Advances in Mathematics **163**, 258–286 (2001)
doi:10.1006/aima.2001.2003, available online at http://www.idealibrary.com on IDEAL®

Hopf Algebra Actions on Strongly Separable Extensions of Depth Two

Lars Kadison[1]

Chalmers University of Technology/Göteborg University, Matematiskt Centrum, S-412 96 Göteborg, Sweden
E-mail: lkadison@online.no

and

Dmitri Nikshych

U.C.L.A., Department of Mathematics, Los Angeles, California 90095-1555
E-mail: nikshych@math.ucla.edu

Received May 26, 2000; accepted April 20, 2001

We bring together ideas in analysis on Hopf $*$-algebra actions on II_1 subfactors of finite Jones index [9, 24] and algebraic characterizations of Frobenius, Galois and cleft Hopf extensions [3, 13, 14] to prove a non-commutative algebraic analogue of the classical theorem: a finite degree field extension is Galois iff it is separable and normal. Suppose $N \hookrightarrow M$ is a separable Frobenius extension of k-algebras with trivial centralizer $C_M(N)$ and split as N-bimodules. Let $M_1 := \mathrm{End}(M_N)$ and $M_2 := \mathrm{End}(M_1)_M$ be the endomorphism algebras in the Jones tower $N \hookrightarrow M \hookrightarrow M_1 \hookrightarrow M_2$. We place depth 2 conditions on its second centralizers $A := C_{M_1}(N)$ and $B := C_{M_2}(M)$. We prove that A and B are semisimple Hopf algebras dual to one another, that M_1 is a smash product of M and A, and that M is a B-Galois extension of N.

1. INTRODUCTION

Three well-known functors associated to the induced representations of a subalgebra pair $N \subseteq M$ are restriction $\mathscr{R}$ of M-modules to N-modules, its adjoint $\mathscr{T}$ which tensors N-modules by M, and its co-adjoint $\mathscr{H}$ which applies $\mathrm{Hom}_N(M, -)$ to N-modules. The algebra extension M/N is said to

[1] The first author thanks A. A. Stolin for useful discussions, and NorFA in Oslo for financial support.

0001-8708/01 $35.00

be *Frobenius* if $\mathscr{T}$ is naturally isomorphic to $\mathscr{H}$ [18]. M/N is said to be *separable* if the counit of adjunction $\mathscr{T}\mathscr{R} \dot{\to} 1$ is naturally split epi; and M/N is a *split extension* if the unit of adjunction $1 \dot{\to} \mathscr{R}\mathscr{T}$ is naturally split monic [20]. An algebraic model for finite Jones index subfactor theory is given in [11, 12] using a *strongly separable extension*, which has all three of these properties. Over a ground field k, an *irreducible* extension M/N, which is characterized by having trivial centralizer $C_M(N) = k1$, is strongly separable if it is split, separable and Frobenius.

In this paper we extend the results of Szymański [24] and others [16, 6] on Hopf $*$-algebra actions and finite index subfactors with trace (i.e., linear $\phi: M \to k$ such that $\phi(mm') = \phi(m'm)$ for all $m, m' \in M$ *and* $\phi(1) = 1_k$) to strongly separable, irreducible extensions. We will not require of our algebras that they possess a trace. However, we require some hypotheses on the endomorphism algebra M_1 of the natural module M_N, to which there is a monomorphism given by the left regular representation of M in $\mathrm{End}(M_N)$. We require a *depth two condition* that two successive endomorphism algebra extensions, $M \hookrightarrow M_1$ and $M_1 \hookrightarrow M_2$, be free with bases in the second centralizers, $A := C_{M_1}(N)$ and $B := C_{M_2}(M)$. Working over a field of arbitrary characteristic, we prove in Theorem 5.3 and Theorem 6.3:

THEOREM 1.1. *The Jones tower $M \subseteq M_1 \subseteq M_2$ over a strongly separable, irreducible extension $N \subseteq M$ of depth 2 has centralizers A and B that are involutive semisimple Hopf algebras dual to one another, with an action of B on M_1 and another action of A on M such that M_1 and M_2 are smash products: $M_2 \cong M_1 \# B$ and $M_1 \cong M \# A$.*

The main theorem 1.1 is of intrinsic interest in extending [24] to the case of an irreducible finite index pair of von Neumann factors of arbitrary type (I, II, or III). Secondly, it gives a proof that M_1 is a smash product without appeal to a tunnel construction; i.e., assuming the strong hypotheses in a characterization of a strongly separable extension M/N that is the endomorphism algebra extension of some N/R. Thirdly, the main theorem is the difficult piece in the proof of a non-commutative analogue of the classical theorem in field theory [23]:

THEOREM 1.2. *A finite degree field extension E'/F' is Galois if and only if E'/F' is separable and normal.*

By E'/F' Galois we mean that the Galois group G of F'-algebra automorphisms of E' has F' as its fixed field E'^G. From a modern point of view, the right non-commutative generalization of Galois extension is the Hopf-Galois extension (cf. Section 3) [17], with classical Galois groups interpreted as cosemisimple Hopf algebras. From the modern cohomological point of view, the non-commutative separable extensions mentioned above are a direct generalization of separable field extensions (cf. Section 2) [10]. The trace map $T: E' \to F'$ for finite separable field extensions [15] is a Frobenius homomorphism for a Frobenius extension (cf. Section 2), while the trace map for Galois extensions is the action of an integral on the overfield (corresponding to the mapping E in the proof of Theorem 3.14). In Section 6 we prove the following non-commutative analogue of Theorem 1.2:

THEOREM 1.3. *If M/N is an irreducible extension of depth 2, then M/N is strongly separable if and only if M/N is an H-Galois extension, where H is a semisimple, cosemisimple Hopf algebra.*

In Sections 2 and 3 we note that the non-commutative notions of separable extension and Hopf–Galois extension generalize separability and Galois extension, respectively, for finite field extensions. However, Theorem 1.3 is not a generalization of the classical theorem, since non-trivial field extensions are not irreducible. The proof of Theorem 1.3 follows from Theorems 3.14 and 1.1. Theorem 3.14 is the easier result with roots in [14, 4, 12]. The smash product result on M_2 in Theorem 1.1 follows from the depth 2 properties in Section 3, the non-degenerate pairing of A and B in Section 4, and the action of B on M_1 in Section 5 together with the key Proposition 4.6. The non-degenerate pairing in Eq. (14) transfers the algebra structures of A and B to coalgebra structures on B and A, respectively, that result in the Hopf algebra structures on these. The antipodes on A and B result from a basic symmetry in the definition of the pairing. From the action of B on M_1 with fixed subalgebra M, we dualize in Section 6 to an A-extension M_1/M, compute that it is A-cleft, and use the Hopf algebra-theoretic characterization of these as crossed products: we show that M_1 is a smash product of M with A from the triviality of the cocycle. Each section begins with an introduction to the main terminology, theory and results in the section.

2. STRONGLY SEPARABLE EXTENSIONS WITH TRIVIAL CENTRALIZER

In this section, we recall the most basic definitions and facts for irreducible and split extensions, Frobenius extensions and algebras, separable extensions and algebras, and strongly separable extensions and algebras. We introduce Frobenius homomorphisms and their dual bases, which characterize Frobenius extensions, noting that Frobenius homomorphisms are faithful, and have Nakayama automorphisms measuring their deviation from being a trace on the centralizer. After introducing separability and strongly separable extensions, we come to the important theory of the basic construction M_1, conditional expectation $E_M: M_1 \to M$ and Jones idempotent $e_1 \in M_1$. The basic construction is repeated to form the tower of algebras $N \subseteq M \subseteq M_1 \subseteq M_2$, and the braid-like relations between e_1 and $e_2 \in M_2$ are pointed out.

Throughout this paper, k denotes a field. Let M and N be associative unital k-algebras with N a unital subalgebra of M. We refer to $N \subseteq M$ or a (unity-preserving) monomorphism $N \hookrightarrow M$ as an *algebra extension* M/N. We note the endomorphism algebra extension $\mathrm{End}(M_N)/M$ obtained from $m \to \lambda_m$ for each $m \in M$, where λ_m is left multiplication by $m \in M$, a right N-module endomorphism of M.

In this section, we denote the *centralizer* of a bimodule ${}_N P_N$ by $P^N := \{p \in P \mid \forall n \in N, pn = np\}$, a special case of which is the centralizer subalgebra of N in M: $C_M(N) = M^N$. The algebra extension M/N will be called *irreducible* if the centralizer subalgebra is trivial, i.e., $C_M(N) = k1$. Since the centers $Z(M)$ and $Z(N)$ both lie in $C_M(N)$, they are trivial as well. If $\mathscr{E}$ denotes $\mathrm{End}(M_N)$ and M^{op} denotes the opposite algebra of M, we note that

$$C_{\mathscr{E}}(M) = \{f \in \mathscr{E} \mid mf(x) = f(mx), \forall m \in M\} = \mathrm{End}({}_M M_N) \cong C_M(N)^{op}. \tag{1}$$

Whence the endomorphism algebra extension is irreducible too.

M/N is a *split extension* if there is an N-bimodule projection $E: M \to N$. Thus, $E(1) = 1$, $E(nmn') = nE(m)\,n'$, for all $n, n' \in N, m \in M$, and $M = N \oplus \ker E$ as N-bimodules, the last being an equivalent condition. The condition mentioned in the first paragraph of Section 1 is easily shown to be equivalent as well [20].

