Algebra & Number Theory

Volume 11

2017

No. 8

Quasi-Galois theory in symmetric monoidal categories

Bregje Pauwels

msp

ALGEBRA AND NUMBER THEORY 11:8 (2017)
dx.doi.org/10.2140/ant.2017.11.1891

Quasi-Galois theory in symmetric monoidal categories

Bregje Pauwels

Given a ring object A in a symmetric monoidal category, we investigate what it means for the extension $\mathbb{1} \to A$ to be (quasi-)Galois. In particular, we define splitting ring extensions and examine how they occur. Specializing to tensor-triangulated categories, we study how extension-of-scalars along a quasi-Galois ring object affects the Balmer spectrum. We define what it means for a separable ring to have constant degree, which is a necessary and sufficient condition for the existence of a quasi-Galois closure. Finally, we illustrate the above for separable rings occurring in modular representation theory.

Introduction

Classical Galois theory is the study of field extensions l/k through the group of automorphisms of l that fix k. If f is a polynomial over k, the *splitting field of f over k* is the smallest extension over which f decomposes into linear factors. If $f \in k[x]$ is moreover separable, its splitting field is the smallest extension l such that

MSC2010: primary 18BXX; secondary 16GXX, 18GXX.
Keywords: tensor triangulated category, separable, etale, Galois, ring-object, stable category.

$l \otimes_k k[x]/(f) \cong l^{\times \deg(f)}$. The field extension l/k is often called *quasi-Galois*[1] if l is the splitting field of some polynomial in $k[x]$. Then, an algebraic field extension is called *Galois* whenever it is quasi-Galois and separable.

The generalization of Galois extensions from fields to rings originated with Auslander and Goldman [1960, Appendix]; see also Remark 5.6. Grothendieck [SGA 1 1971] took on an axiomatic viewpoint to Galois theory and revealed its relation with the fundamental group. Janelidze [2001] adopted a purely categorical approach which covered the above examples. More recently, Rognes [2008] introduced a Galois theory up-to-homotopy. For more generalizations in various directions, see [Chase and Sweedler 1969; Hess 2009; Kreimer 1967].

In this paper, we adapt some of these ideas to the context of ring objects in an additive symmetric monoidal category $(\mathcal{K}, \otimes, \mathbb{1})$, with special emphasis on tensor-triangulated categories. That is, our analogue of a field extension will be a monoid $\eta : \mathbb{1} \to A$ in $\mathcal{K}$ with associative commutative multiplication $\mu : A \otimes A \to A$. We call A a *ring in* $\mathcal{K}$, and moreover assume that A is *separable*, which means μ has an (A, A)-bilinear right inverse $A \to A \otimes A$.

Separable ring objects play an important (though at times invisible) role in various areas of mathematics. In algebraic geometry, for instance, they appear as étale extensions of quasicompact and quasiseparated schemes; see [Balmer 2016a; Neeman 2015]. More precisely, given a separated étale morphism $f : V \to X$, the object $A := Rf_*(\mathcal{O}_V)$ in $D^{\mathrm{qcoh}}(X)$ is a separable ring, and we can understand $D^{\mathrm{qcoh}}(V)$ as the category of A-modules in $D^{\mathrm{qcoh}}(X)$. In representation theory, we can let $\mathcal{K}(G)$ be the (derived or stable) module category of a group G over a field $\mathbb{k}$, and consider a subgroup $H < G$ of finite index. Balmer [2015] showed there is a separable ring A^G_H in $\mathcal{K}(G)$ such that the category of A^G_H-modules in $\mathcal{K}(G)$ coincides with $\mathcal{K}(H)$, and such that the restriction functor

$$\mathrm{Res}^G_H : \mathcal{K}(G) \to \mathcal{K}(H)$$

is just extension-of-scalars along A^G_H. In the same vein, extension-of-scalars along a separable ring recovers restriction to a subgroup in equivariant stable homotopy theory, in equivariant KK-theory and in equivariant derived categories; see [Balmer et al. 2015]. For more examples of separable rings in stable homotopy categories, we refer to [Baker and Richter 2008; Rognes 2008].

Thus motivated, we study how much Galois theory carries over. Recall that a ring A in $\mathcal{K}$ is *indecomposable* if it does not decompose as a product of nonzero rings. Separable ring objects have a well-behaved notion of degree [Balmer 2014] and our first Galois-flavored result (Theorem 4.5) shows that the number of ring endomorphisms of a separable indecomposable ring in $\mathcal{K}$ is bounded by its degree.

[1] see [Bourbaki 1981, V.9.3]. In the literature, a quasi-Galois extension is sometimes called normal or Galois, probably because these notions coincide when l/k is separable and finite.

Definition. Let A and B be separable rings of finite degree in $\mathcal{K}$. We say B *splits* A if $B \otimes A \cong B^{\times \deg(A)}$ as (left) B-algebras in $\mathcal{K}$. We call an indecomposable ring B a *splitting ring of* A if B splits A and any ring morphism $C \to B$, where C is an indecomposable ring splitting A, is an isomorphism.

Definition. If A is a ring in $\mathcal{K}$ and Γ is a group of ring automorphisms of A, we call A *quasi-Galois in* $\mathcal{K}$ *with group* Γ if the A-algebra homomorphism

$$\lambda_\Gamma : A \otimes A \to \prod_{\gamma \in \Gamma} A$$

defined by $\mathrm{pr}_\gamma \lambda_\Gamma = \mu(1 \otimes \gamma)$ is an isomorphism.

Under mild conditions on $\mathcal{K}$, Corollary 6.10 shows an indecomposable ring B is quasi-Galois in $\mathcal{K}$ for some group Γ if and only if B is a splitting ring of some separable ring A in $\mathcal{K}$. By Theorem 5.9, this happens exactly when B has $\deg(B)$ distinct ring endomorphisms in $\mathcal{K}$. Moreover, Proposition 6.9 shows that every separable ring in $\mathcal{K}$ has (possibly multiple) splitting rings. In particular, l is a splitting field of a separable polynomial f over k if and only if l is a splitting ring of $k[x]/(f)$ in the category k-mod; our terminology matches classical field theory.

If, in addition, we assume that $\mathcal{K}$ is tensor-triangulated, we can say more about the way splitting rings arise. Balmer [2005] introduced a topological space $\mathrm{Spc}(\mathcal{K})$ associated to $\mathcal{K}$, in which every object $x \in \mathcal{K}$ has a support $\mathrm{supp}(x) \subset \mathrm{Spc}(\mathcal{K})$. The *Balmer spectrum* $\mathrm{Spc}(\mathcal{K})$ provides an algebro-geometric approach to the study of triangulated categories, and a complete description of the spectrum is equivalent to a classification of the thick $\otimes$-ideals in the category.

For the remainder of the introduction, we assume $\mathcal{K}$ is tensor-triangulated and nice (say, $\mathrm{Spc}(\mathcal{K})$ is noetherian or $\mathcal{K}$ satisfies Krull–Schmidt). If A is a separable ring in $\mathcal{K}$, the *Eilenberg–Moore category* $A\text{-Mod}_{\mathcal{K}}$ of A-modules in $\mathcal{K}$ admits a triangulation such that extension-of-scalars $\mathcal{K} \to A\text{-Mod}_{\mathcal{K}}$ is exact; see [Balmer 2011, Corollary 4.3]. We can thus extend scalars along a separable ring without leaving the tensor-triangulated world or descending to a model category. If A is quasi-Galois with group Γ in $\mathcal{K}$, then Γ acts on $A\text{-Mod}_{\mathcal{K}}$ and on the spectrum $\mathrm{Spc}(A\text{-Mod}_{\mathcal{K}})$. By Theorem 9.1, the Γ-orbits of $\mathrm{Spc}(A\text{-Mod}_{\mathcal{K}})$ are given by $\mathrm{supp}(A) \subset \mathrm{Spc}(\mathcal{K})$. In particular, we recover $\mathrm{Spc}(\mathcal{K})$ from $\mathrm{Spc}(A\text{-Mod}_{\mathcal{K}})$ if $\mathrm{supp}(A) = \mathrm{Spc}(\mathcal{K})$, which happens exactly when $A \otimes f = 0$ implies f is $\otimes$-nilpotent for every morphism f in $\mathcal{K}$.

