Available online at www.sciencedirect.com
ScienceDirect
JOURNAL OF PURE AND APPLIED ALGEBRA
Journal of Pure and Applied Algebra 212 (2008) 1822–1839
www.elsevier.com/locate/jpaa

Finite depth and Jacobson–Bourbaki correspondence

Lars Kadison[1]

Department of Mathematics, University of Pennsylvania, David Rittenhouse Lab, 209 S. 33rd St., Philadelphia, PA 19104, United States

Received 25 July 2007; received in revised form 8 November 2007
Available online 21 February 2008

Communicated by C. Kassel

Abstract

We introduce a notion of depth three tower $C \subseteq B \subseteq A$ with depth two ring extension $A|B$ being the case $B = C$. If $A = \operatorname{End} B_C$ and $B|C$ is a Frobenius extension with $A|B|C$ depth three, then $A|C$ is depth two. If A, B and C correspond to a tower $G > H > K$ via group algebras over a base ring F, the depth three condition is the condition that K has normal closure K^G contained in H. For a depth three tower of rings, a pre-Galois theory for the ring $\operatorname{End}\ {}_B A_C$ and coring $(A \otimes_B A)^C$ involving Morita context bimodules and left coideal subrings is applied to specialize a Jacobson–Bourbaki correspondence theorem for augmented rings to depth two extensions with depth three intermediate division rings.

MSC: Primary: 13B05; 16W30; secondary: 46L37; 81R15

1. Introduction

Depth two theory is a type of Galois theory for non-commutative ring extensions, where the Galois group in field theory is replaced by a Hopf algebroid (with or perhaps without antipode). The Galois theory of depth two ring extensions has been studied in a series of papers by the author [14–17] in collaboration with Nikshych [12,11], Szlachányi [13], and Külshammer [10], with a textbook treatment by Brzeziński and Wisbauer [2]. There are a number of issues that remain unexplored or unanswered in full including chirality [14,15], normality [10,16], a Galois inverse problem and a Galois correspondence problem [25].

The Galois correspondence problem places before the Galois theorist a tower of three rings $C \subseteq B \subseteq A$. With no further assumption on the rings, we should impose at least a relative condition on the tower to arrive at results. With this in mind we propose to generalize the notion of depth two (D2) ring extension $A|B$ to a notion of depth three (D3) tower $A|B|C$. In more detail, the tower $A|B|C$ is right depth three (rD3) if $A \otimes_B A$ is A-C-isomorphic to a direct summand of $A \oplus \cdots \oplus A$ (finitely many times). Many depth two theoretic results generalize suitably, such as a decomposition of an endomorphism ring into a crossed product with a quantum algebraic structure. If $A \supseteq C$ is D2 and B a D3 intermediate ring, we may make use of Jacobson–Bourbaki theorems pairing certain ring extensions,

E-mail address: lkadison@math.upenn.edu.

[1] To David Harbater and the Penn Galois seminar thanks for inviting me to give a talk and posing several interesting questions.

0022-4049/$ - see front matter
doi:10.1016/j.jpaa.2007.11.007

such as division rings or simple algebras, with their endomorphism rings, in order to obtain theorems pairing D3 intermediate rings B with left coideal subrings End ${}_C A_B$ of the bialgebroid End ${}_C A_C$ over the centralizer A^C.

The notion of D3 tower will also serve to give a transparent and workable algebraic definition of finite depth, originally an analytic notion in subfactor theory. A finite Jones index subfactor may be thought of algebraically as a Frobenius extension, where the conditional expectation and Pimsner–Popa orthonormal bases are the Frobenius coordinate system. If $B|C$ is then a Frobenius extension with $A = \text{End}\, B_C$ and $B \hookrightarrow A$ the left regular representation, then a depth three tower $A|B|C$ is a D3 Frobenius extension (cf. [12] and [13, preprint version]). More generally, $B|C$ is depth $n \geq 2$ if $A_{n-2}|A_{n-3}|C$ is a depth three tower, where

$$C \hookrightarrow B \hookrightarrow A \hookrightarrow A_2 \hookrightarrow \cdots \hookrightarrow A_n \hookrightarrow \cdots \tag{1}$$

is the Jones tower of iterated right endomorphism rings (and where $A_2 = \text{End}\, A_B, \ldots, A = A_1$, $B = A_0$ and $C = A_{-1}$). We have the following algebraic generalization of the embedding theorem for subfactors of Nikshych and Vainerman [20]: if $C \hookrightarrow B$ is depth n, then $C \hookrightarrow A_m$ is a depth two Frobenius extension for some $m \geq n - 2$.

The paper is organized as follows. In Section 2 we note that right or left D3 ring towers are characterized in terms of the tensor-square, H-equivalent modules, quasibases or the endomorphism ring. We prove a Theorem 2.5 that a D3 Frobenius extension $B|C$ embeds in a depth two extension $A|C$ (where $A = \text{End}\, B_C$). In a more technical Section 8 we extend this technique to define a finite depth Frobenius extension and prove an embedding theorem for these as well: this answers a problem raised by Nikshych and the author in [11, Remark 5.2]. In Section 3 we show that a tower of subgroups $G > H > K$ of finite index with the condition that the normal closure $K^G < H$ ensures that the group algebras $F[G] \supseteq F[H] \supseteq F[K]$ are a depth three tower w.r.t. any base ring F. We propose that the converse is true if G is a finite group and $F = \mathbb{C}$. In Section 4 we study the right coideal subring $E = \text{End}\, {}_B A_C$ as well as the bimodule and coring $P = (A \otimes_B A)^C$, which provide the quasibases for a right D3 tower $A|B|C$. We show that right depth three towers may be characterized by P being finite projective as a left module over the centralizer $V = A^C$ and a pre-Galois isomorphism $A \otimes_B A \xrightarrow{\cong} A \otimes_V P$.

In Section 5 we study further the Galois properties of D3 towers, such as the smash product decomposition of an endomorphism ring and the invariants as a bicommutator. In Section 6, we generalize the Jacobson–Bourbaki correspondence, which associates End E_F to subfields F of E (or skew fields), and conversely associates End ${}_{\mathcal{R}}E$ to closed subrings $\mathcal{R} \subseteq \text{End}\, E_F$. We then compose this correspondence with an anti-Galois correspondence to prove the main Theorem 6.3: viz., there is a Galois correspondence between D3 intermediate division rings of a D2 extension of an augmented ring A over a division ring C, on the one hand, with Galois left coideal subrings of the bialgebroid End ${}_C A_C$, on the other hand. In Section 7, we apply Jacobson–Bourbaki correspondence to show that the Galois connection for separable field extensions in [25] is a Galois correspondence between weak Hopf subalgebras and intermediate fields.

2. Definition and first properties of depth three towers

Let A, B and C denote rings with identity element, and $C \to B$, $B \to A$ denote ring homomorphisms preserving the identities. We use ring extension notation $A|B|C$ for $C \to B \to A$ and call this a tower of rings: an important special case if of course $C \subseteq B \subseteq A$ of subrings B in A and C in B. Of most importance to us are the induced bimodules such as ${}_B A_C$ and ${}_C A_B$. We may naturally also choose to work with algebras over commutative rings, and obtain almost identical results.

We denote the centralizer subgroup of a ring A in an A-A-bimodule M by $M^A = \{m \in M \mid \forall a \in A, ma = am\}$. We also use the notation $V_A(C) = A^C$ for the centralizer subring of C in A. This should not be confused with our notation K^G for the normal closure of a subgroup $K < G$. Notation like End B_C will denote the ring of endomorphisms of the module B_C under composition and addition. We let N_R^n denote the n-fold direct sum of a right R-module N with itself; let $M_R \oplus * \cong N_R^n$ denote the module M is isomorphic to a direct summand of N_R^n. Finally, the symbol $\cong$ denotes isomorphism and occasionally will denote anti-isomorphism when we can safely ignore opposite rings (such as "two anti-isomorphisms compose to give an isomorphism," or "two opposite rings are Morita equivalent iff the rings are Morita equivalent").

Definition 2.1. A tower of rings $A|B|C$ is right depth three (rD3) if the tensor-square $A \otimes_B A$ is isomorphic as A-C-bimodules to a direct summand of a finite direct sum of A with itself: in module-theoretic symbols, this becomes, for some positive integer N,

$$ {}_A A \otimes_B A_C \oplus * \cong {}_A A^N_C \, . \tag{2}$$

By switching to C-A-bimodules instead, we similarly define a *left D3 tower* of rings. The theory for these is dual to that for rD3 towers; we briefly consider it at the end of this section. Define a D3 ring tower as a left and right D3 ring tower. As an alternative to referring to a rD3 tower $A|B|C$, we may refer to B as an rD3 *intermediate ring* of $A|C$, if $C \to A$ factors through $B \to A$ and $A|B|C$ is rD3.

Recall that over a ring R, two modules M_R and N_R are H-equivalent if $M_R \oplus * \cong N_R^n$ and $N_R \oplus * \cong M_R^m$ for some positive integers n and m. In this case, the endomorphism rings End M_R and End N_R are Morita equivalent with context bimodules $\mathrm{Hom}(M_R, N_R)$ and $\mathrm{Hom}(N_R, M_R)$.

Lemma 2.2. *A tower $A|B|C$ of rings is $r D3$ iff the natural A-C-bimodules $A \otimes_B A$ and A are H-equivalent.*

Proof. We note that for any tower of rings, $A \oplus * \cong A \otimes_B A$ as A-C-bimodules, since the epi $\mu : A \otimes_B A \to A$ splits as an A-C-bimodule arrow. $\square$

Since for any tower of rings End ${}_A A_C$ is isomorphic to the centralizer $V_A(C) = A^C$ (or anti-isomorphic according to convention), we see from the lemma that the notion of rD3 has something to do with classical depth three. Indeed,

Example 2.3. If $B|C$ is a Frobenius extension, with Frobenius system (E, x_i, y_i) satisfying for each $a \in A$,

$$\sum_i E(ax_i)y_i = a = \sum_i x_i E(y_i a) \tag{3}$$

then $B \otimes_C B \cong \mathrm{End}\, B_C := A$ via $x \otimes_B y \mapsto \lambda_x \circ E \circ \lambda_y$ for left multiplication λ_x by element $x \in B$. Let $B \to A$ be the mapping $B \hookrightarrow \mathrm{End}\, B_C$ given by $b \mapsto \lambda_b$. It is then easy to show that ${}_A B \otimes_C B \otimes_C B_C \cong {}_A A \otimes_B A_C$, so that for Frobenius extensions, condition (2) is equivalent to the condition for rD3 in preprint [13], which in turn slightly generalizes the condition in [12] for D3 free Frobenius extension.

Another litmus test for a correct notion of depth three is that depth two extensions should be depth three in a certain sense. Recall that a ring extension $A|B$ is right depth two (rD2) if the tensor-square $A \otimes_B A$ is A-B-bimodule isomorphic to a direct summand of N copies of A in a direct sum with itself:

$$ {}_A A \otimes_B A_B \oplus * \cong {}_A A^N_B \, . \tag{4}$$

Since the notions pass from ring extension to tower of rings, there are several cases to look at.