Frobenius Extensions

M/N is said to be a *Frobenius extension* if the natural right N-module M_N is finitely generated projective and there is the following bimodule isomorphism of M with its (algebra extension) dual: ${}_N M_M \cong {}_N\mathrm{Hom}(M_N, N_N)_M$ [13]. This definition is equivalent to the condition that M/N has a bimodule homomorphism $E: {}_N M_N \to {}_N N_N$, called a *Frobenius homomorphism*, and elements in M, $\{x_i\}_{i=1}^n$, $\{y_i\}_{i=1}^n$, called *dual bases*, such that the equations

$$\sum_{i=1}^{n} E(mx_i)\, y_i = m = \sum_{i=1}^{n} x_i E(y_i m) \tag{2}$$

hold for every $m \in M$ [13].[2] In particular, Frobenius extension may be defined equivalently in terms of the natural *left* module $_NM$ instead. The Hattori-Stallings rank of the projective modules M_N or $_NM$ are both given by $\sum_i E(y_i x_i)$ in $N/[N, N]$ [11]. It is not hard to check that the *index* $[M : N]_E := \sum_i x_i y_i \in Z(M)$ (use Eqs. (2)) depends only on E, and $E(1) \in Z(N)$. Furthermore, M/N is split if and only if there is a $d \in C_M(N)$ such that $E(d) = 1$ [11].

If M_N is free, M/N is called a *free Frobenius extension* [13]. By choosing dual bases $\{x_i\}$, $\{f_i\}$ for M_N such that $f_i(x_j) = \delta_{ij}$, we arrive at *orthogonal dual bases* $\{x_i\}$, $\{y_i\}$, which satisfy $E(y_i x_j) = \delta_{ij}$. Conversely, with E, x_i and y_i satisfying this equation, it is clear that M/N is free Frobenius.

If N is the unit subalgebra $k1$, M is a *Frobenius algebra*, a notion introduced in a 1903 paper of Frobenius [8]. Such an algebra M is characterized by having a *faithful*, or non-degenerate, linear functional $E: M \to k$; i.e., $E(Mm) = 0$ implies $m = 0$, or equivalently, $E(mM) = 0$ implies $m = 0$ (in one direction a trivial application of Eqs. (2)).

We note the following *transitivity* result with an easy proof. Consider the tower of algebras $N \subseteq M \subseteq R$. If M/N and R/M are Frobenius extensions, then so is the composite extension R/N. Moreover, the following proposition has a proof left to the reader:

Proposition 2.1. *If M/N and R/M are algebra extensions with Frobenius homomorphisms $E: M \to N$, $F: R \to M$ and dual bases $\{x_i\}$, $\{y_i\}$ and $\{z_j\}$, $\{w_j\}$, respectively, then R/N has Frobenius homomorphism $E \circ F$ and dual bases $\{z_j x_i\}$, $\{y_i w_j\}$.*

If M/N and R/M are irreducible, the composite index satisfies the Lagrange equation:

$$[R : N]_{EF} = [R : M]_F \, [M : N]_E.$$

Nakayama Automorphism

Given a Frobenius homomorphism $E: M \to N$ and an element c in the centralizer $C_M(N)$, the maps cE and Ec defined by $cE(x) := E(xc)$ and $Ec(x) = E(cx)$ are both N-bimodule maps belonging to the N-centralizers of both the N-bimodules $\mathrm{Hom}_N(M_N, N_N)$ and $\mathrm{Hom}_N({}_NM, {}_NN)$. Since $m \mapsto Em$ is a bimodule isomorphism, ${}_NM_M \cong {}_N\mathrm{Hom}^r_N(M, N)_M$, it follows that there is a unique $c' \in C_M(N) = M^N$ such that $Ec' = cE$. The mapping

[2] For if $\{x_i\}$, $\{f_i\}$ is a projective base for M_N and E is the image of 1, then there is $y_i \mapsto Ey_i = f_i$ such that $\sum_i x_i E y_i = \mathrm{id}_M$. The other equation follows. Conversely, M_N is explicitly finitely generated projective, while $x \mapsto Ex$ is bijective.

$q: c \mapsto c'$ on $C_M(N)$ is clearly an automorphism, called the *Nakayama automorphism*, or modular automorphism, with defining equation given by

$$E(q(c)\, m) = E(mc) \tag{3}$$

for every $c \in C_M(N)$ and $m \in M$ [13]. M/N is a *symmetric* Frobenius extension if q is an inner automorphism. In case $N = k1$, this recovers the usual notion of *symmetric algebra* (a finite-dimensional algebra with non-degenerate or faithful trace), for if $q: M \to M$ is given by $q(m) = umu^{-1}$, then Eu is such a trace by Eq. (3).

Separability

Throughout this paper we consider $M \otimes_N M$ with its natural M-M-bimodule structure. M/N is said to be a *separable extension* if the multiplication epimorphism $\mu: M \otimes_N M \to M$ has a right inverse as M-M-bimodule homomorphisms [10]. This is clearly equivalent to the existence of an element $e \in M \otimes_N M$ such that $me = em$ for every $m \in M$ and $\mu(e) = 1$, called a *separability element*: separable extensions are precisely the algebra extensions with trivial relative Hochschild cohomology groups in degree one or more [10]. A Frobenius extension M/N with E, x_i, y_i as before is separable if and only if there is a $d \in C_M(N)$ such that $\sum_i x_i\, dy_i = 1$ [10].

If $N = k1_M$, M/N is a separable extension iff M is a separable k-algebra; i.e., a finite dimensional, semisimple k-algebra with matrix blocks over division algebras D_i where $Z(D_i)$ is a finite separable (field) extension of k. If k is algebraically closed, each $D_i = k$ and M is isomorphic to a direct product of matrix blocks of order n_i over k.

For example, if E'/F' is a finite separable field extension, $\alpha \in E'$ the primitive element such that $E' = F'(\alpha)$, and $p(x) = x^n - \sum_{i=0}^{n-1} c_i x^i$ the minimal polynomial of α in $F'[X]$, then a separability element is given by

$$\sum_{i=0}^{n-1} \alpha^i \otimes_{F'} \frac{\sum_{j=0}^{i} c_j \alpha^j}{p'(\alpha)\, \alpha^{i+1}}.$$

A k-algebra M is said to be *strongly separable* in Kanzaki's sense if M has a *symmetric* separability element e (necessarily unique); i.e., $\tau(e) = e$ where τ is the twist map on $M \otimes_k M$. An equivalent condition is that M has a trace $t: M \to k$ (i.e., $t(mn) = t(nm)$ for all $m, n \in M$) and elements $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ such that $\sum_i t(mx_i)\, y_i = m$ for all $m \in M$ and $\sum_i x_i y_i = 1_M$. A third equivalent condition is that M has an invertible Hattori–Stalling rank over its center [2]. It follows that the characteristic of k does not divide the orders n_i of the matrix blocks (i.e., $n_i 1_k \neq 0$); for a separable k-algebra M, this is also a sufficient condition for strong separability in case k is algebraically closed.

Strongly Separable Extensions

We are now ready to define the main object of investigation in this paper.

DEFINITION 2.2 (cf. [11, 12]). A k-algebra extension $N \subseteq M$ is called a *strongly separable, irreducible extension* if M/N is an irreducible Frobenius extension with Frobenius homomorphism $E: M \to N$, and dual bases $\{x_i\}$, $\{y_i\}$ such that

(1) $E(1) \neq 0$,
(2) $\sum_i x_i y_i \neq 0$,

Remark 2.3. Since M/N is irreducible, the centers of M and N are trivial, so $E(1) = \mu 1_S$ for some nonzero $\mu \in k$. Then $\frac{1}{\mu} E$, μx_i, y_i is a new Frobenius homomorphism with dual bases for M/N. With no loss of generality then, we assume that

$$E(1) = 1. \tag{4}$$

It follows that $M = N \oplus \operatorname{Ker} E$ as N-N-bimodules and $E^2 = E$ when E is viewed in $\operatorname{End}_N(M)$. Also

$$\sum_i x_i y_i = \lambda^{-1} 1_M \tag{5}$$

for some nonzero $\lambda \in k$. It follows that $\lambda \sum_i x_i \otimes y_i$ is a separability element and M/N is separable. The data E, x_i, y_i for a strongly separable, irreducible extension, satisfying Eqs. (4) and (2), is uniquely determined.[3]

[3] There is a close but complicated relationship between Kanzaki strongly separable k-algebras and strongly separable extensions $A/k1$ in the sense of [12]. Note that $A = M_2(F_2)$, where F_2 is a field of characteristic 2, is not Kanzaki strongly separable, but is a strongly separable extension $A/F_2 1$ since $E(A) = a_{11} + a_{12} + a_{21}$ and

$$\sum_i x_i \otimes y_i = e_{11} \otimes e_{21} + e_{12} \otimes e_{11} + e_{12} \otimes e_{21} + e_{22} \otimes e_{12} + e_{22} \otimes e_{22} + e_{21} \otimes e_{22},$$

satisfies $\sum_i x_i y_i = 1$, $E(1) = 1$, E a Frobenius homomorphism with dual bases x_i, y_i. However, a strongly separable extension $A/k1$ with Markov trace [12] is Kanzaki strongly separable; and conversely, if $k = Z(A)$.

The Basic Construction

The basic construction begins with the following *endomorphism ring theorem*, whose proof we sketch here for the sake of completeness:

THEOREM 2.4 (Cf. [11, 12]). *$\mathcal{E}/M$ is a strongly separable, irreducible extension of index λ^{-1}.*

Proof. For a Frobenius extension M/N, we have $\mathcal{E} \cong M \otimes_N M$ by sending $f \mapsto \sum_i f(x_i) \otimes y_i$ with inverse $m \otimes n \mapsto \lambda_m E \lambda_n$ in the notation above. We denote $M_1 := M \otimes_N M$, and note that the multiplication on M_1 induced by composition of endomorphisms is given by the *E-multiplication*:

$$(m_1 \otimes m_2)(m_3 \otimes m_4) = m_1 E(m_2 m_3) \otimes m_4. \tag{6}$$

The unity element is $1_1 := \sum_i x_i \otimes y_i$ in the notation above. It is easy to see that $E_M := \lambda\mu$, where μ is the multiplication mapping $M_1 \to M$, is a normalized Frobenius homomorphism, and $\{\lambda^{-1} x_i \otimes 1\}$, $\{1 \otimes y_i\}$ are dual bases satisfying Eqs. (4) and (5). ▮

We make note of the *first Jones idempotent*, $e_1 := 1 \otimes 1 \in M_1$, which cyclically generates M_1 as an M-M-bimodule: $M_1 = \{\sum_i x_i e_1 y_i \mid x_i, y_i \in M\}$. In this paper, a Frobenius homomorphism E satisfying $E(1) = 1$ is called a *conditional expectation*. We describe M_1, e_1, E_M as the "basic construction" of $N \subseteq M$.