Recall that for a quasi-Galois field extension l/k, any irreducible polynomial $f \in k[x]$ with a root in l splits in l; see [Bourbaki 1981, V.9.3]. Proposition 9.6 provides us with a tensor triangular analogue:

Proposition. Let A be a separable ring in $\mathcal{K}$ such that the spectrum $\mathrm{Spc}(A\text{-Mod}_{\mathcal{K}})$ is connected, and suppose B is an A-algebra with $\mathrm{supp}(A) = \mathrm{supp}(B)$. If B is quasi-Galois in $\mathcal{K}$, then B splits A.

Finally, Theorem 9.7 reveals which separable rings have a *quasi-Galois closure* in $\mathcal{K}$. Given $\mathcal{P} \in \mathrm{Spc}(\mathcal{K})$, we consider *the local category* $\mathcal{K}_{\mathcal{P}}$ *at* $\mathcal{P}$, the idempotent completion of the Verdier quotient $\mathcal{K}/\mathcal{P}$. We say a ring A has *constant degree in* $\mathcal{K}$ if the degree of A as a ring in $\mathcal{K}_{\mathcal{P}}$ is the same for every prime $\mathcal{P} \in \mathrm{supp}(A)$.

Theorem. If A has constant degree in $\mathcal{K}$ and the spectrum $\mathrm{Spc}(A\text{-Mod}_{\mathcal{K}})$ is connected, then A has a unique splitting ring A^*. Furthermore, $\mathrm{supp}(A) = \mathrm{supp}(A^*)$ and A^* is the quasi-Galois closure of A in $\mathcal{K}$. That is, for any A-algebra B that is quasi-Galois in $\mathcal{K}$ with $\mathrm{supp}(A) = \mathrm{supp}(B)$, there exists a ring morphism $A^* \to \mathrm{B}$.

We conclude this paper by computing degrees and splitting rings for the separable rings $A^G_H := \Bbbk(G/H)$ mentioned above. Here, $H < G$ are finite groups and $\Bbbk$ is a field with characteristic p dividing $|G|$. The degree of A^G_H in $\mathrm{D}^b(\Bbbk G\text{-mod})$ is simply $[G : H]$ and A^G_H is quasi-Galois if and only if H is normal in G. Accordingly, the quasi-Galois closure of A^G_H in $\mathrm{D}^b(\Bbbk G\text{-mod})$ is the ring A^G_N, where N is the normal core of H in G (see Corollary 10.11). On the other hand, Proposition 10.13 shows the degree of A^G_H in $\Bbbk G$-stab is the greatest $0 \le n \le [G : H]$ such that there exist distinct $[g_1], \dots, [g_n]$ in $H\backslash G$ with p dividing $|H^{g_1} \cap \dots \cap H^{g_n}|$. In that case, the splitting rings of A^G_H are exactly the $A^G_{H^{g_1}\cap\dots\cap H^{g_n}}$ with $g_1, \dots, g_n$ as above.

1. The Eilenberg–Moore category

Definition 1.1. Let $\mathcal{K}$ be an additive category. We say $\mathcal{K}$ is *idempotent-complete* if for all $x \in \mathcal{K}$, any morphism $e : x \to x$ with $e^2 = e$ yields a decomposition $x \cong x_1 \oplus x_2$ under which e becomes $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$. Every additive category $\mathcal{K}$ can be embedded in an idempotent-complete category $\mathcal{K}^\natural$ in such a way that $\mathcal{K} \hookrightarrow \mathcal{K}^\natural$ is fully faithful and every object in $\mathcal{K}^\natural$ is a direct summand of some object in $\mathcal{K}$. We call $\mathcal{K}^\natural$ the *idempotent-completion* of $\mathcal{K}$, and [Balmer and Schlichting 2001] shows that $\mathcal{K}^\natural$ stays triangulated if $\mathcal{K}$ was.

Notation 1.2. Throughout, $(\mathcal{K}, \otimes, \mathbb{1})$ denotes an idempotent-complete symmetric monoidal category. For objects $x_1, \dots, x_n$ in $\mathcal{K}$ and a permutation $\tau \in S_n$, we also write $\tau : x_1 \otimes \dots \otimes x_n \to x_{\tau(1)} \otimes \dots \otimes x_{\tau(n)}$ to denote the isomorphism that permutes the tensor factors.

Definition 1.3. A *ring object* $A \in \mathcal{K}$ is a monoid $(A,\ \mu : A \otimes A \to A,\ \eta : \mathbb{1} \to A)$ with associative multiplication μ and two-sided unit η. We call A *commutative* if $\mu(12) = \mu$. All ring objects in this paper will be commutative and we often simply call A a *ring in* $\mathcal{K}$. For rings A and B in $\mathcal{K}$, a *ring morphism* $f : A \to B$ is a morphism in $\mathcal{K}$ that is compatible with the ring structure.

A *(left) A-module* is a pair $(x \in \mathcal{K},\ \varrho : A \otimes x \to x)$, where the action ϱ is compatible with the ring structure in the usual way. *Right A-modules* as well as *(A, A)-bimodules* are defined analogously.

The *Eilenberg–Moore category* $A\text{-Mod}_{\mathcal{K}}$ has left A-modules as objects and A-linear morphisms, which are defined in the usual way. See [Eilenberg and Moore 1965] or [Mac Lane 1998, Chapter VI] for more details. Every object $x \in \mathcal{K}$ gives rise to a *free A-module* $F_A(x) = A \otimes x$ with action given by

$$\varrho : A \otimes A \otimes x \xrightarrow{\mu \otimes 1} A \otimes x.$$

We call the functor $F_A : \mathcal{K} \to A\text{-Mod}_{\mathcal{K}}$ *the extension-of-scalars*, and write U_A for its forgetful right adjoint:

$$\begin{tikzcd} \mathcal{K} \arrow[d, shift right, "F_A"'] \arrow[d, phantom, "\dashv"] \\ A\text{-Mod}_{\mathcal{K}} \arrow[u, shift right, "U_A"'] \end{tikzcd}$$

A ring A in $\mathcal{K}$ is *separable* if the multiplication map μ has an (A, A)-bilinear section $\sigma : A \to A \otimes A$. That is, $\mu\sigma = 1_A$ and the diagram

$$\begin{tikzcd} & A \otimes A \arrow[dl, "\sigma \otimes 1"'] \arrow[d, "\mu"] \arrow[dr, "1 \otimes \sigma"] & \\ A \otimes A \otimes A \arrow[dr, "1 \otimes \mu"'] & A \arrow[d, "\sigma"] & A \otimes A \otimes A \arrow[dl, "\mu \otimes 1"] \\ & A \otimes A & \end{tikzcd}$$

commutes.

Remark 1.4. The module category $A\text{-Mod}_{\mathcal{K}}$ is idempotent-complete whenever $\mathcal{K}$ is idempotent-complete.

