On Kaplansky's fifth conjecture

Yorck Sommerhäuser

Abstract

We prove that the antipode of a semisimple Hopf algebra is an involution if the characteristic of the base field is very large.

1 Introduction

In his Chicago Lecture notes [5], I. Kaplansky set up a series of ten conjectures on Hopf algebras that he considered as important problems inside the theory. Nearly all of these conjectures turned out to be as well as puzzling as fundamental, and therefore have stimulated a lot of research in the area. Recently, important progress has been made on the first (cf. [19]), the sixth (cf. [20], [16]), the eighth (cf. [4], [37], [11]) and the tenth (cf. [33]) of these conjectures. The reader is referred to [18] and [32] for more precise information on the status of these conjectures. Closely related to the eighth conjecture is the classification problem for semisimple Hopf algebras, where A. Masuoka has contributed important results (cf. [12], [13]).

Kaplansky's fifth conjecture states that the antipode of a semisimple Hopf algebra is an involution. This was proved by R. Larson and D. Radford in two closely related papers (cf. [7], [8]) in the case of a base field of characteristic zero. Their proof is carried out in two steps, the first one being to show that the Hopf algebra under consideration is also cosemisimple, the second one being to prove that the antipode of a semisimple and cosemisimple Hopf algebra is an involution. Their methods used for the second step were also powerful enough to prove Kaplansky's seventh conjecture. In the first step, their proof rest on the observation that a complex number times its conjugate yields a nonnegative real number, and therefore does not easily generalize to fields of positive characteristic. In the present paper, we improve on this step and give a proof of the conjecture in the case of a finite dimensional Hopf algebra over a field of large positive characteristic. More precisely, we prove that the antipode of a semisimple Hopf algebra is an involution if the characteristic p of the base field satisfies the inequality $p > m^{m-4}$ where $m = 2\,(dim\ H)^2$. Our techniques rely on the analysis of the structure of the character ring of H, as do the techniques used by G. I. Kac, Y. Zhu and M. Lorenz to prove Kaplansky's eighth conjecture in characteristic zero and the techniques used by W. D. Nichols and M. B. Richmond to prove results on Kaplansky's sixth conjecture.

The article is organized as follows: In section 2, we discuss a technique to adjoin a grouplike element in such a way that the square of the antipode becomes the conjugation with the adjoined grouplike element. In section 3, we study the character of the adjoint representation in order to prove that the character ring of a semisimple Hopf algebra is itself semisimple if the characteristic is sufficiently large. The results of both sections are combined in the final section to prove the stated result on Kaplansky's fifth conjecture.

All vector spaces are defined over a base field that is denoted by K.

2 Inner automorphisms and the square of the antipode

2.1 In this section, H denotes a finite dimensional Hopf algebra. We denote the coproduct, counit, and antipode of H by Δ_H, ϵ_H and S_H respectively. We shall use the following variant of the Heyneman-Sweedler sigma notation for the coproduct:

$$\Delta_H(h) = h_1 \otimes h_2$$

The square of the antipode of H is a Hopf algebra automorphism of H. It is known that in general this is not an inner automorphism (cf. [27], [30], p. 598), although it is an inner automorphism if H is semisimple (cf. [22], Folgerung 3.3.2, p. 13 and subsection 3.2). Here an inner automorphism is meant to be the conjugation by an invertible element. It would be another step to the proof of the general case of Kaplansky's fifth conjecture if it could be shown in the semisimple case that the square of the antipode is given as the conjugation with a grouplike element. In this section, we prove that every finite dimensional Hopf algebra H can be embedded into another finite dimensional Hopf algebra, denoted by $E(H)$, in which the square of the antipode is the conjugation with a grouplike element. We do not consider the obvious generalization to an arbitrary Hopf algebra automorphism because it will not be needed in the sequel.

2.2 Define $n := 2 \; dim \, H$ and denote by $G = \mathbb{Z}/n\mathbb{Z}$ the cyclic group of order n. We denote the generator $\bar{1}$ of G by g. We know from [28], Prop. 6, p. 347 that the fourth power of the antipode is given as the composition of the conjugation with a grouplike element, namely the modular element of H, and the coconjugation with a character of H, namely the modular function. These both mappings commute. Since the order of a grouplike element obviously divides the order of the group $G(H)$ of all grouplike elements, and this order in turn divides the dimension of H by the Nichols-Zoeller theorem (cf. [19], Theorem 7, p. 384, see also [15], Theorem 3.1.5, p. 30), we conclude that $S_H^{2n} = id_H$. Therefore it is possible to turn H into a left module over the group ring $K[G]$ by specifying the action of the generator as:

$$g \rightharpoonup h := S_H^2(h)$$

We also turn H into a left $K[G]$-comodule via the trivial coaction:

$$\delta_H : H \rightarrow K[G] \otimes H, h \mapsto 1 \otimes h$$

In this way, H becomes a left Yetter-Drinfel'd module. (Cf. [15], Def. 10.6.10, p. 213 for the definition of Yetter-Drinfel'd modules, which were introduced in [36].) It is easy to see that H is even a Hopf algebra inside the category of Yetter-Drinfel'd modules (cf [15], §10.5). We can therefore form the Radford biproduct (cf. [29], [15], Theorem 10.6.5):

Definition Define the Hopf algebra $E(H)$ to be the Radford biproduct of the group ring $K[G]$ and the Hopf algebra H:

$$E(H) := H \otimes K[G]$$

It is a Hopf algebra with the multiplication:

$$(h \otimes g^k)(h' \otimes g^l) = hS_H^{2k}(h') \otimes g^{k+l},$$

the tensor product comultiplication:

$$\Delta_{E(H)}(h \otimes g^k) = (h_1 \otimes g^k) \otimes (h_2 \otimes g^k),$$

unit $1_{E(H)} = 1_H \otimes 1_{K[G]}$, counit $\epsilon_{E(H)} = \epsilon_H \otimes \epsilon_{K[G]}$ and with the antipode $S_{E(H)}(h \otimes g^k) = (1_H \otimes g^{-k})(S_H(h) \otimes 1_{K[G]})$.

It is obvious that the dimension of $E(H)$ is: $dim\ E(H) = 2\ (dim\ H)^2$.

2.3 Inside $E(H)$, the square of the antipode is the conjugation with a grouplike element:

Proposition Define $g_E := 1_H \otimes g$. Then g_E is a grouplike element of $E(H)$ that satisfies $S_{E(H)}^2(e) = g_E\ e\ g_E^{-1}$ for all $e \in E(H)$.

Proof. It is obvious that g_E is a grouplike element. Now, on the one hand we have:

$$S_{E(H)}^2(h \otimes g^k) = S_{E(H)}^2(h \otimes 1_{K[G]})\ S_{E(H)}^2(1_H \otimes g^k) = S_H^2(h) \otimes g^k$$

and on the other hand we have:

$$g_E(h \otimes g^k) = S_H^2(h) \otimes g^{k+1} = (S_H^2(h) \otimes g^k)g_E$$

This implies: $S_{E(H)}^2(h \otimes g^k) = g_E\ (h \otimes g^k)\ g_E^{-1}$. □

2.4 For our subsequent applications we need to know when $E(H)$ is semisimple or cosemisimple:

Proposition

1. $E(H)$ is semisimple if and only if H is semisimple and the characteristic p of the base field K does not divide $n = 2\, dim\, H$.
2. $E(H)$ is cosemisimple if and only if H is cosemisimple.

