SEPARABILITY AND HOPF ALGEBRAS

LARS KADISON AND A.A. STOLIN

1. Introduction

Over a field of characteristic zero, the separable algebras and the strongly separable algebras coincide with one another and the class of finite dimensional semisimple algebras. In this case, separability is the cohomological point of view on semisimplicity [16]. Strong separability in this case is an additional constraint of symmetry on the separability idempotent, also an interesting point of view [7]. However, it is over a non-perfect field F of characteristic p that the three classes of algebras form a proper chain of inclusions. For example, there is a textbook example of a finite field extension which is not separable but is of course a semisimple algebra [35]. Moreover, the matrix algebra $M_n(F)$ where p divides n (and F need only have characteristic p), is separable but not strongly separable.

In this paper we survey and study separability and strong separability in its relations to Frobenius and Hopf algebras over a commutative ring k. We study the problem of when Frobenius and Hopf algebras are separable or strongly separable. It turns out that the dual bases tensor, which appears in the study of Frobenius and Hopf algebras (cf. [3, 4, 13, 19, 20]), can be used in the construction of a symmetric separability idempotent (Theorem 4.1). As an application of this result we prove that an involutive, separable Hopf k-algebra is strongly separable (Theorem 5.5). This is generalization of the following well-known result of Kreimer and Larson [22]: if a Hopf algebra H over an algebraically closed field F is involutive and semisimple, then the dimensions of simple H-modules are coprime to the characteristic of the field. Then we generalize a recent result of Etingof and Gelaki [12], which states that if Hopf F-algebra H is semisimple and cosemisimple, then H is involutive. We show that with a small condition on $2 \in k$, if a Hopf k-algebra is separable and coseparable, then H is involutive (Theorem 6.1).

Our paper is organized as follows. In Section 2 we review some of the basics of separable k-algebras and Frobenius k-algebras which are needed. In Section 3, we bring together nine conditions for a strongly separable k-algebras in [21, 14, 8, 7, 1] into one theorem (Theorem 3.4). In Section 4 we apply this theorem to Frobenius k-algebras (Theorem 4.1) and study augmented Frobenius algebras. We prove in Theorem 4.1 that a Frobenius algebra A is strongly separable if and only if the transpose of its dual bases tensor maps under the multiplication mapping to an invertible element in A. In Section 5 we study separability of Hopf k-algebras and apply Theorem 3.4 to involutive separable Hopf k-algebras (Theorem 5.5). In Section 6 we generalize the recent result of Etingof and Gelacki, and obtain involutive results for strongly separable Hopf F-algebras under various constraints on the order of the antipode and the size of p.

1991 *Mathematics Subject Classification.* 16W30, 16H05, 16L60 .

2. Preliminaries on Separable and Frobenius Algebras

Let k denote a commutative ground ring. We refer to k-algebras that are finitely generated and projective over k as being finite projective algebras.

In this section, we set up some notation and recall useful facts for separable algebras (cf. [9]) and for Frobenius algebras [10, 31, 3, 19]. We also define the trace of an endomorphism of a finite projective k-module V, its Hattori-Stallings rank (cf. [5]), as well as the standard trace of a finite projective algebra A.

Given an algebra A over k, we make use of several constructions. First, the dual of A is $A^* := \mathrm{Hom_k(A,k)}$ and is also finite projective over k. A^* has an A-bimodule structure given by

$$(afb)(c) := f(bca) \tag{1}$$

for every $a, b, c \in A$ and $f \in A^*$. An element $f \in A^*$ is called a *trace* if $af = fa$ for every $a \in A$, and a *normalized trace* if moreover $f(1_A) = 1_k$. A nonzero $f \in A^*$ is said to be *nondegenerate* if all $a \in A$ for which $fa = 0$ are zero, or all $a \in A$ for which $af = 0$ are zero.

Second, the tensor-square $A \otimes_k A$ of A has the A-bimodule structure given simply by $a(b \otimes c)d = ab \otimes cd$ for every $a, b, c, d \in A$. An element $\sum_i x_i \otimes y_i \in A \otimes A$ is called *symmetric* if $\sum_i x_i \otimes y_i = \sum_i y_i \otimes x_i$. An element $e \in A \otimes A$ is called a *Casimir element* if $ae = ea$. The A-A-bimodule epimorphism $\mu : A \otimes A \to A$ given on simple tensors by $a \otimes b \mapsto ab$ for every $a, b \in A$ is referred to as the *multiplication mapping*. Equivalently, the tensor-square is canonically identified as left A^e-modules by $a \otimes b \mapsto a \otimes \overline{b}$ with the algebra $A^e := A \otimes A^{\mathrm{op}}$, where A^{op} is the opposite algebra of A and multiplication is given by $(a \otimes \overline{b})(c \otimes \overline{d}) = ac \otimes \overline{db}$. In this way, μ may be viewed as a left A^e-module morphism.

A is a *separable k-algebra* if μ is a split A-A-epimorphism. A is a *central separable algebra, or Azumaya algebra*, if it is a separable C-algebra where C is its center. If A is k-separable and K is any intermediate ground ring for A (i.e., there are ring arrows $k \to K \to C$ forming a commuting triangle with the unit map $k \to C$) then A is separable K-algebra, since the natural mapping $A \otimes_k A \to A \otimes_K A$ pulls back the splitting map for μ.

A *separability element* $e \in A \otimes A$ is the image of 1_A under any splitting mapping of μ; equivalently, e is a Casimir element such that $\mu(e) = 1$. The Casimir condition on $e \in A^e$ is given by $ze = \mu(z)e$ for all $z \in A^e$. If e is symmetric, then $ez = e(\mu'(z) \otimes \overline{1})$ where $\mu'(a \otimes \overline{b}) = ba$. As a consequence, should a symmetric separability element exist, it is unique, since given two of these, e and f, we have

$$e = e(\mu'(f) \otimes \overline{1}) = ef = \mu(e)f = f \tag{2}$$

We will see in Section 3 that having a symmetric separability element is equivalent to A being *strongly separable*, a notion of Kanzaki from 1964 [21].

Separability is a transitive notion, in that if A is a separable k-algebra and k is a separable K-algebra, then A is seen to be a separable K-algebra. For if $\sum_i x_i \otimes y_i$ is a separability element for $k \to A$ and $\sum_j z_j \otimes w_j$ is a separability element for $K \to k$, then it is easily verified that $\sum_{i,j} x_i z_j \otimes_K w_j y_i$ is a separability element for the composite arrow $K \to A$.

If V is a finite projective k-module, there is a notion of *trace* of an endomorphism of V, $f \in \mathrm{End_k(V)}$. Let $\{x_i\}$, $\{g_i\}$ be a finite projective base for V. The trace of f

is defined to be

$$Tr\,(f) := \sum_{i=1}^{n} g_i(f(x_i)), \tag{3}$$

This definition does not depend on the choice of projective base and that $Tr\,(f \circ g) = Tr\,(g \circ f)$, for under the canonical isomorphism

$$V \otimes_k V^* \xrightarrow{\cong} \mathrm{End_k(V)}$$

given by the mapping $v \otimes f \mapsto (w \mapsto vf(w))$ $(v, w \in V, f \in V^*)$, the trace forms a commutative triangle with the multiplication mapping $V \otimes V^* \to k$ given by $v \otimes f \mapsto f(v)$. The Hattori-Stallings (HS) rank of V is the trace of the identity:

$$r_k(V) := Tr\,(\mathrm{Id_V}). \tag{4}$$

Now any algebra A over k that is finite projective has a *standard trace* $t : A \to k$ defined by

$$t(a) := Tr\,(\lambda_a), \tag{5}$$

where $\lambda_a(x) := ax$ is in $\mathrm{End_k(A)}$. Of course, $t(ab) = t(ba)$ since Tr is itself a trace. Note that the standard trace is the so-called "trace of the left regular representation." Note that $t(1) = r_k(A)$ and is not necessarily normalizable. If A is a central separable algebra over k, we will see in Section 3 that $t(1)$ is invertible in k iff A is strongly separable [14, 8].

An algebra A over k is a *Frobenius algebra* if there exists a k-linear mapping $\phi : A \to k$, called a *Frobenius homomorphism* and elements $x_1, \ldots, x_n, y_1, \ldots, y_n \in A$, called *dual bases for* A, such that for every $a \in A$,

$$\sum_i \phi(ax_i)y_i = a \tag{6}$$

or

$$\sum_i x_i\phi(y_i a) = a. \tag{7}$$

Either *dual bases* equation (as we will refer to them) implies the other.