Example 1.5. Let R be a commutative ring and consider the category R-mod of finitely generated R-modules. Let A be a commutative projective R-algebra and suppose A is *separable over R*, that is A is projective as an $A \otimes_R A$-module. Then A is finitely generated as an R-module by [DeMeyer and Ingraham 1971, Proposition 2.2.1], so A defines a separable ring object in R-mod. On the other hand, we can think of $A = A[0]$ as a separable ring object in $\mathrm{D}^{\mathrm{perf}}(R)$, the homotopy category of bounded complexes of finitely generated projective R-modules. Note that the category of A-modules in $\mathrm{D}^{\mathrm{perf}}(R)$ is equivalent to $\mathrm{D}^{\mathrm{perf}}(A)$ by [Balmer 2011, Theorem 6.5].

Notation 1.6. Let A and B be rings in $\mathcal{K}$. The ring structure on $A \otimes B$ is given by $(\mu_A \otimes \mu_B)(23) : (A \otimes B)^{\otimes 2} \to (A \otimes B)$. We write A^e for the enveloping ring $A \otimes A^{\mathrm{op}}$, so that left A^e-modules are just (A, A)-bimodules. We write $A \times B$ for the ring $A \oplus B$ with componentwise multiplication.

Remark 1.7. If A and B are separable rings in $\mathcal{K}$, then so are A^e, $A \otimes B$ and $A \times B$. Conversely, A and B are separable whenever $A \times B$ is separable.

Remark 1.8. Let A be a ring in $\mathcal{K}$. Note that every (left) A-linear endomorphism $A \to A$ is in fact A^e-linear, by commutativity of A. What is more, any two A-linear endomorphisms $A \to A$ commute.

Definition 1.9. We call a nonzero ring A in $\mathcal{K}$ *indecomposable* if the only idempotent A-linear endomorphisms $A \to A$ in $\mathcal{K}$ are the identity 1_A and 0. In other words, A is indecomposable if it does not decompose as a direct sum of nonzero A^e-modules. By the following lemma, this is equivalent to saying A does not decompose as a product of nonzero rings.

Lemma 1.10 [Balmer 2014, Lemma 2.2]. *Let A be a ring in $\mathcal{K}$. Suppose there is an A^e-linear isomorphism $h : A \xrightarrow{\sim} B \oplus C$ for some A^e-modules B, C in $\mathcal{K}$. Then B and C admit unique ring structures under which h becomes a ring isomorphism $h : A \xrightarrow{\sim} B \times C$.*

Let (A, μ, η) be a separable ring in $\mathcal{K}$ with separability morphism σ. In what follows, we define a tensor structure $\otimes_A$ on $A\text{-Mod}_{\mathcal{K}}$ under which extension-of-scalars becomes monoidal. The following results all appear in [Balmer 2014, §1]. For detailed proofs, see [Pauwels 2015, §1.1]. Let (x, ϱ_1) and (y, ϱ_2) be A-modules. Here, we can write ϱ_1 to indicate both a left and right action of A on x, as A is commutative. Seeing how the endomorphism $\upsilon : x \otimes y \to x \otimes y$ given by

$$x \otimes y \xrightarrow{1\otimes\eta\otimes1} x \otimes A \otimes y \xrightarrow{1\otimes\sigma\otimes1} x \otimes A \otimes A \otimes y \xrightarrow{\varrho_1\otimes\varrho_2} x \otimes y$$

is idempotent and $\mathcal{K}$ is idempotent-complete, we can define $x \otimes_A y$ as the direct summand $\operatorname{im}(\upsilon)$ of $x \otimes y$. Note that $x \otimes_A y$ is independent, up to canonical isomorphism, of the choice of separability section σ. We get a split coequalizer in $\mathcal{K}$,

$$x \otimes A \otimes y \underset{1\otimes\varrho_2}{\overset{\varrho_1\otimes1}{\rightrightarrows}} x \otimes y \twoheadrightarrow x \otimes_A y,$$

and A acts on $x \otimes_A y$ by

$$A \otimes x \otimes_A y \hookrightarrow A \otimes x \otimes y \xrightarrow{\varrho_1\otimes1} x \otimes y \twoheadrightarrow x \otimes_A y.$$

Proposition 1.11. *The tensor product $\otimes_A$ yields a symmetric monoidal structure on $A\text{-Mod}_{\mathcal{K}}$ under which F_A becomes monoidal. We will write $\mathbb{1}_A = A$ for the unit object in $A\text{-Mod}_{\mathcal{K}}$.*

Notation 1.12. If A and B are rings in $\mathcal{K}$ and $h : A \to B$ is a ring morphism, we say that B is an *A-algebra*. As usual, we equip B with the A-module structure given by

$$A \otimes B \xrightarrow{h\otimes1} B \otimes B \xrightarrow{\mu_B} B,$$

and we write $\bar{B}$ for the corresponding object in $A\text{-Mod}_{\mathcal{K}}$, so that $B = U_A(\bar{B})$.

Remark 1.13. Let A be a separable ring in $\mathcal{K}$. There is a one-to-one correspondence between A-algebras B in $\mathcal{K}$ and rings $\bar{B}$ in $A\text{-Mod}_{\mathcal{K}}$. More precisely, if (B, μ, η) is a ring in $\mathcal{K}$ and $h : A \to B$ is a ring morphism, then $(\bar{B},\ \bar{\mu},\ \bar{\eta} := h)$ defines a ring in $A\text{-Mod}_{\mathcal{K}}$, with $\mu : B \otimes B \twoheadrightarrow B \otimes_A B \xrightarrow{\bar{\mu}} B$. Moreover, B is separable in $\mathcal{K}$ if and only if $\bar{B}$ is separable in $A\text{-Mod}_{\mathcal{K}}$.

Remark 1.14. Let A be a separable ring in $\mathcal{K}$ and suppose B is an A-algebra via $h : A \to B$. For every A-module x, we let B act on the left factor of $F_h(x) := \bar{B} \otimes_A x$ as usual. This defines a functor $F_h : A\text{-Mod}_{\mathcal{K}} \to B\text{-Mod}_{\mathcal{K}}$ and the following diagram commutes up to isomorphism:

$$\begin{tikzcd} & \mathcal{K} \arrow[dl, "F_A"'] \arrow[dr, "F_B"] & \\ A\text{-Mod}_{\mathcal{K}} \arrow[rr, "F_h"] & & B\text{-Mod}_{\mathcal{K}} \end{tikzcd}$$

Note also that $F_{gh} \cong F_g F_h$ for any ring morphism $g : B \to C$.

Proposition 1.15. *Let A be a separable ring in $\mathcal{K}$ and suppose B is a separable A-algebra, say $\bar{B} \in \mathcal{L} := A\text{-Mod}_{\mathcal{K}}$. There is an equivalence $B\text{-Mod}_{\mathcal{K}} \simeq \bar{B}\text{-Mod}_{\mathcal{L}}$ of symmetric monoidal categories such that*

$$\begin{tikzcd} \mathcal{K} \arrow[r, "F_A"] \arrow[d, "F_B"] & \mathcal{L} \arrow[d, "F_{\bar{B}}"] \\ B\text{-Mod}_{\mathcal{K}} \arrow[r, "\simeq"] & \bar{B}\text{-Mod}_{\mathcal{L}}, \end{tikzcd}$$

commutes up to isomorphism.