Proof. It is easy to see that $\Gamma_G := \sum_{k=0}^{n-1} g^k$ is a left and a right integral in $K[G]$ and that the projection to the unit component:

$$p_1 : K[G] \to K,\ \sum_{k=0}^{n-1} \alpha_k g^k \mapsto \alpha_0$$

is a left and right integral on $K[G]$, i. e. in $K[G]^*$ (cf. [15], Examples 2.1.2, p. 17, Definition 2.4.4, p. 26). Now choose a nonzero right integral $\Gamma_H \in H$ and a nonzero right integral $\rho_H \in H^*$. We then know from [29], Prop. 3, p. 333 that $\Gamma_H \otimes \Gamma_G$ is a right integral in $E(H)$ and from [29], Prop. 4, p. 335 that $\rho_H \otimes p_1$ is a right integral on $E(H)$. We now conclude from the Larson-Sweedler-Maschke theorem (cf. [9], Proposition 3, p. 84, [15], Theorem 2.2.1, p. 20) that we have:

$$\begin{aligned} E(H) \text{ is semisimple } &\Leftrightarrow \epsilon_{E(H)}(\Gamma_H \otimes \Gamma_G) \neq 0 \Leftrightarrow n\, \epsilon_H(\Gamma_H) \neq 0 \\ &\Leftrightarrow H \text{ is semisimple and } p \nmid n \end{aligned}$$

Similarly, we have:

$$\begin{aligned} E(H) \text{ is cosemisimple} &\Leftrightarrow (\rho_H \otimes p_1)(1_H \otimes 1_{K[G]}) \neq 0 \Leftrightarrow \rho_H(1_H) \neq 0 \\ &\Leftrightarrow H \text{ is cosemisimple} \end{aligned}$$

which proves the second statement. □

3 Characters and orders

3.1 In this section, H denotes a semisimple Hopf algebra. H is therefore finite dimensional (cf. [34], Cor. 2.7, p. 330 or [35], Chap. V, Ex. 4, p. 108). We shall assume throughout the whole section that the base field K is algebraically closed. By Wedderburn's theorem, H is therefore isomorphic to a finite product of full matrix rings. We denote the simple components of H by $I_1, \ldots, I_k$:

$$H = \bigoplus_{i=1}^{k} I_i$$

Choose a system $V_1, \ldots, V_k$ of irreducible modules of H such that I_i is isomorphic to $End(V_i)$, and denote the corresponding representation by:

$$\rho_i : H \to End(V_i),\ i = 1, \ldots, k$$

The dimension of V_i as a K-vector space will be denoted by: $dim\ V_i = n_i$. For every $i = 1, \dots, k$, we introduce the character χ_i of V_i as the function on H defined by:

$$\chi_i : H \longrightarrow K,\ h \mapsto Tr(\rho_i(h))$$

We can assume that $V_1 = K$, the base field, regarded as a trivial H-module via ϵ_H, which implies that $\chi_1 = \epsilon_H$. The subspace of H^* generated by the characters $\chi_1, \dots, \chi_k$ is called the character ring of H, and is denoted by $Ch(H)$. It is easy to see that it really is a subalgebra of H^* which consists precisely of the cocommutative elements of H^*.

3.2 We summarize some known properties of the character ring that will be needed in the sequel. For every module V_i, the dual vector space V_i^* is again an irreducible module, and therefore is isomorphic to one of these modules, which is denoted by $V_{\bar{i}}$. We know that separable algebras are symmetric Frobenius algebras (see subsections 3.4 and 3.8 for definitions and references). Therefore, we can conclude from [22], Folgerung 3.3.2, p. 13 that the square of the antipode is an inner automorphism. This implies that $V_i \cong V_i^{**}$ which means that the map $i \mapsto \bar{i}$ is an involution. Since we have $S_{H^*}(\chi_i) = \chi_{\bar{i}}$, where S_{H^*} is the transpose of S_H, we see that the transpose of the antipode restricts to an involution of the character ring.

It is important to note that the character ring is in fact defined over $\mathbb{Z}$. This $\mathbb{Z}$-form will be called the Grothendieck ring and be denoted by $G_0(H)$. It is also called the representation ring in K-theory or the fusion ring in conformal field theory. It is defined as follows: The tensor product of two irreducible modules decomposes into a direct sum of irreducible modules:

$$V_i \otimes V_j \cong \bigoplus_{l=1}^{k} V_l^{N_{ij}^l}$$

The number N_{ij}^l is called the multiplicity of V_l in $V_i \otimes V_j$. Now define the Grothendieck ring $G_0(H)$ to be the free $\mathbb{Z}$-module with basis $\hat{\chi}_1, \dots, \hat{\chi}_k$ and the multiplication which is defined on the basis elements by:

$$\hat{\chi}_i\ \hat{\chi}_j = \sum_{l=1}^{k} N_{ij}^l\ \hat{\chi}_l$$

This turns $G_0(H)$ into a ring with unit $\hat{\chi}_1$. The map $\hat{\chi}_i \mapsto \hat{\chi}_{\bar{i}}$ extends to a ring antihomomorphism

$$\bar{\ } : G_0(H) \ \rightarrow\ G_0(H),\ \hat{\chi} \ \mapsto\ \bar{\hat{\chi}}$$

Similarly, we have a ring homomorphism

$$\epsilon_D : G_0(H) \ \rightarrow\ \mathbb{Z},\ \hat{\chi}_i \mapsto n_i$$

which will be called the dimension character. We shall refer to the elements of the Grothendieck ring as virtual characters.

The character ring can be obtained from the Grothendieck ring by change of scalars: Namely, the map

$$K \otimes_{\mathbb{Z}} G_0(H) \;\to\; Ch(H),\; 1 \otimes \hat{\chi}_i \;\mapsto\; \chi_i$$

is a ring isomorphism. Under this isomorphism, the above antihomomorphism corresponds to the transpose of the antipode, whereas the dimension character corresponds to the evaluation at 1_H, i. e. the counit of H^* restricted to $Ch(H)$.

3.3 Two characters will play an exceptional role in the sequel: The character of the regular representation and the character of the adjoint representation. Define the left regular representation to be:

$$rg_H : H \to End(H),\; h \mapsto (h' \mapsto hh')$$

The character of the left regular representation will be denoted by χ_H: $\chi_H(h) = Tr(rg_H(h))$.

On the other hand, we have the left adjoint representation, which is defined as:

$$ad_H : H \to End(H),\; h \mapsto (h' \mapsto h_1 h' S_H(h_2))$$

We shall denote the character of the adjoint representation by χ_A: $\chi_A(h) = Tr(ad_H(h))$.

We now want to express the characters of the regular representation and the adjoint representation in terms of the irreducible characters. First of all it is clear that the two-sided ideals $I_1, \ldots, I_k$ are invariant subspaces for both representations. The restriction of the regular representation to the ideal I_i corresponds via ρ_i after the choice of a basis in V_i to the left multiplication with a matrix inside a matrix ring $M_K(n_i \times n_i)$. Here, the space of matrices with arbitrary entries in some column and zero entries in all other columns forms again an invariant subspace, and the whole matrix ring is the direct sum of n_i invariant subspaces of this form. Stated in terms of ideals, we have:

$$I_i \cong V_i^{n_i}$$

if I_i is considered as a submodule of the left regular representation. This implies:

$$\chi_H \;=\; \sum_{i=1}^{k} n_i \chi_i$$

On the other hand, if I_i is regarded as submodule of the adjoint representation, then it is easy to see that the map

$$I_i \to End(V_i) \to V_i \otimes V_i^*$$

which is the composition of ρ_i and the inverse of the canonical isomorphism $V_i \otimes V_i^* \to End(V_i), v \otimes \phi \mapsto (v' \mapsto \phi(v')v)$ is the composition of two H-linear isomorphisms and therefore itself an H-linear isomorphism. This implies:

$$\chi_A = \sum_{i=1}^{k} \chi_i \chi_{\bar{i}}$$

These calculations provide the motivation for defining the following two elements in the Grothendieck ring:

$$\hat{\chi}_H := \sum_{i=1}^{k} n_i \hat{\chi}_i \qquad \hat{\chi}_A := \sum_{i=1}^{k} \hat{\chi}_i \hat{\chi}_{\bar{i}}$$

The elements $\hat{\chi}_H$ and $\hat{\chi}_A$ will be called the virtual characters of the regular and of the adjoint representation, respectively. Note that both elements have been studied before, mostly in their dual form. For example in [7] and [8], the analogue of χ_H is denoted by x, whereas in [21] the analogue of χ_A is denoted by z. The basic properties of these two elements are stated in the next Proposition. The first statement and its proof are taken from [32], Lemma 3.12, p. 35. The dual of the second statement also appears in [21], Remark 21.