Proposition 2.4. *Suppose that $A|B|C$ is a tower of rings. We note:*

(1) *If $B = C$ and $B \to C$ is the identity mapping, then $A|B|C$ is $r D3 \Leftrightarrow A|B$ is $r D2$.*
(2) *If $A|B$ is $r D2$, then $A|B|C$ is $r D3$ w.r.t. any ring extension $B|C$.*
(3) *If $A|C$ is $r D2$ and $B|C$ is a separable extension, then $A|B|C$ is $r D3$.*
(4) *If $B|C$ is left D2, and $A = \mathrm{End}\, B_C$, then $A|B|C$ is left D3.*
(5) *If C is the trivial subring, any ring extension $A|B$, where ${}_B A$ is finite projective, together with C is $r D3$.*

Proof. The proof follows from comparing Eqs. (2) and (4), noting that $A \otimes_B A \oplus * \cong A \otimes_C A$ as natural A-A-bimodules if $B|C$ is a separable extension (thus having a separability element $e = e^1 \otimes_C e^2 \in (B \otimes_C B)^B$ satisfying $e^1 e^2 = 1$), and finally from [14] that $B|C$ left D2 extension $\Rightarrow A|B$ is left D2 extension if $A = \mathrm{End}\, B_C$. The last statement follows from tensoring ${}_B A \oplus * \cong {}_B B^n$ by ${}_A A \otimes_B -$. $\square$

The next theorem is a converse and algebraic simplification of a key fact in subfactor Galois theory (the $n = 3$ case): a D3 subfactor $N \subseteq M$ yields a depth two subfactor $N \subseteq M_1$, w.r.t. its basic construction $M_1 \cong M \otimes_N M$. We may call a ring extension $B|C$ rD3 if the endomorphism ring tower $A|B|C$ is right depth three, where $A = \mathrm{End}\, B_C$ and $A|B$ has underlying map $\lambda : B \to \mathrm{End}\, B_C$, the left regular mapping given by $\lambda(x)(b) = xb$ for all $x, b \in B$. (This definition will extend to identify depth $n > 3$ Frobenius extensions as well in Section 8.) We next prove a theorem which says that an rD3 extension embeds in a depth two extension via its endomorphism ring.

Theorem 2.5. *Suppose that $B|C$ is a Frobenius extension and $A = \mathrm{End}\, B_C$. If the tower $A|B|C$ is $r D3$, then the composite extension $A|C$ is $D2$.*

Proof. Begin with the well-known bimodule isomorphism for a Frobenius extension $B|C$, between its endomorphism ring and its tensor-square, ${}_B A_B \cong {}_B B \otimes_C B_B$. Tensoring by ${}_A A \otimes_B - \otimes_B A_A$, we obtain $A \otimes_C A \cong A \otimes_B A \otimes_B A$ as natural A-A-bimodules. Now restrict the bimodule isomorphism in Eq. (2) on the left to B-modules and tensor by ${}_A A \otimes_B -$ to obtain ${}_A A \otimes_C A_C \oplus * \cong {}_A A \otimes_B A_C^N$ after substitution of the tensor-cube over B by the tensor-square over C. By another application of Eq. (2) we arrive at

$$ {}_A A \otimes_C A_C \oplus * \cong {}_A A_C^{N^2}. $$

Thus $A|C$ is right D2. Since it is a Frobenius extension as well, it is also left depth two. $\square$

We introduce quasibases for right depth three towers.

Theorem 2.6. *A tower $A|B|C$ is right depth three iff there are N elements each of $\gamma_i \in \mathrm{End}\, {}_B A_C$ and of $u_i \in (A \otimes_B A)^C$ satisfying (for each $x, y \in A$)*

$$ x \otimes_B y = \sum_{i=1}^{N} x\gamma_i(y)u_i. \tag{5} $$

Proof. From the condition (2), there are obviously N maps each of

$$ f_i \in \mathrm{Hom}({}_A A_C, {}_A A \otimes_B A_C), \qquad g_i \in \mathrm{Hom}({}_A A \otimes_B A_C, {}_A A_C) \tag{6} $$

such that $\sum_{i=1}^N f_i \circ g_i = \mathrm{id}_{A \otimes_B A}$. First, we note that for any tower of rings, not necessarily rD3,

$$ \mathrm{Hom}({}_A A_C, {}_A A \otimes_B A_C) \cong (A \otimes_B A)^C \tag{7} $$

via $f \mapsto f(1_A)$. The inverse is given by $p \mapsto ap$ where $p = p^1 \otimes_B p^2 \in (A \otimes_B A)^C$ using a Sweedler-type notation that suppresses a possible summation over simple tensors.

The other hom-group above also has a simplification. We note that for any tower,

$$ \mathrm{Hom}({}_A A \otimes_B A_C, {}_A A_C) \cong \mathrm{End}\, {}_B A_C \tag{8} $$

via $F \mapsto F(1_A \otimes_B -)$. Given $\alpha \in \mathrm{End}\, {}_B A_C$, we define an inverse sending α to the homomorphism $x \otimes_B y \mapsto x\alpha(y)$.

Let f_i correspond to $u_i \in (A \otimes_B A)^C$ and g_i correspond to $\gamma_i \in \mathrm{End}\, {}_B A_C$ via the mappings just described. We compute:

$$ x \otimes_B y = \sum_i f_i(g_i(x \otimes y)) = \sum_i f_i(x\gamma_i(y)) = \sum_i x\gamma_i(y)u_i, $$

which establishes the rD3 quasibases equation in the theorem, given an rD3 tower.

For the converse, suppose that we have $u_i \in (A \otimes_B A)^C$ and $\gamma_i \in \mathrm{End}\, {}_B A_C$ satisfying the equation in the theorem. Then map $\pi : A^N \to A \otimes_B A$ by

$$ \pi : (a_1, \ldots, a_N) \longmapsto \sum_i a_i u_i, $$

an A-C-bimodule epimorphism split by the mapping $\sigma : A \otimes_B A \hookrightarrow A^N$ given by

$$ \sigma(x \otimes_B y) := (x\gamma_1(y), \ldots, x\gamma_N(y)). $$

It follows from the equation above that $\pi \circ \sigma = \mathrm{id}_{A \otimes_B A}$. $\square$

2.1. Left D3 towers and quasibases

A tower of rings $A|B|C$ is left D3 (or ℓD3) if the tensor-square $A \otimes_B A$ is a C-A-bimodule direct summand of A^N for some N. If $B = C$, this recovers the definition of a left depth two extension $A|B$. There is a left version of all results in this paper: we note that $A|B|C$ is a right D3 tower if and only if $A^{\mathrm{op}}|B^{\mathrm{op}}|C^{\mathrm{op}}$ is a left D3 tower (cf. [14]).

The notation in the theorem below refers to that in the example above. Note that the theorem implies that a Frobenius extension is D3 if rD3.

Theorem 2.7. *Suppose that $B|C$ is a Frobenius extension with $A = \mathrm{End}\, B_C$. Then $A|B|C$ is right depth three if and only if $A|B|C$ is left depth three.*

Proof. It is well-known that also $A|B$ is a Frobenius extension. Then $A \otimes_B A \cong \mathrm{End}\, A_B$ as natural A-A-bimodules.

Now note the following characterization of left D3 with proof almost identical with that of [16, Prop. 3.8]: If $A|B|C$ is a tower where A_B if finite projective, then $A|B|C$ is left D3 $\Leftrightarrow$ $\mathrm{End}\, A_B \oplus * \cong A^N$ as natural A-C-bimodules. The proof involves noting that $\mathrm{End}\, A_B \cong \mathrm{Hom}(A \otimes_B A_A, A_A)$ as natural A-C-bimodules via

$$f \longmapsto (a \otimes a' \mapsto f(a)a').$$

The finite projectivity is used for reflexivity in hom'ming this isomorphism, thus proving the converse statement.

Of course a Frobenius extension satisfies the finite projectivity condition. Comparing the isomorphisms of $\mathrm{End}\, A_B$ and $A \otimes_B A$ to direct summands of finitely many copies of A just above and in Eq. (2), we note that the tower is ℓD3 $\Leftrightarrow$ rD3. $\square$

In a fairly obvious reversal to opposite ring structures in the proof of Theorem 2.6, we see that a tower $A|B|C$ is left D3 iff there are N elements $\beta_j \in \mathrm{End}\, {}_C A_B$ and N elements $t_j \in (A \otimes_B A)^C$ such that for all $x, y \in A$, we have

$$x \otimes_B y = \sum_{j=1}^{N} t_j \beta_j(x) y. \tag{9}$$

We note explicitly that if $A|B$ is a Frobenius extension with Frobenius system (E, x_i, y_i), then $A|B|C$ is rD3 iff the tower is ℓD3. For example, starting with the ℓD3 quasibases data above, a right D3 quasibases is given by

$$\{E(-t_j^1)t_j^2\} \quad \left\{ \sum_i \beta_j(x_i) \otimes_B y_i \right\}. \tag{10}$$

as one may readily compute.

We record the characterization of left D3, noted above in the proof, for towers satisfying a finite projectivity condition.

Theorem 2.8. *Suppose that $A|B|C$ is a tower of rings where A_B is finite projective. Then this tower is left D3 if and only if the natural A-C-bimodules satisfy for some N,*

$$\mathrm{End}\, A_B \oplus * \cong A^N. \tag{11}$$

In other words, a right projective tower is left D3 iff the natural A-C-bimodules $\mathrm{End}\, A_B$ and A are H-equivalent, since for any tower we have $A \oplus * \cong \mathrm{End}\, A_B$. Dually we establish that if $A|B|C$ is a tower where ${}_B A$ is finite projective, then $A|B|C$ is right D3 if and only if $\mathrm{End}\, {}_B A$ and A are H-equivalent as natural C-A-bimodules.

The two theorems in this section involving Frobenius extension and the theorems in Section 8 are extendable to a quasiFrobenius extension $B|C$, using the facts from QF theory such as $B \otimes_C B$, $\mathrm{End}\, B_C$ and $\mathrm{End}\, {}_C B$ are H-equivalent as B-B-bimodules. This will be established in a future paper.

3. Depth three for towers of groups

Fix a base ring F. Groups give rise to rings via $G \mapsto F[G]$, the functor associating the group algebra $F[G]$ to a group G. Therefore we can pull back the notion of depth 2 or 3 for ring extensions or towers to the category of groups when reference is made to the base ring.

In the paper [10], a depth two subgroup w.r.t. the complex numbers is shown to be equivalent to the notion of normal subgroup for finite groups. This consists of two results. The easier result is that over any base ring, a normal subgroup of finite index is depth two by exhibiting left or right D2 quasibases via coset representatives and projection onto cosets. This proof suggests that the converse hold as well. The second result is a converse for complex finite-dimensional D2 group algebras where normality of the subgroup is established using character theory and Mackey's subgroup theorem.