2. Separable rings

Proposition 2.1. *Let A be a separable ring in $\mathcal{K}$. If $A \cong B \times C$ for rings B, C in $\mathcal{K}$, then any indecomposable ring factor of A is a ring factor of B or C. In particular, if A can be written as a product of indecomposable A-algebras $A \cong A_1 \times \cdots \times A_n$, this decomposition is unique up to isomorphism.*

Proof. Suppose $A_1 \in \mathcal{K}$ is an indecomposable ring factor of A, say $A \cong A_1 \times A_2$ for some ring A_2 in $\mathcal{K}$. The category $A\text{-Mod}_{\mathcal{K}}$ decomposes as

$$A\text{-Mod}_{\mathcal{K}} \cong A_1\text{-Mod}_{\mathcal{K}} \times A_2\text{-Mod}_{\mathcal{K}},$$

with $\mathbb{1}_A$ corresponding to $(\mathbb{1}_{A_1}, \mathbb{1}_{A_2})$. Accordingly, the A-algebras $\bar{B}$ and $\bar{C}$ correspond to (B_1, B_2) and (C_1, C_2) respectively, with B_i, C_i in $A_i\text{-Mod}_{\mathcal{K}}$ for $i = 1, 2$, such that $\bar{B} \cong B_1 \times B_2$ and $\bar{C} \cong C_1 \times C_2$ in $A\text{-Mod}_{\mathcal{K}}$. Given that $\mathbb{1}_A \cong \bar{B} \times \bar{C}$, we see $\mathbb{1}_{A_1} \cong B_1 \times C_1$, hence $A_1 \cong B_1$ or $A_1 \cong C_1$. $\square$

Lemma 2.2. *Let A be a separable ring in $\mathcal{K}$.*

(a) *For every ring morphism $\alpha : A \to \mathbb{1}$, there exists a unique idempotent A-linear morphism $e : A \to A$ such that $\alpha e = \alpha$ and $e\eta\alpha = e$.*

(b) *Suppose $\mathbb{1}$ is indecomposable. If $\alpha_i : A \to \mathbb{1}$ are distinct ring morphisms for $1 \leq i \leq n$, with corresponding idempotent morphisms $e_i : A \to A$ as above, then $e_i e_j = \delta_{i,j} e_i$ and $\alpha_i e_j = \delta_{i,j}\alpha_i$.*

Proof. Let σ be a separability morphism for A. To show (a), consider the A-linear map $e := (\alpha \otimes 1)\sigma : A \to A$. We immediately see that $\alpha e = \alpha(\alpha \otimes 1)\sigma = \alpha\mu\sigma = \alpha$. Idempotence of e follows from the diagram

$$\begin{tikzcd}
A \arrow[r, "\sigma"] \arrow[dd, equal] & A \otimes A \arrow[r, "\alpha\otimes 1"] \arrow[d, "1\otimes\sigma"] & A \arrow[d, "\sigma"] \\
& A \otimes A \otimes A \arrow[r, "\alpha\otimes 1\otimes 1"] \arrow[d, "\mu\otimes 1"] & A \otimes A \arrow[d, "\alpha\otimes 1"] \\
A \arrow[r, "\sigma"] & A \otimes A \arrow[r, "\alpha\otimes 1"] & A
\end{tikzcd}$$

in which the left square commutes by bilinearity of σ. Seeing how

$$\begin{tikzcd}
A \arrow[r, "\alpha"] \arrow[d, "1\otimes\eta"] & \mathbb{1} \arrow[r, "\eta"] & A \arrow[d, "\sigma"] \\
A \otimes A \arrow[r, "1\otimes\sigma"] \arrow[d, "\mu"] & A \otimes A \otimes A \arrow[r, "\alpha\otimes 1\otimes 1"] \arrow[d, "\mu\otimes 1"] & A \otimes A \arrow[d, "\alpha\otimes 1"] \\
A \arrow[r, "\sigma"] & A \otimes A \arrow[r, "\alpha\otimes 1"] & \mathbb{1} \otimes A
\end{tikzcd}$$

commutes, we moreover get $e\eta\alpha = e$. Suppose e' is also an A-linear morphism with $\alpha e' = \alpha$ and $e'\eta\alpha = e'$. Then, $e = e\eta\alpha = e\eta\alpha e' = ee' = e'e = e'\eta\alpha e = e'\eta\alpha = e'$ by Remark 1.8. For (b), let $1 \leq i, j \leq n$. From the commuting diagram

$$\begin{tikzcd}
A \arrow[r, "\alpha_i"] \arrow[d, "1\otimes\eta"] & \mathbb{1} \arrow[r, "\eta"] & A \arrow[d, "e_j"] \\
A \otimes A \arrow[r, "1\otimes e_j"] \arrow[d, "\mu"] & A \otimes A \arrow[r, "\alpha_i\otimes 1"] \arrow[d, "\mu"] & A \arrow[d, "\alpha_i"] \\
A \arrow[r, "e_j"] & A \arrow[r, "\alpha_i"] & \mathbb{1},
\end{tikzcd}$$

we see that $\alpha_i e_j \eta \alpha_i = \alpha_i e_j$. Hence, $(\alpha_i e_j \eta)(\alpha_i e_j \eta) = \alpha_i e_j e_j \eta = \alpha_i e_j \eta$, so the morphism $\alpha_i e_j \eta : \mathbb{1} \to \mathbb{1}$ is idempotent and equals 0 or $1_{\mathbb{1}}$. In the first case, $\alpha_i e_j = \alpha_i e_j \eta \alpha_j = 0$ and $e_i e_j = e_i \eta \alpha_i e_j = 0$, in particular $i \neq j$. On the other hand, if $\alpha_i e_j \eta = 1_{\mathbb{1}}$ we get $\alpha_i e_j = \alpha_i e_j \eta \alpha_i = \alpha_i$ and $\alpha_i e_j = \alpha_i e_j \eta \alpha_j = \alpha_j$, so $i = j$. $\square$

Lemma 2.3. *Let (A, μ_A, η_A) and (B, μ_B, η_B) be separable rings in $\mathcal{K}$.*

(a) *Suppose $f : A \to B$ and $g : B \to A$ are ring morphisms such that $gf = 1_A$. We equip A with the structure of B^e-module via the morphism g. There exists a B^e-linear morphism $\tilde{f} : A \to B$ such that $g\tilde{f} = 1_A$. In particular, A is a direct summand of B as a B^e-module.*

(b) *Suppose A is indecomposable. Let $g_i : B \to A$ be distinct ring morphisms for $1 \leq i \leq n$ and suppose $f : A \to B$ is a ring morphism with $g_i f = 1_A$. Then $A^{\oplus n}$ is a direct summand of B as a B^e-module, with projections $g_i : B \to A$ for $1 \leq i \leq n$.*

Proof. Considering the A-module structure on B given by f, we note that $g : B \to A$ is A-linear:

$$\begin{tikzcd} A \otimes B \arrow[r, "f\otimes 1"] \arrow[d, "1\otimes g"] & B \otimes B \arrow[r, "\mu_B"] \arrow[d, "g\otimes g"] & B \arrow[d, "g"] \\ A \otimes A \arrow[r, equal] & A \otimes A \arrow[r, "\mu_A"] & A \end{tikzcd}$$