Proposition

1. For all virtual characters $\hat{\chi} \in G_0(H)$, we have: $\hat{\chi}\hat{\chi}_H = \hat{\chi}_H\hat{\chi} = \epsilon_D(\hat{\chi})\hat{\chi}_H$.
2. For all virtual characters $\hat{\chi} \in G_0(H)$, we have: $\hat{\chi}\hat{\chi}_A = \hat{\chi}_A\hat{\chi}$

Proof. We shall denote H by H_{rg} if it is viewed as an H-module via the left regular representation, and by H_{ad} if viewed as an H-module via the left adjoint representation. If V is an arbitrary H-module, we denote by V_{ϵ_H} the H-module that is obtained by regarding the vector space V as a trivial H-module via ϵ_H. Consider the map

$$f : H_{rg} \otimes V_{\epsilon_H} \to H_{rg} \otimes V,\ h \otimes v \mapsto h_1 \otimes (h_2 \to v)$$

where the arrow denotes the module action. This map is an H-linear isomorphism with inverse

$$f^{-1} : H_{rg} \otimes V \to H_{rg} \otimes V_{\epsilon_H},\ h \otimes v \mapsto h_1 \otimes (S_H(h_2) \to v)$$

Therefore, the virtual characters of both modules are equal, which implies $\hat{\chi}_H\hat{\chi} = \epsilon_D(\hat{\chi})\hat{\chi}_H$, which proves the second equality. Since $n_i = dim\ V_i = dim\ V_i^* = n_{\bar{i}}$, we see that $\hat{\chi}_H$ is invariant under the antihomomorphism. Applying the antihomomorphism to the second equality yields the first equality.

To prove the second assertion, look at the map

$$g : H_{ad} \otimes V \to V \otimes H_{ad},\ h \otimes v \mapsto (h_1 \to v) \otimes h_2$$

We prove that g is H-linear:

$$\begin{aligned} g(h \rightharpoonup (h' \otimes v)) &= g(h_1 h' S_H(h_2) \otimes (h_3 \rightharpoonup v)) \\ &= (h_1 h'_1 S_H(h_4) h_5 \rightharpoonup v) \otimes h_2 h'_2 S_H(h_3) \\ &= h \rightharpoonup g(h' \otimes v) \end{aligned}$$

Obviously, g is invertible with inverse

$$g^{-1} : V \otimes H_{ad} \to H_{ad} \otimes V, \; v \otimes h \mapsto h_2 \otimes (S_H^{-1}(h_1) \rightharpoonup v)$$

Therefore, the virtual characters of the modules $H_{ad} \otimes V$ and $V \otimes H_{ad}$ are equal, which proves the second assertion. □

We remark that the module $H_{ad} \otimes V$ contains the module V with at least multiplicity 1 since the map

$$H_{ad} \otimes V \to V, \; h \otimes v \mapsto (h \rightharpoonup v)$$

is an H-linear surjection. This observation will be improved in subsection 3.7.

3.4 Some properties of the character ring can be better understood by looking at it as a symmetric Frobenius algebra. Recall that a Frobenius algebra is a finite-dimensional algebra A which admits a nondegenerate bilinear form $\langle \cdot, \cdot \rangle : A \otimes A \to K$ which is associative in the sense that we have $\langle aa', a'' \rangle = \langle a, a'a'' \rangle$ for all a, a' and $a'' \in A$. Such a form obviously can be written as

$$\langle a, a' \rangle = f(aa')$$

for some linear form $f : A \to K$ which is determined by the bilinear form via $f(a) = \langle a, 1 \rangle = \langle 1, a \rangle$. This linear form is called the Frobenius homomorphism. (This notion is not related to the same notion used in Galois theory.) A Frobenius algebra is called symmetric if the bilinear form above is symmetric.

The following Proposition was explained to me by H.-J. Schneider (cf. also [28], Prop. 3, p. 340):

Proposition Suppose that A is a Frobenius algebra which is augmented by $\epsilon : A \to K$. Then the space of left integrals $\{x \in A \mid \forall a \in A : ax = \epsilon(a)x\}$ and also the space of right integrals $\{x \in A | \forall a \in A : xa = \epsilon(a)x\}$ is one-dimensional.

Proof. Consider the left coregular action of A on A^*: An element a of A acts on an element g of A^* yielding the element $a \rightharpoonup g$ of A^* which is defined as $(a \rightharpoonup g)(a') = g(a'a)$. One can restate the definition of a Frobenius algebra by saying that the mapping

$$A \to A^*, a \mapsto (a \rightharpoonup f)$$

is bijective, that is, A^* is a free cyclic A-module generated by the Frobenius homomorphism f. Our assertion will be proved if we can show that x is a left integral if and only if $x \rightharpoonup f$ is a multiple of ϵ. But observe that:

$$\begin{aligned}
\exists \lambda \in K : x \rightharpoonup f = \lambda\epsilon &\Leftrightarrow \exists \lambda \in K\ \forall a \in A : f(ax) = \lambda\epsilon(a) \\
&\Leftrightarrow \forall a \in A : f(ax) = f(x)\epsilon(a) \\
&\Leftrightarrow \forall a, a' \in A : f(aa'x) = f(x)\epsilon(aa') = f(x)\epsilon(a)\epsilon(a') \\
&\Leftrightarrow \forall a, a' \in A : f(aa'x) = f(a\epsilon(a')x) \\
&\Leftrightarrow \forall a' \in A : a'x = \epsilon(a')x
\end{aligned}$$

The assertion on right integrals follows by considering the opposite algebra A^{op} instead of A. $\Box$

Since the form $\langle\cdot,\cdot\rangle$ is nondegenerate, we can choose dual bases $x_1, \dots, x_n$ and $y_1, \dots, y_n$ satisfying $\langle y_i, x_j\rangle = \delta_{ij}$. From linear algebra we know that we have $a = \sum_{i=1}^n \langle a, x_i\rangle y_i = \sum_{i=1}^n \langle y_i, a\rangle x_i$ for all $a \in A$. This implies that we have:

$$\sum_{i=1}^n a x_i \otimes y_i = \sum_{i=1}^n x_i \otimes y_i a$$

The element $\sum_{i=1}^n x_i \otimes y_i$ is therefore called the Casimir element of A. It does not depend on the choice of the dual bases, but of course it does depend on the bilinear form. It is clear that $\sum_{i=1}^n x_i y_i$ is a central element of A. This element is sometimes called the Casimir element, too (cf. [1], sec. 5).

3.5 Now, it turns out that the character ring is a symmetric Frobenius algebra. This fact is also observed in [11], and similar statements can be found in several references in conformal field theory (cf. for example [1], sec. 5.8, p. 13). Essentially, this is equivalent to the well-known orthogonality relations for the characters, which in turn follow easily from Schur's Lemma. Note first that it is clear that the character χ_i vanishes on I_j if $i \neq j$. In particular, since I_1 is precisely the one-dimensional subspace of integrals, we have for some integral Λ_H that $\chi_i(\Lambda_H) = 0$ if $i \neq 1$, that is, $\chi_i \neq \epsilon_H$. If we assume that $\epsilon_H(\Lambda_H) = 1$, then, since the component of the trivial representation inside the H-module $Hom_K(V_i, V_j) \cong V_j \otimes V_i^*$ is the space of H-linear maps $Hom_H(V_i, V_j)$ which has dimension one or zero by Schur's Lemma, we have:

$$(\chi_j\ \chi_{\bar{i}})\,(\Lambda_H) \;=\; \delta_{ij}$$

This are the orthogonality relations for the characters which appear in a dualized form for arbitrary Hopf algebras in [6].

Proposition $Ch(H)$ is a symmetric Frobenius algebra with respect to the Frobenius homomorphism:

$$t_C : Ch(H) \to K, \chi \mapsto \chi(\Lambda_H)$$

The corresponding Casimir element is $\sum_{i=1}^{k} \chi_i \otimes \chi_{\bar{i}}$. The space of integrals for the character

$$\epsilon_C : Ch(H) \to K,\ \chi \mapsto \chi(1_H)$$

is spanned by χ_H.

Proof. We have to prove that the bilinear form

$$\langle \cdot, \cdot \rangle : Ch(H) \times Ch(H) \to K,\ (\chi, \chi') \mapsto t_C(\chi\chi')$$

is nondegenerate. But this is obvious since we have already found dual bases with respect to this form, since we have $\langle \chi_i, \chi_{\bar{j}} \rangle = \delta_{ij}$. Since this expression is symmetric in i and j, the form is also symmetric. The form of the Casimir element follows from the definition and the form of the integrals from Proposition 3.3. Note that $\chi_H \neq 0$ since $\chi_H(\Lambda_H) = 1$. $\square$

This also gives us another proof for the fact that χ_A is central in $Ch(H)$ which we observed in Proposition 3.3, since we now see that $\chi_A = \sum_{i=1}^{k} \chi_i \chi_{\bar{i}}$ comes from a Casimir element via multiplication of the tensorands. We note that all the structures considered above are already defined over $\mathbb{Z}$, that is, on the level of the Grothendieck ring, since if we define

$$t_G : G_0(H) \to \mathbb{Z},\ \hat{\chi}_i \mapsto \delta_{i1},$$

then by the same proof we have $t_G(\hat{\chi}_i \hat{\chi}_{\bar{j}}) = \delta_{ij}$, and ϵ_C and χ_H are also defined on the level of the Grothendieck ring.

