HOPF ALGEBRA ACTIONS OF CENTRALIZERS ON SEPARABLE EXTENSIONS

LARS KADISON AND DMITRI NIKSHYCH

ABSTRACT. Suppose k is a field and $N \subseteq M$ is a separable Frobenius extension of k-algebras with trivial centralizer $C_M(N)$ and N a direct summand in M as N-bimodules. We assume the existence of a Markov trace. Let $M_1 := \text{End}(M_N)$ and $M_2 := \text{End}(M_1)_M$ be the successive endomorphism rings in a Jones tower $N \subseteq M \subseteq M_1 \subseteq M_2$. We define a depth 2 condition on this tower by simply requiring that a basis of $A := C_{M_1}(N)$ freely generates M_1 as an M-module and a basis of $B := C_{M_2}(M)$ freely generates M_2 as an M_1-module. We then prove that A and B have involutive strongly separable Hopf algebra structures dual to one another. As our main result, we prove that M_1 is a B-module algebra with subalgebra M of invariants and M_2 is the smash product $M_1 \# B$. This paper then extends results of Szymański [S] for finite index, irreducible subfactors of depth 2 by different proofs. We relate our main result and a converse to a non-commutative analogue of the classical theorem: a finite field extension is Galois if and only if it is separable and normal.

1. INTRODUCTION

In this paper we extend the results of Szymański on Hopf $*$-algebra actions and finite index subfactors [S] to the algebraic set-up in [K1] for subalgebra pairs with a Pimsner-Popa orthonormal basis and Markov trace. To this set-up we add conditions of irreducibility and depth 2 on the centralizers and work over a field k of arbitrary characteristic. We replace all arguments based on positivity, star operations or functional analysis with algebraic ones. We prove in Section 4:

Theorem 1.1 (=Theorem 4.4). *The Jones tower $M \subseteq M_1 \subseteq M_2$ over a separable Markov extension $N \subseteq M$ of depth 2 has centralizers $A = C_{M_1}(N)$ and $B = C_{M_2}(M)$ that are involutive semisimple Hopf algebras dual to one another, with an action of B on M_1 such that M_2 is a smash product: $M_2 \cong M_1 \# B$.*

There are a couple of reasons why this result is interesting. First, it extends [S] to other cases of irreducible finite Watatani index pairs of C^*-algebras with a finite trace. In particular, it can be applied to inclusions of simple AF-algebras (inductive limits of finite dimensional C^*-algebras).

Secondly, the theorem above is the difficult part of a non-commutative analogue of the classical theorem in field theory:

Theorem 1.2. *A finite field extension E/F is Galois if and only if it is separable and normal.*

2000 *Mathematics Subject Classification.* 12F10,16W30, 22D30, 46L37.

The authors thank J. Cuntz, E. Effros, S. Montgomery, P. Schauenburg, A. Stolin, W. Szymański, and L. Vainerman for useful discussions and advice.

The second author is grateful to M.I.T. and P. Etingof for the kind hospitality during his visit.

From a modern point of view, the right non-commutative generalization of Galois extension is the Hopf-Galois extension [M]. Recall that if H is a finite dimensional Hopf k-algebra with counit ε and comultiplication $\Delta(h) = h_{(1)} \otimes h_{(2)}$, its dual H^* is a Hopf algebra as well. Then 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 $N = \{b \in M | \, \rho(b) = b \otimes 1\}$ if and only if M/N is a left H-module algebra extension with action of H on M given by $h \triangleright a = a_{(0)} \langle a_{(1)}, h \rangle$ and $N = \{b \in M | \, \forall h \in H, \, h \triangleright b = \varepsilon(h) b\}$.

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 $a \otimes a' \mapsto a a'_{(0)} \otimes a'_{(1)}$ is bijective. Now it has been known for some time that Hopf-Galois extensions are separable Frobenius extensions if H is cosemisimple (cf. [KT, K2]). To this we add a Markov trace and a bimodule projection onto N under certain conditions on M and H, and note in Section 2 that

Theorem 1.3. *Under the conditions on M and H given in Theorem 2.14, a right H^*-Galois extension M/N with trivial centralizer is a separable Markov extension of depth 2.*

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 relations $ah = (h_{(1)} \triangleright a) h_{(2)}$ 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, $\Psi : M \# H \to \mathrm{End}(M_N)$ given by $m \# h \mapsto m(h \triangleright \cdot)$. We will then use the basic result:

Proposition 1.4 ([KT, U])**.** 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.