In this section, we will similarly do the first step by showing what group-theoretic notion corresponds to depth three tower of rings. Let $G > H > K$ be a tower of groups, where G is a finite group, H is a subgroup, and K is a subgroup of H. Let $A = F[G]$, $B = F[H]$ and $C = F[K]$. Then $A|B|C$ is a tower of rings, and we may ask what group-theoretic notion on $G > H > K$ will guarantee, with fewest possible hypotheses, that $A|B|C$ is rD3.

Theorem 3.1. *The tower of groups algebras $A|B|C$ is D3 if the corresponding tower of groups $G > H > K$ satisfies*

$$K^G < H \tag{12}$$

where K^G denotes the normal closure of K in G.

Proof. Let $\{g_1, \ldots, g_N\}$ be double coset representatives, so $G = \coprod_{i=1}^N Hg_iK$. Define $\gamma_i(g) = 0$ if $g \notin Hg_iK$ and $\gamma_i(g) = g$ if $g \in Hg_iK$. Of course, $\gamma_i \in \operatorname{End}{}_BA_C$ for $i = 1, \ldots, N$.

Since $K^G \subseteq H$, we have $gK \subseteq Hg$ for each $g \in G$. Hence for each $k \in K$, $g_jk = hg_j$ for some $h \in H$. It follows that

$$g_j^{-1} \otimes_B g_jk = g_j^{-1}h \otimes_B g_j = kg_j^{-1} \otimes_B g_j.$$

Given $g \in G$, we have $g = hg_jk$ for some $j = 1, \ldots, N$, $h \in H$, and $k \in K$. Then we compute:

$$1 \otimes_B g = 1 \otimes_B hg_jk = hg_jg_j^{-1} \otimes_B g_jk = hg_jkg_j^{-1} \otimes_B g_j$$

so $1 \otimes_B g = \sum_i \gamma_i(g)g_i^{-1} \otimes_B g_i$ where $g_i^{-1} \otimes_B g_i \in (A \otimes_B A)^C$. By theorem then, $A|B|C$ is an rD3 tower.

The proof that the tower of group algebras is left D3 is entirely symmetrical via the inverse mapping. $\square$

The theorem is also valid for infinite groups where the index $[G : H]$ is finite, since $HgK = Hg$ for each $g \in G$.

Notice how the equivalent notions of depth two and normality for finite groups over $\mathbb{C}$ yields the Proposition 2.4 for groups. Suppose that we have a tower of groups $G > H > K$ where $K^G \subseteq H$. If $K = H$, then H is normal (D2) in G. If $K = \{e\}$, then it is rD3 together with any subgroup $H < G$. If $H \lhd G$ is a normal subgroup, then necessarily $K^G \subseteq H$. If $K \lhd G$, then $K^G = K < H$ and the tower is D3.

Question: Can the character-theoretic proof in [10] be adapted to prove that a D3 tower $\mathbb{C}[G] \supseteq \mathbb{C}[H] \supseteq \mathbb{C}[K]$ where G is a finite group satisfies $K^G < H$?

4. Algebraic structure on End ${}_BA_C$ and $(A \otimes_B A)^C$

In this section, we study the calculus of some structures definable for an rD3 tower $A|B|C$, which reduce to the dual bialgebroids over the centralizer of a ring extension in case $B = C$ and their actions/coactions. Throughout the section, $A|B|C$ will denote a right depth three tower of rings,

$$P := (A \otimes_B A)^C, \qquad Q := (A \otimes_C A)^B,$$

which are bimodules with respect to the two rings familiar in depth two theory,

$$T := (A \otimes_B A)^B, \qquad U := (A \otimes_C A)^C.$$

Note that P and Q are isomorphic to two A-A-bimodule Hom-groups:

$$P \cong \operatorname{Hom}(A \otimes_C A, A \otimes_B A), \qquad Q \cong \operatorname{Hom}(A \otimes_B A, A \otimes_C A). \tag{13}$$

Recall that T and U have multiplications given by

$$tt' = t'^1t^1 \otimes_B t^2t'^2, \qquad uu' = u'^1u^1 \otimes_C u^2u'^2,$$

where $1_T = 1_A \otimes 1_A$ and a similar expression for 1_U. Namely, the bimodule ${}_T P_U$ is given by

$$ {}_T P_U : \; t \cdot p \cdot u = u^1 p^1 t^1 \otimes_B t^2 p^2 u^2. \tag{14} $$

The bimodule ${}_U Q_T$ is given by

$$ {}_U Q_T : \; u \cdot q \cdot t = t^1 q^1 u^1 \otimes_C u^2 q^2 t^2. \tag{15} $$

We have the following result, also mentioned in passing in [15] with several additional hypotheses.

Proposition 4.1. *The bimodules P and Q over the rings T and U form a Morita context with associative multiplications*

$$ P \otimes_U Q \to T, \qquad p \otimes q \mapsto pq = q^1 p^1 \otimes_B p^2 q^2 \tag{16} $$

$$ Q \otimes_T P \to U, \qquad q \otimes p \mapsto qp = p^1 q^1 \otimes_C q^2 p^2. \tag{17} $$

If $B|C$ is an H-separable extension, then T and U are Morita equivalent rings via this context.

Proof. The equations $p(qp') = (pq)p'$ and $q(pq') = (qp)q'$ for $p, p' \in P$ and $q, q' \in Q$ follow from the four equations directly above.

Note that

$$ T \cong \mathrm{End}\; {}_A A \otimes_B A_A, \qquad U \cong \mathrm{End}\; {}_A A \otimes_C A_A $$

as rings. We now claim that the hypotheses on $A|B$, $A|C$ and $B|C$ imply that the A-A-bimodules $A \otimes_B A$ and $A \otimes_C A$ are H-equivalent. Then the endomorphism rings above are Morita equivalent via context bimodules given by Eq. (13), which proves the proposition.

Since $B|C$ is H-separable, it is in particular separable, and the canonical A-A-epi $A \otimes_C A \to A \otimes_B A$ splits via an application of a separability element. Thus, $A \otimes_B A \oplus * \cong A \otimes_C A$. The defining condition for H-separability is $B \otimes_C B \oplus * \cong B^N$ as B-B-bimodules for some positive integer N. Therefore, $A \otimes_C A \oplus * \cong A \otimes_B A^N$ as A-A-bimodules by an application of the functor $A \otimes_B - \otimes_B A$. Hence, $A \otimes_B A$ and $A \otimes_C A$ are H-equivalent A^e-modules (i.e., A-A-bimodules). □

We denote the centralizer subrings A^B and A^C of A by

$$ R := V_A(B) \subseteq V_A(C) := V. \tag{18} $$

From $R \cong \mathrm{Hom}(A \otimes_B A, A)$ and $V \cong \mathrm{Hom}(A \otimes_C A, A)$ and composition with Eq. (13), we obtain the generalized anchor mappings (cf. [15]),

$$ R \otimes_T P \longrightarrow V, \qquad r \otimes p \longmapsto p^1 r p^2 \tag{19} $$

$$ V \otimes_U Q \longrightarrow R, \qquad v \otimes q \longmapsto q^1 v q^2. \tag{20} $$

Proposition 4.2. *The two generalized anchor mappings are bijective if $B|C$ is H-separable.*

Proof. Denote $r \cdot p := p^1 r p^2$ and $v \cdot q := q^1 v q^2$. From the previous proposition, there are elements $p_i \in P$ and $q_i \in Q$ such that $\sum_i p_i q_i = 1_T$; in addition, $p'_j \in P$ and $q'_j \in Q$ such that $1_U = \sum_j q'_j p'_j$. Let $v \in V$, then

$$ v = v \cdot 1_U = \sum_j v \cdot (q'_j p'_j) = \sum_j (v \cdot q'_j) \cdot p'_j $$

and a similar computation starting with $r = r \cdot 1_T$ shows that the two generalized anchor mappings are surjective.

In general, we have the corestriction of the inclusion $T \subseteq A \otimes_B A$,

$$ {}_T T \hookrightarrow {}_T P \tag{21} $$

which is split as a left T-module monic by $p \mapsto e^1 p e^2$ in case there is a separability element $e = e^1 \otimes_C e^2 \in B \otimes_C B$. Similarly,

$$ {}_U Q \hookrightarrow {}_U U \tag{22}$$

is a split monic in case $B|C$ is separable. If $\sum_i v_i \otimes_U q_i \in \ker(V \otimes_U Q \to R)$ then $\sum_i v_i \otimes_U q_i \mapsto \sum_i v_i \cdot q_i \otimes_U 1_U = 0$ via an injective mapping, whence $\ker(V \otimes_U Q \to R) = \{0\}$.

Of course, if $B|C$ is H-separable, we note from Proposition 4.1 and Morita theory that P and Q are projective generators on both sides, (and faithfully flat). If $K := \ker(R \otimes_T P \to V)$, then $K \otimes_U Q = 0$, since $\sum_j r_j \cdot p_j = 0$ implies

$$\sum_j r_j \otimes_T p_j \otimes_U q \longmapsto \sum_j r_j \otimes_T p_j q \otimes_U 1_U = 0$$

via an injective mapping. It follows from faithful flatness of ${}_U Q$ that $K = \{0\}$. □

Note that P is a V-V-bimodule (via the commuting homomorphism and anti-homomorphism $V \to U \leftarrow V$):

$$ {}_V P_V : \ v \cdot p \cdot v' = v p^1 \otimes_B p^2 v'. \tag{23}$$

Note too that $E = \mathrm{End}\, {}_B A_C$ is an R-V-bimodule via

$$ {}_R E_V : \ r \cdot \alpha \cdot v = r\alpha(-)v. \tag{24}$$

Note the subring and overring

$$\mathrm{End}\, {}_B A_B \subseteq E \subseteq \mathrm{End}\, {}_C A_C \tag{25}$$

which are the total algebras of the left R- and V-bialgebroids in depth two theory [13–15].

Lemma 4.3. *The modules ${}_V P$ and E_V are finitely generated projective. In case $A|C$ is left D2, the subring E is a right coideal subring of the left V-bialgebroid* $\mathrm{End}\, {}_C A_C$.

Proof. This follows from Eq. (5), since $p \in P \subseteq A \otimes_B A$, so

$$p = \sum_i p^1 \gamma_i(p^2) u_i$$

where $u_i \in P$ and $p \mapsto p^1 \gamma_i(p^2)$ is in $\mathrm{Hom}\,({}_V P, {}_V V)$, thus dual bases for a finite projective module. The second claim follows similarly from

$$\alpha = \sum_i \gamma_i(-) u_i^1 \alpha(u_i^2)$$

where $\gamma_i \in E$ and $\alpha \mapsto u^1 \alpha(u^2)$ are mappings in $\mathrm{Hom}(E_V, V_V)$.