3.6 The question that we study next is the question under which circumstances the element $\chi_A \in Ch(H)$ is invertible, because this will imply that the character ring is separable. For this purpose, it is useful to introduce some more notation. First of all, we shall use a modification of the bilinear form arising from the Frobenius homomorphism t_G. Define:

$$\langle \cdot, \cdot \rangle_* : G_0(H) \times G_0(H) \to \mathbb{Z},\ (\hat{\chi}, \hat{\chi}') \mapsto \langle \hat{\chi}, \hat{\chi}' \rangle_* := t_G(\hat{\chi}\overline{\hat{\chi}'})$$

We shall use the same notation for the bilinear form on $G_0(H) \otimes_{\mathbb{Z}} \mathbb{Q}$ which is obtained by extension of scalars. This modified bilinear form has the advantage that it puts the orthogonality relations for the characters into the more symmetric form $\langle \hat{\chi}_i, \hat{\chi}_j \rangle_* = \delta_{ij}$. This equation shows in particular that this bilinear form is symmetric and positive definite. We shall also use the convention to denote the left regular representation of the character ring or the Grothendieck ring by L_χ resp. $L_{\hat{\chi}}$, that is, we define:

$$L_\chi : Ch(H) \to Ch(H),\ \chi' \mapsto L_\chi(\chi') := \chi\chi'$$

The adjoint of $L_{\hat{\chi}}$ with respect to our scalar product then is $L_{\bar{\hat{\chi}}}$, that is, we have $\langle L_{\hat{\chi}}(\hat{\chi}'), \hat{\chi}'' \rangle_* = \langle \hat{\chi}', L_{\bar{\hat{\chi}}}(\hat{\chi}'') \rangle_*$. This holds because of the simple calculation, which of course well known in the representation theory of groups and is carried out similarly in [1], sec. 5 and [21], Theorem 8:

$$\langle \hat{\chi}\hat{\chi}', \hat{\chi}'' \rangle_* = t_G(\hat{\chi}\hat{\chi}'\overline{\hat{\chi}''}) = t_G(\hat{\chi}'\overline{\hat{\chi}''}\hat{\chi}) = t_G(\hat{\chi}'\overline{\bar{\hat{\chi}}\hat{\chi}''}) = \langle \hat{\chi}', \bar{\hat{\chi}}\hat{\chi}'' \rangle_*$$

Besides these, we have a third bilinear form on $G_0(H)$, namely the trace form:

$$G_0(H) \times G_0(H) \to \mathbb{Z},\ (\hat{\chi}, \hat{\chi}') \mapsto Tr(L_{\hat{\chi}\hat{\chi}'})$$

These three bilinear forms are linked as follows (cf. [1], sec. 5, Eq. (5.8)):

Proposition For all $\hat{\chi}, \hat{\chi}' \in G_0(H)$, we have:

$$Tr(L_{\hat{\chi}\hat{\chi}'}) = t_G(\hat{\chi}_A\hat{\chi}\hat{\chi}') = \langle \hat{\chi}_A\hat{\chi}, \overline{\hat{\chi}'} \rangle_*$$

Proof. The second equality follows directly from the definitions. For the first equality, it obviously suffices to prove $Tr(L_{\hat{\chi}}) = t_G(\hat{\chi}_A\hat{\chi})$. Now, since $\hat{\chi}_1, \ldots, \hat{\chi}_k$ is an orthonormal basis with respect to $\langle \cdot, \cdot \rangle_*$, we know from linear algebra that $L_{\hat{\chi}}(\hat{\chi}_j) = \sum_{i=1}^k \langle L_{\hat{\chi}}(\hat{\chi}_j), \hat{\chi}_i \rangle_* \hat{\chi}_i$. This implies:

$$Tr(L_{\hat{\chi}}) = \sum_{j=1}^k \langle \hat{\chi}\hat{\chi}_j, \hat{\chi}_j \rangle_* = \sum_{j=1}^k t_G(\hat{\chi}\hat{\chi}_j\hat{\chi}_{\bar{j}}) = t_G(\hat{\chi}\hat{\chi}_A)$$

which proves the assertion since $\hat{\chi}_A$ is central. $\square$

3.7 We now introduce a major object of our investigation, namely the matrix representation of the left multiplication by $\hat{\chi}_A$:

Definition Define $M = (m_{ij})_{i,j=1,\ldots,k}$ to be the matrix representation of the left multiplication by $\hat{\chi}_A$ with respect to the basis $\hat{\chi}_1, \ldots, \hat{\chi}_k$, that is, we have:

$$\hat{\chi}_A\hat{\chi}_j = \sum_{i=1}^k m_{ij}\hat{\chi}_i$$

Note that since $\hat{\chi}_1, \ldots, \hat{\chi}_k$ is an orthonormal basis with respect to $\langle \cdot, \cdot \rangle_*$, we have $\hat{\chi}_A\hat{\chi}_j = \sum_{i=1}^k \langle \hat{\chi}_A\hat{\chi}_j, \hat{\chi}_i \rangle_* \hat{\chi}_i$. The matrix elements m_{ij} therefore can be expressed as:

$$m_{ij} = \langle \hat{\chi}_A\hat{\chi}_j, \hat{\chi}_i \rangle_* = t_G(\hat{\chi}_A\hat{\chi}_j\hat{\chi}_{\bar{i}}) = Tr(L_{\hat{\chi}_j\hat{\chi}_{\bar{i}}})$$

We now summarize the basic properties of the matrix M in the following Theorem:

Theorem The matrix M has the following properties:

1. The diagonal elements of M satisfy: $dim\ Ch(H) \leq m_{ii} \leq dim\ H$, where $m_{11} = dim\ Ch(H)$.
2. M is symmetric and positive definite.
3. The eigenvalues of M are positive real algebraic integers.
4. $dim\ H$ is the greatest eigenvalue of M.
5. $dim\ H$ divides $det\ M$.

Proof. Although most of the statements are obvious, we proceed in steps.

(1) We have that $t_G(\hat{\chi}_A) = Tr(L_{\hat{\chi}_1}) = dim\ Ch(H) = k$. This means that we have for some nonnegative integers $q_2, \ldots, q_k$:

$$\hat{\chi}_A = k\hat{\chi}_1 + \sum_{i=2}^{k} q_i \hat{\chi}_i$$

and this implies $\hat{\chi}_A \hat{\chi}_j = k\hat{\chi}_j + \sum_{i=2}^{k} q_i \hat{\chi}_i \hat{\chi}_j$ and therefore $m_{jj} \geq k$. On the other hand, it is clear from dimension considerations that the module $H_{ad} \otimes V_j$ cannot contain the module V_j with a multiplicity which is greater than $dim\ H$. This proves the first statement.

(2) To prove the symmetry of M, we calculate:

$$m_{ij} = \langle \hat{\chi}_A \hat{\chi}_j, \hat{\chi}_i \rangle_* = \langle \hat{\chi}_j, \bar{\hat{\chi}}_A \hat{\chi}_i \rangle_* = \langle \hat{\chi}_j, \hat{\chi}_A \hat{\chi}_i \rangle_* = \langle \hat{\chi}_A \hat{\chi}_i, \hat{\chi}_j \rangle_* = m_{ji}$$

To prove definiteness, we observe that M is the fundamental matrix of the bilinear form $(\hat{\chi}, \hat{\chi}') \mapsto \langle \hat{\chi}_A \hat{\chi}, \hat{\chi}' \rangle_*$ on $G_0(H)$ with respect to the basis $\hat{\chi}_1, \ldots, \hat{\chi}_k$. The definiteness of M therefore follows from the definiteness of this bilinear form which in turn follows from the definiteness of $\langle \cdot, \cdot \rangle_*$:

$$\langle \hat{\chi}_A \hat{\chi}, \hat{\chi} \rangle_* = \sum_{i=1}^{k} \langle \hat{\chi}_i \hat{\chi}_{\bar{i}} \hat{\chi}, \hat{\chi} \rangle_* = \sum_{i=1}^{k} \langle \hat{\chi}_{\bar{i}} \hat{\chi}, \hat{\chi}_{\bar{i}} \hat{\chi} \rangle_* \geq 0$$

and $\langle \hat{\chi}_A \hat{\chi}, \hat{\chi} \rangle_* = 0$ implies $\hat{\chi}_{\bar{i}} \hat{\chi} = 0$ for all $i = 1, \ldots, k$, which for $i = 1$ implies $\hat{\chi} = 0$.