The Jones Tower

The basic construction is repeated in order to produce the Jones tower of k-algebras above $N \subseteq M$:

$$N \subseteq M \subseteq M_1 \subseteq M_2 \subseteq \cdots \tag{7}$$

In this paper we will only need to consider M_2, which is the basic construction of $M \subseteq M_1$. As such it is given by

$$M_2 = M_1 \otimes_M M_1 \cong M \otimes_N M \otimes_N M \tag{8}$$

with E_M-multiplication, and conditional expectation $E_{M_1} := \lambda\mu : M_2 \to M_1$ given by

$$m_1 \otimes m_2 \otimes m_3 \mapsto \lambda m_1 E(m_2) \otimes m_3.$$

The second Jones idempotent is given by

$$e_2 = 1_1 \otimes 1_1 = \sum_{i,j} x_i \otimes y_i x_j \otimes y_j,$$

and satisfies $e_2^2 = e_2$ in the E_M-multiplication of M_2.

The Braid-Like Relations

Note that $1_2 = \sum_i \lambda^{-1} x_i \otimes 1 \otimes y_i$ and $E_{M_i}(e_{i+1}) = \lambda 1$ where M_0 denotes M. Then the following relations between e_1, e_2 are readily computed in M_2 without the hypothesis of irreducibility:

PROPOSITION 2.5.

$$e_1 e_2 e_1 = \lambda e_1 1_2$$
$$e_2 e_1 e_2 = \lambda e_2.$$

Proof. The proof may be found in [11, Ch. 3]. ∎

3. DEPTH 2 PROPERTIES

In this section, we place depth 2 conditions on the modules ${}_M M_1$ and ${}_{M_1} M_2$ by requiring that they be free with bases in $A := C_{M_1}(N)$ and $B := C_{M_2}(M)$, respectively. We then show that A and B are separable algebras with $E_M|_A$ and $E_{M_1}|_B$, respectively, as faithful linear functionals. The classical depth 2 property, coming from subfactor theory [9], is established for the large centralizer, $C := C_{M_2}(N)$; i.e., C is the basic construction of A or B over the trivial centralizer with conditional expectations E_A and E_B studied later in the section. We next establish the important property that $F := E_M \circ E_{M_1}$ restricts to a faithful linear functional on C. We interpret the various Nakayama automorphisms arising from F, $E_M|_A$ and $E_{M_1}|_B$. The important Pimsner-Popa identities are established. We end this section by recalling the basic properties of Hopf–Galois extensions, and prove Theorem 3.14 which states that an H-Galois extension is strongly separable of depth 2 if H is a semisimple, cosemisimple Hopf algebra. This establishes one of the implications in Theorem 1.3.

Finite Depth and Depth 2 Conditions

We extend the notion of *depth* known in subfactor theory [9] to Frobenius extensions.

LEMMA 3.1. *For all $n \geqslant 1$ in the Jones tower* (7) *the following conditions are equivalent (we denote $M_{-1} = N$ and $M_0 = M$):*

(1) *M_{n-1} is a free right M_{n-2}-module with a basis in $C_{M_{n-1}}(N)$ (respectively, M_n is a free right M_{n-1}-module with a basis in $C_{M_n}(M)$).*

(2) *There exist orthogonal dual bases for $E_{M_{n-2}}$ in $C_{M_{n-1}}(N)$ (respectively, there exist orthogonal dual bases for $E_{M_{n-1}}$ in $C_{M_n}(M)$).*

Proof. We show that (1) implies (2), the other implication is trivial. Denote by $\{z_i\}$ and $\{w_i\}$ orthogonal dual bases in M_{n-1} for $E_{M_{n-2}}$, where $\{z_i\} \subset C_{M_{n-1}}(N)$. We compute that $w_i \in C_{M_{n-1}}(N)$:

$$xw_i = \sum_j xE_{M_{n-2}}(w_i z_j)\, w_j = \sum_j \delta_{ij} x\, w_j = \sum_j E_{M_{n-2}}(w_i x z_j)\, w_j = w_i x$$

for every $x \in N$. The second statement in the proposition is proven similarly with dual bases $\{u_j\}$ in $C_{M_n}(M)$ and therefore $\{v_j\}$ in $C_{M_n}(M)$. ∎

We say that a Frobenius extension M/N has a *finite depth* if the equivalent conditions of Lemma 3.1 are satisfied for some $n \geqslant 1$. It is not hard to check that in this case they also hold true for $n+1$ (and, hence, for all $k \geqslant n$). Indeed, if $\{u_j\}$ and $\{v_j\}$ are as above, then $\{\lambda^{-1} u_j e_{n+1}\}$, $\{e_{n+1} v_j\} \subset C_{M_{n+1}}(M)$ is a pair of orthogonal dual bases for E_{M_n}. We then define the *depth* of a finite depth extension M/N to be the smallest number n for which these conditions hold. In the trivial case, an irreducible extension of depth 1 leads to $M = N$.

Let A and B denote the "second" centralizer algebras:

$$A := C_{M_1}(N),\ B := C_{M_2}(M).$$

The *depth 2 conditions* that we will use in this paper are then explicitly:

(1) M_1 is a free right M-module with basis in A;

(2) M_2 is a free right M_1-module with basis in B.

It is easy to show that M_1 and M_2 are also free as left M- and M_1-modules, respectively. Note that the depth 2 conditions make sense for an arbitrary ring extension M/N where M_1 and M_2 stand for the successive endomorphism rings.

In what follows, we assume that M/N has depth 2 and denote $\{z_i\}$, $\{w_i\} \subset A$ orthogonal dual bases for E_M and $\{u_i\}$, $\{v_i\} \subset B$ orthogonal dual bases for E_{M_1} that exist by Lemma 3.1.

PROPOSITION 3.2. *A and B are separable algebras.*

Proof. For all $a \in A$, we have $\sum_i E_M(az_i)\, w_i = a = \sum_i z_i E_M(w_i a)$ where $E_M(az_i)$ and $E_M(w_i a)$ lie in $C_M(N) = k1_M$. $\{z_i\}$ is linearly independent over M, whence over k, so A, similarly B, is finite dimensional.

It follows that E_M restricted to A is a Frobenius homomorphism. Since $\{z_i\}$, $\{w_i\}$ are dual bases and $[M_1 : M]_{E_M} = \lambda^{-1}$, it follows that $\lambda \sum_i z_i \otimes w_i$ is a separability element. Similarly, B is a Frobenius algebra with Frobenius homomorphism E_{M_1}, and a separable algebra with separability element $\lambda \sum_j u_j \otimes v_j$. ∎

The lemma below is a first step to the main result that M_2 is a smash product of B and M_1 (cf. Theorem 5.3).

LEMMA 3.3. *We have $M_1 \cong M \otimes_k A$ as M-A-bimodules, and $M_2 \cong M_1 \otimes_k B$ as M_1-B-bimodules.*

Proof. We map $w \in M_1$ into $\sum_i E_M(wz_i) \otimes w_i \in M \otimes A$, which has inverse mapping $m \otimes a \in M \otimes A$ into $ma \in M_1$.

The proof of the second statement is completely similar. ∎

We let $C = C_{M_2}(N)$. Note that $A \subseteq C$ and $B \subseteq C$. Of course $A1_2 \cap B = k1_2$ since $C_{M_1}(M) = k1_1$. We will now show in a series of steps the classical depth 2 property that C is the basic construction of A or B over the trivial centralizer.

LEMMA 3.4. *$C \cong A \otimes_k B$ via multiplication $a \otimes b \mapsto ab$ and $C \cong B \otimes_k A$ via $b \otimes a \mapsto ba$.*

Proof. If $c \in C$, then $\sum_j E_{M_1}(cu_j) \otimes v_j \in A \otimes B$, which provides an inverse to the first map above. The second part is established similarly. ∎

LEMMA 3.5. *We have $e_2 A = e_2 C$ and $Ae_2 = Ce_2$ as subsets of M_2. Also, $e_1 B = e_1 C$ and $Be_1 = Ce_1$ in M_2.*

Proof. For each $b \in B$ we have $b_j, b'_j \in M_1$ such that

$$e_2 b = 1_1 \otimes 1_1 \sum_j b_j \otimes b'_j = e_2 \sum_j E_M(b_j)\, b'_j \in ke_2$$

since $\sum_j E_M(b_j)\, b'_j \in C_{M_1}(M) = k1$. Then $e_2 C = e_2 BA = e_2 A$. The second equality is proven similarly. The second statement is proven in the same way by making use of $e_1 A = Ae_1 = ke_1$. ∎

We place the E_M-multiplication on $A \otimes A$, and the E_{M_1}-multiplication on $B \otimes B$ below.

PROPOSITION 3.6 (Depth 2 property). *We have $C = Ae_2A$ and $C \cong A \otimes_k A$ as rings. Also, $C = Be_1B$ and $C \cong B \otimes_k B$ as rings.*

Proof. Clearly $Ae_2A \subseteq C$. Conversely, if $c \in C$, then $c = \sum_j E_{M_1}(cu_j)\, v_j$. But $\sum_j u_j \otimes v_j = \lambda^{-1} \sum_i z_i e_2 \otimes e_2 w_i$ by the endomorphism ring theorem and the fact that both are dual bases to E_{M_1}. Then $c = \lambda^{-1} \sum_i E_{M_1}(cz_i e_2)\, e_2 w_i \in Ae_2A$ as desired.

Since $e_2 w e_2 = E_M(w)\, e_2$ for every $w \in M_1$, we obtain the E_M-multiplication on Ae_2A. Then $C = Ae_2A = A \otimes_M A \cong A \otimes_k A$ since $A \cap M = C_M(N) = k1_M$.