It follows from an application of both dual bases equations that $\sum_i x_i \otimes y_i$ is a Casimir element in $A \otimes A$. As a consequence, it is easy to see that a Frobenius algebra A is separable iff there is $d \in A$ such that

$$\sum_i x_i d y_i = 1. \tag{8}$$

Since $\{x_i\}$, $\{\phi y_i\}$ is a projective base for the underlying k-module of a Frobenius algebra A, it follows that the trace of a k-endomorphism $f \in \mathrm{End_k(A)}$ is

$$Tr\,(f) = \sum_i \phi(y_i f(x_i)) \tag{9}$$

and the HS rank of A_k is $\sum_i \phi(y_i x_i)$. For example, let $A = M_n(k)$, ϕ the trace of a matrix, with dual bases given by the matrix units e_{ij}, e_{ji}. Then the standard trace $Tr\, = n\phi$ and the HS rank of A over k is $n^2 1_k$.

Another characterization of a Frobenius algebra A is that A is finite projective, and either $A_A \cong A^*_A$ or ${}_AA \cong {}_AA^*$. The free generator of A^* as an A-module in either case is a Frobenius homomorphism, and a finite projective base translates via the isomorphism to dual bases.

If k is itself a Frobenius algebra over another commutative ring K, then A is a Frobenius algebra also over K. For suppose $\psi : k \to K$ is a Frobenius homomorphism with dual bases $\{z_j\}$, $\{w_j\}$ in k. Then it is easy to verify the equations 6 and 7 for $\psi \circ \phi : A \to K$ and $\{x_i z_j\}$, $\{w_j y_i\}$. We say then that being Frobenius is a transitive notion. (Transitivity for separability and Frobenius is best formulated for noncommutative ring extensions [31, 15, 19].)

The *Nakayama automorphism* $\eta : A \to A$ may be defined by either

$$\eta(x) = \sum_i \phi(x_i x) y_i, \tag{10}$$

for every $x \in A$ or the equation in A^* given by

$$x\phi = \phi\eta(x) \tag{11}$$

for every $x \in A$ [10, 19]. It follows from either of these equations and the dual bases equations that for every $a \in A$,

$$\sum_i x_i a \otimes y_i = \sum_i x_i \otimes \eta(a) y_i. \tag{12}$$

If ψ is another Frobenius homomorphism for A, then by a theorem we call the *comparison theorem* there is an invertible $d \in A$ such that $\psi = \phi d$ in A^*. If $\{z_j\}$, $\{w_j\}$ are dual bases for ψ, it follows from Equation 7 that

$$\sum_j z_j \otimes w_j = \sum_i x_i \otimes d^{-1} y_i. \tag{13}$$

The next proposition shows that a finite projective, separable extension A/S of commutative rings is a special type of symmetric S-algebra ([2, Prop. A.4] with the different proof sketched in [8]). A *symmetric algebra* is a Frobenius algebra A such that

$${}_A A_A \cong {}_A A^*_A, \tag{14}$$

equivalently, one of the Frobenius homomorphisms is a trace (and the Nakayama automorphism is any case an inner automorphism). This proposition will be a stepping-stone to proving a similar result for noncommutative separable algebras in the next section.

Proposition 2.1. *Suppose A is a commutative ring with subring S such that A_S is a finite projective module. Then A is separable algebra over S if and only if* $\mathrm{Hom_S(A,S)}$ *is freely generated as a right A-module by the standard trace t.*

Proof. Let $\{y_i\}_{i=1}^n$ and $\{f_i\}_{i=1}^n$ be a projective basis for A_S, and note that $t(a) = \sum_{i=1}^n f_i(ay_i)$.

($\Leftarrow$) By hypothesis then there are elements $x_i \in A$ such that $x_i t = f_i$ in A^*. Then $\sum_i t(ax_i) y_i = \sum_i f_i(a) y_i = a$ for all $a \in A$ and t is a Frobenius homomorphism with dual bases $\{x_i\}$, $\{y_i\}$. It follows that the dual bases tensor $e := \sum_i x_i \otimes y_i$ is a Casimir element.

We claim that e is moreover a separability element since for all $a \in A$ we have $t(a(1 - \sum_i x_i y_i)) = \sum_i f_i(ay_i) - \sum_i f_i(y_i a) = 0$. Then by the free generator assumption on t, $\sum_i x_i y_i = 1$.

($\Rightarrow$) We may assume that a separability element has the special form $\sum_{i=1}^n x_i \otimes_S y_i$ as each $x \in A$ satisfies $x = \sum_i f_i(x) y_i$. Then, for every $a \in A$,

$$\begin{aligned} \sum_j t(ax_j)y_j &= \sum_j (\sum_i f_i(ax_j y_i)) y_j \\ &= \sum_j \sum_i f_i(ax_j) y_i y_j \\ &= \sum_j ax_j y_j = a \end{aligned} \tag{15}$$

Therefore, $ta = 0$ implies $a = \sum_i t(x_i a) y_i = 0$. In addition,

$$f(x) = \sum_j t(xx_j) f(y_j) = t(x \sum_j x_j f(y_j))$$

for every $f \in A^*$ and $x \in A$. Hence, t is free generator of A^*. □

3. Strong separability

In this section we bring together what is known about strongly separable algebras over a commutative ground ring k [21, 14, 8, 29, 7, 1]. Among the nine characterizations we shall consider, strongly separable algebras are characterized by Demeyer and Hattori as the projective separable algebras with Hattori-Stallings rank equal to an invertible element in its center [8, 14]. The theory of strongly separable algebras introduced by Kanzaki and developed by Demeyer and Hattori shows rather handily that a strongly separable algebra is a symmetric algebra [14]. This development led to the question if all projective separable algebras are symmetric algebras, which was settled in the affirmative by Endo and Watanabe using an extended notion of reduced trace for central separable algebras [11].

We will need several facts about central separable algebras summarized by the Proposition below. The proofs may be found in [2, 9, 30, 19].

Proposition 3.1. *Suppose A is a central separable algebra with center C. Then:*

1. *For every A-bimodule M, we have an A-bimodule isomorphism*
$$\alpha: \ M^A \otimes A \xrightarrow{\cong} M \tag{16}$$
given by $\alpha(m \otimes a) = ma$, where $M^A := \{m \in M | am = ma\}$.
2. *A is a progenerator A^e-module.*
3. *A_C is finite projective, and A^e is ring isomorphic to $\mathrm{End_C A}$ via the mapping β given by ($\forall\, \mathrm{a, b, x} \in \mathrm{A}$)*
$$\beta(a \otimes \overline{b})(x) = axb. \tag{17}$$
4. *There is a C-linear projection $\pi : A \to C$.*

Lemma 3.2. *Suppose A is a k-algebra with center C. Then A is k-separable if and only if A is separable over C and C is a separable over k.*

Proof. ($\Leftarrow$) This follows from transitivity of separability.

($\Rightarrow$) A is C-separable since it is separable over any intermediate ring between k and C. In order to show that C is k-separable, it suffices to show that C is a projective $C^e = C \otimes_k C$-module. By Proposition 3.1, A is projective as a C-module, therefore $A^e = A \otimes_k A^{\mathrm{op}}$ is projective as a $C \otimes_k C$-module by an easy exercise. By Proposition 3.1, C is a direct summand of A with C-linear projection $\pi : A \to C$.

Then $\pi \otimes_C \pi : A^e \to C$ is also a C-linear projection; whence C is a C^e-direct summand of the projective C^e-module A^e. Hence, C is C^e-projective. □

Since a central separable C-algebra A is finite projective over its center C, its standard trace $t : A \to C$ is defined and $t(1)$ is the Hattori-Stallings rank of the projective C-module A. The proof of the next proposition will set the pattern for much of the proof of Theorem 3.4.

Proposition 3.3. *Suppose A is a separable algebra over its center C. Moreover, suppose its Hattori-Stallings rank $c = t(1)$ is invertible in C. Then there exist elements $x_1, \dots, x_n; y_1, \dots, y_n \in A$ such that*

1. $\sum_i x_i \otimes_C y_i$ *is a symmetric separability element,*
2. $\sum_i t(xx_i)y_i = x$,
3. $\sum_i x_i t(y_i x) = x \quad (\forall \mathrm{x} \in \mathrm{A})$.

Proof. Put $t_1 = c^{-1}t$, a C-linear projection and normalized trace from A onto C. By viewing $t_1 \in \mathrm{Hom_C(A, A)}$ and surjectivity of the mapping β in Proposition 3.1, we find elements $x_1, \dots, x_n; y_1, \dots, y_n \in A$ such that $t_1(a) = \sum_i x_i a y_i$. Then $\sum_i x_i y_i = t_1(1) = 1$. Since $\mathrm{Im}\, \mathrm{t}_1 = \mathrm{C}$, we have $a \mapsto \sum_i x x_i a y_i = \sum_i x_i a y_i x$ as mappings of $A \to A$. Then injectivity of β in Proposition 3.1 implies that $\sum_i x_i \otimes_C y_i$ is a Casimir element, whence a separability element.