From this and Theorem 1.1 we conclude that a separable Markov extension M_1/M of depth 2 is A-Galois (Corollary 4.6). This result and Theorem 1.3 then constitute a non-commutative analogue to the classical Theorem 1.2. At the end of Section 4, we make two proposals for further work on extending our results.

2. Separable Markov extensions of depth 2 with trivial centralizer

In 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 M/N as an *algebra extension.* 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. We next define several types of algebra extensions that make up the extensions in the title.

The algebra extension M/N will be called *irreducible* if the centralizer subalgebra of N in M is trivial: i.e., $C_M(N) = k1$. Since the centers $Z(M)$ and $Z(N)$ both lie in $C_M(N)$, these are trivial as well. If $\mathcal{E}$ denotes $\mathrm{End}(M_N)$ and M^{op} denotes the opposite algebra of M, we note that ($\forall m \in M$)

$$(1) \quad C_{\mathcal{E}}(M) = \{f \in \mathcal{E} | \, mf(x) = (fm)(x) = f(mx)\} = \mathrm{End}({}_M M_N) \cong C_M(N)^{op}.$$

Whence the endomorphism algebra extension is irreducible too.

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: ${}_N M_M \cong {}_N\mathrm{Hom}(M_N, N_N)_M$ [K]. 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

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

hold for every $m \in M$ [K].[1] In particular, Frobenius extension may be defined equivalently in terms of the natural *left* module ${}_N M$ instead. The Hattori-Stallings rank of the projective modules M_N or ${}_N M$ are both given by $\sum_i E(y_i x_i)$ in $N/[N, N]$ [K1]. It is not hard to check that the *index* $[M : N]_E := \sum_i x_i y_i \in Z(M)$ (use equations 2) does not depend on E, and $E(1) \in Z(N)$.

If M_N is free, M/N is called a *free Frobenius extension* [K]. 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.

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. This is clearly equivalent to the existence of an element $e \in M \otimes_N M$ such that $me = em$ 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.

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.

A k-algebra M is said to be *strongly separable* 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 (cf. [K1]). 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.

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

[1] 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.

Definition 2.1. A k-algebra extension $N \subseteq M$ is called a *separable Markov extension*[2] if M/N is an irreducible Frobenius extension with Frobenius homomorphism $E : M \to N$, dual bases $\{x_i\}$, $\{y_i\}$ *and trace* $T : N \to k$ such that

1. $E(1) \neq 0$,
2. $\sum_i x_i y_i \neq 0$,
3. $T(1) = 1_k$ and $T_0 := T \circ E : M \to k$ is a trace on M.

Remark 2.2. T is called a *Markov trace* [GHJ]. 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 $\frac{1}{\mu}E, \mu x_i, y_i$ is a new Frobenius homomorphism with dual bases for M/N. With no loss of generality then, we assume that

$$E(1) = 1. \tag{3}$$

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

$$\sum_i x_i y_i = \lambda^{-1} 1_M \tag{4}$$

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 separable Markov extension, satisfying Equations 3 and 2, is uniquely determined.

We note that $[M : N]_E = \lambda^{-1}$ is the trace of the Hattori-Stallings rank,

$$\lambda^{-1} = T_0(\sum_i x_i y_i) = T_0(\sum_i y_i x_i) = T(\sum_i E(y_i x_i)).$$

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

Theorem 2.3 (Cf. [K1, K2]). *$\mathcal{E}/M$ is a separable Markov 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*:

$$(m_1 \otimes m_2)(m_3 \otimes m_4) = m_1 E(m_2 m_3) \otimes m_4. \tag{5}$$

The unity element is $1_1 := \sum_i x_i \otimes y_i$ in the notation above. It is not hard 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 equations 3 and 4. $T_1 := T_0 \circ E_M$ is a trace by [K2, 4.3]. □

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: $M_1 = \{\sum_i x_i e_1 y_i \,|\, x_i, y_i \in M\}$. In this paper, a Frobenius homomorphism E satisfying $E(1) = 1$ is called a *conditional expectation.* We describe M_1, e_1, T_0, E_M as the "basic construction" of $N \subseteq M$.