Now suppose that $\beta_j \in S := \mathrm{End}\, {}_C A_C$ and $t_j \in (A \otimes_C A)^C$ are left D2 quasibases of $A|C$. Recall that the coproduct $\Delta : S \to S \otimes_V S$ given by ($\beta \in S$)

$$\Delta(\beta) = \sum_j \beta(-t_j^1) t_j^2 \otimes_V \beta_j \tag{26}$$

makes S a left V-bialgebroid [13]. Of course this restricts and corestricts to $\alpha \in E$ as follows: $\Delta(\alpha) \in E \otimes_V S$. Hence, E is a right coideal subring of S. □

In fact, if $A|B$ is also D2, and $\mathcal{S} = \mathrm{End}\, {}_B A_B$, then E is similarly shown to be an $\mathcal{S}$-$\mathcal{S}$-bicomodule ring. For we recall the coaction $E \to \mathcal{S} \otimes_R E$ given by

$$\alpha_{(-1)} \otimes_R \alpha_{(0)} = \sum_i \tilde{\gamma}_i \otimes \tilde{u}_i^1 \alpha(\tilde{u}_i^2 -) \tag{27}$$

where $\tilde{\gamma}_i \in \mathcal{S}$ and $\tilde{u}_i \in (A \otimes_B A)^B$ are right D2 quasibases of $A|B$ (restriction of [14, eq. (19)]).

Twice above we made use of a V-bilinear pairing $P \otimes E \to V$ given by

$$\langle p, \alpha \rangle := p^1 \alpha(p^2), \quad (p \in P = (A \otimes_B A)^C,\ \alpha \in E = \operatorname{End}\ {}_B A_C). \tag{28}$$

Lemma 4.4. *The pairing above is non-degenerate. Via $\alpha \mapsto \langle -, \alpha \rangle$, it induces $E_V \cong \operatorname{Hom}({}_V P, {}_V V)$.*

Proof. The mapping has the inverse $F \mapsto \sum_i \gamma_i(-)F(u_i)$ where $\gamma_i \in E, u_i \in P$ are rD3 quasibases for $A|B|C$. Indeed, $\sum_i \langle p, \gamma_i \rangle F(u_i) = F(\sum_i p^1 \gamma_i(p^2) u_i) = F(p)$ for each $p \in P$ since F is left V-linear, and for each $\alpha \in E$, we note that $\sum_i \gamma_i(-)\langle u_i, \alpha \rangle = \alpha$. □

Proposition 4.5. *There is a V-coring structure on P left dual to the ring structure on E.*

Proof. We note that

$$P \otimes_V P \cong (A \otimes_B A \otimes_B A)^C \tag{29}$$

via $p \otimes p' \mapsto p^1 \otimes p^2 p'^1 \otimes p'^2$ with inverse

$$p = p^1 \otimes p^2 \otimes p^3 \mapsto \sum_i (p^1 \otimes_B p^2 \gamma_i(p^3)) \otimes_V u_i.$$

Via this identification, define a V-linear coproduct $\Delta : P \to P \otimes_V P$ by

$$\Delta(p) = p^1 \otimes_B 1_A \otimes_B p^2. \tag{30}$$

Alternatively, using Sweedler notation and rD3 quasibases,

$$p_{(1)} \otimes_V p_{(2)} = \sum_i (p^1 \otimes_B \gamma_i(p^2)) \otimes_V u_i. \tag{31}$$

Define a V-linear counit $\varepsilon : P \to V$ by $\varepsilon(p) = p^1 p^2$. The counital equations follow readily [2].

Recall from Sweedler [24] that the V-coring $(P, V, \Delta, \varepsilon)$ has left dual ring ${}^*P := \operatorname{Hom}({}_V P, {}_V V)$ given by Sweedler notation by

$$(f * g)(p) = f(p_{(1)} g(p_{(2)})) \tag{32}$$

with $1 = \varepsilon$. Let $\alpha, \beta \in E$. If $f = \langle -, \alpha \rangle$ and $g = \langle -, \beta \rangle$, we compute $f * g = \langle -, \alpha \circ \beta \rangle$ below, which verifies the claim:

$$f(p_{(1)} g(p_{(2)})) = \sum_i \langle p^1 \otimes_B \gamma_i(p^2)\langle u_i, \beta \rangle, \alpha \rangle = \langle p^1 \otimes_B \beta(p^2), \alpha \rangle = \langle p, \alpha \circ \beta \rangle. \quad \square$$

In addition, we note that P is V-coring with grouplike element

$$g_P := 1_A \otimes_B 1_A \tag{33}$$

since $\Delta(g_P) = 1 \otimes 1 \otimes 1 = g_P \otimes_V g_P$ and $\varepsilon(g_P) = 1$.

There is a pre-Galois structure on A given by the right P-comodule structure $\delta : A \to A \otimes_V P$, $\delta(a) = a_{(0)} \otimes_V a_{(1)}$ defined by

$$\delta(a) := \sum_i \gamma_i(a) \otimes_V u_i. \tag{34}$$

The pre-Galois isomorphism $\beta : A \otimes_B A \xrightarrow{\cong} A \otimes_V P$ given by

$$\beta(a \otimes a') = a a'_{(0)} \otimes_V a'_{(1)} \tag{35}$$

is utilized below in another characterization of right depth three towers.

Theorem 4.6. *A tower of rings $A|B|C$ is right depth three if and only if ${}_V P$ is finite projective and $A \otimes_V P \cong A \otimes_B A$ as natural A-C-bimodules.*

Proof. ($\Leftarrow$) If ${}_V P \oplus * \cong {}_V V^N$ and $A \otimes_V P \cong A \otimes_B A$, then tensoring by $A \otimes_V -$, we obtain $A \otimes_B A \oplus * \cong A^N$ as natural A-C-bimodules, the rD3 defining condition on a tower.

($\Rightarrow$) By lemma ${}_V P$ is f.g. projective. Map $A \otimes_V P \to A \otimes_B A$ by $a \otimes p \mapsto ap^1 \otimes_B p^2$, clearly an A-C-bimodule homomorphism. The inverse is the "pre-Galois" isomorphism,

$$\beta : A \otimes_B A \to A \otimes_V P, \qquad \beta(a \otimes_B a') = \sum_i a\gamma_i(a') \otimes_V u_i \tag{36}$$

since $\sum_i ap^1\gamma_i(p^2) \otimes_V u_i = a \otimes_V p$ and $\sum_i a\gamma_i(a')u_i = a \otimes a'$ for $a, a' \in A$, $p \in P$. $\square$

If $B|C$ is H-separable, there is more to say about the structure of the Morita equivalent total rings for the bialgebroids T and U and bijective anchor maps in Propositions 4.1 and 4.2. This stems from the fact that for a B-bimodule M, we have an Azumaya-type condition for the centralizers, $M^C \cong M^B \otimes_{Z(B)} B^C$ via $m \otimes c \mapsto mc$ in one direction. This may now be applied to each of the cases $M = A$, $A \otimes_B A$, and $A \otimes_C A$ to obtain formulas relating V and R, T and P, as well as Q and U. We will study the relationship of these remarks to monoidal functors and Takeuchi's $\sqrt{\text{Morita}}$ base change outlined in the paper [22] in another paper.

5. Further Galois properties of depth three

We will show here that the smaller of the endomorphism rings of a depth three tower decomposes tensorially over the overalgebra and the mixed bimodule endomorphism ring studied above. In case the composite ring extension is depth two, this is a smash product decomposition in terms of a coideal subring of a bialgebroid. Finally, we express the invariants of this coideal subring acting on the overalgebra in terms of a bicommutator.

Theorem 5.1. *If $A|B|C$ is left D3, then*

$$\operatorname{End} A_B \cong A \otimes_V \operatorname{End} {}_C A_B \tag{37}$$

via the homomorphism $A \otimes_V \operatorname{End} {}_C A_B \to \operatorname{End} A_B$ given by $a \otimes_V \alpha \mapsto \lambda_a \circ \alpha$.

Proof. Given a left D3 quasibases $\beta_j \in \operatorname{End} {}_C A_B$ and $t_j \in (A \otimes_B A)^C$, note that the mapping $\operatorname{End} A_B \to A \otimes_V \operatorname{End} {}_C A_B$ given by

$$f \longmapsto \sum_j f(t_j^1)t_j^2 \otimes_V \beta_j \tag{38}$$

is an inverse to the homomorphism above. $\square$

Corollary 5.2. *If $A|C$ is additionally D2, then* $\operatorname{End} {}_C A_B$ *a left coideal subring of* $\operatorname{End} {}_C A_C$ *and there is a ring isomorphism with a smash product ring,*

$$\operatorname{End} A_B \cong A \rtimes \operatorname{End} {}_C A_B \,. \tag{39}$$

Proof. Recall from depth two theory [13] that the V-bialgebroid $\operatorname{End} {}_C A_C$ acts on the module algebra A by simple evaluation, $\beta \triangleright a = \beta(a)$. That the action measuring is not hard to see from the formula for the coproduct on $\operatorname{End} {}_C A_C$ given by

$$\Delta(\beta) = \beta_{(1)} \otimes_V \beta_{(2)} := \sum_k \tilde{\gamma}_k \otimes_V \tilde{u}_k^1 \beta(\tilde{u}_k^2 -) \tag{40}$$

where $\tilde{\gamma}_k \in \operatorname{End} {}_C A_C$ and $\tilde{u}_k \in (A \otimes_C A)^C$ are right $D2$ quasibases for the composite ring extension $A|C$. Note then that for $\alpha \in \operatorname{End} {}_C A_B \subseteq \operatorname{End} {}_C A_C$, the equation yields $\alpha_{(1)} \otimes_V \alpha_{(2)} \in \operatorname{End} {}_C A_C \otimes_V \operatorname{End} {}_C A_B$. Hence, $\operatorname{End} {}_C A_B$ is a left coideal subring. The details and verifications of the definition of such an object, over a smaller base ring than that of the bialgebroid, are rather straightforward and left to the reader.

As a consequence of the smash product formula $\operatorname{End} A_C \cong A \rtimes \operatorname{End} {}_C A_C$ over the centralizer V, we restrict to $\operatorname{End} A_B \subseteq \operatorname{End} A_C$, apply the theorem above, to obtain the equation for $\alpha, \beta \in \operatorname{End} {}_C A_B$,

$$(a\#\alpha)(b\#\beta) = a(\alpha_{(1)} \triangleright b)\#\alpha_{(2)} \circ \beta \in A \otimes_V \operatorname{End} {}_C A_B \tag{41}$$

where $a, b \in A$, and $\rtimes$, # are used interchangeably. $\square$

In case $A|C$ continues to be a D2 extension, the theorem below will characterize the subring A^S of invariants of $S = \operatorname{End}{}_C A_C$ as well as $A^{\mathcal{J}}$ where $\mathcal{J} := \operatorname{End}{}_C A_B$, the coideal subring of S, in terms of A as the natural module over $E := \operatorname{End} A_B$. The endomorphism ring $\operatorname{End}{}_E A$ is familiar from the Jacobson–Bourbaki theorem in Galois theory [8,21].