By the trace property of t_1 and again by Proposition 3.1, it follows that $\forall\, \mathrm{a} \in \mathrm{A}$,

$$\sum_i x_i a \otimes_C \overline{y_i} = \sum_i x_i \otimes_C \overline{a y_i}. \tag{18}$$

By applying the transposition C-automorphism on $A \otimes_C A$, we get $(\forall\, \mathrm{a} \in \mathrm{A})$

$$\sum_i a y_i \otimes_C \overline{x_i} = \sum_i y_i \otimes_C \overline{x_i a} \tag{19}$$

Whence $\sum_i y_i x x_i \in C$ for all $x \in A$. Recalling that $[A, A]$ denotes the C-linear space generated by the set $\{[x, y] := xy - yx |\ x, y \in A\}$, we note that

$$A = C \oplus [A, A]$$

as C-modules, since for every $x \in A$, $x = \sum_i x_i y_i x = \sum_i y_i x x_i + \sum_i [x_i, y_i x] \in C + [A, A]$; moreover, $C \cap [A, A] = \{0\}$ since $t_1|_C = \mathrm{Id_C}$ and $t_1([x, y]) = 0$ by the trace property.

It follows that

$$1 = \sum_i x_i y_i = \sum_i y_i x_i + \sum_i [x_i, y_i] = 1 + 0,$$

which implies that $\sum_i y_i x_i = 1$. Hence, $\sum_i y_i \otimes_C x_i$ is also a separability element, which additionally satisfies Equation 18.

We now complete the proof that $e := \sum_i x_i \otimes \overline{y_i}$ is a symmetric separability element.

$$\begin{aligned}\sum_i x_i \otimes \bar{y}_i &= \sum_i x_i(\sum_j x_j y_j) \otimes \overline{y_i} \\ &= \sum_{i,j} x_i y_j \otimes \overline{x_j y_i} \\ &= \sum_j (\sum_i x_i y_i) y_j \otimes \overline{x_j} \\ &= \sum_j y_j \otimes \overline{x_j} \qquad (20)\end{aligned}$$

Now $A^{*A} \otimes_C A \cong A^*$ via the multiplication map α in Proposition 3.1. But A^{*A} is the C-space of (non-normalized) traces. Since $A = C \oplus [A, A]$, A^{*A} is free of rank 1, being just the scalar multiples of t_1 or t. We conclude that $A \cong A^*$ as A-bimodules, so A is a symmetric algebra, with Frobenius homomorphisms t_1 or t (since they differ by an invertible element).

Let $\{u_i\}$, $\{v_i\}$ be dual bases for t_1, so that

$$x = \sum_i t_1(xu_i)v_i \qquad (21)$$

for every $x \in A$, and $\sum_i u_i v_i \in C$. Then $\{t_1 u_i\}$ and $\{v_i\}$ is a projective basis for A_C. It follows that the HS rank of A as a C-module

$$c = \sum_i (t_1 u_i)(v_i) = t_1(\sum_i u_i v_i) = \sum_i u_i v_i. \qquad (22)$$

We note moreover that the dual bases tensor of a trace Frobenius homomorphism is a symmetric element in $A \otimes A$, since for every $a \in A$

$$\begin{aligned}\sum_j au_j \otimes v_j &= \sum_{i,j} v_i \otimes t_1(u_i a u_j) v_j \\ &= \sum_i v_i \otimes u_i a. \qquad (23)\end{aligned}$$

Hence $\hat{e} := c^{-1} \sum_i u_i \otimes v_i$ is a symmetric separability element. By uniqueness of such an element we have $\hat{e} = e$. Since $t = ct_1$, Condition 2 follows from Equation 21 by replacing $\hat{e}$ with e. Condition 3 follows from e being symmetric and t a trace. □

The proposition is partially summarized by saying that a central separable algebra A has a C-linear projection onto its center C given by $a \mapsto \sum_i x_i a y_i$, is a symmetric C-algebra with a dual bases tensor and symmetric separability element $\sum_i x_i \otimes y_i$. The data (t, x_i, y_i) satisfying Conditions 1 to 3 in Proposition 3.3 we temporarily call a *strongly separable base.*

We define a *separable base* for a k-algebra A, finite projective over k, as a k-linear *trace* $f : A \to k$ together with elements $x_1, \ldots, x_n, y_1, \ldots, y_n \in A$ such that $\sum_{i=1}^n f(ax_i)y_i = a$ for all $a \in A$, and $\sum_{i=1}^n x_i y_i = 1$. In fact, f is necessarily the trace map t introduced earlier by an easy computation. For example, a commutative separable algebra A over k has a separable base by the proof of Proposition 2.1.

If (t, x_i, y_i) is a separability basis for A, then $e := \sum_i x_i \otimes_k y_i$ is a symmetric separability element by noting the following. First, a computation like Equation 23 shows that it is symmetric by letting $a = 1$. It is a Casimir element since

$$a \sum_i x_i \otimes y_i = \sum_j y_j \otimes x_j a = \sum_i x_i \otimes y_i a$$

for every $a \in A$. Since $\sum_i x_i y_i = 1$ by definition, e is a symmetric separability element. Whence a separable base is in fact a strongly separable base.

Theorem 3.4. *The nine conditions below on a finite projective k-algebra A with center C are equivalent:*

1. *A is k-separable and the Hattori-Stallings rank of A_C is an invertible element in C;*
2. *The C-algebra A has a separable base, and C is k-separable;*
3. *The standard trace t generates $\mathrm{Hom}_k(A, k)$ as a right A-module;*
4. *The k-algebra A has a separable base;*
5. *There exists an element $e = \sum_i x_i \otimes_k y_i$ such that $\sum_i x_i x \otimes_k y_i = \sum_i x_i \otimes_k x y_i$, $\forall\, x \in A$, and $\sum_i x_i y_i = 1$;*
6. *A is k-separable and there is a C-linear normalized trace map $\lambda : A \to C$;*
7. *A is k-separable and $A = C \oplus [A, A]$ as C-modules;*
8. *A has a symmetric k-separability element.*
9. *For every A-bimodule M, there is a natural k-module isomorphism $M^A \to M/[A, M]$, given by $m \mapsto m + [A, M]$, where $[A, M]$ is the k-span of $\{am - ma | m \in M, a \in A\}$.*

A is said to be strongly separable *over k if it satisfies any of the nine conditions above.*

Proof. We prove that Conditions $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 5 \Rightarrow 6 \Rightarrow 7 \Rightarrow 8 \Rightarrow 1$, and Condition $8 \Rightarrow 9 \Rightarrow 7$.

(Condition $1 \Rightarrow 2$.) ¿From Lemma 3.2, the k-separability of A implies that A is C-separable and C is k-separable. From Proposition 3.3, the C-algebra A has a strongly separable base, which is a special case of a separable base.

(Condition $2 \Rightarrow 3$.) Suppose $(t_2 : A \to C, x_i, y_i)$ is a separable base for the C-algebra A. Then we have seen that $\sum_i x_i \otimes y_i$ is symmetric separability element for A. In particular, A is a central separable algebra, and finite projective over C by Proposition 3.1. Since C is a C-direct summand in A by Proposition 3.1, it is a k-direct summand, so C is projective over k. Denote its standard trace by $t_1 : C \to k$. ¿From Proposition 2.1 and the k-separability of C, it follows that C is a symmetric k-algebra with Frobenius homomorphism t_1.

Since $\sum_i x_i \otimes_C y_i$ is a symmetric separability element, we argue as in the proof of Proposition 3.3 to show that A is a symmetric algebra over C: namely, we deduce that $A = C \oplus [A, A]$, from which it follows that $A^{*A} \cong C$ and by Proposition 3.1 with $M := A^*$ that $A^* \cong A$ as A-bimodules.

Since A is a symmetric C-algebra and C is a symmetric k-algebra, it follows that A is a symmetric k-algebra with trace Frobenius homomorphism $t' = t_1 \circ t_2$. Then t' freely generates $\mathrm{Hom}_k(A, k)$ as a right A-module. But it is readily computed (by choosing projective bases for A and C) that t' is the standard trace $t : A \to k$.

(Condition $3 \Rightarrow 4$.) Let $\{f_i\}$, $\{y_i\}$ be a finite projective basis for A over k. Let x_i be elements of A such that $f_i(x) = t(x x_i)$ for every $x \in A$: then $\sum_i t(x x_i) y_i = x$. It follows that t is a nondegenerate trace, and, from Equation 23, with $a = 1$, that $\sum_i x_i y_i = \sum_i y_i x_i$.

We need to show that $\sum_i x_i y_i = 1$: this will finish a proof that (t, x_i, y_i) is a separable base for A over k. For every $a \in A$,

$$\begin{aligned} t(a(1 - \sum_i x_i y_i)) &= t(a) - t(a \sum_i x_i y_i) \\ &= \sum_i f_i(a y_i) - t(a \sum_i x_i y_i) \\ &= t(a(\sum_i y_i x_i - \sum_i x_i y_i)) = 0. \end{aligned} \tag{24}$$

It follows from nondegeneracy of t that $1 - \sum_i x_i y_i = 0$.