(3) The eigenvalues of a symmetric positive definite matrix are real and positive. On the other hand, since M has integer entries, the characteristic polynomial of M is a monic integral polynomial. Since the eigenvalues satisfy the characteristic equation, they are algebraic integers.

(4) First of all, we observe that $dim\ H$ really is an eigenvalue of M, since we have by Proposition 3.3 that $\hat{\chi}_A \hat{\chi}_H = dim H\ \hat{\chi}_H$. We now proceed to prove that this is the greatest eigenvalue of M. Since M is symmetric, we can achieve by changing the enumeration of the virtual characters $\hat{\chi}_1, \ldots, \hat{\chi}_k$ that M attains a block form:

$$M = \begin{pmatrix} M_1 & & & & \\ & M_2 & & 0 & \\ & & \ddots & & \\ & 0 & & M_{l-1} & \\ & & & & M_l \end{pmatrix}$$

where $M_1, \ldots, M_l$ are indecomposable matrices (in the sense of [3], Def. 2, p. 395) and the entries outside these blocks are zero. Now we know from the Perron-Frobenius theorem (cf. [3], sec. 13.2, p. 398) that each M_i has a unique greatest eigenvalue λ_i which is strictly positive, whose algebraic multiplicity is one, i. e. which is a simple root of the characteristic polynomial of M_i, and whose corresponding eigenvector of M_i can be chosen with strictly positive coordinates. For every M_i, we can enlarge this eigenvector to an eigenvector of M by filling up with zeros. In this way we see that, for every $i = 1, \ldots, l$, M has a strictly positive eigenvalue λ_i such that the corresponding eigenvector $x_i = (x_{ij})_{j=1,\ldots,k}$ has nonnegative coordinates. Define:

$$\hat{\chi} = \sum_{j=1}^{k} x_{ij} \hat{\chi}_j$$

The equation $M x_i = \lambda_i x_i$ then yields $\hat{\chi}_A \hat{\chi} = \lambda_i \hat{\chi}$. Applying the dimension character to this equation we get:

$$dim\ H\ \epsilon_D(\hat{\chi}) = \epsilon_D(\hat{\chi}_A)\epsilon_D(\hat{\chi}) = \lambda_i \epsilon_D(\hat{\chi})$$

Since $\epsilon_D(\hat{\chi}) = \sum_{j=1}^{k} x_{ij} n_j \neq 0$, we conclude that $\lambda_i = dim\ H$. Obviously, the greatest eigenvalue of M is the greatest eigenvalue of some M_i, and therefore is equal to $dim\ H$. Note that we have proved in addition that the algebraic multiplicity of the eigenvalue $dim H$ of M equals the geometric multiplicity, i. e. the multiplicity of $dim\ H$ as a root of the characteristic polynomial equals the dimension of the eigenspace belonging to $dim\ H$, and this equals l, the number of indecomposable blocks of M.

(5) We order the eigenvalues of M in the following way: $dim\ H = \mu_1 \geq \mu_2 \geq \ldots \geq \mu_k$. Then we see that

$$\frac{det\ M}{dim\ H} = \prod_{i=2}^{k} \mu_i$$

is on the one hand a rational number, on the other hand an algebraic integer. Since $\mathbb{Z}$ is integrally closed, it must be an integer. $\square$

3.8 Recall that a finite dimensional algebra A is called separable if there is an element $\sum_i x_i \otimes y_i \in A \otimes A$, called the separability element, such that $\sum_i x_i y_i = 1$ and $\sum_i a x_i \otimes y_i = \sum_i x_i \otimes y_i a$ for all $a \in A$. In this case, A is semisimple. A separable algebra is a symmetric Frobenius algebra (cf. [2], Chap. X, Theorem (71.6), p. 482). This is particularly easy to prove in the case where the base field is algebraically closed, because in this case the ordinary trace function yields a Frobenius homomorphism for every simple component. With our preparations, we can now prove that the character ring is a separable algebra if the characteristic of the base field is large enough. In characteristic zero, this is of course well known, see for example [37], [1], [21], Theorem 9, where in all cases the proof is based on the fact that the positive definiteness of the bilinear form $\langle \cdot, \cdot \rangle_*$ contradicts the existence of a nilpotent ideal. We exclude from the following Theorem the following three cases: $dim\ H = 2$ and $char\ K = 2$, $dim\ H = 3$ and $char\ K = 3$, $dim\ H = 4$ and $char\ K = 2$. In the first case we have the counterexample $H = K[\mathbb{Z}_2]^*$, in the second case we have the counterexample $H = K[\mathbb{Z}_3]^*$, and in the third case we have the counterexamples $H = K[\mathbb{Z}_4]^*$ and $H = K[\mathbb{Z}_2 \times \mathbb{Z}_2]^*$. Note that $K[\mathbb{Z}_2]^*$, $K[\mathbb{Z}_3]^*$, $K[\mathbb{Z}_4]^*$ and $K[\mathbb{Z}_2 \times \mathbb{Z}_2]^*$ are the only semisimple Hopf algebras of dimension ≤ 4 over an algebraically closed field, since by dimension considerations H must be commutative, and therefore [15], Theorem 2.3.1, p. 22 applies.

Theorem Suppose that we do not have: $dim\ H = 2$ and $char\ K = 2$, $dim\ H = 3$ and $char\ K = 3$, $dim\ H = 4$ and $char\ K = 2$. If the characteristic p of K is zero or greater than $(dim\ H)^{(dim\ H - 4)}$, then $\chi_A \in Ch(H)$ is invertible and $Ch(H)$ is a separable algebra with separability element $\sum_{i=1}^k \chi_i \otimes \chi_A^{-1} \chi_{\bar{i}}$. If the characteristic does divide the dimension of H, then χ_A is not invertible and $Ch(H)$ is not semisimple.

Proof. We first rule out the trivial case where $Ch(H) = H^*$, that is, H is commutative. By [15], Theorem 2.3.1, p. 22 we then could conclude that $H \cong K[G]^*$ for some finite group G. We then have that $Ch(H) \cong K[G]$, which is separable by the classical version of Maschke's theorem, and $\chi_A = dim\ H\ \epsilon_H$ is invertible.

We now turn to the more interesting case where $Ch(H) \neq H^*$. Note that in this case H is not commutative, and therefore one of the simple components $I_1, \ldots, I_k$ has dimension at least 4. Therefore, we see that $k \leq dim\ H - 3$.

Now, the matrix representation of L_{χ_A} with respect to the basis consisting of the irreducible characters is the matrix M reduced modulo p. Therefore, L_{χ_A} is invertible if $det\ M$ is not divisible by p. Therefore, we assume on the contrary that p divides $det\ M$. If $dim\ H = \mu_1 \geq \mu_2 \geq \ldots \geq \mu_k$ are the eigenvalues of M, then $det\ M$ is the product of the two integers $dim\ H$ and $\prod_{i=2}^k \mu_i$. Since it does not divide $dim\ H$, it must divide $\prod_{i=2}^k \mu_i$. But this is not possible since every eigenvalue μ_i is smaller than or equal to $dim\ H$, and therefore we see that:

$$\prod_{i=2}^{k} \mu_i \leq (dim\ H)^{k-1} \leq (dim\ H)^{(dim\ H-4)} < p$$

This implies that L_{χ_A}, and therefore χ_A, is invertible. Now the fact that the element $\sum_{i=1}^{k} \chi_i \otimes \chi_A^{-1} \chi_{\bar{i}}$ is a separability element follows from Proposition 3.5.