Theorem 5.3. *Let $A|B|C$ be left D3 and*

$$A^{\mathcal{J}} = \{x \in A | \forall \alpha \in \mathcal{J}, \alpha(x) = \alpha(1)x\}.$$

Then $A^{\mathcal{J}} \cong \operatorname{End}{}_E A$ via the anti-isomorphism $x \mapsto \rho_x$.

Proof. We first note that $A^{\mathcal{J}} = \{x \in A | \forall f \in E, y \in A, f(yx) = f(y)x\}$. The inclusion $\supseteq$ easily follows from letting $y = 1_A$ and $\alpha \in \mathcal{J} \subseteq E$. The reverse inclusion follows from Theorem 5.1. Since $E \cong A \otimes_V \mathcal{J}$, note that $f \circ \lambda_y \in E$ decomposes as $\sum_j f(yt_j^1)t_j^2 \otimes \beta_j \in A \otimes_V \mathcal{J}$ for an arbitrary $y \in A$. Given $x \in A$ such that $\alpha(x) = \alpha(1)x$ for each $\alpha \in \mathcal{J}$, then

$$f(yx) = \sum_j f(yt_j^1)t_j^2\beta_j(x) = \sum_j f(yt_j^1)t_j^2\beta_j(1)x = f(y)x.$$

It follows from these considerations that $\rho_x \in \operatorname{End}{}_E A$ for $x \in A^{\mathcal{J}}$, since $\rho_x(f(a)) = f(\rho_x(a))$ for each $f \in E, a \in A$.

Now an inverse mapping $\operatorname{End}{}_E A \to A^{\mathcal{J}}$ is given by $G \mapsto G(1)$. Of course $\rho_x(1) = x$. Note that $G(1) \in A^{\mathcal{J}}$, since for $\alpha \in \mathcal{J}$, we have $\alpha(G(1)) = G(\alpha(1)) = \lambda_{\alpha(1)}G(1)$, since $\lambda_a \in E$ for all $a \in A$. Finally, we note that $G(a) = G \circ \lambda_a(1) = aG(1)$, whence $G = \rho_{G(1)}$ for each $G \in \operatorname{End}{}_E A$. $\square$

The following clarifies and extends part of [13, 4.1]. Let S denote the bialgebroid $\operatorname{End}{}_B A_B$ below and E as before is $\operatorname{End} A_B$.

Corollary 5.4. *If $A|B$ is left D2, then $A^S \cong \operatorname{End}{}_E A$. Thus if A_B is balanced, $A^S = B$.*

Proof. Follows by Proposition 2.4 and from the theorem by letting $B = C$. We note additionally from its proof that

$$A^S = \{x \in A | \forall \alpha \in S, \alpha(x) = x\alpha(1)\} \tag{42}$$

since $\rho_{\alpha(1)} \in E$ in this case.

If A_B is balanced, $\operatorname{End}{}_E A = \rho(B)$ by definition. This recovers the result in [13, Section 4]. $\square$

In other words, this corollary states that the invariant subring of A under the action of the bialgebroid S is (anti-isomorphic to) the bicommutator of the natural module A. Sugano studies the derived ring extension $A^*|B^*$ of bicommutants of a ring extension $A|B$, where M_A is a faithful module, $E := \operatorname{End} M_A$, $\mathcal{E} := \operatorname{End} M_B$, $A^* = \operatorname{End}{}_E M$, $B^* = \operatorname{End}{}_{\mathcal{E}} M$ and there are natural monomorphisms $A \to A^*$ and $B \to B^*$ commuting with the mappings $B \to A$ and $B^* \to A^*$ [23]: in these terms, $A^S \subseteq A$ is then the bicommutator of A_A over the depth two extension $A|B$.

6. A Jacobson–Bourbaki correspondence for augmented rings

The Jacobson–Bourbaki correspondence is usually given between subfields F of finite codimension in a field E on the one hand, and their linear endomorphism rings $\operatorname{End} E_F$ on the other hand. A subring of $\operatorname{End} E_F$ which is itself an endomorphism ring of this form is characterized by containing $\lambda(E)$ and being finite-dimensional over this. The inverse correspondence associates to such a subring $R \subseteq \operatorname{End} E_F$, the subfield $\operatorname{End}{}_R E$, since ${}_R E$ is simple as a module. (The centralizer or commutant of R in $\operatorname{End} E_{\mathbb{Z}}$ in other words.) The correspondences are inverse to one another by the Jacobson–Chevalley density theorem, and may be extended to division rings [8, Section 8.2].

Usual Galois theory follows from this correspondence, for if $E^G = F$ where G is a finite group of automorphisms of E, then $\operatorname{End} E_F \cong E\#G$ and subrings of the form $\operatorname{End} E_K$ correspond to the subrings $E\#H$ where H is a subgroup of G such that $E^H = K$ for an intermediate field K of $F \subseteq E$. In this section, we will use a similar idea to pass from the Jacobson–Bourbaki correspondence to the correspondence $A|B \mapsto \operatorname{End}{}_B A_B$ and inverse $S \mapsto A^S$ for certain Hopf subalgebroids S of $\operatorname{End}{}_B A_B$ for certain depth two extensions $A|B$. First, we will give an appropriate generalization of the Jacobson–Bourbaki correspondence to non-commutative algebra, with a proof similar to Winter [26, Section 2].

For the purposes below, we say an *augmented ring* (A, D) is a ring A with a ring homomorphism $A \to D$ where D is a division ring. Examples are division rings, local rings, Hopf algebras and augmented algebras. A subring $\mathcal{R}$ of $\operatorname{End} A := \operatorname{End} A_{\mathbb{Z}}$ containing $\lambda(A)$, left finitely generated over this, where ${}_{\mathcal{R}}A$ is simple, is said to be a *Galois subring*.

Theorem 6.1 (*Jacobson–Bourbaki Correspondence for Non-commutative Augmented Rings*). *Let (A, D) be an augmented ring. There is a one-to-one correspondence between the set of division rings B within A, where B is a subring of A and A_B is a finite-dimensional right vector space, and the set of Galois subrings of* $\operatorname{End} A$. *The correspondence is given by $B \mapsto \operatorname{End} A_B$ with inverse correspondence $\mathcal{R} \mapsto \operatorname{End} {}_{\mathcal{R}}A$.*

Proof. We first show that if B is a division ring and subring of A of finite right codimension, then $E = \operatorname{End} A_B$ is a Galois subring and $\operatorname{End} {}_E A \cong B$. We will need a theory of left or (dually) right vector spaces over a division ring as for example to be found in [7, chap. 4]. Suppose that $[A : B]_r = d$.

Since $\operatorname{End} A_B$ is isomorphic to square matrices of order d over the division ring B, it follows that $\operatorname{End} A_B$ is finitely generated over the algebra $\lambda(A)$ of left multiplications of A. Also ${}_E A$ is simple, since $E = \operatorname{End} A_B$ acts transitively on A. Hence $\operatorname{End} {}_E A$ is a division ring. Since

$$A_B = B_B \oplus W_B \tag{43}$$

for some complementary subspace W over B, it follows from Morita's lemma ("generator modules are balanced") that in fact $B \cong \operatorname{End} {}_E A$.

Conversely, let $\mathcal{R}$ be a Galois subring. Let $F^{\mathrm{op}} = \operatorname{End} {}_{\mathcal{R}}A$ be the division ring (by Schur's lemma) contained in A^{op} (since $A \subseteq \mathcal{R}$ and $\operatorname{End} {}_A A \cong A^{\mathrm{op}}$). To finish the proof we need to show that $[A : F]_r < \infty$ and $\mathcal{R} = \operatorname{End} A_F$.

Since $\mathcal{R}$ is finitely generated over A, we have $s_1, \ldots s_n \in \mathcal{R}$ such that

$$\mathcal{R} = As_1 + \cdots + As_n.$$

Let $e_1, \ldots, e_m \in A$ be linearly independent in the right vector space A over F. Since ${}_{\mathcal{R}}A$ is simple, the Jacobson–Chevalley density theorem ensures the existence of elements $r_1, \ldots, r_m \in \mathcal{R}$ such that for all i and k,

$$r_i(e_k) = \delta_{ik} 1_A.$$

By the lemma below and the hypothesis that A is an augmented ring, $m \le n$. With a maximal linear independent set of vectors e_i in A, we may assume $e_1, \ldots, e_m$ a basis for A_F. By definition of F, we have $\mathcal{R} \subseteq \operatorname{End} A_F$. Let $E_{ij} := e_i r_j$ for $1 \le i, j \le m$ in $\mathcal{R}$. Since $E_{ij}(e_k) = \delta_{jk} e_i$, these are matrix units which span $\operatorname{End} A_F$. Hence $\operatorname{End} A_F = \mathcal{R}$. □

Lemma 6.2. *Let $s_1, \ldots, s_n \in \operatorname{End} A_{\mathbb{Z}}$ where (A, D) is an augmented ring. Suppose that*

$$r_1, \ldots, r_m \in As_1 + \cdots + As_n$$

and there are elements $e_1, \ldots, e_m \in A$ such that $r_i(e_k) = \delta_{ik} 1_A$ for $1 \le i, k \le m$. Then $m \le n$.

Proof. By the hypothesis, there are elements $a_{ij} \in A$ such that $r_i = \sum_{j=1}^n a_{ij} s_j$ for each $i = 1, \ldots, m$. Then for $1 \le i, k \le m$,

$$\sum_{j=1}^{n} a_{ij} s_j(e_k) = r_i e_k = \delta_{ik} 1_A.$$

Applying the ring homomorphism $A \to D$ into the division ring D, where $a_{ij} \mapsto d_{ij}$, $s_j(e_k) \mapsto z_{jk}$, we obtain the matrix product equation,

$$\begin{pmatrix} d_{11} & \cdots & d_{1n} \\ \vdots & \vdots & \vdots \\ d_{m1} & \cdots & d_{mn} \end{pmatrix} \begin{pmatrix} z_{11} & \cdots & z_{1m} \\ \vdots & \vdots & \vdots \\ z_{n1} & \cdots & z_{nm} \end{pmatrix} = \begin{pmatrix} 1_D & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1_D \end{pmatrix}.$$

This shows in several ways that $m \le n$; for example, by the rank + nullity theorem for right vector spaces [7, Ch. 4, Corollary 2.4]. □

Let $A \supseteq C$ be a D2 ring extension, so that $S := \mathrm{End}\,{}_C A_C$ is canonically a left bialgebroid over the centralizer A^C. Any D2 subextension $A \supseteq B$ has sub$R$-bialgebroid $\mathcal{S} := \mathrm{End}\,{}_B A_B$ where $R = A^B \subseteq A^C$. If all extensions are balanced, as in the situation we consider above, we recover the intermediate D2 subring B by $\mathcal{S} \rightsquigarrow A^{\mathcal{S}} = B$. Whence $B \rightsquigarrow \mathcal{S}$ is a surjective correspondence and Galois connection [1] between the set of intermediate D2 subrings of $A \supseteq C$ and the set of sub$R$-bialgebroids of S where R is a subring of A^C. We widen our perspective to include D3 intermediate subrings B, i.e. D3 towers $A \supseteq B \supseteq C$, and left coideal subrings of S in order to pass from surjective Galois connection to Galois correspondence.