(Condition 4 $\Rightarrow$ 5.) Let (t, x_i, y_i) be a separable base. Then $\sum_i x_i \otimes_k y_i$ is a symmetric separability element for A. It follows that $\sum_i x_i x \otimes_k y_i = \sum_j x_j \otimes x y_j$ for every $x \in A$.

(Condition 5 $\Rightarrow$ 6.) Let $\lambda'(a) = \sum_i x_i a y_i$, $\forall\, \mathrm{a} \in \mathrm{A}$. Then $\lambda' : A \to A$ is C-linear, satisfies $\lambda'(xy) = \lambda'(yx)$ and $\lambda'|_C = \mathrm{Id}_\mathrm{C}$. It follows that $C \cap [A, A] = 0$. At the same time, $\sum_j y_j a x_j \in C$ for every $a \in A$: then $a = \sum_i x_i y_i a = \sum_i y_i a x_i + \sum_i [x_i, y_i a] \in C + [A, A]$, so $A = C \oplus [A, A]$ as C-modules. It follows that the projection $\lambda : A \to C$ for this decomposition, defined by $\lambda(a) := \sum_j y_j a x_j$, is a C-linear normalized trace. Also, $1 = \sum_i x_i y_i = \sum_i y_i x_i + \sum_i [x_i, y_i]$, where $1, \sum_i y_i x_i \in C$, whence $\sum_i y_i x_i = 1$. It follows that $\sum_i y_i \otimes_k x_i$ is a separability element for A.

(Condition 6 $\Rightarrow$ 7.) Trivial.

(Condition 7 $\Rightarrow$ 8.) Since A is k-separable, A is C-separable and C is k-separable by Lemma 3.2. Also by hypothesis, we see that there is a C-linear projection and normalized trace λ of A onto C with kernel $[A, A]$. By Proposition 3.1, there is $e = \sum_i x_i \otimes_C \overline{y_i} \in A^e$ such that $\beta(e) = \lambda$.

We now argue just like in the first stage of the proof of Proposition 3.3 that e is a symmetric separability element.

As in the proof of (2 $\Rightarrow$ 3) we see that C is finite projective over k, so there is a trace $t' : C \to k$ forming part of a separable basis (t', u_j, v_j) by Proposition 2.1, equation 15. Then $\sum_j u_j \otimes_k v_j$ is a symmetric separability element for C. It follows that $\sum_{i,j} x_i u_j \otimes_k v_j y_i$ is a symmetric separability element for the k-algebra A.

(Condition 8 $\Rightarrow$ 1) First of all, note that A is C-separable, C-finite projective, and has a symmetric separability element $e = \sum_i x_i \otimes_C y_i$, since this comes from the hypothesis via the canonical epi $A \otimes_k A \to A \otimes_C A$. Let $t : A \to C$ be the standard trace, and denote the C-rank of A, $t(1) = c$.

Now argue with the element e as in the proof of Proposition 3.3 that we have a C-linear projection and normalized trace $\beta(e) := t_1 : A \to C$, that $A = C \oplus [A, A]$, and $A \overset{\cong}{\to} A^*$ as A-bimodules, given by $a \mapsto t_1 a$. Then $\sum_i t_1(x_i) y_i c = 1$ by Equations 21 and 22.

(Condition 8 $\Rightarrow$ 9.) Define an inverse to the natural k-linear mapping $\Phi_M : M^A \to M/[A, M]$ by $\Psi_M : m + [A, M] \mapsto em$, where e is a symmetric separability element and we view M as a left A^e-module. Then Ψ_M is well-defined since e and its twist are Casimir elements, and is an inverse to Φ_M since $\mu(e) = 1$. It follows that M^A and $M/[A, M]$ are naturally isomorphic.

(Condition 9 $\Rightarrow$ 7.) We first let $M = A$. Then the natural mapping $\Phi_A : A^A = C \overset{\cong}{\to} A/[A, A]$ given by $x \mapsto x + [A, A]$ has inverse $\Psi_A : A/[A, A] \to C$. If $\iota : C \to A$ and $\iota' : [A, A] \to A$ denote the inclusion maps, then $\iota \circ \Psi_A$ is a splitting for the cokernel exact sequence of ι',

$$0 \to [A, A] \to A \to A/[A, A] \to 0.$$

This proves that $A = C \oplus [A, A]$.

Now let $M = A \otimes_k A$. Set $e := \Psi_M(1 \otimes 1 + [A, M]) \in (A \otimes A)^A$. Since μ is an A-bimodule homomorphism $M \to A$ sending $1 \otimes 1$ into 1, it follows from naturality of Ψ that $\mu(e) = 1$. □

Let us observe a number of corollaries of this theorem. First, it is clear that a separable commutative algebra A which is projective (and automatically finitely generated by a theorem of Villamayor) over k, satisfies any one of several of the nine conditions, and therefore is strongly separable.

Corollary 3.5. *A separable, projective commutative algebra is strongly separable.*

Secondly, it follows from Condition 3 that a strongly separable algebra A is a symmetric algebra, since t is necessarily nondegenerate, so $A^* \cong A$ as A-bimodules. Consequently, the symmetric separability element $e = \sum_i x_i \otimes_C y_i$ belonging to A is an invertible solution of the Yang-Baxter Equation (YBE), when viewed in $\mathrm{End_k(A \otimes A)}$, by a theorem in Beidar-Fong-Stolin [3]. Now applying Condition 2, Proposition 3.3 and its proof once in the last line below, we have for every $a, b \in A$

$$\begin{aligned} e(a \otimes b)e &= \sum_{i,j} x_i a x_j \otimes y_i b y_j \\ &= \sum_j \sum_i b x_i x_j y_i \otimes y_j a \\ &= b \otimes \sum_j t_1(x_j) y_j a \\ &= c^{-1} b \otimes a \end{aligned} \tag{25}$$

where c is the HS rank of A over C and $t_1 = \beta(e) = c^{-1}t$. Thus $e^{-1} = ce$ and the inner automorphism by e in $\mathrm{Aut}_k\, A \otimes A$ is the permutation solution of the YBE.

It follows from Condition 1 that strong separability and separability are indistinguishable if k is a characteristic zero field.

Corollary 3.6. *If A is a separable algebra over a field k of characteristic zero, then A is strongly separable.*

Proof. By Wedderburn's theory, we have a ring isomorphism,

$$A \cong M_{n_1}(D_1) \times \cdots \times M_{n_t}(D_t), \tag{26}$$

where the center of each division ring D_i is a field F_i finite separable over k and the center of A, $C \cong F_1 \times \cdots \times F_t$. It follows easily from Equation 4 that the HS rank of A over C is

$$r_C(A) = (n_1^2[D_1 : F_1], \ldots, n_t^2[D_t : F_t]) \in C. \tag{27}$$

But each entry is nonzero, so A is strongly separable. □

Corollary 3.7. *If A is a separable algebra over a field k of characteristic p, then A is strongly separable if and only if each simple A-module M has dimension over $Z(\mathrm{End_A(M)})$ not divisible by p.*

Proof. Wedderburn theory gives us the decomposition 26 and consequently the C-rank 27 where $C \cong F_1 \times \cdots \times F_t$. The hypothesis on simple A-modules is equivalent to each entry in 27 being nonzero in the field F_i of characterisic p, since a simple A-module M is of the form $D_i^{n_i}$ and $Z(\mathrm{End_A(M)}) = \mathrm{F_i}$ by Schur theory. It follows that the HS rank of A is invertible and A is strongly k-separable. □

By Proposition 3.3, a central separable k-algebra with Hattori-Stallings rank invertible in k is a strongly separable k-algebra. The reader might enjoy showing how the following obviously separable algebra A with zero HS rank fails each of the nine conditions in the theorem: Let p be a prime, $F = \mathcal{Z}_p$ and $A = M_p(\mathcal{Z}_p)$. For example, the central separable F-algebra A does not satisfy $A = F \oplus [A, A]$ (Condition 7) since $1 \in [A, A]$. Although A has several separability elements, it has no symmetric separability element by the theorem.

We believe that Condition 7 for strong separability in Theorem 3.4 is due to Kanzaki [21], as well as Condition 5, Conditions 2, 3 and 4 are due to Demeyer [8], Condition 1 to Hattori and Demeyer, Condition 6 to Hattori [14], and Condition 9 to Aguiar [1]. Condition 8 for strong separability is stated by Demeyer [8], considered in [7] for $k = \mathcal{C}$, and proven in [18]. Onodera's Condition [29] is closely related to Conditions 1 and 8 via Equations 22 and 23: it states that A is strongly separable iff it has a trace and Frobenius homomorphism t with dual bases $\{u_i\}$, $\{v_i\}$ such that $\sum_i u_i v_i$ is invertible.

4. Augmented Frobenius Algebras

Let k be a commutative ring throughout this section. We first consider when a Frobenius algebra is strongly separable.