To prove the second statement, we observe that $\chi_A \chi_A^{-1} = \epsilon_H$ implies

$$dim\ H\ \chi_A^{-1}(1) = \chi_A(1)\chi_A^{-1}(1) = 1$$

and therefore $p \nmid dim\ H$. On the other hand, assume that $Ch(H)$ is semisimple. Then we have that $ker\ \epsilon_C = \{\chi \in Ch(H) \mid \chi(1_H) = 0\}$ is a two-sided ideal of codimension one which is therefore complemented by a one-dimensional ideal spanned by some nonzero element χ_C. Now, if $\chi \in Ch(H)$ is arbitrary, then we have $\chi - \epsilon_C(\chi)\epsilon_H \in ker\ \epsilon_C$ and therefore $(\chi - \epsilon_C(\chi)\epsilon_H)\chi_C = 0$. This implies

$$\chi\chi_C = \epsilon_C(\chi)\chi_C,$$

i. e. χ_C is a nonzero left integral with respect to the character ϵ_C. Since we already know from Proposition 3.5 that χ_H is also a left integral with respect to ϵ_C, and the space of left integrals is one-dimensional by Proposition 3.4, we can assume that $\chi_C = \chi_H$. But this means that $\chi_H \notin ker\ \epsilon_C$, and therefore $dim\ H = \epsilon_C(\chi_H) \neq 0 \in K$, which means that the characteristic p does not divide $dim\ H$. □

3.9 The Grothendieck ring of a semisimple Hopf algebra has strong similarities with the ring of integers in an algebraic number field: Both are orders in the sense of [31]. In this subsection, we comment briefly on the interrelation of the properties of orders and the properties of the matrix M considered above. A more detailed analysis of the interrelation of the theory of orders and the representation theory of Hopf algebras will be carried out in the complete version of the author's Dissertation.

Suppose that R is a Dedekind ring and denote by L its field of fractions. Define $A := G_0(H) \otimes_{\mathbb{Z}} L$. If the characteristic of L is zero, it follows from the preceding discussion that A is a separable algebra. (As we have already pointed out, similar statements also appear in [37], [32], [10], [21], [11].) Define: $B := G_0(H) \otimes_{\mathbb{Z}} R \subset A$. It is obvious that B is a R-order in A, that is, a subring which is finitely generated as an R-module such that $LB = A$ (cf. [31], sec. 8, p. 108). We shall use the following notation for the images of the virtual characters in B:

$$x_i := \hat{\chi}_i \otimes 1,\ x_H := \hat{\chi}_H \otimes 1,\ x_A := \hat{\chi}_A \otimes 1$$

The following Proposition should be compared with [31], Theorem (41.1), p. 379:

Proposition

1. If C is another R-order in A that contains B, then we have $x_A C \subset B$.

2. If $det\ M$ is invertible as an element of R, then B is a maximal R-order.

3. If B is a maximal R-order in A, then $dim\ H$ is invertible in R if it is invertible in L.

Proof. To prove the first statement, suppose we are given $x \in C$. By elementary properties of integral ring extensions (cf. [26], Theorem 8.5, p. 104), the element $xx_{\bar{i}} \in C$ is integral over R. Therefore, the eigenvalues of the left multiplication $L_{xx_{\bar{i}}}$ also satisfy an integral equation, and their sum, the trace of $L_{xx_{\bar{i}}}$, is an integral element of L which is therefore contained in R. But by Proposition 3.6, we have that $Tr(L_{xx_{\bar{i}}}) = \langle x_A x, x_i \rangle_*$, where we have extended the bilinear form $\langle \cdot, \cdot \rangle_*$ to an L-bilinear form on A. With respect to this form, $x_1, \ldots, x_k$ form an orthonormal basis, and therefore we have:

$$x_A x = \sum_{i=1}^{k} \langle x_A x, x_i \rangle_* x_i \in B$$

To prove the second statement, observe that the matrix represention of the left multiplication with x_A with respect to the basis $x_1, \ldots, x_k$ is of course M, regarded as a matrix with entries in R. The adjoint of M therefore also has entries in R. If $det\ M$ is invertible in R, then M^{-1} has entries in R, which means that L_{x_A} is invertible as an endomorphism of B, which implies that x_A is invertible in B. It therefore follows from the first statement that for every order C that contains B we have $C = x_A^{-1} x_A C \subset x_A^{-1} B \subset B$.

To prove the third statement, observe that $e := x_H / dim\ H$ is a central idempotent in A since we have $x_H^2 = dim\ H\ x_H$ by Proposition 3.3. It is clear that Be and $B(1-e)$ are R-orders in Ae resp. $A(1-e)$, and therefore $Be + B(1-e)$ is an R-order in A. But $B \subset Be + B(1-e)$, and therefore we conclude from the maximality of B that $B = Be + B(1-e)$, which implies $e \in B$. But since

$$e = \frac{1}{dim\ H} x_1 + \sum_{i=2}^{k} \frac{n_i}{dim\ H} x_i,$$

we can conclude that $1/dim\ H \in R$. $\square$

In particular, if p is a prime number that does not divide $det\ M$, then we see that $G_0(H) \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ is a maximal $\mathbb{Z}_{(p)}$-order in $G_0(H) \otimes_{\mathbb{Z}} \mathbb{Q}$, where $\mathbb{Z}_{(p)}$ denotes the localization of $\mathbb{Z}$ at the prime ideal (p).

3.10 We proceed to interrelate the matrix M and the element x_A with the discriminant and the different of B. Differents and discriminants are defined for arbitrary orders, cf. [31], sec. 10 and sec. 25. There, differents and discriminants are defined via the reduced trace map (cf. [31], sec. 9). We shall adopt here a different version of these notion via the unreduced trace map already considered in subsection 3.6. For the sake of clarity, we make this explicit in the following Definition:

Definition

1. The unreduced discriminant $D(B)$ of B over R is the ideal of R which is generated by the elements $det\,(Tr(L_{y_i y_j}))_{i,j=1,...,k}$ for all possible k-tuples $y_1, \ldots, y_k \in B$.

2. The unreduced inverse different $\mathfrak{D}'(B)$ of B over R is defined as:
$$\mathfrak{D}'(B) = \{x \in A \mid \forall y \in B : Tr(L_{xy}) \in R\}$$

3. The unreduced different $\mathfrak{D}(B)$ of B over R is defined as:
$$\mathfrak{D}(B) = \{x \in A \mid \forall y, z \in \mathfrak{D}'(B) : yxz \in \mathfrak{D}'(B)\}$$

The unreduced discriminant and the unreduced different can be expressed as follows:

Theorem Suppose that the characteristic of L is zero or does not divide $det\,M$.

1. The unreduced discriminant is the principal ideal of R generated by $det\ M$: $D(B) = (det\ M)$

2. The unreduced different is the principal ideal of B generated by x_A: $\mathfrak{D}(B) = (x_A) := x_A B$

3. $\mathfrak{D}(B)$ is a two-sided ideal of B. If L is an algebraic number field and R is its ring of integers, then the order of the quotient ring is finite and given explicitly as: $card\,(B/\mathfrak{D}(B)) = (det\ M)^{[L:\mathbb{Q}]}$.

Proof. As in [31], Theorem (10.2) it can be shown that, since B is a free R-module with basis $x_1, \ldots, x_k$, $D(B)$ is the principal ideal of R generated by $det\ (Tr(L_{x_i x_j}))$. But this determinant is equal to $det\ (Tr(L_{x_i x_{\bar{j}}}))$, up to a sign which is equal to the the determinant of the permutation matrix that describes the change of basis from $x_1, \ldots, x_k$ to $x_{\bar{1}}, \ldots, x_{\bar{k}}$. Now we know from subsection 3.7 that this is precisely the determinant of the transpose of M.

To prove the second statement, we first calculate the unreduced inverse different. We have $x \in \mathfrak{D}'(B)$ if and only if $Tr(L_{xy}) \in R$ for all $y \in B$. Since B is a free R-module with basis $x_{\bar{i}}, i = 1, \ldots, k$, this will happen if and only if we have $Tr(L_{xx_{\bar{i}}}) \in R$ for all $i = 1, \ldots, k$. But we have $Tr(L_{xx_{\bar{i}}}) = \langle x_A x, x_i \rangle_*$ by Proposition 3.6, and since $x_1, \ldots, x_k$ is an orthonormal basis with respect to this form, we have: $x_A x = \sum_{i=1}^{k} \langle x_A x, x_i \rangle_* x_i$. This implies that $x \in \mathfrak{D}'(B)$ if and only if $x_A x \in B$.

Now, if $char\ L$ is zero or does not divide $det\ M$, the same argument as in subsection 3.8 proves that $x_A \in A$ is invertible. We therefore have $\mathfrak{D}'(B) = x_A^{-1}B$. By definition, we see that $x \in \mathfrak{D}(B)$ if and only if $x_A^{-1}yxx_A^{-1}z \in x_A^{-1}B$ for all $y, z \in B$, which is, since x_A is central, equivalent to $yxz \in x_A B$. Therefore, we see that $\mathfrak{D}(B) = x_A B$.