The Galois correspondence given by $B \rightsquigarrow \mathrm{End}\,{}_C A_B$ and $\mathcal{J} \rightsquigarrow A^{\mathcal{J}}$ factors through the Jacobson–Bourbaki correspondence sketched in the theorem above. We apply Theorem 5.3, Corollary 5.2, and 2.8 below to do this. We need a notion of *Galois left coideal subring* $\mathcal{J}$ of a left V-bialgebroid S. For this we require the left coideal subring $\mathcal{J} \subseteq \mathrm{End}\,{}_C A_C$ that

(1) the module ${}_V\mathcal{J}$ is finitely generated projective where $V = A^C$;
(2) A has no proper $\mathcal{J}$-stable left ideals.

Theorem 6.3. *Let $A \supseteq C$ be a D2 extension of an augmented ring A over a division ring C, with centralizer A^C denoted by V and left V-bialgebroid* $\mathrm{End}\,{}_C A_C$ *by S. Suppose that A_V is faithfully flat. Then the left D3 intermediate division rings of $A \supseteq C$ are in Galois correspondence with the Galois left coideal subrings of S.*

Proof. Since $C \subseteq A$ is D2 and left or right split (as in Eq. (43)), we may apply a projection ${}_C A \to {}_C C$ to the left D2 quasibases equation to see that A_C is a finite-dimensional right vector space. For the same reasons, each extension $A \supseteq B$ (for an intermediate division ring B) is balanced by Morita's lemma. If B is additionally a left D3 intermediate ring, with $\mathcal{J} = \mathrm{End}\,{}_C A_B$ a left coideal subring of the bialgebroid S by Corollary 5.2 we have by Theorem 5.3 that the invariant subring $A^{\mathcal{J}} = B$. We just note that ${}_V\mathcal{J}$ is f.g. projective by the dual of Lemma 4.3, and that a proper $\mathcal{J}$-stable left ideal of A would be a proper $\mathrm{End}\,A_B$-stable left ideal in contradiction of the transitivity argument in Theorem 6.1. Thus $B \mapsto \mathrm{End}\,{}_C A_B$ is a surjective order-reversing correspondence between the set of left D3 intermediate division rings $A \supseteq B \supseteq C$ into the set of Galois left coideal subrings of the V-bialgebroid S.

Suppose that we are given a Galois left coideal subring $\mathcal{I}$ of $S = \mathrm{End}\,{}_C A_C$. Then the smash product ring $A \rtimes \mathcal{I}$ has image we denote by $\mathcal{R}$ in $\mathrm{End}\,A_C$ via $a \otimes_V \alpha \mapsto \lambda_a \circ \alpha$ that is clearly a Galois subring, since $\lambda(A) \subseteq \mathcal{R}$ and is a finitely generated extension; also the module ${}_{\mathcal{R}}A$ is simple by hypothesis (2) above. Then $B = \mathrm{End}\,{}_{\mathcal{R}}A$ is an intermediate division ring between $C \subseteq A$, and $\mathcal{R} = \mathrm{End}\,A_B$ by Theorem 6.1. Since $\mathcal{I} \hookrightarrow S$ and ${}_V\mathcal{I}$ is flat, it follows from $A \otimes_V S \cong \mathrm{End}\,A_C$ that $\mathrm{End}\,A_B \cong A \otimes_V \mathcal{I}$ via the mapping above. Note that $\mathcal{I} \subseteq \mathrm{End}\,A_B \cap S = \mathrm{End}\,{}_C A_B$ and let Q be the cokernel. Since $A \otimes_V \mathcal{I} \cong \mathcal{R} \cong A \otimes_V \mathrm{End}\,{}_C A_B$ it follows that $A \otimes_V Q = 0$. Since A_V is faithfully flat, $Q = 0$, whence $\mathcal{I} = \mathrm{End}\,{}_C A_B$. Finally, $\mathrm{End}\,A_B$ is isomorphic to an A-C-bimodule direct summand of A^N, since ${}_V\mathcal{I} \oplus * \cong V^N$ for some N, to which we apply the functor ${}_A A_C \otimes_V -$. Since A_B is finite free, it follows from Theorem 2.8 that $A \supseteq B \supseteq C$ is left D3. $\square$

If A or V is a division ring, the faithful flatness hypothesis in the theorem is clearly satisfied. In connection with this theorem we note the following criterion for a depth three tower of division algebras.

Proposition 6.4. *Suppose that $C \subseteq B \subseteq A$ is a tower of division rings where the right vector space A_B has basis $\{a_1, \ldots, a_n\}$ such that*

$$Ca_i \subseteq a_i B \quad (i = 1, \ldots, n). \tag{44}$$

Then $A|B|C$ is left D3.

Proof. It is easy to compute that $x \otimes_B 1 = \sum_i a_i \otimes_B a_i^{-1}\beta_i(x)$ for all $x \in A$. Here β_i is the rank one projection onto the right B-span of the basis element a_i along the span of $a_1, \ldots, \hat{a}_i, \ldots, a_n$, and $a_i^{-1} \otimes_B a_i \in (A \otimes_B A)^C$ for each i. Of course, $\beta_i \in \mathrm{End}\,{}_C A_B$, so $A|B$ is left D3. $\square$

We may similarly prove that the tower is rD3 if ${}_B A$ has basis $\{a_i\}$ satisfying $a_i C \subseteq B a_i$. When $B = C$ we deduce the following criterion for a depth two subalgebra pair of division rings. For example, the real quaternions $A = \mathbb{H}$, and subring $B = \mathbb{C}$ meet this criterion.

Corollary 6.5. *Suppose that $B \subseteq A$ is a subring pair of division rings where the left vector space ${}_BA$ has basis $\{a_1, \ldots, a_n\}$ such that*

$$a_i B = Ba_i \quad (i = 1, \ldots, n). \tag{45}$$

Then $A|B$ is depth two.

We remark that if the centralizer V of a depth two proper extension $A|C$ is contained in C (as in the example $C = \mathbb{C}$ and $A = \mathbb{H}$ just mentioned above), then End ${}_CA_C$ is a skew Hopf algebra over the commutative base ring V [17]. Any intermediate ring B of $A|C$, for which $A|B$ is D2, has skew Hopf algebra End ${}_BA_B$ over $R = A^B$ for the same reason, since $R \subseteq V \subseteq C \subseteq B$. It is interesting to determine under what conditions these are skew Hopf subalgebras, i.e., the antipodes are compatible under the sub$R$-bialgebroid structures.

7. Application to field theory

Given a separable finite field extension $F \subseteq E$ Szlachányi shows that there is a Galois connection between intermediate fields and weak Hopf subalgebras of End E_F. A *weak Hopf algebra* H the reader will recall from the already classic [3] is a weakening of the notion of Hopf algebra to include certain non-unital coproducts, non-homomorphic counits with weakened antipode equations. There are certain canonical coideal subalgebras H^L and H^R that are separable algebras and anti-isomorphic copies of one another via the antipode. Nikshych and Etingof [5] have shown that H is a Hopf algebroid over the separable algebra H^L, and conversely the author and Szlachányi [13] have shown that Hopf algebroids over a separable algebra are weak Hopf algebras. Let us revisit one of the important, motivating examples.

Example 7.1. Let $\mathcal{G}$ be a finite groupoid with $x, y \in \mathcal{G}_{\mathrm{obj}}$ the objects and $g, h \in \mathcal{G}_{\mathrm{arrows}}$ the invertible arrows (with sample elements). Let $s(g)$ and $t(g)$ denote the source and target objects of the arrow g. Suppose that k is a field. Then the groupoid algebra $H = k\mathcal{G}$ (defined like a quiver algebra, where $gh = 0$ if $t(h) \neq s(g)$) is a weak Hopf algebra with coproduct $\Delta(g) = g \otimes_k g$, counit $\varepsilon(g) = 1$, and antipode $S(g) = g^{-1}$. Since the identity is $1_H = \sum_{x \in \mathcal{G}_{\mathrm{obj}}} \mathrm{id}_x$, we see that $\Delta(1_H) \neq 1_H \otimes 1_H$ if $\mathcal{G}_{\mathrm{obj}}$ has two or more objects. Notice too that $\varepsilon(gh) \neq \varepsilon(g)\varepsilon(h)$ if $gh = 0$.

The Hopf algebroid structure has total algebra H, and has base algebra the separable algebra $k\mathcal{G}_{\mathrm{obj}}$, which is a product algebra k^N where $N = |\mathcal{G}_{\mathrm{obj}}|$. The source and target maps of the Hopf algebras $s_L, t_L : R \to H$ are simply $s_L = t_L : x \mapsto \mathrm{id}_x$. The resulting bimodule structure ${}_RH_R = {}_{s_L, t_L}H$ is given by $x \cdot g \cdot y = g$ if $x = y = t(g)$, 0 otherwise. The coproduct is $\Delta(g) = g \otimes_R g$, counit $\varepsilon(g) = t(g)$, and antipode $S(g) = g^{-1}$. This defines a Hopf algebroid in the sense of Lu and Xu. This is also a Hopf algebroid in the sense of Böhm–Szlachányi may be seen by defining a right bialgebroid structure on H via the counit $\varepsilon_r(g) = s(g)$.

If $\mathcal{G}$ is the finite set $\{\underline{1}, \ldots, \underline{n}\}$ with singleton hom-groups, suggestively denoted by $\mathrm{Hom}(\underline{i}, \underline{j}) = \{e_{ji}\}$ for all $1 \leq i, j \leq n$, the groupoid algebra considered above is the full matrix algebra $H \cong M_n(k)$ and R is the subalgebra of diagonal matrices. Note that the projection Π^L ($= \varepsilon_t$ in [5]) defined as $\Pi^L(x) = \varepsilon(1_{(1)}x)1_{(2)}$ is given here by $e_{ij} \mapsto e_{ii}$. Similarly, $\Pi^R(e_{ij}) = e_{jj}$.

In [25], Szlachányi shows that although Hopf–Galois separable field extensions do not have a universal Hopf algebra as "Galois quantum group," they have a universal weak Hopf algebra or "Galois quantum groupoid." For example, the field $E = \mathbb{Q}(\sqrt[4]{2})$ is a four-dimensional separable extension of $F = \mathbb{Q}$ which is Hopf–Galois with respect to two non-isomorphic Hopf algebras, H_1 and H_2 [6]. However, the endomorphism ring End E_F is then a smash product in two ways, $E\#H_i$, $i = 1, 2$, and is a weak Hopf algebra over the separable F-algebra E. It is universal in a category of weak Hopf algebras viewed as left bialgebroids [25, Theorem 2.2], with modifications to the definition of the arrows resulting (see [25, Prop. 1.4] for the definition of weak left morphisms of weak bialgebras). The separable field extensions that are Hopf–Galois may then be viewed as being weak Hopf–Galois with a uniqueness property.