Theorem 4.1. *Suppose A is a Frobenius algebra with Frobenius homomorphism ϕ and dual basis $\{x_i\}$, $\{y_i\}$. Then*

$$u := \sum_i y_i x_i$$

is invertible in A if and only if A is strongly separable. Moreover, the Nakayama automorphism is given by

$$\eta(x) = uxu^{-1} \tag{28}$$

for every $x \in A$.

Proof. ($\Rightarrow$) Consider the element $e := \sum_i y_i \otimes x_i u^{-1}$ in $A \otimes A$. Then e satisfies the Kanzaki Condition 5 for strong separability by choice of u and the fact that the dual bases tensor is Casimir.

¿From Equation 12 we obtain

$$\eta(a)e = \sum_i y_i \otimes x_i a u^{-1},$$

for every $a \in A$. Applying the multiplication mapping μ to both sides of this equation, we obtain Equation 28.

($\Leftarrow$) By Demeyer's Condition 4 for strong separability, A has a (stongly) separable base (t, z_j, w_j) where t is the standard trace on A $\{z_j\}$, $\{w_j\}$ form dual bases for t, $\sum_j z_j \otimes w_j$ is symmetric, and $\sum_j z_j w_j = 1$. Then by the comparison theorem there exists $d \in A^\circ$ such that $t = \phi d$. Then by Equation 13 we have

$$\sum_i x_i \otimes y_i = \sum_j z_j \otimes dw_j.$$

Then

$$u := \sum_i y_i x_i = d \sum_j w_j z_j = d$$

and u is invertible.

We finally note from Equations 6 and 10 that for every $x \in A$,

$$\eta(x) = \sum_i \phi(x_i x) y_i = \sum_i t u^{-1}(z_j x) u w_j = u x u^{-1}. \quad \square$$

The implication $\Leftarrow$ for k a field of characteristic zero is equivalent to Beidar-Fong-Stolin's [3, Proposition 4.3].

A k-algebra A is said to be an *augmented algebra* if there is an algebra homomorphism $\epsilon : A \to k$, called an *augmentation*. An element $t \in A$ satisfying $ta = \epsilon(a)t$, $\forall\, \mathrm{a} \in \mathrm{A}$, is called a *right integral* of A. It is clear that the set of right integrals, denoted by $\int_A^r$, is a two-sided ideal of A, since for each $a \in A$, the element at is also a right integral. Similarly for the space of left integrals, denoted by $\int_A^\ell$.

Now suppose that A is a Frobenius algebra with augmentation ϵ. We claim that a nontrivial right integral exists in A. Since $A^* \cong A$ as right A-modules, an element $n \in A$ exists such that $\phi n = \epsilon$ where ϕ is a Frobenius homomorphism. Call n the *right norm* in A with respect to ϕ. Given $a \in A$, we compute in A^*:

$$\phi n a = (\phi n) a = \epsilon a = \epsilon(a)\epsilon = \phi n \epsilon(a).$$

By nondegeneracy of ϕ, n satisfies $na = n\epsilon(a)$ for every $a \in A$.

Proposition 4.2. *If A is an augmented Frobenius algebra, then the set $\int_A^r$ of right integrals is a two-sided ideal which is free cyclic k-summand of A generated by a right norm.*

Proof. The proof is nearly the same as in [32, Theorem 3], which assumes that A is also a Hopf algebra. The proof depends on establishing the equation, for every right integral t,

$$t = \phi(t) n. \quad \square \tag{29}$$

The right norm in A is unique up to a unit in k. Similarly the space $\int_A^\ell$ of left integrals is a rank one free summand in A, generated by any left norm. If $\int_A^r = \int_A^\ell$, A is said to be *unimodular*. In general the spaces of right and left integrals do not coincide, and one defines an augmentation on A that measures the deviation from unimodularity. In the notation of the proposition and its proof, for every $a \in A$, the element an is a right integral since the right norm n is. From Equation 29 one concludes that $an = \phi(an)n = (n\phi)(a)n$. The function,

$$m := n\phi : A \to k \tag{30}$$

is called the *right modular function*, which is an augmentation since $\forall\, \mathrm{a, b} \in \mathrm{A}$ we have $(ab)n = m(ab)n = a(bn) = m(a)m(b)n$ and n is a free generator of $\int_A^r$.

We moreover have

$$m \circ \alpha = \epsilon. \tag{31}$$

by [20, Prop. 3.2]. As a consequence, if A is an augmented symmetric algebra, then A is unimodular.

Proposition 4.3. *Suppose A is a separable augmented Frobenius algebra with norm n and augmentation ϵ. Then $\epsilon(n)$ is invertible and A is unimodular.*

Proof. For any augmented Frobenius algebra $(A, \phi, x_i, y_i, \epsilon)$ we note the useful identity for the right norm n,

$$n = \sum_i \phi(nx_i)y_i = \sum_i \epsilon(x_i)y_i. \tag{32}$$

If A is moreover separable, there is $d \in A$ such that $\sum_i x_i d y_i = 1$ by Equation 8. Then by Equation 32

$$\sum_i \epsilon(x_i)\epsilon(d)\epsilon(y_i) = \epsilon(d)\epsilon(n) = 1.$$

It follows that $\epsilon(n)$ is a unit in k. But for every $x \in A$, a computation like in [25], namely,

$$\epsilon(x)\epsilon(n)n = nxn = m(x)n^2 = m(x)\epsilon(n)n,$$

gives $\epsilon(x)\epsilon(n) = m(x)\epsilon(n)$, whence $\epsilon(x) = m(x)$. Thus, A is unimodular. ☐

5. Hopf Algebras

Pareigis proved in [32] that every finite projective Hopf algebra H has a bijective antipode S (with inverse denoted by S^{-1}). In addition, the dual Hopf algebra H^* has a right Hopf module structure over H with right H-comodule H^* the dual of the natural H^*-module H^* and right H-module H^* the twist by S of the natural left H-module H^* [32]. The fundamental theorem of Hopf modules then leads to the isomorphism,

$$\int_{H^*}^{\ell} \otimes H \cong H^*$$

as left H-modules. Whence H is a so-called P-Frobenius algebra where $P := (\int_{H^*}^{\ell})^*$, where $\int_{H^*}^{\ell}$ is the invertible k-module of left integrals in H^* [34]. If $P \cong k$, H is an ordinary Frobenius algebra with Frobenius homomorphism a left norm in H^* [24, k = pid]. That $\int_{H^*}^{\ell} \cong P \cong k$ is guaranteed if k has Picard group zero (e.g. when k is a field, semi-local or a polynomial ring).

In this section, k will continue to denote a commutative ring and *a Hopf algebra H is always finite projective as a k-module; moreover, we will assume H is a Frobenius algebra with a special Frobenius homomorphism $f : H \to k$.* We require of f that it be a right norm in the dual Hopf algebra H^*, which is no loss of generality since S is an anti-automorphism and Sf is a left norm in H^*. We will refer to such an H as simply Hopf algebra in this section.[1] It has been shown that also H^* and the quantum double $D(H)$ are Hopf algebras in this sense [20], and more detailed proofs may be found in either of [13] or [19].

[1] These Hopf algebras have been called FH-algebras by Pareigis [33].

Proposition 5.1. *Let H be a Hopf algebra with Frobenius homomorphism and right norm f and right norm t in H. Then $(f, S^{-1}t_2, t_1)$ is a Frobenius system for H.*

Proof. This follows from a short computation like that in [13, Lemma 1.5] using $a \leftharpoonup f = 1_H f(a)$ for every $a \in H$:

$$\begin{aligned}\sum_{(t)} S^{-1}(t_2)f(t_1 a) &= \sum_{(t),(a)} S^{-1}(t_3)f(t_1 a_1)t_2 a_2 \\ &= \sum_{(a)} f(ta_1)a_2 \\ &= f(t)a = a,\end{aligned}$$

since $ft = \epsilon$, the counit, and so $f(t) = 1$. □

This proposition has two corollaries.

Corollary 5.2. *A Hopf algebra H is separable if and only if $\epsilon(t)$ is invertible.*

Proof. The forward implication follows from Proposition 4.3. The backward implication follows from the proposition, since $\frac{1}{\epsilon(t)} \sum_{(t)} S^{-1}(t_2) \otimes t_1$ is a separability element. □

Recall that a Hopf subalgebra of H is a subalgebra K such that $S(K) = K$ and $\Delta(K) \subseteq K \otimes K$. The next corollary is generalizes a proposition in [25] for semisimple Hopf algebras over a field.

Corollary 5.3. *Suppose k is a local ring. If H is a separable Hopf algebra free over k and K is a k-free Hopf subalgebra, then K is separable as well.*

Proof. It follows from [20, Lemma 5.2] that H is free as the natural right K-module. Let n be a right norm for K. By expanding t in basis for H over K, we find $\Lambda \in H$ such that $t = \Lambda n$. Then $\epsilon(t) = \epsilon(\Lambda)\epsilon(n)$. Since $\epsilon(t)$ is invertible and the non-units in k form an ideal, $\epsilon(n)$ is invertible. Whence K is separable. □

We use the notation $a \leftharpoonup g := \sum_{(a)} g(a_1)a_2$ and $g \rightharpoonup a := \sum a_1 g(a_2)$ for the standard right and left actions of $g \in H^*$ on $a \in H$.