For the second statement, we observe:

$$C = Ae_2A = Ae_2e_1e_2A \subseteq Ce_1C = Be_1B,$$

while the opposite inclusion is immediate. The ring isomorphism follows from the identity:

$$e_1 c e_1 = e_1 E_{M_1}(c) \tag{9}$$

for all $c \in C$, since $B \cap N1_2 \subseteq Z(N) = k1$. For there are $a_i, b_i \in A$ such that $c = \sum_i a_i e_2 b_i$, and $\eta, \eta'\colon A \to k$ such that, for all $a \in A$, $e_1 a = e_1 \eta(a)$ while $ae_1 = \eta'(a)\, e_1$ by irreducibility. Then we easily compute that $\eta = \eta'$. Then:

$$\begin{aligned} e_1 c e_1 &= \sum_i e_1 a_i e_2 b_i e_1 = \sum_i \eta(a_i)\, \eta(b_i)\, e_1 e_2 e_1 \\ &= \lambda \sum_i e_1 a_i b_i = e_1 E_{M_1}(c). \quad \blacksquare \end{aligned}$$

In Section 3 it will be apparent that η is the counit ε on A.

COROLLARY 3.7. *If $n = \#\{u_j\} = \#\{v_j\}$, then $C \cong M_n(k)$ where the characteristic of k does not divide n.*

Proof. Since B is a Frobenius algebra with Frobenius homomorphism E_{M_1}, it follows from the isomorphism $\mathrm{End}_k(B) \cong B \otimes B$ that

$$C \cong \mathrm{End}_k(B) \cong M_n(k). \tag{10}$$

We have char $k \nmid n$ since the index $\lambda^{-1} = n1_k \neq 0$. $\blacksquare$

Since we can use A in place of B to conclude that $C \cong \mathrm{End}_k(A)$ in the proof above, we see that $\dim_k A = \dim_k B$. Although C has a faithful trace, we will prefer the faithful linear functional F studied below for its Markov-like properties in Corollary 3.11.

$$\begin{array}{ccc} C & \xrightarrow{q} & C \\ \downarrow & & \downarrow \\ A & \xrightarrow{q_A} & A \end{array}$$

FIG. 1. The vertical arrows are given by the conditional expectation $E_{M_1}|_C$.

PROPOSITION 3.8. *$F := E_M \circ E_{M_1}$ is a faithful linear functional on C.*

Proof. We see that $E_M(E_{M_1}(C)) \in C_M(N) = k1$, and we identify $k1$ with k. If $c = a \in A1_2$, we see that

$$F(aC) = E_M(aE_{M_1}(C)) = E_M(aA) = 0$$

implies that $a = 0$ by Proposition 3.2, since E_M is a Frobenius homomorphism on A and therefore faithful.

If $c = b \in B$, then by Lemma 3.4

$$F(bC) = E_M E_{M_1}(bC) = E_M(E_{M_1}(bB)\, A) = 0$$

implies first $E_{M_1}(bB) = 0$, next $b = 0$.

If $c \in C$, then there are $a_i \in A\ (= E_{M_1}(cu_i))$ such that $c = \sum_i a_i v_i$. Then

$$F(cC) = \sum_i E_M(a_i A)\, E_{M_1}(v_i B) = 0$$

implies that each $a_i = 0$, since if $a_i \neq 0$, then $E_{M_1}(v_i B) = 0$, a contradiction. Hence, F is faithful on C. ∎

Denote the Nakayama automorphism of F on C by $q: C \to C$. It follows from Corollary 3.7 that q is an inner automorphism. We note some other Nakayama automorphisms and study next their inter-relationships. Let $q_A: A \to A$ be the Nakayama automorphism for E_M on A.

Let $q_B: B \to B$ be the Nakayama automorphism for E_{M_1} on B. Let $\tilde{q}: B \to B$ be the Nakayama automorphism for $\hat{F} := E_M \circ E_{M_1} : M_2 \to M$, a Frobenius homomorphism by Proposition 2.1.

PROPOSITION 3.9. *We have $q_B = \tilde{q} = q|_B$, $q_A = q|_A$ and commutativity of the diagram in Figure* 1.

Proof. We have for each $b \in B$, $c \in C$:

$$F(cb) = F(q(b)\, c) = F(\tilde{q}(b)\, c)$$

whence by faithfulness $q|_B = \tilde{q}$. Then q sends B onto itself, so

$$E_{M_1}(q_B(b_2)\, b_1) = E_{M_1}(b_1 b_2) = F(b_1 b_2) = F(q(b_2)\, b_1) = E_{M_1}(q(b_2)\, b_1)$$

for each $b_1, b_2 \in B$, whence $q_B = q|_B$.

As for q_A, we note that

$$F(q(a)\, c) = F(ca) = F(E_{M_1}(c)\, a) = F(q_A(a)\, E_{M_1}(c)) = F(q_A(a)\, c)$$

for every $a \in A$, $c \in C$, whence $q = q_A$ on A.

Commutativity of Figure 1 follows from the computation applying Eq. (11):

$$\begin{aligned} F(q(E_{M_1}(c))\, c') &= F(c' E_{M_1}(c)) = F(E_{M_1}(c')\, c) \\ &= F(q(c)\, E_{M_1}(c')) = F(E_{M_1}(q(c))\, c'), \end{aligned}$$

for all $c, c' \in C$. ▮

We now compute the conditional expectation of C onto B, a lemma we will need in Section 3.

LEMMA 3.10. *The map $E_B\colon C \to B$ defined by $E_B(c) = \sum_j F(cu_j)\, v_j$ for all $c \in C$ is a conditional expectation.*

Proof. We first note that E_B is the identity on B, since $E_{M_1}(bu_j) \in k1_1$, whence $E_B(b) = \sum_j E_M(1_1)\, E_{M_1}(bu_j)\, v_j = b$. Since $E_M(E_{M_1}(cu_j)) \in k1$ for all $c \in C$, we have for each $b, b' \in B$:

$$E_B(be_1 b') = \sum_j F(be_1 b' u_j)\, v_j = \sum_j E_M(e_1 E_{M_1}(b' u_j q^{-1}(b))\, v_j$$

$$= \lambda \sum_j E_{M_1}(bb' u_j)\, v_j = \lambda bb'$$

It follows from Proposition 3.6 that E_B is a B-B-bimodule homomorphism (it corresponds to $\lambda\mu\colon B \otimes B \to B$ under the isomorphism $b \otimes b' \mapsto be_1 b'$ of $B \otimes B$ with C).

That E_B is a Frobenius homomorphism follows from [9, Lemma 2.6.1], if we show it is one-sided faithful, e.g., $E_B(Cc) = 0$ implies $c = 0$. But this follows from F being faithful and orthogonality of the dual bases $\{u_i\}$ and $\{v_i\}$. ▮

The corresponding conditional expectation $E_A: C \to A$ is easily seen to be E_{M_1} restricted to C. We next record several Markov-like properties of $F: C \to k$.

COROLLARY 3.11. *The linear functional F satisfies the following properties with respect to E_{M_1} and E_B:*

$$\begin{aligned} F(aE_{M_1}(c)) &= F(ac), \qquad & F(E_{M_1}(c)\,a) &= F(ca), \\ F(bE_B(c)) &= F(bc), \qquad & F(E_B(c)\,b) &= F(cb), \end{aligned} \tag{11}$$

for all $a \in A, b \in B, c \in C$. In particular, we have the following Markov relations:

$$F(ae_2) = F(e_2a) = \lambda F(a), \qquad F(be_1) = F(e_1b) = \lambda F(b).$$

Proof. According to the definitions of F and E_B, we have $F \circ E_{M_1} = F \circ E_B = F$ and also $E_{M_1}(e_2) = \lambda$, $E_B(e_1) = \lambda$, whence the result. ∎

The Pimsner–Popa Identities

We note that:

$$\lambda^{-1} e_1 E_M(e_1 x) = e_1 x \quad \forall x \in M_1$$

$$\lambda^{-1} e_2 E_{M_1}(e_2 y) = e_2 y \quad \forall y \in M_2.$$

Proof. Let $x = \sum_i m_i \otimes m_i'$ where $m_i, m_i' \in M_1$. Then $e_2 x = e_2 \sum_i E_M(m_i)\, m_i'$, and $E_{M_1}(e_2 x) = \lambda \sum_i E_M(m_i)\, m_i'$ from which one of the equations follows. The other equation is similarly shown, as are the opposite Pimsner–Popa identities.

COROLLARY 3.12. *$e_1 \in Z(A), e_2 \in Z(B)$, and we have $q(e_1) = e_1, q(e_2) = e_2$.*

Proof. From Eq. (9)

$$e_1 a = e_1 a e_1 = a e_1,$$

for all $a \in A$. It is clear from Eq. (3) that a Nakayama automorphism fixes elements in the center of a Frobenius *algebra*. The assertions about e_2 are shown similarly. ∎

When Hopf–Galois Extensions are Strongly Separable

We recall a few facts about Hopf–Galois extensions [17]. If H is a finite dimensional Hopf k-algebra with counit ε and comultiplication

$\Delta(h) = h_{(1)} \otimes h_{(2)}$, then its dual H^* is a Hopf algebra as well (and $H^{**} \cong H$). Thus we have the following dual notions of algebra extension: M/N is a right H^*-comodule algebra extension with coaction $M \to M \otimes H$, denoted by $\rho(a) = a_{(0)} \otimes a_{(1)}$, and $N = \{b \in M \mid \rho(b) = b \otimes 1\}$ if and only if M/N is a left H-module algebra extension with action of H on M given by $h \rhd a = a_{(0)} \langle a_{(1)}, h \rangle$ and $N = \{b \in M \mid \forall h \in H, h \rhd b = \varepsilon(h)\, b\}$. Conversely, given an action of H on M and dual bases $\{u_j\}$, $\{p_j\}$ for H and H^*, a coaction is given by

$$\rho(a) = \sum_j (u_j \rhd a) \otimes p_j. \tag{12}$$

Recall on the one hand that M/N is an *H^*-Galois extension* if it is a right H^*-comodule algebra such that the *Galois map* $\beta : M \otimes_N M \to M \otimes H^*$ given by $a \otimes a' \mapsto aa'_{(0)} \otimes a'_{(1)}$ is bijective.