The following corollary addresses an unanswered question in [25, Section 3.3]. Namely, there is a Galois connection between intermediate fields $K \subseteq F \subseteq E$ of a separable (finite) field extension $E|K$ and weak Hopf subalgebras of the weak Hopf algebra $\mathcal{A} := \mathrm{End}\, E_K$ that include E as left multiplications. The correspondences are denoted by

$$\mathrm{Sub}_{WHA/K}(\mathcal{A}) \xrightarrow{\mathrm{Fix}} \mathrm{Sub}_{Alg/K}(E)$$

which associates to a weak Hopf subalgebra W of $\operatorname{End} E_K$ the subfield

$$\operatorname{Fix}(W) = \{x \in E | \forall \alpha \in W, \alpha(x) = \alpha(1)x\},$$

in other words, E^W, and the correspondence

$$\operatorname{Sub}_{Alg/K}(E) \xrightarrow{\mathrm{Gal}} \operatorname{Sub}_{WHA/K}(\mathcal{A})$$

where the intermediate subfield $K \subseteq F \subseteq E$ gets associated to its Galois algebra

$$\operatorname{Gal}(F) = \{\alpha \in \mathcal{A} | \forall x \in E, y \in F, \alpha(xy) = \alpha(x)y\}.$$

Clearly $\operatorname{Gal}(F) = \operatorname{End} E_F$.

Szlachányi [25, 3.3] notes that Gal is a surjective correspondence, since $F = \operatorname{Fix}(\operatorname{Gal}(F)$ for each intermediate subfield (e.g. since E_F is a generator module, it is balanced by Morita's lemma). Gal is indeed a one-to-one correspondence by

Corollary 7.2. *Gal and Fix are inverse correspondences between intermediate fields of a separable field extension $E|K$ and weak Hopf subalgebras of the full linear endomorphism algebra* $\operatorname{End} E_K$.

Proof. We just need to apply the Jacobson–Bourbaki correspondence with a change of notation. Before changing notation, first note that if $A \supseteq B$ is a depth two extension where B is a commutative subring of the center of A, then the centralizer $A^B = A$ and the left bialgebroid $\operatorname{End} {}_B A_B = \operatorname{End} A_B$ over A. Indeed, a faithfully flat B-algebra A is depth two iff it is finite projective. If A and B are fields, this reduces to: depth two extension $A|B \Leftrightarrow$ finite extension $A|B$. If $A|B$ is a Frobenius extension (as are separable extensions of fields), there is an antipode on $\operatorname{End} {}_B A_B$ defined in terms of the Frobenius homomorphism (such as the trace map of a separable field extension [18]) and its dual bases [4]. Now, changing notation, we have a bialgebroid $\operatorname{End} E_K$ over the separable F-algebra E, or equivalently a weak bialgebra — which becomes a weak Hopf algebra via an involutive antipode given in terms of the trace map and its dual bases [25, eq. (3.5)]).

Given a weak Hopf subalgebra W of $\operatorname{End} E_K$ containing $\lambda(E)$, it is automatically finite-dimensional over E and ${}_W E$ is simple since a submodule is a W-stable ideal, but E is a field. Hence, W is a Galois subring and the Theorem 6.1 shows that $\operatorname{End} {}_W E \cong E^W$ is an intermediate field F between $K \subseteq E$, such that $\operatorname{End} E_F = W$. But $\operatorname{Gal}(F) = \operatorname{End} E_F$ has been noted above. Hence, $\operatorname{Gal}(\operatorname{Fix}(W)) = W$. $\square$

The only reason we need restrict ourselves to *separable* field extensions above is to acquire a fixed base algebra that is a separable algebra, so that we acquire antipodes from Frobenius extensions, and Hopf algebroids become weak Hopf algebras. Let us be clear on what happens when we drop this hypothesis. For the purpose of the next corollary, we define a sub$R$-bialgebroid of bialgebroid $(H, R, s_L, t_L \Delta, \varepsilon)$ to be a subalgebra V of the total algebra H with the same base algebra R, source s_L and target t_L maps having image within V, and V is a sub$R$-coring of (H, Δ, ε).

Corollary 7.3. *Let $E \supseteq K$ be a finite field extension. Then the poset of intermediate subfields is in Galois correspondence with the poset of sub E-bialgebroids of* $\operatorname{End} E_K$.

Proof. This follows from the Jacobson–Bourbaki correspondence, where intermediate field $F \mapsto \operatorname{End} E_F$ with inverse, Galois subring $R \mapsto \operatorname{End} {}_R E$, with the same proof as in the previous corollary. Note from the proof of Jacobson–Bourbaki in the field context that any subring of $\operatorname{End} E_K$ containing $\lambda(E)$ is indeed of the form $\operatorname{End} E_F$ for some intermediate $K \subseteq F \subseteq E$, and therefore the left bialgebroid of the depth two (=finite) field extension $F \subseteq E$, and sub$E$-bialgebroid of $\operatorname{End} E_K$. $\square$

The Jacobson–Bourbaki correspondence also exists between subfields of a finite-dimensional simple algebra A and subalgebras of the linear endomorphism algebra which contain left and right multiplications [21, sect. 12.3], a theorem related to the topic of Brauer group of a field. By the same reasoning, we arrive at Galois correspondences between subfields and bialgebroids over A. Namely, let A^e denote the image of $A \otimes_F A^{\mathrm{op}}$ in the linear endomorphism algebra $\operatorname{End} A_F$ via left and right multiplication $x \otimes y \mapsto \lambda_x \circ \rho_y$, and $Z(A)$ denote the center of A, which is a field since $Z(A) \cong \operatorname{End} {}_{A^e} A$. We note that $\operatorname{End} A_E$ is a bialgebroid over A for any intermediate field $F \subseteq E \subseteq Z(A)$ with Lu structure [19], and a Hopf algebroid in the special case $E = Z(A)$ where A becomes Azumaya so $A \otimes_E A^{\mathrm{op}} \cong \operatorname{End} A_E$. The proof is quite the same as the above and therefore omitted.

Corollary 7.4. *Let A be a simple finite-dimensional F-algebra. Then the fields that are intermediate to $F \subseteq Z(A)$ are in Galois correspondence to the sub A-bialgebroids of* $\mathrm{End}\, A_F$. *In case A is a separable F-algebra, the intermediate fields are in Galois correspondence to weak Hopf subalgebras of* $\mathrm{End}\, A_F$.

8. An embedding theorem for finite depth Frobenius extensions

In this section we define finite depth Frobenius extension using the notion of depth three tower by choosing a suitable three-ring subtower of the Jones tower. We show that this definition is consistent with the previous definitions of finite depth for subfactors and free Frobenius extensions. We show in Theorem 8.5 that any finite depth Frobenius extension extends to a depth two extension somewhere further along in its Jones tower.

Suppose that $M_{-1} \hookrightarrow M_0$ is a Frobenius extension; e.g. a (type II_1) subfactor of finite index [9,12,13] or a Frobenius algebra in the tensor category of bimodules over M_{-1}. Let M_1 denote its basic construction $M_1 = Me_1M$ which is isomorphic to $\mathrm{End}\, M_N$ and to $M \otimes_N M$ where $M := M_0$ and $N := M_{-1}$. The ring extension $M_1|M$ is itself a Frobenius extension with M-bimodule Frobenius homomorphism $E_1 : M_1 \to M$ defined by $E_1(e_1) = 1$. The Jones element e_1 maps isomorphically into the Frobenius homomorphism and into the cyclic generator $1_M \otimes_N 1_M$. Iterate this to obtain the Jones tower,

$$N = M_{-1} \hookrightarrow M = M_0 \hookrightarrow M_1 \hookrightarrow M_2 \hookrightarrow \cdots \hookrightarrow M_n \hookrightarrow \cdots, \tag{46}$$

e.g., $M_2 = M_1e_2M_1$ where e_2 maps into the Frobenius homomorphism $E_1 : M_1 \to M_0$ and into $1_{M_1} \otimes_M 1_{M_1}$, $1_{M_1} = \sum_i x_ie_1y_i$. Note that $M_n \cong M \otimes_N \cdots \otimes_N M$ ($n+1$ times M). Each ring extension $M_n|M_{n-1}$ is a Frobenius extension by the endomorphism ring theorem (iterated). Each composite ring extension $M_n|M_{n-k}$ is a Frobenius extension by composing Frobenius homomorphisms, and M_{n+k} is isomorphic to the basic construction of $M_n|M_{n-k}$ by [11, appendix]. While the e_i may not be idempotents or projections, they satisfy $e_ie_{i\pm1}e_i = e_i$, $e_iye_i = E_{i-1}(y)e_i = e_iE_{i-1}(y)$ and $e_ix = e_iE_i(e_ix)$ for all $y \in M_{i-1}$, $x \in M_i$ with Frobenius homomorphisms $E_i : M_i \to M_{i-1}$. For more details on the Jones tower over a Frobenius extension, please see [13, section 6] and [9, chapter 3].

Definition 8.1 (*Finite Depth Frobenius Extensions*). The Frobenius extension $N \hookrightarrow M$ is said to be of depth $n > 1$ if the composite tower $M_{n-2}|M_{n-3}|M_{-1}$ is a right or left depth three tower.

The definition allows for the possibility of a depth n extension being at the same time depth $n+1$, something we note to be true below. In subfactor theory, one speaks of depth n subfactor as the least n for which the relative commutant M_n^N is a basic construction of the two previous semisimple algebras in the derived tower, which we introduce next.

Let M_i^N denote the centralizer of N in M_i. We note the derived tower of Eq. (46):

$$N^N \hookrightarrow M^N \hookrightarrow {M_1}^N \hookrightarrow \cdots \hookrightarrow {M_{n-1}}^N \hookrightarrow {M_n}^N \hookrightarrow \cdots. \tag{47}$$

In classical subfactor theory, depth n is characterized by the least n for which M_n^N is isomorphic to the basic construction of M_{n-1}^N over M_{n-2}^N. We compute that this is so with our new definition, which we also show to be consistent with the definition in [12, 3.1] of depth n free Frobenius extension.

Proposition 8.2. *A depth n Frobenius extension $N \hookrightarrow M$ has n-step centralizer $M_n^N \cong M_{n-1}^N \otimes_{M_{n-2}^N} M_{n-1}^N$. The Frobenius homomorphism E_{n-1} has dual bases elements in M_{n-1}^N.*

Proof. Let $A = M_{n-2}$, $B = M_{n-3}$ and $C = M_{-1}$. Then subtower $A|B|C$ of the Jones tower (46) is D3. Whence the A-C-bimodules $A \otimes_B A$ and A are H-equivalent, and their endomorphism rings are Morita equivalent.