Proposition 5.4. *Given an Hopf algebra H with right norm and Frobenius homomorphism $f \in H^*$ and right norm $t \in H$, the Nakayama automorphism for f and its inverse are given by:*

$$\eta(a) = S^2(a \leftharpoonup m^{-1}) = (S^2 a) \leftharpoonup m^{-1}, \tag{33}$$

$$\eta^{-1}(a) = S^{-2}(a \leftharpoonup m) = (S^{-2}a) \leftharpoonup m.$$

Proof. We compute (like in [13, Lemma 1.5] but opposite Nakayama automorphism) using the right modular function m given by $at = m(a)t$ for all $a \in H$:

$$\begin{aligned} S^2(\eta^{-1}(a)) &= S^2(\sum S^{-1}(t_2)f(at_1)) \\ &= \sum f(at_1)S(t_2) \\ &= \sum f(a_1t_1)a_2t_2S(t_3) \\ &= \sum f(a_1t)a_2 \\ &= \sum m(a_1)a_2 \end{aligned}$$

The rest of the proof follows from noting that m is a group-like element in H^*, so the convolution-inverse $m^{-1} = m \circ S$ and $m \circ S^2 = m$. □

Recall that a Hopf algebra is involutive if $S^2 = \mathrm{Id}$.

Theorem 5.5. *Suppose H is an involutive, separable Hopf algebra. Then H is strongly separable.*

Proof. We continue with the notation in the two propositions above. By Proposition 4.3, H is unimodular and $\epsilon(t)$ is invertible in k by its proof. It follows from Proposition 5.1 that the dual bases tensor is $\sum S^{-1}(t_2) \otimes t_1$, which since $S = S^{-1}$ satisfies

$$\sum_{(t)} t_1S^{-1}(t_2) = \epsilon(t)1_H$$

a unit, whence H is strongly separable by Theorem 4.1. □

As a special case of the last proposition we have similar results over fields by Kreimer, Larson [22], Beidar-Fong-Stolin [4], and Aguiar [1].

We compute the trace of the k-linear automorphism $S^2 : H \to H$ in the next proposition.

Proposition 5.6. *If H is a Hopf algebra with right norms $t \in H$ and $f \in H^*$ such that $f(t) = 1$, then*

$$Tr\,(S^2) = f(1)\epsilon(t) \tag{34}$$

Proof. Since f is a Frobenius homomorphism with dual bases $\{S^{-1}(t_2)\}$, $\{t_1\}$, it follows from Equation 9 that the trace

$$Tr\,(S^2) = \sum_{(t)} f(t_1S^2(S^{-1}(t_2)) = \sum f(t_1S(t_2)) = \epsilon(t)f(1)$$

as claimed. □

If H is a finite dimensional Hopf algebra over a field, it follows that the trace of S^2 is nonzero iff H is semisimple and cosemisimple, a result of Larson-Radford [23]. We then easily obtain the following generalization from Corollary 5.2, also noted in [4]:

Proposition 5.7. *If H is a Hopf k-algebra, then $Tr\,(S^2)$ is invertible if and only if H is separable and coseparable.*

Now let us assume that H is strongly separable over an algebraically closed field k. Then it follows from Theorem 4.1 that $u = \sum_{(t)} t_1 S^{-1}(t_2)$ is invertible. In this case $H \cong \oplus_\lambda M_{n_\lambda}(k)$, where $M_n(k)$ is the algebra of $n \times n$-matrices with k-entries. Then we have the following

Proposition 5.8. *Let tr_λ be the matrix trace on $M_{n_\lambda}(k)$. Then*

$$f(x) = \sum_\lambda n_\lambda tr_\lambda(xu^{-1})$$

.

Proof. First we note that $f(xy) = f(yu^{-1}xu)$ by Theorem 4.1. Then $f(xyu) = f(yuu^{-1}xu) = f(yxu)$ and therefore $f(xu) = \sum_\lambda T_\lambda tr_\lambda(x)$ for some $T_\lambda \in k$ or $f(x) = \sum_\lambda T_\lambda tr_\lambda(xu^{-1})$. We must prove that $T_\lambda = n_\lambda$.

Since H is a Frobenius algebra with Frobenius homomorphism f, we observe $T_\lambda \neq 0$. Let E^λ_{ij} be the matrix units in $M_{n_\lambda}(k)$. Then $\{E^\lambda_{ij}\}$; $\{(1/T_\lambda)E^\lambda_{ji}u\}$ form dual base with respect to f. Let us introduce $u_\lambda = \sum_{ij}(1/T_\lambda)E^\lambda_{ij}E^\lambda_{ji}u$. Then clearly $u = \sum_\lambda u_\lambda$ and we have:

$$u = \sum_\lambda (u_\lambda) = \sum_{ij\lambda}(1/T_\lambda)E^\lambda_{ij}E^\lambda_{ji}u = \sum_\lambda (1/T_\lambda)n_\lambda u_\lambda$$

which proves the Proposition.

□

Corollary 5.9. *Suppose H is an involutive, semisimple Hopf algebra over an algebraically closed field k. Then $Tr(S^2) = dimH$ and if H is cosemisimple then $dimH \neq 0$ in k.*

Proof. Theorem 5.5 and its proof imply that H is strongly separable and $u = \sum_{(t)} t_1 S^{-1}(t_2) = \epsilon(t)1_H$ Then

$$Tr\,(S^2) = \epsilon(t)f(1) = \epsilon(t)\sum_\lambda n_\lambda tr_\lambda(u^{-1}) = \sum_\lambda n_\lambda tr_\lambda(1_{M_{n_\lambda}(k)}) = \sum_\lambda n^2_\lambda = dimH$$

If H is cosemisimple we already know that $Tr\,(S^2) \neq 0$ and hence $dimH \neq 0$. □

6. Separability and Order of the Antipode

It was proved recently in [12] that if a Hopf algebra H over a field k is semisimple and cosemisimple, then $S^2 = \mathrm{Id}$. Equivalently if H is separable and coseparable over a field k, then $S^2 = \mathrm{Id}$. Using this result we prove the corresponding statement for Hopf algebras over rings.

Theorem 6.1. *Let k be a commutative ring in which 2 is not a zero divisor. Let H be separable and coseparable Hopf algebra which is finite projective over k. Then $S^2 = \mathrm{Id}$.*

Proof. First we note that H is unimodular and counimodular. Then it follows from [4, Corollary 3.9] or [20, Theorem 4.7] that $S^4 = \mathrm{Id}$. Localizing with respect to the set $T = \{2^n, n = 0, 1, ..\}$ we may assume that 2 is invertible in k. Then $H = H_+ \oplus H_-$ where $H_\pm = \{h \in H : S^2(h) = \pm h\}$, respectively. We have to prove that $H_- = 0$. It suffices to prove that $(H_-)_m = 0$ for any maximal ideal m in H. Since H_m/mH_m is separable and coseparable over the field k/m, we deduce from the main theorem in [12] that $(H_-)_m \subset mH_m$ and therefore $(H_-)_m \subset m(H_-)_m$.

The required result follows from the Nakayama Lemma because H_- is a direct summand in H. □

Corollary 6.2. *If H is separable and coseparable over a commutative ring k, then H is strongly separable over k.*

We believe that strong separability of a Hopf algebra H over a field k and the fact that $gcd\ (dimH,\ char(k)) = 1$ imply that H is coseparable. This fact is known in case of fields of characteristic 0 simply because strong separability is equivalent to separability in this case [23]. *For the remainder of this paper we will assume that k is algebraically closed, H is strongly separable over k, $char(k)) > 2$ and $gcd\ (dimH,\ char(k)) = 1$.* We continue with the notation we used in Section 5.

Lemma 6.3. *Let $u = \sum_{(t)} t_1 S^{-1}(t_2)$. Then $tr_\lambda(u) = tr_\lambda(u_\lambda) = n_\lambda \epsilon(t)$.*

Proof. We already know from the proof of Proposition 5.8 that $\{E^\lambda_{ij}\}$, $\{(1/n_\lambda)E^\lambda_{ji}u\}$ form dual bases with respect to f. Therefore we have:

$$\sum_\lambda \sum_{ij} (1/n_\lambda) E^\lambda_{ji} u E_{ij} = \sum_\lambda n_\lambda^{-1} tr_\lambda(u) 1_{M_{n_\lambda}(k)} = \sum_{(t)} S^{-1}(t_2) t_1 = \epsilon(t) 1_H$$

Hence $tr_\lambda(u) = tr_\lambda(u_\lambda) = n_\lambda \epsilon(t)$ as required. □

Now we recall that $\eta(x) = uxu^{-1}$ by Theorem 4.1. On the other hand, $\eta^{2n} = \mathrm{Id_H}$ by [13] where $n = dimH$. Therefore we see that $u_\lambda^{2n} = q_\lambda E_{M_{n_\lambda}(k)}$, where $q_\lambda \neq 0 \in k$ and $E_{M_{n_\lambda}(k)} := 1_\lambda$ is the unit matrix in $M_{n_\lambda}(k)$ (in the sequel we will denote $xE_{M_{n_\lambda}(k)} := x1_\lambda \in M_{n_\lambda}(k)$ by x_λ).