Recall on the other hand that given a left H-module algebra M, there is the smash product $M \# H$ with subalgebras $M = M \# 1$, $H = 1 \# H$ and commutation relation $ha = (h_{(1)} \rhd a)\, h_{(2)}$ for all $a \in M, h \in H$. If N again denotes the subalgebra of invariants, then there is a natural algebra homomorphism of the smash product into the right endomorphism ring, $\Psi \colon M \# H \to \mathrm{End}(M_N)$ given by $m \# h \mapsto m(h \rhd \cdot\,)$. We will use the following basic proposition in Section 5 (and prove part of the forward implication below):

Proposition 3.13 [14, 25]. *An H-module algebra extension M/N is H^*-Galois if and only if $M \# H \xrightarrow{\cong} \mathrm{End}(M_N)$ via Ψ, and M_N is a finitely generated projective module.*

The following theorem is a converse to our main theorem in 5.5. Let H be a finite dimensional, semisimple and cosemisimple Hopf algebra.

Theorem 3.14 (Cf. [12], 3.2). *Suppose M is a k-algebra and left H-module algebra with subalgebra of invariants N. If M/N is an irreducible right H^*-Galois extension, then M/N is a strongly separable, irreducible extension of depth 2 with $\mathrm{End}(M_N) \cong M \# H$.*

$$\begin{array}{ccc} M \otimes_N M & \xrightarrow{\ \beta\ } & M \otimes H^* \\ \downarrow & & \downarrow \cong \\ \mathrm{End}\, M_N & \xleftarrow{\ \Psi\ } & M \# H \end{array}$$

FIG. 2. Commutative diagram where the left vertical mapping is given by $m \otimes m' \mapsto \lambda_m E \lambda_{m'}$ and the right vertical mapping is the isomorphism $\mathrm{id} \otimes \theta$.

Proof. Since H is finite dimensional (co)semisimple, H is (co)unimodular and there are integrals $f \in \int_{H^*}$ and $t \in \int_H$ such that $f(t) = f(S(t)) = 1_k$, $\varepsilon(t) = 1$ and $f(1) \neq 0$. Moreover, $g \mapsto (t \leftharpoonup g)$ gives a Frobenius isomorphism $\theta: H^* \xrightarrow{\cong} H$, where $t \leftharpoonup f = f(t_{(1)})\, t_{(2)} = 1_H$, since f integral in H^* means $x \leftharpoonup f = f(x)\, 1_H$ for every $x \in H$.

If $\beta: M \otimes_N M \to M \otimes H^*$ is the Galois isomorphism, given by $m \otimes m' \mapsto mm'_{(0)} \otimes m'_{(1)}$, then $\psi = (\mathrm{id}_M \otimes \theta) \circ \beta$ is the isomorphism $M \otimes_N M \xrightarrow{\cong} M\#H$ given by

$$m \otimes m' \mapsto mm'_{(0)} \otimes (t \leftharpoonup m'_{(1)}) = m\langle m'_{(1)}, t_{(1)}\rangle\, m'_{(0)} \otimes t_{(2)}$$
$$= m(t_{(1)} \cdot m') \otimes t_{(2)} = mtm'.$$

Now define $E: M \to N$ by $E(m) = t \cdot m$, where $t \cdot m \in N$ since $h \cdot (t \cdot m) = (ht) \cdot m = \varepsilon(h)\, t \cdot m$. Note that E is an N-N-bimodule map and $E(1) = \varepsilon(t)\, 1 = 1$.

Denote $\beta^{-1}(1 \otimes f) = \sum_i x_i \otimes y_i \in M \otimes_N M$. Since $(\mathrm{id} \otimes \theta)(1 \otimes f) = 1\#1$, which is sent by Ψ to id_M, it follows that $\sum_i x_i(Ey_i) = \mathrm{id}_M$ (cf. Figure 2).[4]

The homomorphism $\Psi: M\#H \to \mathrm{End}(M_N)$ (given by $m\#h \mapsto (m' \mapsto m(h \cdot m'))$) is now readily checked to have inverse mapping given by $g \mapsto \sum_i g(x_i)\, ty_i$ [14].

By counitarity of the H^*-comodule M, then $\mu: M \otimes_N M \to M$ factors through β and the map $M \otimes H^* \to M$ given by $m \otimes g \mapsto mg(1)$. Then $\sum_i x_i y_i = f(1_H)\, 1_M$, whence the k-index $[M : N]_E$ is $\lambda^{-1} = f(1_H)$.

It is not hard to compute that $C_{M\#H}(N) = C_M(N)\#H$ which is H since M/N is irreducible. Since $M\#H$ is free over M with basis in H, we see that the first half of the depth 2 condition is satisfied.

The second half of depth 2 follows from noting that $M\#H$ is a right H-Galois extension of M. For the coaction $M\#H \to (M\#H) \otimes H$ is given by

$$m\#h \mapsto m\#h_{(1)} \otimes h_{(2)}. \tag{13}$$

One may compute the inverse of the Galois map to be given by $\beta^{-1}(m\#h \otimes h') = mhS(h'_{(1)}) \otimes h'_{(2)}$. Then $M_2 \cong M\#H\#H^*$ and the rest of the proof proceeds as in the previous paragraph. ∎

[4] E is in fact a Frobenius homomorphism with dual bases $\{x_i\}$, $\{y_i\}$, the other equation, $\sum_i (x_i E)\, y_i = \mathrm{id}_M$, following readily from a computation using $\beta' = \eta \circ \beta$, where β' is the "opposite" Galois mapping given by $\beta'(m \otimes m') = m_{(0)}m' \otimes m_{(1)}$ and η is an automorphism of $M \otimes H^*$ given by $\eta(m \otimes g) = m_{(0)} \otimes m_{(1)}S(g)$ [14].

The proof shows that an H-Galois extension M/N has an endomorphism ring theorem: $\mathscr{E}/M$ is an H^*-Galois extension. A converse to the endomorphism ring theorem depends on $\mathscr{E}/M$ being H^*-*cleft*, as discussed in Section 6.

4. HOPF ALGEBRA STRUCTURES ON CENTRALIZERS

In this section, we define and study an important non-degenerate pairing of A and B given by Eq. (14). This transfers the algebra structure of A onto a coalgebra structure of B, and conversely. The rest of the section is devoted to showing that B is a Hopf algebra with an antipode S satisfying $S^2 = \mathrm{id}$. The key step in this section and the next is Proposition 4.6.

A Duality Form

As in Section 2, we let $N \subset M \subset M_1 \subset M_2 \subset \cdots$ be the Jones tower constructed from a strongly separable irreducible extension $N \subset M$ of depth 2, $F = E_M \circ E_{M_1}$ denote the functional on C defined in Proposition 3.8, $e_1 \in M_1$, $e_2 \in M_2$ be the first two Jones idempotents of the tower, and $\lambda^{-1} = [M : N]$ be the index.

PROPOSITION 4.1. *The bilinear form*

$$\langle a, b\rangle = \lambda^{-2} F(ae_2e_1b), \qquad a \in A, \quad b \in B, \tag{14}$$

is non-degenerate on $A \otimes B$.

Proof. If $\langle a, B\rangle = 0$ for some $a \in A$, then we have $F(ae_2e_1c) = 0$ for all $c \in C$, since $e_1B = e_1C$ by Lemma 3.5. Taking $c = e_2q^{-1}(a')(a' \in A)$ and using the braid-like relations between Jones idempotents and Markov property (Corollary 3.11) of F we have

$$F(a'a) = \lambda^{-1}F(a'ae_2) = \lambda^{-1}F(ae_2q^{-1}(a')) = \lambda^{-2}F(ae_2e_1(e_2q^{-1}(a')) = 0$$

for all $a' \in A$, therefore $a = 0$ (by Proposition 3.2).

Similarly, if $\langle A, b\rangle = 0$ for some b, then $F(ce_2e_1b) = 0$ for all $c \in C$, which for $c = q(b')\, e_1$ $(b' \in B)$ gives

$$F(bb') = \lambda^{-1}F(e_1bb') = \lambda^{-1}F(q(b')\, e_1b) = \lambda^{-2}F((q(b')\, e_1)\, e_2e_1b) = 0$$

for all $b' \in B$, therefore $b = 0$. ∎

Observe that since k is a field the Proposition above shows that the map $b \mapsto E_{M_1}(e_2 e_1 b)$ is a linear isomorphism between B and A. Indeed, $E_{M_1}(e_2 e_1 b) = 0$ implies that for all $a \in A$ one has

$$F(ae_2e_1b) = F(aE_{M_1}(e_2e_1b)) = 0,$$

whence $b = 0$ by nondegeneracy.

A Coalgebra Structure

Using the above duality form we introduce a coalgebra structure on B.

