Hua Lu, Min Yan & Yong-Chang Zhu, *On Set-theoretical Yang–Baxter equation*, Duke Math. J., to appear.

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

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

[L3] ______, *Introduction to quantum groups*, Birkhäuser, 1993.

[Ma1] S. Majid, *More examples of bicrossproduct and double cross product Hopf algebras*, Israel J. Math. **72** (1990), pp. 133–148.

[Ma2] ______, *Crossed products by braided groups and bosonization*, J.Algebra **163** (1994), pp. 165–190.

[Ma3] ______, *Foundations of Quantum Group Theory.* Cambridge Univ. Press, 1995.

[MS] S. Majid and Y. Soibelman, *Bicrossproduct structure of the quantum Weyl group*, J.Algebra **163** (1994), pp. 68–87.

[Mk1] A. Masuoka, *Quotient theory of Hopf algebras*, in "Advances in Hopf algebras", Lect. Notes in Pure and Appl. Math. **158** (1994), ed. J. Bergen and S. Montgomery, 107–133.

[Mk2] ______, *Self dual Hopf algebras of dimension p^3 obtained by extension*, J. Algebra **178** (1995), pp. 791–806.

[Mk3] ______, *The p^n Theorem for Hopf algebras*, Proc. Amer. Math. Soc. **124** (1996), pp. 187–195.

[Mk4] ______, *Semisimple Hopf algebras of dimension $2p$*, Commun. Alg. **23** (1995), pp. 1931–1940.

[Mk5] ______, *Some Further Classification Results on Semisimple Hopf algebras*, Commun. Alg. **21** (1996), pp. 307–329.

[Mk6] ______, *Calculations of some groups of Hopf algebra extensions*, J. Algebra **191** (1997), pp. 568–588; *Corrigendum*, J. Algebra **197** (1997), pp. 656.

[Mk7] ______, *Extensions of Hopf algebras and Lie bialgebras*, Trans. Amer. Math. Soc., to appear.

[Mk8] ______, *Extensions of Hopf algebras*, (1999), Trab. Mat. 41/99 (FaMAF).

[MiS] A. Milinski and H.-J. Schneider, *Pointed Indecomposable Hopf Algebras over Coxeter Groups*, Contemp. Math., to appear.

[MM] J. Milnor and J.C. Moore, *On the structure of Hopf algebras*, Ann. of Math. **81** (1965), pp. 211–264.

[Mo1] S. Montgomery, *Hopf Algebras and their Actions on Rings*, AMS (1993), CMBS **82**.

[Mo2] ______, *Classifying finite dimensional semisimple Hopf algebras*, Contemp. Math **229** (1998), AMS, pp. 265–279.

[MoW] S. Montgomery and S. Witherspoon, *Irreducible representations of Crossed Products*, J. Pure Appl. Alg. **129** (1998), 315–326.

[Mv] M. Movshev, *Twisting in group algebras of finite groups*, Funct. anal. appl. **27** (1994), pp. 240–244.

[Mu1] E. Müller, *Some topics on Frobenius-Lusztig kernels, I*, J. Algebra **206** (1998), 624–658.

[Mu2] ______, *Finite subgroups of the quantum general linear group*, Proc. London Math. Soc., to appear.

[Mus] I. Musson, *Finite Quantum Groups and Pointed Hopf Algebras*, preprint (1999).

[Na1] S. Natale, *On semisimple Hopf algebras of dimension pq^2*, J. Algebra **221** (1999), pp. 242–278.

[Na2] ______, *On semisimple Hopf algebras of dimension pq^2, II*, Algebr. Represent. Theory, to appear.

[Na3] ______, *Hopf algebras of dimension 12*, Preprint (March 2000).

[Na4] ______, *Quasitriangular Hopf algebras of odd dimension pq are semisimple*, Preprint (May 2000).

[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.

[Nk] D. Nikshych, *K_0-rings and twisting of finite dimensional semisimple Hopf algebras*, Commun. Alg.**26** (1998), 321–342; *Corrigendum* Commun. Alg. **26** (1998), 2019.

[OS1] U. Oberst and H.-J. Schneider, *Über Untergruppen endlicher algebraischer Gruppen*, Manuscripta Math. **8** (1973), pp. 217–241.

[OS2] ———, *Untergruppen formeller Gruppen von endlichen Index*, J. Algebra **31** (1974), pp. 10–44.

[P] B. Pareigis, *Forms of Hopf algebras and Galois theory*, in Topics in algebra, Part 1 (Warsaw, 1988), Banach Center Publ. **26** (1990), pp. 75–93, Part 1, PWN, Warsaw, 1990.

[R1] D. Radford, *The order of the antipode of a finite dimensional Hopf algebra is finite*, Amer.J. of Math. **98** (1976), pp. 333–355.

[R2] ———, *Hopf algebras with projection*, J. Algebra **92** (1985), 322–347.

[R3] ———, *Minimal Quasitriangular Hopf algebras*, J. Algebra **157** (1993), 285–315.

[RS] Reshetikhin, N. and M. Semenov-Tian-Shansky, *Quantum R-matrices and factorization problems*, J. Geom. Phys. **5**, (1988), 533–550.

[Ri] C. Ringel, *PBW-bases of quantum groups*, J. reine angew. Math. **470** (1996), 51–88.