We can thus apply Lemma 2.2 to the ring morphism $\bar{g} : \bar{B} \to \mathbb{1}_A$ in A-$\mathrm{Mod}_{\mathcal{K}}$ and find an idempotent $\bar{B}^e$-linear morphism $\bar{e} : \bar{B} \to \bar{B}$ such that $\bar{g}\bar{e} = \bar{g}$ and $\bar{e}\eta_{\bar{B}}\bar{g} = \bar{e}$. Forgetting the A-action, $U_A(\bar{e}) := e : B \to B$ is idempotent and B^e-linear, with $ge = g$ and $efg = e$. Let $\tilde{f} := ef$. We need to show that $\tilde{f}$ is B^e-linear, where B^e acts on A via g. Left B-linearity of $\tilde{f}$ follows from the commuting diagram

$$\begin{tikzcd} B \otimes A \arrow[r, "g\otimes 1"] \arrow[dd, "1\otimes f"] & A \otimes A \arrow[r, "\mu_A"] \arrow[d, "f\otimes f"] & A \arrow[d, "f"] \\ & B \otimes B \arrow[r, "\mu_B"] \arrow[d, "e\otimes 1"] & B \arrow[d, "e"] \\ B \otimes B \arrow[r, "e\otimes 1"] \arrow[d, "1\otimes e"] & B \otimes B \arrow[r, "\mu_B"] & B \arrow[d, equal] \\ B \otimes B \arrow[rr, "\mu_B"] & & B \end{tikzcd}$$

and right B-linearity follows similarly. Finally, $g\tilde{f} = gef = gf = 1_A$.

For (b), let $g_i : B \to A$ be distinct ring morphisms with $g_i f = 1_A$ for $1 \leq i \leq n$. As in part (a), we find idempotent B^e-linear morphisms $e_i : B \to B$ and B^e-linear morphisms $\tilde{f}_i := e_i f$ with $g_i \tilde{f}_i = 1_A$ and $e_i = \tilde{f}_i g_i$. In fact, Lemma 2.2(b) shows the e_i are orthogonal. Seeing how $A = \mathrm{im}(e_i)$, we conclude $A^{\oplus n}$ is a direct summand of B as a B^e-module, with projections $g_i : B \to A$ for $1 \leq i \leq n$. $\square$

Corollary 2.4. *Let A and B be separable rings in $\mathcal{K}$ and suppose B is an A-algebra. The corresponding ring $\bar{B}$ in A-$\mathrm{Mod}_{\mathcal{K}}$ is a ring factor of $F_A(B)$.*

Proof. Applying Lemma 2.3 to the ring morphisms $f : B \xrightarrow{\eta_A \otimes 1_B} A \otimes B$ and g given by the action of A on B, we see that B is a direct summand of $A \otimes B$ as $(A \otimes B)^e$-modules in $\mathcal{K}$. In particular, $\bar{B}$ is a direct summand of $F_A(B)$ as $F_A(B)^e$-modules in A-$\mathrm{Mod}_{\mathcal{K}}$. By Lemma 1.10, $\bar{B}$ admits a ring structure under which $\bar{B}$ becomes a ring factor of $F_A(B)$. This new ring structure on $\bar{B}$ is the original one, seeing how the projection $g : F_A(B) \to \bar{B}$ is a ring morphism for both structures. □

3. Degree of a separable ring

We recall Balmer's definition [2014] of the degree of a separable ring in a tensor-triangulated category, and show the definition works for any idempotent-complete symmetric monoidal category $\mathcal{K}$.

Theorem 3.1. *Let A and B be separable rings in $\mathcal{K}$. Suppose $f : A \to B$ and $g : B \to A$ are ring morphisms such that $gf = 1_A$. There exists a separable ring C in $\mathcal{K}$ and a ring isomorphism $h : B \xrightarrow{\sim} A \times C$ such that $\mathrm{pr}_1 h = g$. If we equip C with the A-algebra structure coming from $\mathrm{pr}_2 hf$, it is unique up to isomorphism of A-algebras.*

Proof. This proposition is proved in [Balmer 2014, Theorem 2.4] when $\mathcal{K}$ is a tensor-triangulated category. In our case, Lemma 2.3 yields an isomorphism $h : B \xrightarrow{\sim} A \oplus C$ of B^e-modules with $\mathrm{pr}_1 h = g$. By Lemma 1.10, A and C admit ring structures under which h becomes a ring isomorphism. This new ring structure on A is the original one, seeing how

$$1_A : A \xrightarrow{f} B \xrightarrow{\mathrm{pr}_1 h} A$$

is a ring morphism. The rest of the proof is identical to the proof in [loc. cit.]. □

Definition 3.2 [Balmer 2014, Definition 3.1]. Let (A, μ, η) be a separable ring in $\mathcal{K}$. Applying Theorem 3.1 to the ring morphisms $f = 1_A \otimes \eta : A \to A \otimes A$ and $g = \mu : A \otimes A \to A$, we find a separable A-algebra A', unique up to isomorphism, and a ring isomorphism $h : A \otimes A \xrightarrow{\sim} A \times A'$ such that $\mathrm{pr}_1 h = \mu$.

The *splitting tower*

$$\mathbb{1} = A^{[0]} \xrightarrow{\eta} A = A^{[1]} \to A^{[2]} \to \cdots \to A^{[n]} \to A^{[n+1]} \to \cdots$$

is defined inductively by $A^{[n+1]} = (A^{[n]})'$, where we consider $A^{[n]}$ as a ring in $A^{[n-1]}$-$\mathrm{Mod}_{\mathcal{K}}$. We say the *degree* of A is d, writing $\deg_{\mathcal{K}}(A) = d$, if $A^{[d]} \neq 0$ and $A^{[d+1]} = 0$. We say A has *infinite degree* if $A^{[d]} \neq 0$ for all $d \geq 0$.

Remark 3.3. By construction, we have $(A^{[n]})^{[m+1]} \cong A^{[n+m]}$ as $A^{[n+m-1]}$-algebras for all $m \geq 0$ and $n \geq 1$, where we regard $A^{[n]}$ as a ring in $A^{[n-1]}$-$\mathrm{Mod}_{\mathcal{K}}$. In other words, $\deg_{A^{[n-1]}\text{-}\mathrm{Mod}_{\mathcal{K}}}(A^{[n]}) = \deg_{\mathcal{K}}(A) - n + 1$ for $1 \leq n \leq \deg_{\mathcal{K}}(A) + 1$.

Example 3.4. Let R be a commutative ring and suppose A is a commutative projective separable R-algebra. If $\operatorname{Spec} R$ is connected, then the degree of A as a ring in $\mathrm{D}^{\mathrm{perf}}(R)$ (see Example 1.5) recovers its rank as an R-module. This will follow from Proposition 7.9.

Proposition 3.5. *Let A and B be separable rings in $\mathcal{K}$.*

(a) *We have $F_{A^{[n]}}(A) \cong \mathbb{1}_{A^{[n]}}^{\times n} \times A^{[n+1]}$ as $A^{[n]}$-algebras.*

(b) *Let $F : \mathcal{K} \to L$ be an additive monoidal functor. For every $n \geq 0$, the rings $F(A^{[n]})$ and $F(A)^{[n]}$ are isomorphic. In particular, $\deg_{\mathcal{L}}(F(A)) \leq \deg_{\mathcal{K}}(A)$.*

(c) *Suppose A is a B-algebra. Then $\deg_{B\text{-}\mathrm{Mod}_{\mathcal{K}}}(F_B(A)) = \deg_{\mathcal{K}}(A)$.*

Proof. The proofs for (a) and (b) in [op. cit., Theorems 3.7 and 3.9] still hold in our (not necessarily triangulated) setting. To prove (c), note that $A^{[n]}$ is a B-algebra and hence a direct summand of $F_B(A^{[n]}) \cong F_B(A)^{[n]}$. This means $F_B(A)^{[n]} \neq 0$ when $A^{[n]} \neq 0$ so that $\deg_{B\text{-}\mathrm{Mod}_{\mathcal{K}}}(F_B(A)) \geq \deg_{\mathcal{K}}(A)$. $\square$