DEFINITION 4.2. The algebra B has a comultiplication $\Delta: B \to B \otimes B$, $b \mapsto b_{(1)} \otimes b_{(2)}$ defined by

$$\langle a, b_{(1)} \rangle \langle a', b_{(2)} \rangle = \langle aa', b \rangle \tag{15}$$

for all $a, a' \in A$, $b \in B$, and counit $\varepsilon: B \to k$ given by ($\forall b \in B$)

$$\varepsilon(b) = \langle 1, b \rangle. \tag{16}$$

PROPOSITION 4.3. *For all $b, c \in B$ we have :*

$$\varepsilon(b) = \lambda^{-1} F(be_2), \tag{17}$$

$$\Delta(1) = 1 \otimes 1, \tag{18}$$

$$\varepsilon(bb') = \varepsilon(b)\, \varepsilon(b'). \tag{19}$$

Proof. We use the Pimsner–Popa identities together with Corollaries 3.11 and 3.12 to compute

$$\begin{aligned} \varepsilon(b) &= \lambda^{-2} F(e_2e_1b) = \lambda^{-2} F(e_1be_2) = \lambda^{-1} F(be_2), \\ \langle a, 1 \rangle \langle a', 1 \rangle &= \lambda^{-4} F(ae_2e_1)\, F(a'e_2e_1) \\ &= \lambda^{-2} F(ae_1)\, F(a'e_1) = \lambda^{-2} F(aE_M(a'e_1)\, e_1) \\ &= \lambda^{-1} F(aa'e_1) = \langle aa', 1 \rangle, \\ \varepsilon(b)\, \varepsilon(b') &= \lambda^{-2} F(be_2)\, F(b'e_2) = \lambda^{-2} F(bE_{M_1}(b'e_2)\, e_2) \\ &= \lambda^{-1} F(bb'e_2) = \varepsilon(bb'), \end{aligned}$$

for all $a, a' \in A$, $b, b' \in B$ (note that the restriction of $E_M|_A = F$ and the restriction of $E_{M_1}|_B = F$, identifying k and $k1$). ∎

The Antipode of B

Recall that the map $b \mapsto E_{M_1}(e_2 e_1 b)$ is a linear isomorphism between B and A. But considering the Jones tower $N^{op} \subset M^{op} \subset M_1^{op} \subset M_2^{op}$ of the opposite algebras, we conclude that the map $b \mapsto E_{M_1}(b e_1 e_2)$ is a linear isomorphism as well. This lets us define a linear map $S\colon B \to B$, called the *antipode*, as follows.

DEFINITION 4.4. For every $b \in B$ define $S(b) \in B$ to be the unique element such that

$$F(q(b)\, e_1 e_2 a) = F(a e_2 e_1 S(b)), \qquad \text{for all} \quad a \in A,$$

or, equivalently,

$$E_{M_1}(b e_1 e_2) = E_{M_1}(e_2 e_1 S(b)).$$

Remark 4.5. Note that S is bijective and that the above condition implies

$$E_{M_1}(b x e_2) = E_{M_1}(e_2 x S(b)), \qquad \text{for all} \quad x \in M_1. \tag{20}$$

Indeed, B commutes with M and any $x \in M_1$ can be written as $x = \sum_i m_i e_1 n_i$ with $m_i, n_i \in M$, so that

$$E_{M_1}(b x e_2) = \Sigma_i m_i E_{M_1}(b e_1 e_2)\, n_i = \Sigma_i m_i E_{M_1}(e_2 e_1 S(b))\, n_i = E_{M_1}(e_2 x S(b)).$$

A and B are Hopf Algebras

To prove that B is Hopf algebra, it remains to show that Δ is a homomorphism and that S satisfies the antipode axioms. The next proposition is also the key ingredient for an action of B on M_1 which makes M_2 a smash product.

PROPOSITION 4.6. *For all $b \in B$ and $y \in M_1$ we have*

$$yb = \lambda^{-1} b_{(2)} E_{M_1}(e_2\, y b_{(1)}).$$

Proof. First, let us show that the above equality holds true in the special case $y = e_1$. Let E_B be the conditional expectation from C to B given by $E_B(c) = \Sigma_i F(c u_i)\, v_i$ as in Proposition 3.10.

We claim that for any $c \in C$ we have $c = 0$ if $\langle a, E_B(ca')\rangle = 0$ for all $a, a' \in A$. For since $C = BA$, let $c = \sum_i b_i a_i$ with $a_i \in A$ and $b_i \in B$, then

$$\langle a, E_B(ca')\rangle = \sum_i \langle a, b_i E_B(a_i a')\rangle = \sum_i \langle a, b_i\rangle\, F(a_i a'),$$

and the latter expression is equal to 0 for all $a, a' \in A$ only if for each i either $a_i = 0$ or $b_i = 0$.

Observe that q restricted to A coincides with the Nakayama automorphism $q_A\colon A \to A$ of the Frobenius extension M_1/N since

$$F(q(a)\,c) = F(ca) = F(E_{M_1}(c)\,a) = E \circ E_M(q_A(a)\,E_{M_1}(c)) = F(q_A(a)\,c),$$

therefore, using the Pimsner–Popa identity for $C = Be_1B$, we establish the proposition for $y = e_1$:

$$\begin{aligned}\langle a, E_B(e_1ba')\rangle &= \lambda^{-2}F(ae_2e_1E_B(e_1ba'))\\ &= \lambda^{-1}F(ae_2e_1ba') = \lambda\langle q(a')\,a, b\rangle,\\ \langle a, \lambda^{-1}b_{(2)}E_B(E_{M_1}(e_2e_1b_{(1)})\,a')\rangle &= \lambda^{-1}\langle a, b_{(2)}\rangle\,F(e_2e_1b_{(1)}a')\\ &= \lambda\langle a, b_{(2)}\rangle\langle q(a'), b_{(1)}\rangle = \lambda\langle q(a')\,a, b\rangle,\end{aligned}$$

since $E_B|_A = F$.

Next, arguing as in Remark 4.5 we write $y = \Sigma_i m_ie_1n_i$ with $m_i, n_i \in M$, whence

$$yb = \Sigma_i m_ie_1bn_i = \lambda^{-1}\Sigma_i m_ib_{(2)}E_{M_1}(e_2e_1b_{(1)})\,n_i = b_{(2)}E_{M_1}(e_2\,yb_{(1)}). \quad \blacksquare$$

Corollary 4.7. *For all $b \in B$ and $x, y \in M_1$ we have:*

$$E_{M_1}(e_2xyb) = \lambda^{-1}E_{M_1}(e_2xb_{(2)})\,E_{M_1}(e_2\,yb_{(1)}).$$

Proof. The result follows from multiplying the identity from Proposition 4.6 by e_2x on the left and taking E_{M_1} from both sides. $\blacksquare$

Although the antipode axiom (cf. Prop. 4.12) implies that S is a coalgebra anti-homomorphism, we will have to establish these two properties of S in the reverse order, as stepping stones to Propositions 4.11 and 4.12.

Lemma 4.8. *S is a coalgebra anti-automorphism.*

Proof. For all $a, a' \in A$ and $b \in B$ we have by Corollary 4.7

$$\begin{aligned}\langle aa', S(b)\rangle &= \lambda^{-2}F(q(b)\,e_1e_2aa') = \lambda^{-3}F(e_1e_2E_{M_1}(e_2aa'b))\\ &= \lambda^{-4}F(e_1e_2E_{M_1}(e_2ab_{(2)})\,E_{M_1}(e_2a'b_{(1)}))\\ &= \lambda^{-6}F(e_1e_2E_{M_1}(e_2ab_{(2)}))\,F(e_1e_2E_{M_1}(e_2a'b_{(1)}))\\ &= \lambda^{-4}F(e_1e_2ab_{(2)})\,F(e_1e_2a'b_{(1)})\\ &= \lambda^{-4}F(q(b_{(2)})\,e_1e_2a)\,F(q(b_{(1)})\,e_1e_2a')\\ &= \langle a, S(b_{(2)})\rangle\langle a', S(b_{(1)})\rangle,\end{aligned}$$

where we use the definition of S, the Pimsner–Popa identity, and Corollary 3.11. Thus, $\Delta(S(b)) = S(b_{(2)}) \otimes S(b_{(1)})$. ∎

COROLLARY 4.9. *For all $b \in B$ and $x, y \in M_1$ we have:*

$$E_{M_1}(bxye_2) = \lambda^{-1} E_{M_1}(b_{(1)}xe_2)\, E_{M_1}(b_{(2)}\, ye_2)$$

Proof. We obtain this formula by replacing b with $S(b)$ in Corollary 4.7 and using Eq. (20) as well as Lemma 4.8. ∎

PROPOSITION 4.10. $S^2 = q|_B^{-1}$.

Proof. The statement follows from the direct computation:

$$\begin{aligned} F(ae_2e_1q^{-1}(b)) &= \lambda^{-1}F(E_{M_1}(bae_2)\, e_2e_1) \\ &= \lambda^{-1}F(E_{M_1}(e_2aS(b))\, e_2e_1) \\ &= \lambda^{-1}F(e_2E_{M_1}(e_2aS(b))\, e_1) \\ &= F(e_2aS(b)\, e_1) = F(aE_{M_1}(S(b)\, e_1e_2)) \\ &= F(ae_2e_1S^2(b)), \end{aligned}$$

for all $a \in A$ and $b \in B$, using Remark 4.5 and Corollary 3.12. ∎

PROPOSITION 4.11. *Δ is an algebra homomorphism.*

Proof. Note that $q|_B$ is a coalgebra automorphism by Proposition 4.10. By Corollary 4.9 we have, for all $a, a' \in A$ and $b, b' \in B$:

$$\begin{aligned} \langle aa', bb' \rangle &= \langle \lambda^{-1}E_{M_1}(q(b')\, aa'e_2), b \rangle \\ &= \langle \lambda^{-2}E_{M_1}(q(b')_{(1)}\, ae_2)\, E_{M_1}(q(b')_{(2)}\, a'e_2), b \rangle \\ &= \langle \lambda^{-1}E_{M_1}(q(b'_{(1)})\, ae_2), b_{(1)} \rangle \langle \lambda^{-1}E_{M_1}(q(b'_{(2)})\, a'e_2), b_{(2)} \rangle \\ &= \langle a, b_{(1)}b'_{(1)} \rangle \langle a', b_{(2)}b'_{(2)} \rangle, \end{aligned}$$

whence $\Delta(bb') = \Delta(b)\, \Delta(b')$. ∎

PROPOSITION 4.12. *For all $b \in B$ we have $S(b_{(1)})\, b_{(2)} = \varepsilon(b)\, 1 = b_{(1)}S(b_{(2)})$.*

Proof. Using Corollary 4.9 and the definition of the antipode we have

$$\begin{aligned} \langle a, S(b_{(1)})\, b_{(2)} \rangle &= \lambda^{-1} \langle E_{M_1}(q(b_{(2)})\, ae_2), S(b_{(1)}) \rangle \\ &= \lambda^{-3}F(q(b_{(1)})\, e_1e_2E_{M_1}(q(b_{(2)})\, ae_2)) \\ &= \lambda^{-3}F(E_{M_1}(q(b_{(1)})\, e_1e_2)\, E_{M_1}(q(b_{(2)})\, ae_2)) \\ &= \lambda^{-2}F(q(b)\, e_1ae_2) = \lambda^{-2}F(e_1ae_2b) \\ &= \lambda^{-2}F(e_1a)\, F(be_2) = \langle a, 1\varepsilon(b) \rangle, \end{aligned}$$