[Ro1] M. Rosso, *Groupes quantiques et algebres de battage quantiques*, C.R.A.S. (Paris) **320** (1995), 145–148

[Ro2] ———, *Quantum groups and quantum shuffles*, Inventiones Math. **133** (1998), 399–416.

[Rz] J. Rozanski, *Braided antisymmetrizer as bialgebras homomorphism*, Reports on Math. Phys. **38** (1996), pp. 273–277.

[Sf] B. Scharfschwerdt, *The Nichols-Zöller theorem for braided Hopf algebras*, preprint (1999).

[Sbg1] P. Schauenburg, *A characterization of the Borel-like subalgebras of quantum enveloping algebras*, Comm. in Algebra **24** (1996), pp. 2811–2823.

[Sbg2] ———, *Faithful flatness over Hopf subalgebras - counterexamples*, to appear in "Interactions between ring theory and representations of algebras", Proceedings of the Murcia Euroconference.

[Sch1] H.-J. Schneider, *Normal basis and transitivity for crossed products of Hopf algebras*, J. Algebra **151** (1992), pp. 289–312.

[Sch2] ———, *Some remarks on exact sequences of quantum groups*, Commun. Algebra **21** (1993), pp. 3337–3358.

[Sch3] ———, *Lectures on Hopf algebras*, (1995), Trab. Mat. 31/95 (FaMAF).

[Sch4] ———, *Finiteness results for semisimple Hopf algebras*, Lectures at the Universidad de Córdoba (1996).

[Sch5] ———, *Some properties of factorizable Hopf algebras*, Proc. Amer. Math. Soc., to appear.

[Se1] J.-P. Serre, *Représentations linéaires des groupes finis* (1971), Hermann, Paris, Deuxièmé édition, refondue.

[Se2] ———, *Cohomologie Galoisienne* (1994), Springer, Berlin, Cinquième édition, révisée et complétée, Lecture Notes in Maths. **5**.

[Se3] ———, *Gèbres*, Enseign. Math. (2) **39** (1993), pp. 33–85.

[Si] W. Singer, *Extension theory for connected Hopf algebras*, J. Algebra **21** (1972), 1–16.

[So] A. Soloviev, *Non-unitary set-theoretical solutions to the quantum Yang–Baxter equation*, `q-alg 0003194`.

[Sr1] Y. Sommerhäuser, *Yetter-Drinfeld Hopf algebras over groups of prime order*, Preprint gk-mp-9905/59, München (1999).

[Sr2] ———, *On Kaplansky's conjectures*, in "Interactions between ring theory and representations of algebras", ed. F. van Oystaeyen and M. Saorin, M. Dekker.

[St1] D. Stefan, *Hopf subalgebras of pointed Hopf algebras and applications*, Proc. Amer. Math. Soc. **125** (1997), 3191–3193.

[St2] ———, *The set of types of n-dimensional semisimple and cosemisimple Hopf algebras is finite*, J. Algebra **193** (1997), 571–580.

[St3] ———, *Hopf algebras of low dimension*, J. Algebra **211** (1999), 343–361.

[SvO] D. Stefan and F. van Oystaeyen, *Hochschild cohomology and coradical filtration of pointed Hopf algebras*, J. Algebra **210** (1998), 535–556.

[Sul] J. Sullivan, *The uniqueness of integrals for Hopf algebras and some existence theorems of integrals for commutative Hopf algebra*, J. Algebra **19** (1971), 426-440.

[Sw] M.E. Sweedler, *Hopf algebras*, Benjamin, New York, 1969.

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

[T1] M. Takeuchi, *The Nichols-Zöller theorem for braided Hopf algebras*, preprint (1999).

[T2] ———, *Survey on braided Hopf algebras*, Contemp. Math., to appear.

[TO] J. Tate and F. Oort, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3** (1970), pp. 1–21.

[TZ] Y. Tsang and Y. Zhu, *On the Drinfeld double of a Hopf algebra*, Preprint (1998).

[Wl] R. Williams, *Finite dimensional Hopf algebras*, Ph. D. Thesis, Florida State University (1988).

[Wi1] S. J. Witherspoon, *The representation ring of the quantum double of a finite group*, J. Algebra **179** (1996), pp. 305–329.

[Wi2] ______, *The representation ring and the centre of a Hopf algebra*, Can. J. Math. **51** (1999), pp. 881–896.

[W1] S. L. Woronowicz, *Compact matrix pseudogroups*, Comm. Math. Phys. **111** (1987), pp. 613–665.

[W2] ______, *Differential calculus on compact matrix pseudogroups (quantum groups)*, Comm. Math. Phys. **122** (1989), pp. 125–170.

[ZS] S. Zhu, *On finite dimensional Hopf algebras*, Comm. Algebra **21** (1993), pp. 3871–3885.

[Z1] Y. Zhu, *Hopf algebras of prime dimension*, Internat. Math. Res. Notes **1** (1994), pp. 53–59.

[Z2] ______, *A commuting pair in Hopf algebras*, Proc. Am. Math. Soc. **125** (1997), pp. 2847-2851.

FaMAF. Medina allende y Haya de la Torre. Universidad Nacional de Córdoba. (5000) Ciudad Universitaria. Córdoba. Argentina

E-mail address: andrus@mate.uncor.edu

URL: http://www.mate.uncor.edu/andrus