Lemma 3.6 [Balmer 2014, Lemma 3.11]. *Let $n \geq 1$ and $A := \mathbb{1}^{\times n} \in \mathcal{K}$. There is an isomorphism $A^{[2]} \cong A^{\times(n-1)}$ of A-algebras.*

Proof. We prove there is an A-algebra isomorphism $\lambda : A \otimes A \xrightarrow{\sim} A \times A^{\times(n-1)}$ with $\mathrm{pr}_1 \lambda = \mu_A$. We write $A = \prod_{i=0}^{n-1} \mathbb{1}_i$, $A \otimes A = \prod_{0 \leq i,j \leq n-1} \mathbb{1}_i \otimes \mathbb{1}_j$ and $A^{\times n} = \prod_{k=0}^{n-1} \prod_{i=0}^{n-1} \mathbb{1}_{ik}$ with $\mathbb{1} = \mathbb{1}_i = \mathbb{1}_{ik}$ for all i, k. Define $\lambda : A \otimes A \to A^{\times n}$ by mapping the factor $\mathbb{1}_i \otimes \mathbb{1}_j$ identically to $\mathbb{1}_{i(i-j)}$, with indices in $\mathbb{Z}_n$. Then, λ is an A-algebra isomorphism and $\mathrm{pr}_{k=0} \lambda = \mu_A$. $\square$

Corollary 3.7. *Let $n \geq 1$. Then $\deg_{\mathcal{K}}(\mathbb{1}^{\times n}) = n$ and $(\mathbb{1}^{\times n})^{[n]} \cong \mathbb{1}^{\times n!}$ in $\mathcal{K}$.*

Proof. Let $A := \mathbb{1}^{\times n}$. The result is clear when $n = 1$, and we proceed by induction on n. By Lemma 3.6, we know $A^{[2]} \cong \mathbb{1}_A^{\times(n-1)}$ in $A\text{-}\mathrm{Mod}_{\mathcal{K}}$. Assuming the induction hypothesis, $\deg_{A\text{-}\mathrm{Mod}_{\mathcal{K}}}(A^{[2]}) = n - 1$ and

$$A^{[n]} \cong (A^{[2]})^{[n-1]} \cong \mathbb{1}_A^{\times(n-1)!} \cong (\mathbb{1}^{\times n})^{\times(n-1)!} \cong \mathbb{1}^{\times n!}. \qquad \square$$

Lemma 3.8. *Let A and B be separable rings of finite degree in $\mathcal{K}$. Then,*

(a) $\deg(A \times B) \leq \deg(A) + \deg(B)$

(b) $\deg(A \times \mathbb{1}^{\times n}) = \deg(A) + n$

(c) $\deg(A^{\times t}) = \deg(A) \cdot t$.

Proof. To prove (a), let $n := \deg(A \times B)$ and $C := (A \times B)^{[n]}$. Writing $A' := F_C(A)$ and $B' := F_C(B)$, we know from Proposition 3.5(a) that

$$A' \times B' = F_C(A \times B) \cong \mathbb{1}_C^{\times n}.$$

If we let $D := (A')^{[\deg(A')]}$ and apply F_D to the isomorphism, we get

$$\mathbb{1}_D^{\times \deg(A')} \times F_D(B') \cong \mathbb{1}_D^{\times n}.$$

Similarly, putting $E := (F_D(B'))^{[\deg(F_D(B'))]}$ and applying F_E gives

$$\mathbb{1}_E^{\times \deg(A')} \times \mathbb{1}_E^{\times \deg(F_D(B'))} \cong \mathbb{1}_E^{\times n}.$$

This shows $n = \deg(A') + \deg(F_D(B')) \leq \deg(A) + \deg(B)$ by Proposition 3.5(b). For (b), let $B := A^{[\deg(A)]}$. Then, $F_B(A \times \mathbb{1}^{\times n}) \cong \mathbb{1}_B^{\times \deg(A)} \times \mathbb{1}_B^{\times n}$ and we find

$$\deg(A \times \mathbb{1}^{\times n}) \geq \deg(F_B(A \times \mathbb{1}^{\times n})) = \deg(A) + n.$$

To prove (c), we write $B := A^{[\deg(A)]}$ again and note that $F_B(A^{\times t}) \cong (\mathbb{1}_B^{\times \deg(A)})^{\times t}$. Hence, $\deg(A^{\times t}) \geq \deg(F_B(A^{\times t})) = \deg(A) \cdot t$. □

4. Counting ring morphisms

Lemma 4.1. *Let A be a separable ring in $\mathcal{K}$ and suppose $\mathbb{1}$ is indecomposable. If there are n distinct ring morphisms $A \to \mathbb{1}$, then A has $\mathbb{1}^{\times n}$ as a ring factor. In particular, there are at most* $\deg A$ *distinct ring morphisms $A \to \mathbb{1}$.*

Proof. Let $\alpha_i : A \to \mathbb{1}$ be distinct ring morphisms for $1 \leq i \leq n$. By Lemma 2.3(b), we know that $\mathbb{1}^{\oplus n}$ is a direct summand of A as an A^e-module, with projections $\alpha_i : A \to \mathbb{1}$ for $1 \leq i \leq n$. Moreover, Lemma 1.10 shows that every such summand $\mathbb{1}$ admits a ring structure, under which $\mathbb{1}^{\times n}$ becomes a ring factor of A and the projections α_i are ring morphisms. In fact, these new ring structures on $\mathbb{1}$ are the original one, seeing how $\alpha_i \eta_A = 1_{\mathbb{1}}$ is a ring morphism for every $1 \leq i \leq n$. Finally, Lemma 3.8(b) shows that $\deg(A) \geq n$. □

Proposition 4.2. *Let A and B be separable rings in $\mathcal{K}$ and suppose B is indecomposable. Let $n \geq 1$. The following are equivalent*:

(i) *There are* (*at least*) *n distinct ring morphisms $A \to B$ in $\mathcal{K}$.*

(ii) *The ring $\mathbb{1}_B^{\times n}$ is a ring factor of $F_B(A)$ in B-*$\mathrm{Mod}_{\mathcal{K}}$.

(iii) *There is a ring morphism $A^{[n]} \to B$ in $\mathcal{K}$.*

Proof. Firstly, we claim there is a one-to-one correspondence between ring morphisms $\alpha : A \to B$ in $\mathcal{K}$ and ring morphisms $\beta : F_B(A) \to \mathbb{1}_B$ in B-$\mathrm{Mod}_{\mathcal{K}}$. Indeed, this correspondence sends $\alpha : A \to B$ in $\mathcal{K}$ to the B-algebra morphism

$$B \otimes A \xrightarrow{1_B \otimes \alpha} B \otimes B \xrightarrow{\mu} B,$$

and conversely, $\beta : F_B(A) \to \mathbb{1}_B$ gets mapped to $A \xrightarrow{\eta_B \otimes 1_A} B \otimes A \xrightarrow{\beta} B$ in $\mathcal{K}$.