The Markov property. Observe that the trace T_1 has the following useful *Markov property* : $T_1(me_1) = \lambda T_0(m)$ for all $m \in M$. Indeed, we have $T_1(me_1) = T_0 \circ E_M(me_1) = T_0(mE_M(e_1)) = \lambda T_0(m)$.

[2] or an irreducible stongly separable extension with Markov trace [K1]

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

$$N \subseteq M \subseteq M_1 \subseteq M_2 \subseteq \cdots \tag{6}$$

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

$$M_2 = M_1 \otimes_M M_1 \cong M \otimes_N M \otimes_N M \tag{7}$$

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. We denote the Markov traces on M, M_1 and M_2 by $T_0 = TE$, $T_1 = T_0 E_M$, and $T_2 = T_1 E_{M_1}$, respectively.

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 hypotheses of irreducibility or Markov trace:

Proposition 2.4.

$$\begin{aligned} e_1 e_2 e_1 &= \lambda e_1 1_2 \\ e_2 e_1 e_2 &= \lambda e_2. \end{aligned}$$

Proof. The proof may be found in [K1, Ch. 3]. □

A Tunnel Construction. Under special circumstances M is itself the basic construction of N with respect to a commutator subalgebra R. We prove such a result below. This subsection will only be needed in the discussion at the end of this paper.

Proposition 2.5. If M has an idempotent e_0 such that $E(e_0) = \lambda 1$ and $M = N e_0 N$, then N is a separable Markov extension over $R := C_N(\{e_0\})$, with M and E isomorphic to the basic construction.

Proof. First note that identities such as $e_0 n = n' e_0$ $(n, n' \in N)$ imply $n = n'$ by applying E. Then define $E_R : N \to R$ by

$$e_0 E_R(n) = e_0 n e_0, \tag{8}$$

whence it is easily shown that E_R is a well-defined R-bimodule projection.

Suppose $1_M = \sum_i p_i e_0 q_i$. Then $\lambda \sum_i p_i q_i = 1$. Then

$$e_0 n = \sum_i e_0 n p_i e_0 q_i = e_0 \sum_i E_R(n p_i) q_i,$$

and it is now easy to see that N/R is a separable Frobenius extension with conditional expectation E_R. That $T \circ E_R = T$ follows from applying T_0 to Equation 8, whence T_R is a Markov trace.

The mapping $N \otimes_R N \to M$ given by $n \otimes n' \mapsto n e_0 n'$ is shown to be an isomorphism. Finally, we see that $E : M \to N$ completes a commutative triangle with the map $\lambda\mu : N \otimes_R N \to N$. □

Finite depth and depth 2 conditions. We extend the notion of a *depth* known in subfactor theory [GHJ] to Frobenius extensions.

Lemma 2.6. *For all $n \geq 1$ in the Jones tower (6) 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 (i) implies (ii), the other implication being 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 separable Markov extension M/N has a *finite depth* if the equivalent conditions of Lemma 2.6 are satisfied for some $n \geq 1$. It is not hard to check that in this case they also hold true for $n+1$ (and, hence, for all $k \geq n$). 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:

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

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.

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 2.6.

Proposition 2.7. A and B are strongly 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.

We note that $E_M(a) = T_1(a)1_M$ for every $a \in A$, whence $\{\lambda^{-1} T_1|_A, \lambda z_i, w_i\}$ is a separable base, whence A is strongly separable. Similarly, $\{\lambda^{-1} T_2|_B, \lambda u_i, v_i\}$ is a separable base for B. □

The lemma below is a first step to the main result M_2 is a smash product of B and M_1 (cf. Theorem 4.4).

Lemma 2.8. *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 the classical depth 2 property that C is the basic construction of A or B over the trivial centralizer.

Lemma 2.9. *$C \cong A \otimes_k B$ via multiplication $a \otimes b \mapsto ab$.*

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. □

Lemma 2.10. *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 2.11 (Depth 2 property)**.** We have $C = Ae_2 A$ and $C \cong A \otimes_k A$ as rings. Also, $C = Be_1 B$ and $C \cong B \otimes_k B$ as rings.

Proof. Clearly $Ae_2 A \subseteq C$. 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 $c = \lambda^{-1} \sum_i E_{M_1}(cz_i e_2)e_2 w_i \in Ae_2 A$ 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 $Ae_2 A$. Then $C = Ae_2 A = A \otimes_M A \cong A \otimes_k A$ since $A \cap M = C_M(N) = k1_M$.