We now prove the third statement. The fact that $\mathfrak{D}(B)$ is a two-sided ideal follows from the fact that x_A is central. Consider the exact sequence:

$$0 \longrightarrow G_0(H) \xrightarrow{L_{\hat{\chi}_A}} G_0(H) \longrightarrow G_0(H)/(\hat{\chi}_A) \longrightarrow 0$$

By the Weierstraß elementary divisors theorem, there exist $\mathbb{Z}$-bases $y_1, \ldots, y_k$ and $z_1, \ldots, z_k$ of $G_0(H)$ such that we have:

$$L_{\hat{\chi}_A}(y_i) = d_i z_i,\ i = 1, \ldots, k$$

where $d_1|d_2|\ldots|d_k$. This implies that:

$$G_0(H)/(\hat{\chi}_A) \cong \prod_{i=1}^{k} \mathbb{Z}/d_i\mathbb{Z}$$

and therefore we have that $card\ G_0(H)/(\hat{\chi}_A) = d_1 \cdot \ldots \cdot d_k$. But now, if Q denotes the matrix of the base change from $y_1, \ldots, y_k$ to $\hat{\chi}_1, \ldots, \hat{\chi}_k$, and P the matrix of the base change from $z_1, \ldots, z_k$ to $\hat{\chi}_1, \ldots, \hat{\chi}_k$, we have for $D = diag(d_1, \ldots, d_k)$:

$$M = P\, D\, Q^{-1}$$

Since $P, Q \in GL(k, \mathbb{Z})$, their determinants are units in $\mathbb{Z}$, and therefore we have $det\ M = \pm d_1 \cdot \ldots \cdot d_k$. Since M is positive definite, $det\ M$ is positive, and therefore the positive sign in the last equation is correct.

Now consider the following commutative diagram:

$$\begin{array}{ccccc}
G_0(H) \otimes_{\mathbb{Z}} R & \xrightarrow{L_{\hat{\chi}_A} \otimes id} & G_0(H) \otimes_{\mathbb{Z}} R & \longrightarrow & G_0(H)/(\hat{\chi}_A) \otimes_{\mathbb{Z}} R \\
\downarrow & & \downarrow & & \downarrow \\
B & \xrightarrow[L_{x_A}]{} & B & \longrightarrow & B/\mathfrak{D}(B)
\end{array}$$

From the diagram we conclude that $B/\mathfrak{D}(B) \cong G_0(H)/(\hat{\chi}_A) \otimes_{\mathbb{Z}} R$. Since R is a free $\mathbb{Z}$-module of rank $[L : \mathbb{Q}]$ (cf. [17], Satz (2.10), p. 13), we have that $G_0(H)/(\hat{\chi}_A) \otimes_{\mathbb{Z}} R \cong (G_0(H)/(\hat{\chi}_A))^{[L:\mathbb{Q}]}$, which implies that $card\ B/\mathfrak{D}(B) = (det\ M)^{[L:\mathbb{Q}]}$. $\Box$

The proof shows that without the assumption on the characteristic of L, the first statement still holds, while from the proof of the second statement we get that $\mathfrak{D}'(B) = \{x \in A \,|\, x_A x \in B\}$. It is easy to see that this implies at least that

$x_A B \subset \mathfrak{D}(B)$. The third statement allows the following analogy with algebraic number theory: By a theorem of Dedekind, the norm of the different is the discriminant (cf. [31], Theorem (25.2), p. 218), and in addition the norm of a principal ideal is the norm of the generating element (cf. [17], Kap. I, §6, p. 37), i. e. x_A, which is precisely $(det\ M)^{[L:\mathbb{Q}]}$. We shall call the ring $G_0(H)/(\hat{\chi}_A)$ the adjunction quotient ring of H.

3.11 To conclude this section, we change our viewpoint and investigate what can be said about the eigenvalues of M if the conclusions we want to derive are satisfied. We shall see that over fields of characteristic zero, the eigenvalues are actually integers. In order to formulate the result, we introduce some notation.

In this subsection, we shall assume that the antipode of H is an involution and that the character ring $Ch(H)$ is semisimple. Suppose that $U_1, \ldots, U_l$ is a system of irreducible $Ch(H)$-modules of dimensions $m_1, \ldots, m_l$ such that every irreducible $Ch(H)$-module is isomorphic to precisely one of these. We denote the representation and the character corresponding to U_j by σ_j resp. ξ_j:

$$\xi_j(\chi) = Tr(\sigma_j(\chi))$$

Every H^*-module can be restricted to a $Ch(H)$-module. In particular, the left regular representation of H^* restricts to a $Ch(H)$-module, and we get a decomposition:

$$H^* \cong \bigoplus_{j=1}^{l} U_j^{q_j}$$

We refer to the integer q_j as the multiplicity of the module U_j in the (restricted) left regular representation of H^*.

As in subsection 3.9, we denote by $\mathbb{Z}_{(p)}$ the localization of $\mathbb{Z}$ at the prime ideal (p), where $p = char\ K$. In particular, we have $\mathbb{Z}_{(0)} = \mathbb{Q}$. We denote by $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$ the field that contains p elements (and not the ring of p-adic integers), for $p = 0$ we define $\mathbb{Z}_0 = \mathbb{Q}$. By the universal property of localizations (cf. [26], Theorem 7.8, p. 81), we have a canonical map $\mathbb{Z}_{(p)} \to \mathbb{Z}_p$, which is the identity in the case $p = 0$. If we apply this map to all entries of M, we get a matrix M_p which we call the reduction of M modulo p. Now it turns out that often the eigenvalues of M_p are contained in the prime field $\mathbb{Z}_p$.

Theorem Suppose that S_H is an involution and that $Ch(H)$ is semisimple. Suppose furthermore that, if $p > 0$, the dimensions $m_1, \ldots, m_l$ of the irreducible $Ch(H)$-modules are not divible by p. Then the multiplicities $q_1, \ldots, q_l$ are also not divisible by p. The eigenvalues of M_p are contained in the prime field $\mathbb{Z}_p$, they are given explicitly as the images of the rational numbers

$$dim\ H\ \frac{m_1}{q_1}, \ldots, dim\ H\ \frac{m_l}{q_l}$$

under the canonical map $\mathbb{Z}_{(p)} \to \mathbb{Z}_p$, occuring with multiplicities $m_1^2, \ldots, m_l^2$.

Proof. We have seen that χ_A is a central element of $Ch(H)$. If $f_1, \ldots, f_l$ are the primitive central idempotents of $Ch(H)$, we can write:

$$\chi_A = \sum_{j=1}^{l} \beta_j f_j$$

Since M_p is the matrix representation of the left multiplication by χ_A, it is obvious that $\beta_1, \ldots, \beta_l$ are the eigenvalues of M_p, occuring with multiplicities $m_1^2, \ldots, m_l^2$.

We know from [8], Theorem 4.4, p. 279 that for $\varphi \in H^*$, we have $\chi_{H^*}(\varphi) = \mathit{dim}\ H\ \varphi(\Lambda_H)$, where Λ_H is a (two-sided) integral of H satisfying $\epsilon_H(\Lambda_H) = 1$ and χ_{H^*} denotes the character of the left regular representation of H^*. If $\varphi = \chi \in Ch(H)$, this equality reads:

$$\mathit{dim}\ H\ t_C(\chi) = \sum_{j=1}^{l} q_j \xi_j(\chi)$$

Inserting $\chi = \chi_A f_i = \beta_i f_i$, we can conclude from Proposition 3.6 that:

$$\mathit{dim}\ H\ m_i^2 = \mathit{dim}\ H\ Tr(L_{f_i}) = \dim\ H\ t_C(\chi_A f_i) = \beta_i q_i \xi_i(f_i) = \beta_i q_i m_i$$

Since we have assumed that $Ch(H)$ is semisimple, we can conclude from Theorem 3.8 that $\mathit{dim}\, H$ is not divisible by p. Therefore the left hand side in the last equality is nonzero in $\mathbb{Z}_p$, which means that β_i and q_i are nonzero in K. This implies the assertion. $\Box$

If the characteristic of the base field is zero, the above Theorem asserts that the eigenvalues of M are rational numbers. Since we have already seen in Theorem 3.7 that they are algebraic integers, they must be natural integers. In his very interesting recent article [11], M. Lorenz derives a method which can be used to give a rather different proof of the above Theorem for fields of characteristic zero. His method, which is only slightly more complicated than the one above, yields the refined result that already the number $\mathit{dim}\ H/q_j$ is an integer, which is the main assertion in the so-called class equation for Hopf algebras first proved by G. I. Kac and Y. Zhu (cf. [4], [37]).