To show (i) $\Rightarrow$ (ii), note that n distinct ring morphisms $A \to B$ in $\mathcal{K}$ give n distinct ring morphisms $F_B(A) \to \mathbb{1}_B$ in B-$\mathrm{Mod}_{\mathcal{K}}$. By Lemma 4.1, $\mathbb{1}_B^{\times n}$ is a ring factor of $F_B(A)$. For (ii) $\Rightarrow$ (i), suppose $\mathbb{1}_B^{\times n}$ is a ring factor of $F_B(A)$ in B-$\mathrm{Mod}_{\mathcal{K}}$ and consider the projections $\mathrm{pr}_i : F_B(A) \to \mathbb{1}_B$ with $1 \leq i \leq n$. By the claim, there are at least n distinct ring morphisms $A \to B$ in $\mathcal{K}$.

We show (ii) $\Rightarrow$ (iii) by induction on n. The case $n = 1$ has already been proven. Let $n \geq 1$ and suppose $\mathbb{1}_B^{\times(n+1)}$ is a ring factor of $F_B(A)$. By the induction hypothesis, there exists a ring morphism $A^{[n]} \to B$. As usual, we write $\bar{B}$ for the separable ring in $A^{[n]}\text{-Mod}_{\mathcal{K}}$ corresponding to the $A^{[n]}$-algebra B in $\mathcal{K}$. The diagram

$$\begin{tikzcd} \mathcal{K} \arrow[r, "F_{A^{[n]}}"] \arrow[d, "F_B"] & A^{[n]}\text{-Mod}_{\mathcal{K}} \arrow[d, "F_{\bar{B}}"] \\ B\text{-Mod}_{\mathcal{K}} \arrow[r, "\simeq"] & \bar{B}\text{-Mod}_{A^{[n]}\text{-Mod}_{\mathcal{K}}} \end{tikzcd} \tag{4.3}$$

from Proposition 1.15 shows that $F_B(A)$ is mapped to $F_{\bar{B}}(F_{A^{[n]}}(A))$ under the equivalence $B\text{-Mod}_{\mathcal{K}} \simeq \bar{B}\text{-Mod}_{A^{[n]}\text{-Mod}_{\mathcal{K}}}$. It follows that $\mathbb{1}_{\bar{B}}^{\times(n+1)}$ is a ring factor of $F_{\bar{B}}(F_{A^{[n]}}(A))$. On the other hand, by Proposition 3.5(a) we know that

$$F_{\bar{B}}(F_{A^{[n]}}(A)) \cong F_{\bar{B}}(\mathbb{1}_{A^{[n]}}^{\times n} \times A^{[n+1]}) \cong \mathbb{1}_{\bar{B}}^{\times n} \times F_{\bar{B}}(A^{[n+1]}). \tag{4.4}$$

Hence, $\mathbb{1}_{\bar{B}}$ is a ring factor of $F_{\bar{B}}(A^{[n+1]})$ by Proposition 2.1 and we conclude there exists a ring morphism $A^{[n+1]} \to \bar{B}$ in $A^{[n]}\text{-Mod}_{\mathcal{K}}$.

To show (iii) $\Rightarrow$ (ii), suppose B is an $A^{[n]}$-algebra and write $\bar{B}$ for the corresponding separable ring in $A^{[n]}\text{-Mod}_{\mathcal{K}}$. Using diagram (4.3) again, it is enough to show that $\mathbb{1}_{\bar{B}}^{\times n}$ is a ring factor of $F_{\bar{B}}(F_{A^{[n]}}(A))$. This follows from (4.4). $\square$

Theorem 4.5. *Let A and B be separable rings in $\mathcal{K}$, where A has finite degree and B is indecomposable. There are at most* $\deg(A)$ *distinct ring morphisms from A to B.*

Proof. If there are n distinct ring morphisms from A to B, we know $\mathbb{1}_B^{\times n}$ is a ring factor of $F_B(A)$ by Proposition 4.2. So, $n \leq \deg_{B\text{-Mod}_{\mathcal{K}}}(F_B(A)) \leq \deg_{\mathcal{K}}(A)$ by Proposition 3.5(b) and Lemma 3.8(b). $\square$

Remark 4.6. The assumption B is indecomposable is necessary in Theorem 4.5. Indeed, $\deg(\mathbb{1}^{\times n}) = n$ but $\mathbb{1}^{\times n}$ has at least $n!$ ring endomorphisms.

5. Quasi-Galois theory

Suppose (A, μ, η) is a nonzero ring in $\mathcal{K}$ and Γ is a finite set of ring endomorphisms of A with $1_A \in \Gamma$. Consider the ring $\prod_{\gamma\in\Gamma} A_\gamma$, where we write $A_\gamma = A$ for all $\gamma \in \Gamma$ to keep track of the different copies of A. We define ring morphisms $\varphi_1 : A \to \prod_{\gamma\in\Gamma} A_\gamma$ by $\mathrm{pr}_\gamma\, \varphi_1 = 1_A$ and $\varphi_2 : A \to \prod_{\gamma\in\Gamma} A_\gamma$ by $\mathrm{pr}_\gamma\, \varphi_2 = \gamma$ for all $\gamma \in \Gamma$. Thus, φ_1 renders the (standard) left A-module structure on $\prod_{\gamma\in\Gamma} A_\gamma$ and we introduce a right A-module structure on $\prod_{\gamma\in\Gamma} A_\gamma$ via φ_2.

Definition 5.1. We will consider the following ring morphism:

$$\lambda_\Gamma = \lambda : A \otimes A \longrightarrow \prod_{\gamma\in\Gamma} A_\gamma \quad \text{with } \mathrm{pr}_\gamma\, \lambda = \mu(1 \otimes \gamma).$$

Note that $\lambda(1\otimes\eta)=\varphi_1$ and $\lambda(\eta\otimes 1)=\varphi_2$,

$$\begin{tikzcd} & A \arrow[dl, shift right, "1\otimes\eta"'] \arrow[dl, shift left, "\eta\otimes 1"] \arrow[dr, shift left, "\varphi_2"] \arrow[dr, shift right, "\varphi_1"'] & \\ A\otimes A \arrow[rr, "\lambda"] & & \prod_{\gamma\in\Gamma} A_\gamma \end{tikzcd} \tag{5.2}$$

so that λ is an A^e-algebra morphism.

Lemma 5.3. *Suppose $\lambda_\Gamma : A\otimes A\to\prod_{\gamma\in\Gamma} A_\gamma$ is an isomorphism.*

(a) *There is an A^e-linear morphism $\sigma : A\to A\otimes A$ such that $\mu(1\otimes\gamma)\sigma=\delta_{1,\gamma}$ for every $\gamma\in\Gamma$. In particular, A is separable.*

(b) *Let $\gamma\in\Gamma$. If there exists a nonzero ring B in $\mathcal{K}$ and ring morphism $\alpha : A\to B$ with $\alpha\gamma=\alpha$, then $\gamma=1$.*

(c) *The separable ring A has degree $|\Gamma|$ in $\mathcal{K}$.*

Proof. To prove (a), consider the A^e-linear morphism $\sigma := \lambda^{-1}\,\mathrm{incl}_1 : A\to A\otimes A$. The following diagram shows that $\mu(1\otimes\gamma)\sigma=\delta_{1,\gamma}$:

$$\begin{tikzcd} A \arrow[rr, "\sigma"] \arrow[dr, hook, "\mathrm{incl}_1"'] & & A\otimes A \arrow[r, "1\otimes\gamma"] \arrow[dr, "\lambda"'] & A\otimes A \arrow[r, "\mu"] & A \\ & \prod_{\gamma\in\Gamma} A_\gamma \arrow[ur, "\lambda^{-1}"'] & & \prod_{\gamma\in\Gamma} A_\gamma \arrow[ur, "\mathrm{pr}_\gamma"'] & \end{tikzcd}$$