For the second statement, we observe:

$$C = Ae_2 A = Ae_2 e_1 e_2 A \subseteq Ce_1 C = Be_1 B,$$

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 $\eta, \eta' : A \to k$ 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:

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

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

Corollary 2.12. 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 $k \not| n$ since the index $\lambda^{-1} = n1_k \neq 0$. □

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 $\dim_k A = \dim_k B$. We now compute the (unique) trace-preserving conditional expectation of C onto B, a lemma we will need in Section 3.

Lemma 2.13. *The map $E_B : C \to B$ defined by $E_B(c) = \sum_j E_M(E_{M_1}(cu_j))v_j$ for all $c \in C$ is a conditional expectation and satisfies $T \circ E_B = T|_C$.*

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 the Markov trace $T_2 = T_0 \circ E_M \circ E_{M_1}$ and $E_M(E_{M_1}(cu_j)) \in k1$ for all $c \in C$, we have:

$$\begin{aligned} E_B(be_1b') &= \sum_j T_2(be_1b'u_j)v_j = \sum_j T_1(e_1E_{M_1}(b'u_jb))v_j \\ &= \lambda \sum_j E_{M_1}(bb'u_j)v_j = \lambda bb' \end{aligned}$$

It follows from Proposition 2.11 that E_B is a B-B-bimodule homomorphism. Since $c = \sum_j E_{M_1}(cu_j)v_j$ and $E_B(c) = \sum_j T_2(cu_j)v_j$, it follows that $T_2(E_B(c)) = T_2(c)$ for all $c \in C$.

That E_B is a Frobenius homomorphism follows from [GHJ, Lemma 2.6.1], if we show it is faithful: i.e., $E_B(Cc) = 0$ implies $c = 0$. But this follows from $T_2|_C$ being faithful, since $C \cong M_n(k)$ and char $k \not| n$. □

The Pimsner-Popa identities. We note that:

$$\begin{aligned} \lambda^{-1}e_1E_M(e_1x) &= e_1x \quad \forall x \in M_1 \\ \lambda^{-1}e_2E_{M_1}(e_2y) &= e_2y \quad \forall y \in M_2. \end{aligned}$$

Proof. Let $x = \sum_i m_i \otimes m_i'$ where $m_i, m_i' \in M_1$. Then $e_2x = e_2\sum_i E_M(m_i)m_i'$, and $E_{M_1}(e_2x) = \lambda\sum_i E_M(m_i)m_i'$ from which one of the equations follows. The other equation is similarly shown, as are the opposite Pimsner-Popa identities.

When Galois extensions are separable Markov. The following theorem is a converse to our main theorem in 4.6. Let H be a finite dimensional, involutive, semisimple and cosemisimple Hopf algebra.

Theorem 2.14 (Cf. [K2], 3.2). *Suppose M is a k-algebra with normalized trace T 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 separable Markov extension of depth 2 with End(M_N) $\cong M\#H$.*

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

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

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 $\sum_i x_i E y_i = \mathrm{id}_M$ and that E is a Frobenius homomorphism with dual bases $\{x_i\}$, $\{y_i\}$ [KT].

The homomorphism $\psi : M\#H \to \mathrm{End}(M_N)$, $m\#h \longmapsto (m' \mapsto m(h \cdot m'))$ is an isomorphism by [KT, 1.7] with inverse given by $g \mapsto \sum_i g(x_i)ty_i$.

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 $\lambda^{-1} = f(1_H)$.

We check that $T|_N \circ E$ is a trace:

$$T(t \cdot (mm')) = T((t_{(1)} \cdot m)(t_{(2)} \cdot m')) = T((t_{(1)} \cdot m')(t_{(2)} \cdot m)) = T(t \cdot (m'm)),$$

by the formula $t_{(2)} \otimes t_{(1)} = t_{(1)} \otimes (S^2 t_{(2)})b$ [R, p. 595], where $S^2 = \mathrm{id}$ by assumption and $b = 1$ is the distinguished group-like in H, trivial by counimodularity.