Note that

$$\mathrm{End}\,_A A \otimes_B A_C \cong \mathrm{End}\,_A (M_{n-1})_N \cong M_n^N,$$

since M_{n-1} is isomorphic to the basic construction of $M_{n-2}|M_{n-3}$ and anti-isomorphic to $\mathrm{End}\,_B A$. We use as well that the C-centralizer $(\mathrm{End}\,_B A)^C \cong \mathrm{End}\,_B A_C$.

On the other hand, we note

$$\mathrm{End}\,_A A_C \cong A^C \cong M_{n-2}^N,$$

so we conclude that M_n^N and M_{n-2}^N are Morita equivalent rings. The Morita context bimodules are the A-C-bimodule hom-groups $\mathrm{Hom}(A \otimes_B A, A)$ and $\mathrm{Hom}(A, A \otimes_B A)$. In Section 2 we saw that first of all,

$$\mathrm{Hom}(A \otimes_B A, A) \cong \mathrm{End}\ {}_B A_C \cong M_{n-1}^N,$$

since M_{n-1} is anti-isomorphic to the left endomorphism ring of $M_{n-2}|M_{n-3}$. Since the Frobenius extension $A|B$ satisfies $\mathrm{End}\ {}_B A \cong A \otimes_B A$, we also obtain that the C-centralizers,

$$\mathrm{End}\ {}_B A_C \cong (A \otimes_B A)^C \cong \mathrm{Hom}(A, A \otimes_B A)$$

the last step following from Section 2. In other words, M_{n-1}^N doubles as both of the Morita context bimodules between M_n^N and M_{n-2}^N.

By Morita theory, it follows that the Morita context bimodules satisfy $M_n^N \cong M_{n-1}^N \otimes_{M_{n-2}^N} M_{n-1}^N$.

The last statement is proven as [10, Theorem 2.1, part (5)] and [13, Prop. 6.4]. Toward this end, we note that $M_{n-1} \cong Ae_{n-1}A$ and $M_{n-1}^N \cong (A \otimes_B A)^C \cong \mathrm{End}\ {}_C A_B$. Suppose that a left D3 quasibases given by $t_i = t_i^1 e_{n-1} t_i^2$ and $\beta_i \in \mathrm{End}\ {}_C A_B = (\mathrm{End}\, A_B)^C$; with $\sum_j x_j \otimes_B y_j \in (A \otimes_B A)^A$ dual bases for the Frobenius homomorphism $E_{n-2} : A \to B$. Then $E_{n-1} : M_{n-1} = Ae_{n-1}A \to A$ has dual bases $t_i = t_i^1 e_{n-1} t_i^2$ and $\sum_j \beta_i(x_j) e_{n-1} y_j$, both in M_{n-1}^N. □

We note that depth n Frobenius extensions are depth $n+1$ as follows.

Lemma 8.3 (*Endomorphism Ring Lemma for D3 Towers*). *Suppose that $A|B|C$ is D3 where $A|B$ is a Frobenius extension. Let $D = \mathrm{End}\, A_B$ and $D|A$ denote the left regular mapping $a \mapsto \lambda_a$. Then the tower $D|A|C$ is D3.*

Proof. Since $A|B$ is a Frobenius extension, we note that ${}_D D_A \cong {}_D A \otimes_B A_A$ given by $d \mapsto \sum_i d(x_i) \otimes_B y_i$ in the Frobenius system notation above. Hence ${}_D D \otimes_A D_C \cong {}_D A \otimes_B A \otimes_B A_C$. To ${}_A A \otimes_B A_C \oplus * \cong {}_A A_C^m$ we apply the functor ${}_D A \otimes_B -$. We obtain after substitution, ${}_D D \otimes_A D_C \oplus * \cong {}_D D_C^m$, i.e. the tower $D|A|C$ is rD3. We have noted above Eq. (10) that $D|A|C$ is necessarily also ℓD3 since $D|A$ is a Frobenius extension. □

The next lemma argues as in Theorem 2.5.

Lemma 8.4 (*Tunneling Lemma*). *Suppose that the tower $A|B|C$ is rD3. Let $C \to B$ factor through a Frobenius extension $D \to B$ such that $A \cong \mathrm{End}\, B_D$. Then $A|D|C$ is rD3.*

Proof. We have $A \cong B \otimes_D B$, from which we obtain $A \otimes_B A \otimes_B A \cong A \otimes_D A$. Tensoring $A \otimes_B A \oplus * \cong A^n$ by $A \otimes_B -$, we obtain this fact. □

The next theorem shows that a depth $n = 2^m + 1 = 3, 5, 9, 17, \ldots$ Frobenius extension $N \hookrightarrow M$ is embedded in ("is a factor of") the depth two extension $N \hookrightarrow M_{n-2}$.

Theorem 8.5. *If $N \hookrightarrow M$ is a depth n Frobenius extension, where $n = 2^m + 1$ for a positive integer m, then $N \hookrightarrow M_{n-2}$ is a depth two Frobenius extension.*

Proof. By hypothesis, the Jones subtower $M_{n-2}|M_{n-3}|M_{-1}$ is D3. Since $M_{n-2} \cong M_{n-3} \otimes_{M_{n-4}} M_{n-3}$, it follows from the tunneling lemma that the tower $M_{n-2}|M_{n-4}|M_{-1}$ is D3. Iterating use of the lemma, also the tower $M_{n-2}|M_{n-6}|M_{-1}$ is D3. Continuing $m-1$ steps, $M_{n-2}|M_{2^{m-1}-1}|M_{-1}$ is D3. But $M_{n-2} \cong M_{2^{m-1}-1} \otimes_N M_{2^{m-1}-1}$ since $n - 2 = 2^m - 1$ (and recalling $M_i = M^{\otimes_N\, i+1}$). By Theorem 2.5 $M_{n-2}|N$ is D2. □

Suppose that a Frobenius extension $N \hookrightarrow M$ is depth n, where $2^{m-1} < n \leq 2^m$. Then by the endomorphism ring lemma this extension is also depth $2^m + 1$, so $N \hookrightarrow M_{2^m-1}$ is D2 by the theorem. This proves:

Corollary 8.6. *Any finite depth Frobenius extension $N \hookrightarrow M$ embeds into a depth two extension of N in an nth iterated endomorphism ring M_n.*

This result may be viewed as an algebraic version of a result in [20] and an answer to a question in [11, appendix]. The theory above seems to indicate that one of a variety of extensions of Jacobson–Bourbaki correspondence to pairs of simple algebras by the Japanese school of ring theory (Hirata, Müller, Onodera, Sugano, Szeto, Tominaga, and others) would adapt via depth two extensions and depth three towers to an algebraic version of the Galois theory for subfactors in Nikshych and Vainerman [20]. This will be investigated in a future paper.

Since group algebras and their finite index subgroups form Frobenius extensions, we pose the following question in character theory and group theory in extension of the discussion and results in Sections 3 and 8 of this paper.

Question: what precisely are the group-theoretic conditions on a subgroup of a finite group $H < G$ that its Frobenius algebra extension $N = \mathbb{C}[H] \subseteq M = \mathbb{C}[G]$ be depth n?

References

[1] F. Borceaux, G. Janelidze, Galois Theories, in: C.S.A.M., vol. 72, Cambridge University Press, 2001.
[2] T. Brzeziński, R. Wisbauer, Corings and Comodules, in: L.M.S., vol. 309, Cambridge University Press, 2003.
[3] G. Böhm, F. Nill, K. Szlachányi, Weak Hopf algebras, I. Integral theory and C^*-structure, J. Algebra 221 (1999) 385–438.
[4] G. Böhm, K. Szlachányi, Hopf algebroids with bijective antipodes: Axioms, integrals and duals, J. Algebra 274 (2004) 708–750.
[5] P. Etingof, D. Nikshych, Dynamical quantum groups at roots of 1, Duke Math. J. 108 (2001) 135–168.
[6] C. Greither, B. Pareigis, Hopf Galois theory for separable field extensions, J. Algebra 106 (1987) 239–258.
[7] T. Hungerford, Algebra, Holt, Rinehart & Winston, New York, 1974.
[8] N. Jacobson, Basic Algebra, II, Freeman, San Francisco, 1980.
[9] L. Kadison, New Examples of Frobenius Extensions, in: University Lect. Ser., vol. 14, AMS, 1999.
[10] L. Kadison, B. Külshammer, Depth two, normality and a trace ideal condition for Frobenius extensions, Comm. Algebra. 34 (2006) 3103–3122.
[11] L. Kadison, D. Nikshych, Frobenius extensions and weak Hopf algebras, J. Algebra 244 (2001) 312–342.
[12] L. Kadison, D. Nikshych, Hopf algebra actions on strongly separable extensions of depth two, Adv. in Math. 163 (2001) 258–286.
[13] L. Kadison, K. Szlachányi, Bialgebroid actions on depth two extensions and duality, Adv. in Math. 179 (2003) 75–121. ArXiv Preprint RA/0108067.
[14] L. Kadison, The endomorphism ring theorem for Galois and depth two extensions, J. Algebra 305 (2006) 163–184.
[15] L. Kadison, Anchor maps and stable modules in depth two, Appl. Categ. Struct., in press (doi:10.1007/s10485-006-9053-4).
[16] L. Kadison, Centralizers and induction, J. Algebra. Appl. 6 (3) (2007) 505–527.
[17] L. Kadison, Skew Hopf algebras and irreducible extensions, preprint, QA/0701427.
[18] S. Lang, Algebra, 3rd edn, Addison-Wesley, Paris, 1993.
[19] J.-H. Lu, Hopf algebroids and quantum groupoids, Internat. J. Math. 7 (1996) 47–70.
[20] D. Nikshych, L. Vainerman, A Galois correspondence for actions of quantum groupoids on II_1-factors, J. Funct. Anal. 178 (2000) 113–142.
[21] R.S. Pierce, Associative Algebras, in: G.T.M., vol. 88, Springer, Heidelberg, 1982.
[22] P. Schauenburg, Morita base change in quantum groupoids, in: Locally Compact Quantum Groups and Groupoids (Strasbourg, 2002), in: IRMA Lect. Math. Theor. Phys., vol. 2, de Gruyter, Berlin, 2003, pp. 79–103.
[23] K. Sugano, On bicommutators of modules over H-separable extension rings III, Hokkaido Math. J. 23 (1994) 277–289.
[24] M.E. Sweedler, The predual theorem to the Jacobson–Bourbaki theorem, Trans. Amer. Math. Soc. 213 (1975) 391–406.
[25] K. Szlachányi, Galois actions by finite quantum groupoids, in: Locally Compact Quantum Groups and Groupoids (Strasbourg, 2002), in: IRMA Lect. Math. Phys., vol. 2, de Gruyter, Berlin, 2003, pp. 105–125.
[26] D.J. Winter, A Galois theory of commutative rings, J. Algebra 289 (2005) 380–411.