By considering the Jordan normal form of u_λ and recalling the assumption $gcd\,(n, char(k)) = 1$, we can assume without loss of generality that $u_\lambda = a_\lambda diag(\zeta_{2n}^{k_s})$, where $a_\lambda \neq 0 \in k$ and ζ_{2n} is a primitive $2n$-root of unity in k. Clearly numbers a_λ are defined up to ζ^k_{2n} and $tr_\lambda(u_\lambda) = a_\lambda f_\lambda(\zeta_{2n})$ where $f_\lambda(z) = \sum_{k=0}^{2n-1} f_k z^k$ is a polynomial with non-negative integer coefficients.

Let k_0 be the prime subfield of k. We see that $f_\lambda(\zeta_{2n}) \in k_0[\zeta_{2n}]$. Let us introduce a *formal complex conjugation* in the following way.

Let $P_N \subset k_0[x]$ be the set of all polynomials of degree $< N$. Let $\sigma : P_N \to P_N$ be a linear map defined by $\sigma(x^k) = x^{N-k}$. Then if $q(x) \in P_N$ and $q(\zeta_N) = a \in k$, we define $\sigma_N(a) := (\sigma q)(\zeta_N)$.

It is clear that if $char(k) = 0$ then this is the *usual complex conjugation.*

Corollary 6.4. *We have the following formula for $Tr(S^2)$:*

$$Tr(S^2) = \sum_\lambda n_\lambda^2 \cdot \frac{\epsilon(t)}{a_\lambda} \cdot \sigma_{2n}(\frac{\epsilon(t)}{a_\lambda}) = \sum_\lambda f_\lambda(\zeta_{2n})(\sigma_{2n} f_\lambda)(\zeta_{2n}).$$

Remark 6.5. We see that in the case $char(k) = 0$, $Tr(S^2) \neq 0$ as it is a sum of *strictly positive* numbers; whence H is coseparable and $S^2 = \mathrm{Id_H}$. If we managed to prove that the operator of left multiplication by u on H had eigenvalue $\epsilon(t)$ on each $H_\lambda := M_{n_\lambda}(k)$, then it would follow that $Tr(S^2) = dimH \neq 0$ in k. However we only know that this is true on $H_{\lambda_0} := M_1(k)$ generated by $t \in H$ because

$$ut = \epsilon(u)t = t\sum_{(t)} \epsilon(t_1)\epsilon(S^{-1}(t_2)) = t\sum_{(t)} \epsilon(t_1\epsilon(t_2)) = \epsilon(t)t$$

It is well-known that if $S^4 = \mathrm{Id_H}$ and $char(k) > dimH$ then semisimplicity implies cosemisimplicity. The following theorem enables us to improve this result.

Theorem 6.6. *Let $S^{2m} = \mathrm{Id_H}$, where $gcd(m, char(k)) = 1$. Then there exists a diagonal invertible $d \in H$ such that $S^2(x) = dxd^{-1}$, $d_\lambda^m = \pm 1_\lambda$, $\sigma_{2m}(tr_\lambda(d)) = tr_\lambda(d)$ and $Tr(S^2) = \sum_\lambda (tr_\lambda(d))^2$.*

Proof. Let $x^t \in H$ be the transpose of $x \in H$. Then $\phi(x) = S(x^t)$ is an automorphism of H and therefore there exists an invertible $A \in H$ such that $S(x) = A^{-1}x^tA$. Further $S^2(x) = A^{-1}A^tx(A^{-1}A^t)^{-1} = uxu^{-1}$ (since for unimodular Hopf algebras $S^2 = \eta$ by Proposition 5.4) and we deduce that $u = dc$ where $d = A^{-1}A^t$ and c is in the center of H. Clearly we have that $S^2(x) = dxd^{-1}$. We recall that $u_\lambda = a_\lambda diag(\zeta_m^{k_s})$ and it follows that $d_\lambda := dE_{M_{n_\lambda}(k)}$ is a diagonal matrix. On the other hand we have: $A^t = dA$ and we obtain that $A = A^td = dAd$ or $d_\lambda^{-1} = A_\lambda d_\lambda A_\lambda^{-1}$. Taking into account that $u_\lambda^m = a_\lambda^m E_{M_{n_\lambda}(k)}$ we conclude that $d_\lambda^m = bE_{M_{n_\lambda}(k)} = d_\lambda^{-m} = b^{-1}E_{M_{n_\lambda}(k)}$ for some $b \in k$. Then $b^2 = 1$ and $d_\lambda^m = \pm E_{M_{n_\lambda}(k)}$. The latter implies that entries of d are $2m$-roots of unity. Then $\sigma_{2m}(tr_\lambda(d))$ is well-defined and it follows that

$$\sigma_{2m}(tr_\lambda(d)) = tr_\lambda(d^{-1}) = tr_\lambda(A_\lambda d_\lambda A_\lambda^{-1}) = tr_\lambda(d).$$

Since $u_\lambda = c_\lambda d_\lambda$ for some $c_\lambda \in k$ and $tr_\lambda(u) = n_\lambda \epsilon(t)$ (by Lemma 6.3) we have:

$$\begin{aligned} Tr(S^2) &= \epsilon(t)\sum_\lambda n_\lambda tr_\lambda(u^{-1}) \\ &= \epsilon(t)\sum_\lambda c_\lambda^{-1} n_\lambda tr_\lambda(d^{-1}) \\ &= \epsilon(t)\sum_\lambda c_\lambda^{-1}(\epsilon(t))^{-1} tr_\lambda(u) tr_\lambda(d^{-1}) \\ &= \sum_\lambda (tr_\lambda(d))^2 \end{aligned}$$

which completes the proof. □

Corollary 6.7.
1. *Let H be strongly separable over a field k of characteristic $p = 8N \pm 3 > dimH$ (this is equivalent to that of $\sqrt{2} \notin \mathbb{F}_p$). If $S^{16} = \mathrm{Id_H}$, then $S^2 = \mathrm{Id_H}$.*
2. *Let H be strongly separable over a field k of characteristic $p = 4N+3 > dimH$ (this is equivalent to that of $\sqrt{-1} \notin \mathbb{F}_p$). If $S^8 = \mathrm{Id_H}$, then $S^2 = \mathrm{Id_H}$.*

Proof. We prove the first statement. It is sufficient to prove that $Tr(S^2) \neq 0$. Let us consider separately two cases, one where $d_\lambda^8 = 1_\lambda$ and the other where $d_\lambda^8 = -1_\lambda$.

In the first case the eigenvalues of d_λ are ζ_8^j of multiplicities A_j^λ, $j = 0, 1, ..7$. Then $dimH_\lambda = (\sum_{j=0}^7 A_j^\lambda)^2$. We note that $\zeta_8^4 = -1$ and $\zeta_8 - \zeta_8^3 = \zeta_8 + \zeta_8^{-1} = \sqrt{2} \notin \mathbb{F}_p$.

Then the condition $tr_\lambda(d) = tr_\lambda(d^{-1})$ implies that $(A_1 - A_5 + A_3 - A_7)(\zeta_8 + \zeta_8^3) = 2(A_6 - A_2)\zeta_8^2$ and consequently $-2(A_1 - A_5 + A_3 - A_7)^2 = -4(A_6 - A_2)^2$. Since $\sqrt{2} \notin \mathbb{F}_p$ we deduce that $A_2^\lambda = A_6^\lambda$ and $A_1^\lambda + A_3^\lambda - A_5^\lambda - A_7^\lambda = 0$. Then

$$tr_\lambda(d) = A_0^\lambda - A_4^\lambda + (A_1^\lambda - A_5^\lambda)\zeta_8 + (A_3^\lambda - A_7^\lambda)\zeta_8^3 =$$
$$A_0^\lambda - A_4^\lambda + (A_1^\lambda - A_5^\lambda)(\zeta_8 - \zeta_8^3) = A_0^\lambda - A_4^\lambda + (A_1^\lambda - A_5^\lambda)\sqrt{2}$$

and

$$(tr_\lambda(d))^2 = (A_0^\lambda - A_4^\lambda)^2 + 2(A_1^\lambda - A_5^\lambda)^2 + 2\sqrt{2}(A_0^\lambda - A_4^\lambda)(A_1^\lambda - A_5^\lambda) \quad = \\ (A_0^\lambda - A_4^\lambda)^2 + (A_1^\lambda - A_5^\lambda)^2 + (A_3^\lambda - A_7^\lambda)^2 + X\sqrt{2},\ X \in \mathbb{F}_p$$