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: we note that $M\#H$ is a right H-Galois extension of M, where the coaction $M\#H \to (M\#H) \otimes H$ is given by $m\#h \mapsto m\#h_{(1)} \otimes h_{(2)}$. 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 $M_2 \cong M\#H\#H^*$. □

3. Hopf algebra structures on centralizers

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 separable (irreducible) Markov extension $N \subset M$ of depth 2, T denote the Markov trace on M_2 *and* its subalgebras, $e_1 \in M_1$, $e_2 \in M_2$ be the first two Jones idempotents of the tower, and $\lambda^{-1} = [M : N]$ be the index.

Proposition 3.1 (Cf. [S], Proposition 10)**.** The bilinear form,

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

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

Proof. If $\langle a, B \rangle = 0$ for some $a \in A$, then for all $x \in C_{M_2}(N)$ we have $T(ae_2e_1x) = 0$, since $e_1B = e_1C_{M_2}(N)$ (depth 2 property). Taking $x = e_2a'$ $(a' \in A)$ and using Lemma 2.10, the braid-like relation between Jones idempotents, and Markov property of T we have

$$T(aa') = \lambda^{-1}T(ae_2e_1(e_2a')) = 0 \qquad \text{for all } a' \in A,$$

therefore $a = 0$. Similarly, one proves that $\langle A, b \rangle = 0$ implies $b = 0$. □

Observe that since k is a field the Proposition above shows that the map $b \mapsto E_{M_1}(e_2e_1b)$ is a linear isomorphism between B and A. Indeed, $E_{M_1}(e_2e_1b) = 0$ implies that for all $a \in A$ one has

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

whence $b = 0$ by nondegeneracy.

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

Definition 3.2. The coalgebra structure on B has comultiplication $B \to B \otimes B$, $b \mapsto b_{(1)} \otimes b_{(2)}$ given by

$$\langle a_1, b_{(1)} \rangle \langle a_2, b_{(2)} \rangle = \langle a_1a_2, b \rangle \tag{11}$$

for all $a_1, a_2 \in A$, $b \in B$, and counit $\varepsilon : B \to k$ given by $(\forall b \in B)$

$$\varepsilon(b) = \langle 1, b \rangle. \tag{12}$$

Proposition 3.3. We note that: (for all $b, c \in B$)

$$\varepsilon(b) = \lambda^{-1}T(e_2b), \tag{13}$$

$$\Delta(1) = 1 \otimes 1, \tag{14}$$

$$\varepsilon(bc) = \varepsilon(b)\varepsilon(c). \tag{15}$$

Proof. Using the Pimsner-Popa identities and the Markov property we compute:

$$\varepsilon(b) = \lambda^{-2}T(e_2e_1b) = \lambda^{-3}T(E_{M_1}(be_2)e_2e_1) = \lambda^{-1}T(e_2b),$$

$$\begin{aligned}
\langle a_1, 1 \rangle \langle a_2, 1 \rangle &= \lambda^{-4}T(a_1e_2e_1)T(a_2e_2e_1) \\
&= \lambda^{-2}T(a_1e_1)T(a_2e_1) = \lambda^{-2}T(a_1E_M(a_2e_1)e_1) \\
&= \lambda^{-1}T(a_1a_2e_1) = \langle a_1a_2, 1 \rangle, \\
\varepsilon(b)\varepsilon(c) &= \lambda^{-2}T(e_2b)T(e_2c) = \lambda^{-2}T(e_2E_{M_1}(e_2b)c) \\
&= \lambda^{-1}T(e_2bc) = \varepsilon(bc),
\end{aligned}$$

for all $a_1, a_2 \in A$, $b, c \in B$, since $C_M(N) = C_{M_1}(M) = k1$, so that the restriction of E_M (resp. E_{M_1}) on A (resp. B) coincides with T. □

The antipode of B. Recall that the map $b \mapsto E_{M_1}(e_2e_1b)$ 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 $b \mapsto E_{M_1}(be_1e_2)$ is a linear isomorphism as well. This lets us define a linear map $S : B \to B$, called the *antipode*, as follows.

Definition 3.4. For every $b \in B$ define $S(b) \in B$ to be the unique element such that

$$T(be_1e_2a) = T(ae_2e_1S(b)), \qquad \text{for all } a \in A,$$

or, equivalently,

$$E_{M_1}(be_1e_2) = E_{M_1}(e_2e_1S(b)).$$

Remark 3.5. Note that S is bijective and that the above condition implies

$$E_{M_1}(bxe_2) = E_{M_1}(e_2 x S(b)), \qquad \text{for all } x \in M_1. \tag{16}$$

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

$$E_{M_1}(bxe_2) = \Sigma_i\, x_i E_{M_1}(be_1e_2)y_i = \Sigma_i\, x_i E_{M_1}(e_2e_1S(b))y_i = E_{M_1}(e_2xS(b)).$$

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 3.6. 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 unique T-preserving conditional expectation from C to B given by $E_B(c) = \Sigma_i\, T(cu_i)v_i$ as in Proposition 2.13.