$\forall a \in A$, $b \in B$. The second identity follows similarly from Corollary 4.7 and the corollary $q \circ S = S^{-1}$ from Proposition 4.10:

$$\begin{aligned}\langle a, b_{(1)} S(b_{(2)})\rangle &= \lambda^{-1}\langle E_{M_1}(q(S(b_{(2)}))\, ae_2), b_{(1)}\rangle \\ &= \lambda^{-3} F(E_{M_1}(q(S(b_{(2)}))\, ae_2)\, e_2 e_1 b_{(1)}) \\ &= \lambda^{-3} F(E_{M_1}(S^{-1}(b_{(2)})\, ae_2)\, e_2 e_1 b_{(1)}) \\ &= \lambda^{-3} F(E_{M_1}(e_2 a b_{(2)})\, E_{M_1}(e_2 e_1 b_{(1)})) \\ &= \lambda^{-2} F(e_2 a e_1 b) = \lambda^{-2} F(a e_1 b e_2) = \langle a, 1\varepsilon(b)\rangle,\end{aligned}$$

i.e., S satisfies the antipode properties. ▮

THEOREM 4.13. *A and B are semisimple Hopf algebras.*

Proof. Follows from Propositions 4.3, 4.11, 4.12, and 3.2. Note that semisimplicity and separability are notions that coincide for finite dimensional Hopf algebras [17]. The non-degenerate duality form of Proposition 4.1 makes A the Hopf algebra dual to B. ▮

COROLLARY 4.14. *The antipodes of A and B satisfy $S^2 = id$, F is a trace, and A, B are Kanzaki strongly separable.*

Proof. Etingof and Gelaki proved that a semisimple and cosemisimple Hopf algebra is involutive [7]. It follows from Proposition 4.10 that $q_B = \mathrm{id}_B$. But we compute:

$$\langle a, q^{-1}(b)\rangle = \lambda^{-2} F(bae_2e_1) = \lambda^{-2} F(q(a)\, e_2 e_1 b) = \langle q(a), b\rangle$$

for all $a \in A$, $b \in B$, from which it follows that $S_A^2 = q_A = \mathrm{id}_A$. Since $C = BA$, we have $q = \mathrm{id}_C$. Whence F, E_M and E_{M_1} are traces on C, A and B, respectively.

It follows from Proposition 3.2 that $\{\lambda^{-1} E_{M_1}|_B, \lambda u_i, v_i\}$ is a separable base for B; similarly, $\{\lambda^{-1} E_M|_A, \lambda z_i, w_i\}$ is a separable base for A, whence A and B are strongly separable algebras. ▮

Remark 4.15. Note that e_2 is a (2-sided) integral in B, since $\langle a, e_2 b\rangle = \langle a, e_2\rangle\, \varepsilon(b) = \langle a, be_2\rangle$ by the Pimsner–Popa identity. Similarly, e_1 is an integral in A.

5. ACTION OF B ON M_1 AND M_2 AS A SMASH PRODUCT

In this section, we define the Ocneanu-Szymański action of B on M_1, which makes M_1 a B-module algebra (cf. Eq. (21)). We then describe M as its subalgebra of invariants and M_2 as the smash product algebra of B and M_1. As a corollary, we note that M_1/M and M_2/M_1 are respectively A- and B-Galois extensions.

PROPOSITION 5.1. *The map* $\triangleright : B \otimes M_1 \to M_1$:

$$b \triangleright x = \lambda^{-1} E_{M_1}(bxe_2) \tag{21}$$

defines a left B-module algebra action on M_1, *called the Ocneanu–Szymański action.*

Proof. The above map defines a left B-module structure on M_1, since $1 \triangleright x = \lambda^{-1} E_{M_1}(xe_2) = x$ and

$$b \triangleright (c \triangleright x) = \lambda^{-2} E_{M_1}(bE_{M_1}(cxe_2)\, e_2) = \lambda^{-1} E_{M_1}(bcxe_2) = (bc) \triangleright x.$$

Next, Corollary 4.9 implies that $b \triangleright xy = (b_{(1)} \triangleright x)(b_{(2)} \triangleright y)$. Finally, $b \triangleright 1 = \lambda^{-1} E_{M_1}(be_2) = \lambda^{-1} F(be_2)\, 1 = \varepsilon(b)\, 1$. ▮

We note that an application of Proposition 4.6 provides another formula for the action of B on M_1:

$$b \triangleright x = b_{(1)} x S(b_{(2)}). \tag{22}$$

PROPOSITION 5.2. $M_1^B = M$, *i.e.,* M *is the subalgebra of invariants of* M_1.

Proof. If $x \in M_1$ is such that $b \triangleright x = \varepsilon(b)\, x$ for all $b \in B$, then $E_{M_1}(bxe_2) = \lambda \varepsilon(b)\, x$. Letting $b = e_2$ we obtain $E_M(x) = \lambda^{-1} E_{M_1}(e_2 x e_2) = \varepsilon(e_2)\, x = x$, therefore $x \in M$.

Conversely, if $x \in M$, then x commutes with e_2 and

$$b \triangleright x = \lambda^{-1} E_{M_1}(be_2 x) = \lambda^{-1} E_{M_1}(be_2)\, x = \varepsilon(b)\, x,$$

therefore $M_1^B = M$. ▮

Note from the proof that $e_2 \triangleright x = E_M(x)$, i.e., the conditional expectation E_M is action on M_1 by the integral e_2 in B. The rest of this section is strictly speaking not required for Section 6.

THEOREM 5.3. *The map* $\theta\colon x \# b \mapsto xb$ *defines an algebra isomorphism between the smash product algebra* $M_1 \# B$ *and* M_2.

Proof. The bijectivity of θ follows from Lemma 3.3.

To see that θ is a homomorphism it suffices to note that $by = (b_{(1)} \triangleright y)\, b_{(2)}$ for all $b \in B$ and $y \in M_1$. Indeed, using Eq. (22),

$$(b_{(1)} \triangleright y)\, b_{(2)} = b_{(1)}\, yS(b_{(2)})\, b_{(3)}$$
$$= b_{(1)}\, y\varepsilon(b_{(2)}) = by. \quad \blacksquare$$

From this and Lemma 3.4, we conclude that:

COROLLARY 5.4. $C \cong A\# B$.

COROLLARY 5.5. *M_1/M is an A-Galois extension. M_2/M_1 is a B-Galois extension.*

Proof. Dual to the left B-module algebra M_1 defined above is a right A-comodule algebra M_1 with the same subalgebra of coinvariants M, since $B^* \cong A$. By Theorem 5.3 and the endomorphism ring theorem, $M_1\# B \xrightarrow{\cong} M_2 \xrightarrow{\cong} \mathrm{End}^r_M(M_1)$ is given by the natural map $x\# b \mapsto x(b \triangleright \cdot\,)$ since if $b = \sum_i a_i e_2 a_i'$ for $a_i, a_i' \in A$, then for all $y \in M_1$,

$$x(b \triangleright y) = \lambda^{-1} \sum_i x a_i E_{M_1}(e_2 a_i' y e_2) = x \sum_i a_i E_M(a_i' y).$$

By Proposition 3.13 then, M_1 is a right A-Galois extension of M.

It follows from the endomorphism ring theorem for Hopf–Galois extensions (cf. end of Section 3) that M_2/M_1 is B-Galois. $\blacksquare$

Since M_2 is a smash product of M_1 and B, thus a B-comodule algebra, it has a left A-module algebra action given by applying Eq. (13):

$$a \triangleright (mb) = \langle a, b_{(2)} \rangle\, mb_{(1)},$$

for every $a \in A, m \in M_1, b \in B$.[5] We remark that M_1/M and M_2/M_1 are *faithfully flat* (indeed free) Hopf–Galois extensions with normal basis property [17][Chap. 8].

[5] Alternatively, the depth 2 condition is satisfied by M_1/M due to Theorem 3.14, and $C_{M_3}(M_1) \cong A$ via $a \mapsto d$ where $F(ae_2e_1b) = E_{M_1}E_{M_2}(be_3e_2d)$ for all $b \in B$; whence we may repeat the arguments in Sections 3–5 to define an A-module algebra action on M_2, $a \triangleright m_2 = \lambda^{-1} E_{M_2}(dm_2e_3)$, where M_3, E_{M_2} and e_3 are of course the basic construction of M_2/M_1. This is the same action of A on M_2 by repeating Proposition 6.1.

6. ACTION OF A ON M AND M_1 AS A SMASH PRODUCT

In this section, we note that M_1/M is an A-cleft A-extension (Proposition 6.1). It follows from a theorem in the Hopf algebra literature that M_1 is a crossed product of M and A. The cocycle σ determining the algebra structure of $M \#_\sigma A$ is in this case trivial. Whence $M_1 \cong M \# A$ and M/N is a left B-Galois extension (Theorem 6.3). We end the section with a proof of Theorem 1.3 and a proposal for further study.

From the Ocneanu–Szymański action given in Eq. (21), we note that $B \triangleright A = A$. The next proposition shows, based on Corollary 4.14, that the action of B on A yields a coaction $A \to A \otimes A$ (when dualized) which is identical with the comultiplication on A. Recall that an extension of k-algebras $N' \subseteq M'$ is called an *A-extension* if A is a Hopf algebra co-acting on M' such that M' is a right A-comodule algebra with $N' = M'^{\operatorname{co} A}$ [17]: e.g., M_1/M is an A-extension by duality since A is finite dimensional. An A-extension M'/N' is *A-cleft* if there is a right A-comodule map $\gamma: A \to M'$ which is invertible with respect to the convolution product on $\operatorname{Hom}(A, M')$ [17, 3].