4 Kaplansky's fifth conjecture

4.1 We now combine the results of the two preceding sections to obtain a proof of Kaplansky's fifth conjecture over fields of large positive characteristic. In this section, H continues to denote a semisimple Hopf algebra, but we do no longer assume that the base field is algebraically closed, since the more general case does not offer any additional difficulty. We summarize the technical work in the following Proposition. Note that we have already seen in subsection 3.8 that the antipode of a semisimple Hopf algebra of dimension ≤ 4 is an involution, even if H is not cosemisimple.

Proposition Suppose that $dim\ H \geq 5$. Suppose that the characteristic p of K is zero or satisfies $p > n^{n-4}$ where $n = dim\ H$. Suppose that H contains a grouplike element g that induces the square of the antipode:

$$S_H^2(h) \ = \ ghg^{-1}$$

Then H is cosemisimple and the antipode is an involution.

Proof. Because H is separable, we can assume that K is algebraically closed. Pick right integrals $\Gamma_H \in H$ and $\rho_H \in H^*$ satisfying $\rho_H(\Gamma_H) = 1$. We know from Theorem 3.8 that χ_A is invertible: $\chi_A \chi_A^{-1} = \epsilon_H$. This implies $\chi_A(g)\chi_A^{-1}(g) = 1$ and therefore:

$$Tr(S_H^2) \ = \ \chi_A(g) \neq 0$$

But by [8], Theorem 2.5, p. 274 we know that $Tr(S_H^2) = \epsilon_H(\Gamma_H)\rho_H(1_H)$ and therefore we have $\rho_H(1_H) \neq 0$, that is, H is cosemisimple. If $dim\ H \geq 6$, we now conclude from [7], Theorem 3, p. 194 that the antipode is an involution. If $dim\ H = 5$, we conclude from the Nichols-Zoeller theorem (cf. [19], Theorem 7, p. 384, see also [15], Theorem 3.1.5, p. 30) that the set of grouplike elements $G(H)$ has order 1 or order 5. In the second case, we have $H \cong K[\mathbb{Z}_5]$ and therefore $S_H^2 = id$, in the first case we have $g = 1$ and therefore $S_H^2 = id$. In both cases, we have $\epsilon_H(\Gamma_H)\rho_H(1_H) = Tr(S_H^2) = 5 \neq 0$ and therefore H is cosemisimple. $\square$

4.2 The proof of the main theorem is now trivial:

Theorem Suppose that H is a semisimple Hopf algebra. Suppose that the characteristic p of K is zero or satisfies $p > m^{m-4}$ where $m = 2(dim\, H)^2$. Then H is cosemisimple and the antipode of H is an involution.

Proof. We can assume that $dim\ H \geq 2$. We then have that $dim\ E(H) = 2\,(dim\ H)^2 \geq 8$ and that $p > 2\,(dim\ H)$. Therefore, $E(H)$ is semisimple by Proposition 2.4. Now Proposition 4.1 implies that $E(H)$ is cosemisimple and that $S_{E(H)}$ is an involution. This implies by Proposition 2.4 and the form of $S_{E(H)}$ that H is cosemisimple and that S_H is an involution. $\square$

Acknowledgement This work is part of the author's Dissertation. The author thanks the Mathematics Department of the University of Munich for the permission to publish these results. He also thanks A. Masuoka, B. Pareigis, P. Schauenburg and H.-J. Schneider for interesting discussions. H.-J. Schneider also kindly pointed out ref. [21]. A. Masuoka has given detailed comments on an earlier draft of the manuscript. His important remarks led to an improvement of the results and the presentation.

References

[1] A. Beauville: Conformal blocks, fusion rules and the Verlinde formula, Preprint, 1994

[2] C. W. Curtis/I. Reiner: Representation theory of finite groups and associative algebras, Wiley Interscience, New York, 1962

[3] F. R. Gantmacher: Matrizentheorie, Springer Verlag, Berlin, 1986 (Translated from the Russian)

[4] G. I. Kac: Certain arithmetic properties of ring groups, Funktsional. Anal. i Prilozhen. 6 (1972), 88-90. English translation: Funct. Anal. Appl. 6 (1972), 158-160

[5] I. Kaplansky: Bialgebras, Lecture Notes in Mathematics, University of Chicago, Chicago, 1975

[6] R. G. Larson: Characters of Hopf algebras, J. Algebra 17 (1971), 352-368

[7] R. G. Larson/D. E. Radford: Semisimple cosemisimple Hopf algebras, Amer. J. Math. 110 (1988), 187-195

[8] R. G. Larson/D. E. Radford: Finite dimensional cosemisimple Hopf algebras in characteristic 0 are semisimple, J. Algebra 117 (1988), 267-289

[9] R. G. Larson/M. E. Sweedler: An associative orthogonal bilinear form for Hopf algebras, Amer. J. Math. 91 (1969), 75-93

[10] M. Lorenz: Representations of finite dimensional Hopf algebras, Preprint, 1995, to appear in: J. Algebra

[11] M. Lorenz: On the class equation for Hopf algebras, Preprint, 1996

[12] A. Masuoka: The p^n-theorem for semisimple Hopf algebras, Proc. Amer. Math. Soc. 124 (1996), 735-737

[13] A. Masuoka: Semisimple Hopf algebras of dimension p^3 obtained by an extension, J. Algebra 178 (1995), 791-806

[14] H. Minc: Nonnegative matrices, Wiley Interscience, New York, 1988

[15] S. Montgomery: Hopf Algebras and their Actions on Rings, CBMS Regional Conf. Ser. in Math., no. 82, Amer. Math. Soc., Providence, R. I., 1993

[16] S. Montgomery/S. J. Witherspoon: Irreducible representations of crossed products, Preprint, 1996

[17] J. Neukirch: Algebraische Zahlentheorie, Springer Verlag, Berlin, 1992

[18] W. D. Nichols: Cosemisimple Hopf algebras. In: Advances in Hopf algebras, Marcel Dekker, New York, 1994

[19] W. D. Nichols/M. B. Zoeller: A Hopf algebra freeness theorem, Amer. J. Math. 111 (1989), 381-385

[20] W. D. Nichols/M. B. Richmond: The Grothendieck group of a Hopf algebra, J. Pure Appl. Algebra 106 (1996), 297-306

[21] W. D. Nichols/M. B. Richmond: The Grothendieck algebra of a Hopf algebra I, Preprint, 1996

[22] U. Oberst/H.-J. Schneider: Über Untergruppen endlicher algebraischer Gruppen, Manuscripta Math. 8 (1973), 217-241

[23] B. Pareigis: Endliche Hopf-Algebren, Algebra-Ber., Uni-Druck, Munich, 1973

[24] B. Pareigis: On K-Theory for Hopf algebras of finite type, Algebra-Ber., Uni-Druck, Munich, 1973

[25] D. S. Passman, D. Quinn: Involutory Hopf algebras, Trans. Amer. Math. Soc. 347 (1995), 2658-2668

[26] C. Peskine: An algebraic introduction to complex projective geometry, I. Commutative algebra, Cambridge Stud. Adv. Math. 47, Cambridge Univ. Press, Cambridge, 1996

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

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

[29] D. Radford: The structure of Hopf algebras with a projection, J. Algebra 92 (1985), 322-347

[30] D. Radford: The trace function and Hopf algebras, J. Algebra 163 (1994), 583-622

[31] I. Reiner: Maximal orders, London Math. Soc. Monogr. 5, Academic Press, London, 1975

[32] H.-J. Schneider: Lectures on Hopf algebras, Universidad de Cordoba Trabajos de Matematica, Serie "B", No. 31/95, Cordoba, Argentina, 1995

[33] D. Ştefan: The set of types of n-dimensional semisimple and cosemisimple Hopf algebras is finite, Preprint, 1995

[34] M. E. Sweedler: Integrals for Hopf algebras Ann. of Math. (2) 89 (1969), 323-335

[35] M. E. Sweedler: Hopf algebras, W. A. Benjamin, New York, 1969

[36] D. N. Yetter: Quantum groups and representations of monoidal categories, Math. Proc. Cambridge Philos. Soc. 108 (1990), 261-290

[37] Y. Zhu: Hopf algebras of prime dimension, Internat. Math. Res. Notices 1 (1994), 53-59