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 if $c \in B$ this follows from non-degeneracy of the duality form; if $c = a \in A$ this follows from $E_B(a) = T(a)1$ and noting that T is a faithful trace on A (cf. Proposition 2.7). We put the two facts together with $C = BA$ to prove the claim.

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

$$\begin{aligned}
\langle\, a,\, E_B(e_1ba')\,\rangle &= \lambda^{-2} T(ae_2e_1E_B(e_1ba')) \\
&= \lambda^{-1} T(a'ae_2e_1b) = \lambda \langle\, a'a,\, b\,\rangle, \\
\langle\, a,\, \lambda^{-1} b_{(2)} E_B(E_{M_1}(e_2e_1b_{(1)})a')\,\rangle &= \lambda^{-1} \langle\, a,\, b_{(2)}\,\rangle T(e_2e_1b_{(1)}a') \\
&= \lambda \langle\, a,\, b_{(2)}\,\rangle \langle\, a',\, b_{(1)}\,\rangle = \lambda \langle\, a'a,\, b\,\rangle.
\end{aligned}$$

Next, arguing as in Remark 3.5 we write $y = \Sigma_i\, m_i e_1 n_i$ with $m_i, n_i \in M$, whence

$$yb = \Sigma_i\, m_i e_1 b n_i = \lambda^{-1} \Sigma_i\, m_i b_{(2)} E_{M_1}(e_2e_1b_{(1)}) n_i = b_{(2)} E_{M_1}(e_2 y b_{(1)}). \quad \square$$

Corollary 3.7. For all $b \in B$ and $x, y \in M_1$ we have:

$$E_{M_1}(e_2xyb) = \lambda^{-1} E_{M_1}(e_2xb_{(2)}) E_{M_1}(e_2yb_{(1)}).$$

Proof. The result follows from multiplying the identity from Proposition 3.6 by e_2x on the left and taking E_{M_1} from both sides. $\square$

Although the antipode axiom (cf. Prop. 3.11) implies that S is a coalgebra antihomomorphism, we will have to establish these two properties of S in the reverse order, as stepping stones to Propositions 3.10 and 3.11.

Lemma 3.8. *S is a coalgebra anti-automorphism.*

Proof. For all $a, a' \in A$ and $b \in B$ we have by Corollary 3.7

$$\begin{aligned}
\langle\, aa',\, S(b)\,\rangle &= \lambda^{-2} T(be_1e_2aa') = \lambda^{-3} T(e_1e_2E_{M_1}(e_2aa'b)) \\
&= \lambda^{-4} T(e_1e_2E_{M_1}(e_2ab_{(2)})E_{M_1}(e_2a'b_{(1)})) \\
&= \lambda^{-6} T(e_1e_2E_{M_1}(e_2ab_{(2)}))T(e_1e_2E_{M_1}(e_2a'b_{(1)})) \\
&= \langle\, a, S(b_{(2)})\,\rangle \langle\, a', S(b_{(1)})\,\rangle,
\end{aligned}$$

where we use the fact that $a \mapsto \lambda^{-2}T(e_1e_2a) = \lambda^{-1}T(e_1a)$ is the counit homomorphism from A to k, as in Proposition 3.3. Thus, $\Delta(S(b)) = S(b_{(2)}) \otimes S(b_{(1)})$. □

Corollary 3.9. 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 Proposition 3.6 and using Equation 16 as well as Lemma 3.8. □

Proposition 3.10. Δ is an algebra homomorphism.