Proposition 6.1. *The natural inclusion $\imath: A \hookrightarrow M_1$ is a total integral such that the A-extension M_1/M is A-cleft.*

Proof. Since $\imath(1) = 1$, we show that $\imath$ is a total integral by showing it is a right A-comodule morphism [3]. Denoting the coaction $M_1 \to M_1 \otimes A$ (which is the dual of Action 21) by $w \mapsto w_{(0)} \otimes w_{(1)}$, we have $w_{(0)} \langle w_{(1)}, b \rangle = b \triangleright w$ for every $b \in B$. Since each $a_{(0)} \in A$ by Eq. (12), it suffices to check that $a_{(0)} \otimes a_{(1)} = a_{(1)} \otimes a_{(2)}$:

$$\begin{aligned} \langle a_{(1)}, b \rangle \langle a_{(2)}, b' \rangle = \langle a, bb' \rangle &= \lambda^{-2} F(a e_2 e_1 b b') \\ &= \lambda^{-3} F(E_{M_1}(b' a e_2)\, e_2 e_1 b) = \langle \lambda^{-1} E_{M_1}(b' a e_2), b \rangle \\ &= \langle a_{(0)}, b \rangle \langle a_{(1)}, b' \rangle. \end{aligned}$$

Finally, we note that $\imath$ has convolution inverse in $\operatorname{Hom}(A, M_1)$ given by $\imath \circ S$ where $S: A \to A$ denotes the antipode on A. ∎

We recall the following result of Doi and Takeuchi (see also [17, Prop. 7.2.3] and [1]):

Proposition 6.2 [3]. *Suppose M'/N' is an A-extension, which is A-cleft by a total integral $\gamma: A \to M'$. Then there is a crossed product action of A on N' given by*

$$a \cdot n = \gamma(a_{(1)})\, n \gamma^{-1}(a_{(2)}) \tag{23}$$

for all $a \in A$, $n \in N'$, *and a cocycle* $\sigma\colon A \otimes A \to N'$ *given by*

$$\sigma(a, a') = \gamma(a_{(1)})\, \gamma(a'_{(1)})\, \gamma^{-1}(a_{(2)} a'_{(2)}) \tag{24}$$

for all $a, a' \in A$, *such that* M' *is isomorphic as algebras to a crossed product of* A *with* N' *and cocycle* σ*:*

$$M' \cong N' \#_\sigma A$$

given by $n \# a \mapsto n\gamma(a)$.

Applied to our A-cleft A-extension M_1/M, we conclude:

THEOREM 6.3. *M_1 is isomorphic to the smash product $M \# A$ via $m \# a \mapsto ma$.*

Proof. The cocycle σ associated to $\iota\colon A \to M_1$ is trivial, since

$$\sigma(a, a') = a_{(1)} a'_{(1)} S(a_{(2)} a'_{(2)}) = \varepsilon(a)\, \varepsilon(a')\, 1_1.$$

It follows from Eq. (23) and [17, Lemma 7.1.2]) that M is an A-module algebra with action $A \otimes M \to M$ given by

$$a \rhd m = a_{(1)} m S(a_{(2)}). \tag{25}$$

It follows from Proposition 6.2 and triviality of the crossed product that M_1 is a smash product of M and A as claimed. ∎

LEMMA 6.4. *The fixed point algebra is $M^A = N$.*

Proof. That $N \subseteq M^A$ follows from the definition of A and its Hopf algebra structure. Conversely, suppose that $m \in M$ is such that $a \rhd m = \varepsilon(a)\, m$ for all $a \in A$. In a computation similar to that of [22] [fourth conjecture], we note that $am = ma$ in M_1 for any $a \in A$:

$$am = a_{(1)} m S(a_{(2)})\, a_{(3)} = (a_{(1)} \rhd m)\, a_{(2)} = ma.$$

Letting $a = e_1$, we see that m commutes with e_1, so that $E(m)\, e_1 = e_1 m e_1 = e_1 m$. Applying E_M to this, we arrive at $m = E(m) \in N$. ∎

THEOREM 6.5. *M/N is a B-Galois extension.*

Proof. This follows from Theorem 6.3 and Proposition 3.13, if we prove that $\Psi\colon M \# A \to \operatorname{End}(M_N)$ given by

$$m \# a \mapsto (x \mapsto m(a \rhd x))$$

is an isomorphism.

Towards this end, we claim that $e_1 \rhd x = E(x)$ for every $x \in M$. Let $G = e_1 \rhd \cdot$. A few short calculations using Lemma 6.4 show that $G \in \mathrm{Hom}_{N-N}(M, N)$ such that $G|_N = \mathrm{id}_N$, since

$$ae_1 = \lambda^{-1} E_M(ae_1)\, e_1 = \lambda^{-2} F(ae_2 e_1)\, e_1 = \varepsilon_A(a)\, e_1$$

and

$$\varepsilon_A(e_1) = \lambda^{-2} F(e_1 e_2 e_1) = 1.$$

Since E freely generates $\mathrm{Hom}_N(M, N)$ (as a Frobenius homomorphism), there is $d \in C_M(N) = k1$ such that $G = Ed$, whence $E = G$ as claimed.

Then $\Psi((m\#e_1)(m'\#1_A)) = \lambda_m E \lambda_{m'}$ for all $m, m' \in M$ is surjective. An inverse mapping may be defined by $f \mapsto \sum_i (f(x_i)\#e_1)(y_i\#1_A)$ for each $f \in \mathrm{End}(M_N)$, where $\{x_i\}$, $\{y_i\}$ are dual bases for E as in Section 2. ∎

We are now in a position to note the proof of Theorem 1.3.

THEOREM 6.6 (=Theorem 1.3). *If M/N is an irreducible extension of depth 2, then M/N is strongly separable if and only if M/N is an H-Galois extension, where H is a semisimple, cosemisimple Hopf algebra.*

Proof. The forward implication follows from Theorem 6.5. The reverse implication follows from Theorem 3.14. ∎

We propose the following two problems related to this paper:

(1) Are conditions 1 and 2 in the depth 2 conditions independent?

(2) What is a suitable definition of normality for M/N extending the notion of normal field extensions?[6]

REFERENCES

1. R. J. Blattner, M. Cohen, and S. Montgomery, Crossed products and inner actions of Hopf algebras, *Trans. A.M.S.* **298** (1986), 671–711.
2. F. DeMeyer, The trace map and separable algebras, *Osaka J. Math.* **3** (1966), 7–11.
3. Y. Doi and M. Takeuchi, Cleft comodule algebras for a bialgebra, *Comm. Algebra* **14** (1986), 801–818.
4. Y. Doi, Hopf extensions and Maschke type theorems, *Israel J. Math.* **72** (1990), 99–108.
5. S. Elliger, Über Automorphismen und Derivationen von Ringen, *J. Reine Ang. Mat.* **277** (1975), 155–177.
6. M. Enock and R. Nest, Irreducible inclusions of factors and multiplicative unitaries, *J. Func. Analysis* **137** (1996), 466–543.

[6] There is an early definition of non-commutative normality in [5].

7. P. Etingof and S. Gelaki, On finite-dimensional semisimple and cosemisimple Hopf algebras in positive characteristic, *Internat. Math. Res. Notices* **16** (1998), 851–864.
8. F. G. Frobenius, "Gesammelte Abhandlungen" (J.-P. Serre, Ed.), Vol. III, Springer-Verlag, Berlin, 1968.
9. F. Goodman, P. de la Harpe, and V. F. R. Jones, "Coxeter Graphs and Towers of Algebras," M.S.R.I. Publ., Vol. 14, Springer, Heidelberg, 1989.
10. K. Hirata and K. Sugano, On semisimple extensions and separable extensions over non commutative rings, *J. Math. Soc. Japan* **18** (1966), 360–373.
11. L. Kadison, "New Examples of Frobenius Extensions," University Lecture Series, Vol. 14, A.M.S., Providence, 1999.
12. L. Kadison, The Jones polynomial and certain separable Frobenius extensions, *J. Algebra* **186** (1996), 461–475.
13. F. Kasch, Projektive Frobenius erweiterungen, *Sitzungsber. Heidelberg. Akad. Wiss. Math.-Natur. Kl.* (1960/1961), 89–109.
14. H. Kreimer and M. Takeuchi, Hopf algebras and Galois extensions of an algebra, *Indiana Univ. Math. J.* **30** (1981), 675–692.
15. S. Lang, "Algebra," 3rd ed., Addison–Wesley, New York, 1993.
16. R. Longo, A duality for Hopf algebras and for subfactors I, *Commun. Math. Phys.* **159** (1994), 133–150.
17. S. Montgomery, "Hopf Algebras and Their Actions on Rings," CBMS Regional Conf. Series in Math., Vol. 82, A.M.S., Providence, 1993.
18. K. Morita, Adjoint pairs of functors and Frobenius extensions, *Sc. Rep. T.K.D. Sect. A* **9** (1965), 40–71.
19. D. Nikshych and L. Vainerman, A characterization of depth 2 subfactors of II_1 factors, *J. Func. Analysis* **171** (2000), 278–307.
20. R. Pierce, "Associative Algebras," Grad. Text in Math., Vol. 88, Springer, Heidelberg, 1982.
21. M. Pimsner and S. Popa, Entropy and index for subfactors, *Ann. Sci. Ecole Norm. Sup. (4)* **19**, No. 3 (1986), 57–106.
22. Y. Sommerhäuser, On Kaplansky's conjectures, *in* "Interactions between Ring Theory and Representations of Algebras" (F. van Oysteyen and M. Saorin, Eds.), Lecture Notes, Vol. 210, Marcel Dekker, New York, 2000.
23. E. Steinitz, Algebraische Theorie den Körpern, *J. Reine Ang. Mat.* **137** (1909), 167–309.
24. W. Szymański, Finite index subfactors and Hopf algebra crossed products, *Proc. Amer. Math. Soc.* **120**, No. 2 (1994), 519–528.
25. K. H. Ulbrich, Galois Erweiterungen von nicht-kommutativen Ringen, *Comm. Algebra* **10** (1982), 655–672.