In the second case the eigenvalues of d_λ are ζ_{16}^{2j-1} of multiplicities B_j^λ, $j = 1, ...8$. Since $\zeta_{16}^8 = -1$ and $\zeta_{16}^2 = \zeta_8$ we can write that $tr_\lambda(d) = \sum_{s=1}^4 (B_s - B_{s+4})\zeta_{16}^{2s-1}$ In this case $\sigma_{16}(tr_\lambda(d)) = tr_\lambda(d)$ implies that $(B_1 - B_5 + B_4 - B_8)(\zeta_{16} + \zeta_{16}^7) = -(B_2 - B_6 + B_3 - B_7)(\zeta_{16}^3 + \zeta_{16}^5)$ and therefore $R(1 + \zeta_8^3) = S(\zeta_8 + \zeta_8^2)$, where $R = B_1 - B_5 + B_4 - B_8$, $S = -(B_2 - B_6 + B_3 - B_7)$. It follows that $R(\zeta_8 + \zeta_8^{-1}) = R + S$ and hence

$$R = S = B_1^\lambda - B_5^\lambda + B_4^\lambda - B_8^\lambda = B_2^\lambda - B_6^\lambda + B_3^\lambda - B_7^\lambda = 0$$

Therefore we have obtained the following expression for $tr_\lambda(d)$:

$$tr_\lambda(d) = (B_1^\lambda - B_5^\lambda)(\zeta_{16} - \zeta_{16}^7) + (B_2^\lambda - B_6^\lambda)(\zeta_{16}^3 - \zeta_{16}^5)$$

Then we compute $(tr_\lambda(d))^2$:

$$(tr_\lambda(d))^2 = 2(B_1^\lambda - B_5^\lambda)^2 + 2(B_2^\lambda - B_6^\lambda)^2 + Y\sqrt{2} = \\ (B_1^\lambda - B_5^\lambda)^2 + (B_2^\lambda - B_6^\lambda)^2 + (B_3^\lambda - B_7^\lambda)^2 + (B_4^\lambda - B_8^\lambda)^2 + Y\sqrt{2},\ Y \in \mathbb{F}_p$$

Let us assume that $Tr(S^2) = x + y\sqrt{2} = 0$. This means that $x = y = 0$ because $\sqrt{2} \notin \mathbb{F}_p$. In our case we have:

$$x = \sum_\lambda (A_0^\lambda - A_4^\lambda)^2 + (A_1^\lambda - A_5^\lambda)^2 + (A_3^\lambda - A_7^\lambda)^2 + \\ \sum_\lambda (B_1^\lambda - B_5^\lambda)^2 + (B_2^\lambda - B_6^\lambda)^2 + (B_3^\lambda - B_7^\lambda)^2 + (B_4^\lambda - B_8^\lambda)^2$$

Let us consider x as an element of $\mathbb{Z}$. It is clear that $x < dimH < p$. On the other hand $x > 0$ because we have the *one-dimensional* component H_{λ_0} on which the corresponding $A_0^{\lambda_0}$ is 1 and the other multiplicities A_i^λ, B_j^λ are zeroes. It follows that $Tr(S^2) \neq 0$ in k. □

Acknowledgements. The authors thank NorFA of Norway and NFR of Sweden, respectively, for their support of this paper.

References

[1] M. Aguiar, Symmetrically separable algebras and a right adjoint to the tensor coproduct of comodules, preprint, Northwestern Univ., 1996.

[2] M. Auslander and O. Goldman, The Brauer group of a commutative ring, *Trans. A.M.S.* **97** (1960), 367–409.

[3] K. Beidar, Y. Fong, and A. Stolin, On Frobenius algebras and the quantum Yang-Baxter equation, *Trans. A.M.S.* **349** (1997), 3823–3836.

[4] K. Beidar, Y. Fong, and A. Stolin, On antipodes and integrals in Hopf algebra over rings and the quantum Yang-Baxter equation, *J. Algebra* **194** (1997), 36–52.

[5] K.S. Brown, *Cohomology of Groups*, Springer Graduate Texts **87**, 1982.

[6] A. Connes and H. Moscovici, Hopf algebras, cyclic cohomology and the transverse index theorem, IHES preprint, May 1998.

[7] J. Cuntz and D. Quillen, Operators on noncommutative differential forms and cyclic homology, Universität Heidelberg preprint, 1992.

[8] F. Demeyer, The trace map and separable algebras, *Osaka J. Math.* **3** (1966), 7-11.

[9] F. Demeyer and E. Ingraham, *Separable algebras over commutative rings*, Lect. Notes in Math. **181**, Springer Verlag, 1970.

[10] S. Eilenberg and T. Nakayama, On the dimensions of modules and algebras, II. (Frobenius algebras and quasi-Frobenius rings), *Nagoya Math. J.* **9** (1955), 1–16.

[11] S. Endo and Y. Watanabe, On separable algebras over a commutative ring, *Osaka J. Math.* **4** (1967), 233–242.

[12] P. Etingof and S. Gelaki, On finite-dimensional semisimple and cosemisimple Hopf algebras in positive characteristic, q-alg/9805106.

[13] D. Fischman, S. Montgomery, and H.-J. Schneider, Frobenius extensions of subalgebras of Hopf algebras, *Trans. Amer. Math. Soc.* **349** (1997), 4857–4895.

[14] A. Hattori, On strongly separable algebras, *Osaka J. Math.* **2** (1965), 369–372.

[15] K. Hirata and K. Sugano, On semisimple extensions and separable extensions over non commutative rings, *J. Math. Soc. Japan* **18** (1966), 360–373.

[16] G. Hochschild, On the cohomology groups of an associative algebra, *Annals Math.* **46** (1945), 58–67.

[17] L. Kadison, The Jones polynomial and certain separable Frobenius extensions, *J. Algebra* **186** (1996), 461–475.

[18] L. Kadison, *Separability*, NTNU preprint 1/1997.

[19] L. Kadison, *New Examples of Frobenius Extensions*, A.M.S. University Lecture Series, vol. 14, Providence, Rhode Island, 1999.

[20] L. Kadison and A.A. Stolin, Frobenius systems and Hopf algebras over rings, Chalmers preprint 20/1999 (ps.viewable under www.math.chalmers.se).

[21] T. Kanzaki, Special type of separable algebra over commutative ring, *Proc. Japan Acad.* **40** (1964), 781–786.

[22] R.G. Larson, Characters of Hopf algebras, *J. Algebra* **17** (1971), 352–368.

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

[24] R.G. Larson and M. Sweedler, An associative orthogonal bilinear form for Hopf algebras, *Amer. J. Math.* **91** (1969), 75–93.

[25] S. Montgomery, Hopf algebras and their actions on rings, *CBMS Regional Conf. Series in Math.* **82**, A.M.S., 1993.

[26] B. Müller, Quasi-Frobenius Erweiterungen I, *Math. Zeit.* **85** (1964), 345–368. Quasi-Frobenius Erweiterungen II, *ibid.* **88** (1965), 380–409.

[27] T. Nakayama and T. Tsuzuku, On Frobenius extensions I. *Nagoya Math. J.* **17** (1960), 89–110. On Frobenius extensions II. *ibid.* **19** (1961), 127–148.

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

[29] T. Onodera, A characterization of strongly separable algebras, *J. Fac. Sci. Hokkaido Univ. Ser. I*, **19** (1966), 71–73.

[30] M. Orzech and C. Small, *The Brauer group of commutative rings*, Lect. Notes in Math. **11**, M. Dekker, New York, 1975.

[31] B. Pareigis, Einige Bemerkung über Frobeniuserweiterungen, *Math. Ann.* **153** (1964), 1–13.

[32] B. Pareigis, When Hopf algebras are Frobenius algebras, *J. Algebra* **18** (1971), 588-596.

[33] B. Pareigis, On the cohomology of modules over Hopf algebras, *J. Algebra* **22** (1972), 161-182.

[34] B. Pareigis, *Endliche Hopf-Algebren*, Vorlesung-Ausarbeitung, Universität München, 1973.

[35] R. Pierce, *Associative Algebras*, Grad. Text in Math. **88**, Springer, 1982.
[36] D. Radford, The order of the antipode of a finite dimensional Hopf algebra is finite, *Amer. J. Math.* **98** (1976), 333–355.
[37] H.-J. Schneider, Lectures on Hopf Algebras, *Preprint Ciudad University,* Cordoba, Argentina, Trabajos de Matematica, serie B, no. **31**, 1995.
[38] J.R. Silvester, *Introduction to Algebraic K-theory*, Chapman and Hall, London, 1981.

Chalmers University of Technology/Göteborg University, S-412 96 Göteborg, Sweden
E-mail address: kadison@math.ntnu.no astolin@math.chalmers.se