Proof. By Corollary 3.9 we have, for all $a_1, a_2 \in A$ and $b, c \in B$:

$$\begin{aligned}
\langle\, a_1a_2,\, bc\,\rangle &= \langle\, \lambda^{-1}E_{M_1}(ca_1a_2e_2),\, b\,\rangle \\
&= \langle\, \lambda^{-2}E_{M_1}(c_{(1)}a_1e_2)E_{M_1}(c_{(2)}a_2e_2),\, b\,\rangle \\
&= \langle\, \lambda^{-1}E_{M_1}(c_{(1)}a_1e_2), b_{(1)}\,\rangle\langle\, \lambda^{-1}E_{M_1}(c_{(2)}a_2e_2),\, b_{(2)}\,\rangle \\
&= \langle\, a_1,\, b_{(1)}c_{(1)}\,\rangle\langle\, a_2,\, b_{(2)}c_{(2)}\,\rangle,
\end{aligned}$$

whence $\Delta(bc) = \Delta(b)\Delta(c)$. □

Proposition 3.11. For all $b \in B$ we have $S(b_{(1)})b_{(2)} = \varepsilon(b)1 = b_{(1)}S(b_{(2)})$.

Proof. Using Corollary 3.9 and the definition of the antipode we have

$$\begin{aligned}
\langle\, a,\, S(b_{(1)})b_{(2)}\,\rangle &= \lambda^{-1}\langle\, E_{M_1}(b_{(2)}ae_2),\, S(b_{(1)})\,\rangle \\
&= \lambda^{-4}T(E_{M_1}(b_{(2)}ae_2)e_2E_{M_1}(e_2e_1S(b_{(1)}))) \\
&= \lambda^{-3}T(E_{M_1}(b_{(1)}e_1e_2)E_{M_1}(b_{(2)}ae_2)) \\
&= \lambda^{-2}T(be_1ae_2) = \lambda^{-2}T(e_1a)T(be_2) = \langle\, a,\, 1\varepsilon(b)\,\rangle,
\end{aligned}$$

$\forall a \in A$, $b \in B$. The second identity follows similarly from Corollary 3.7. □

Theorem 3.12. *$(B, \Delta, \varepsilon, S)$ is an involutive strongly separable Hopf algebra.*

Proof. Follows from Propositions 3.3, 3.10, 3.11, and 2.7. That $S^2 = \mathrm{id}$ follows from the computation:

$$\begin{aligned}
T(ae_2e_1b) &= \lambda^{-1}T(E_{M_1}(bae_2)e_2e_1) \\
&= \lambda^{-1}T(E_{M_1}(e_2aS(b))e_2e_1) \\
&= \lambda^{-1}T(e_2E_{M_1}(e_2aS(b))e_1) \\
&= T(S(b)e_1e_2a) = T(ae_2e_1S^2(b)),
\end{aligned}$$

using Remark 3.5 and the Markov property of T. □

Remark 3.13. The non-degenerate duality form of Proposition 3.1 makes A the Hopf algebra dual to B.

Note that e_2 is an integral in B, since $\langle\, a, e_2b\,\rangle = \langle\, a, e_2\,\rangle\varepsilon(b) = \langle\, a, be_2\,\rangle$ by the Pimsner-Popa identity. Similarly, e_1 is an integral in A.

4. Action and smash product

In this section we define a canonical action of B on M_1 making it a B-module algebra. We then describe M as its subalgebra of invariants and M_2 as the smash product (or crossed product) algebra of B and M_1.

Proposition 4.1 (Cf. [S], Proposition 17)**.** The map $\triangleright : B \otimes M_1 \to M_1$:

$$b \triangleright x = \lambda^{-1} E_{M_1}(bxe_2) \tag{17}$$

defines a left B-module algebra structure on M_1.

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 3.9 implies that $b \triangleright xy = (b_{(1)} \triangleright x)(b_{(2)} \triangleright y)$. Finally, $b \triangleright 1 = \lambda^{-1} E_{M_1}(be_2) = \lambda^{-1} T(be_2)1 = \varepsilon(b)1$. □

Note that $B \triangleright A = A$. We next show 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.

Proposition 4.2. The natural inclusion $\iota : A \hookrightarrow M_1$ is a total integral.

Proof. Since $\iota(1) = 1$, we need only show that ι is a right A-comodule morphism [D]. Denoting the coaction $M_1 \to M_1 \otimes A$ (which is the dual of Action 17) 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 the depth 2 condition, it suffices to check that $a_{(0)} \otimes a_{(1)} = a_{(1)} \otimes a_{(2)}$:

$$\begin{aligned} \langle a_{(1)}, b \rangle \langle a_{(2)}, b' \rangle &= \langle a, bb' \rangle = \lambda^{-2} T(ae_2e_1bb') \\ &= \lambda^{-3} T(E_{M_1}(b'ae_2)e_2e_1b) = \langle \lambda^{-1} E_{M_1}(b'ae_2), b \rangle \\ &= \langle a_{(0)}, b \rangle \langle a_{(1)}, b' \rangle. \quad \square \end{aligned}$$

Proposition 4.3. $M_1^B = M$, 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 $E_M(x) = \lambda^{-1} E_{M_1}(e_2xe_2) = \varepsilon(e_2)x = x$, therefore $x \in M$.

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

$$b \triangleright x = \lambda^{-1} E_{M_1}(be_2x) = \lambda^{-1} E_{M_1}(be_2)x = \varepsilon(b)x,$$

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.

Theorem 4.4 (Cf. [S], Theorem 20)**.** *The map $\theta : x\#b \mapsto xb$ defines an algebra isomorphism between the smash product algebra $M_1\#B$ and M_2.*

Proof. The bijectivity of θ follows from Lemma 2.8.

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 Propositions 3.6, 3.11 and the Pimsner-Popa identity we have:

$$\begin{aligned} (b_{(1)} \triangleright y)b_{(2)} &= \lambda^{-1} E_{M_1}(b_{(1)}ye_2)b_{(2)} \\ &= \lambda^{-2} b_{(3)} E_{M_1}(e_2 E_{M_1}(b_{(1)}ye_2)b_{(2)}) \\ &= \lambda^{-1} b_{(3)} E_{M_1}(e_2 y S(b_{(1)})b_{(2)}) = by. \quad \square \end{aligned}$$

From this and Lemma 2.9, we conclude that:

Corollary 4.5. $C \cong A\#B$.

Corollary 4.6. M_1/M is an A-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 the theorem 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 1.4 then, M_1 is a right A-Galois extension of M. □

M_1/M is of course a *faithfully flat Galois extension* because the extension is free: cf. [M] for many nice properties such as "affine quotients."

We propose the following two problems related to this paper:

1. Are conditions 1 and 2 in the depth 2 conditions independent?
2. If M_1/M is A-Galois in a Jones tower, is M/N B-Galois? Equivalently, if M_2 is a smash product of M_1 and B, is M_1 a smash product of M and A?

There is an affirmative answer to the second question in case the extension M/N has a tunnel construction N/R as in Proposition 2.5 satisfying a depth 2 condition. In this case, A is replaced by $C_M(R)$, B by A, M_2 by M_1 in the proofs above and Theorem 4.4 shows that M_1 is the smash product of M and A.

References

[D] Y. Doi, *Algebras with total integrals*, Comm. Algebra **13** (1985), 2137–2159.

[GHJ] F. Goodman, P. de la Harpe, and V.F.R. Jones, *Coxeter Graphs and Towers of Algebras*, M.S.R.I. Publ. **14**, Springer, Heidelberg, 1989.

[K1] L. Kadison *New examples of Frobenius extensions*, University Lecture Series, vol. 14, American Mathematical Society, Providence, RI, 1999.

[K2] L. Kadison *The Jones polynomial and certain separable Frobenius extensions*, J. Algebra **186** (1996), no. 2, 461–475.

[K] F. Kasch *Projektive Frobenius Erweiterungen*, Sitzungsber. Heidelberg. Akad. Wiss. Math.-Natur. Kl. (1960/1961), 89–109.

[KT] H. Kreimer and M. Takeuchi, *Hopf algebras and Galois extensions of an algebra*, Indiana Univ. Math. J. **30** (1981), 675–692.

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

[PP] M. Pimsner and S. Popa, *Entropy and index for subfactors*, Ann. Sci. Ecole Norm. Sup. (4) **19** (1986), no. 3, 57–106.

[R] D. Radford, *The trace function and Hopf algebras*, J. Algebra **163** (1994), 583–622.

[S] W. Szymański, *Finite index subfactors and Hopf algebra crossed products*, Proc. Amer. Math. Soc. **120** (1994), no. 2, 519–528.

[U] K.H. Ulbrich, *Galois erweiterungen von nicht-kommutativen ringen*, Comm. Algebra **10** (1982), 655-672.

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

U.C.L.A., Department of Mathematics, Los Angeles, CA 90095-1555, USA
Current address: M.I.T., Department of Mathematics, Cambridge, MA 02138-4307, USA
E-mail address: nikshych@math.ucla.edu