For (b), suppose $\alpha\gamma=\alpha$ and $\sigma : A\to A\otimes A$ as in (a). We get

$$\alpha=\alpha\mu\sigma=\mu(\alpha\otimes\alpha)\sigma=\mu(\alpha\otimes\alpha)(1\otimes\gamma)\sigma=\alpha\mu(1\otimes\gamma)\sigma=\alpha\delta_{\gamma,1}.$$

Hence, either $\alpha=0$ or $\gamma=1_A$. Finally, given that $F_A(A)\cong\mathbb{1}_A^{\times|\Gamma|}$ in $A\text{-Mod}_{\mathcal{K}}$, Proposition 3.5(c) shows that $\deg(A)=|\Gamma|$. □

Definition 5.4. Suppose that A is a nonzero ring in $\mathcal{K}$ and Γ is a finite group of ring automorphisms of A. We say that A is *quasi-Galois in $\mathcal{K}$ with group* Γ if $\lambda_\Gamma : A\otimes A\to\prod_{\gamma\in\Gamma} A_\gamma$ is an isomorphism. By the above lemma, it follows that A is separable of degree $|\Gamma|$ in $\mathcal{K}$. We also call $F_A : \mathcal{K}\longrightarrow A\text{-Mod}_{\mathcal{K}}$ a *quasi-Galois extension with group* Γ.

Example 5.5. Let $A := \mathbb{1}^{\times n}$ and consider the ring morphism $\gamma := (1\,2\,\cdots\,n)$ which permutes the factors. Then A is quasi-Galois with group $\Gamma=\{\gamma^i \mid 0\le i\le n-1\}\cong\mathbb{Z}_n$. Indeed, the isomorphism $\lambda : A\otimes A\to A^{\times n}$ constructed in the proof of Lemma 3.6 is exactly λ_Γ. In particular, Γ does not always contain all ring automorphisms of A.

Remark 5.6. The Galois theory of commutative rings was introduced by Auslander and Goldman [1960, Appendix], and was further developed by Chase, Harrison and Rosenberg [Chase et al. 1965] and many others. They considered commutative rings $R \subset A$ such that A is separable and projective as an R-algebra. If Γ is a finite group of ring automorphisms of A fixing R, then A is *Galois over R with group* Γ if the maps $R \hookrightarrow A^\Gamma$ and

$$A \otimes_R A \to \prod_{\gamma\in\Gamma} A, \qquad x \otimes y \mapsto (x \cdot \gamma(y))_{\gamma\in\Gamma}$$

are isomorphisms. In particular, A defines a ring object in the categories $R-\mathrm{mod}$ and $\mathrm{D}^{\mathrm{perf}}(R)$ (see Example 1.5), which is quasi-Galois with group Γ.

Lemma 5.7. *Let A be quasi-Galois of degree d in $\mathcal{K}$ with group Γ and suppose $F : \mathcal{K} \to \mathcal{L}$ is an additive monoidal functor. If $F(A) \neq 0$, then $F(A)$ is quasi-Galois of degree d in $\mathcal{L}$ with group $F(\Gamma) = \{F(\gamma) \mid \gamma \in \Gamma\}$. In particular, being quasi-Galois is stable under extension-of-scalars.*

Proof. We immediately see that

$$F(\lambda_\Gamma) : F(A) \otimes F(A) \cong F(A \otimes A) \to \prod_{\gamma\in\Gamma} F(A)$$

is an isomorphism in $\mathcal{L}$, so it suffices to show $\Gamma \cong F(\Gamma)$ and $F(\lambda_\Gamma) = \lambda_{F(\Gamma)}$. Now, λ_Γ is defined by $\mathrm{pr}_\gamma\, \lambda_\Gamma = \mu_A(1_A \otimes \gamma)$, hence $\mathrm{pr}_\gamma\, F(\lambda_\Gamma) = \mu_{F(A)}(1_{F(A)} \otimes F(\gamma))$ for every $\gamma \in \Gamma$. In particular, the morphisms $\mu_{F(A)}(1_{F(A)} \otimes F(\gamma))$ with $\gamma \in \Gamma$ are distinct. This shows the morphisms $F(\gamma)$ with $\gamma \in \Gamma$ are distinct, so that $\Gamma \cong F(\Gamma)$ and $F(\lambda_\Gamma) = \lambda_{F(\Gamma)}$. ☐

Proposition 5.8. *Suppose A is quasi-Galois in $\mathcal{K}$ with group Γ.*

(a) *If B is a separable indecomposable A-algebra, then Γ acts freely and transitively on the set of ring morphisms from A to B. In particular, there are exactly* $\deg(A)$ *distinct ring morphisms from A to B in $\mathcal{K}$.*

(b) *If A is indecomposable then Γ contains all ring endomorphisms of A.*

Proof. Note that the set S of ring morphisms from A to B is nonempty and Γ acts on S by precomposition. The action is free by Lemma 5.3(b) and transitive because $|S| \le \deg A = |\Gamma|$ by Theorem 4.5. In particular, if A is indecomposable, then A has exactly $\deg A = |\Gamma|$ ring endomorphisms in $\mathcal{K}$. ☐

By the above proposition, we can simply say an indecomposable ring A in $\mathcal{K}$ is quasi-Galois, with the understanding that the Galois group Γ contains all ring endomorphisms of A.

Theorem 5.9. *Let A be a separable indecomposable ring of finite degree in $\mathcal{K}$ and write Γ for the set of ring endomorphisms of A. The following are equivalent:*

(i) $|\Gamma| = \deg(A)$.

(ii) $F_A(A) \cong \mathbb{1}_A^{\times t}$ *in* A-$\mathrm{Mod}_{\mathcal{K}}$ *for some* $t > 0$.

(iii) $\lambda_\Gamma : A \otimes A \to \prod_{\gamma \in \Gamma} A_\gamma$ *is an isomorphism.*

(iv) Γ *is a group and A is quasi-Galois in $\mathcal{K}$ with group Γ.*

Proof. First note that $d := \deg(A) = \deg(F_A(A))$ by Proposition 3.5(c). To show (i) $\Rightarrow$ (ii), recall that $\mathbb{1}_A^{\times d}$ is a ring factor of $F_A(A)$ if $|\Gamma| = d$ by Proposition 4.2. By Lemma 3.8(b), we know $F_A(A) \cong \mathbb{1}_A^{\times d}$. For (ii) $\Rightarrow$ (iii), we note that $t = d$ and consider an A-algebra isomorphism $l : A \otimes A \xrightarrow{\simeq} A^{\times d}$. We define ring endomorphisms

$$\alpha_i : A \xrightarrow{\eta \otimes 1_A} A \otimes A \xrightarrow{l} A^{\times d} \xrightarrow{\mathrm{pr}_i} A, \qquad i = 1, \dots, d,$$

such that $\mu(1_A \otimes \alpha_i) = \mathrm{pr}_i\, l(\mu \otimes 1_A)(1_A \otimes \eta \otimes 1_A) = \mathrm{pr}_i\, l$ for every i. This shows the α_i are all distinct, so that $\Gamma = \{\alpha_i \mid 1 \le i \le d\}$ by Theorem 4.5 and $l = \lambda_\Gamma$. For (iii) $\Rightarrow$ (iv), we show that every $\gamma \in \Gamma$ is an automorphism. By Lemma 5.3(a), we can find an A^e-linear morphism $\sigma : A \to A \otimes A$ such that $\mu(1 \otimes \gamma)\sigma = \delta_{1,\gamma}$ for every $\gamma \in \Gamma$. Let $\gamma \in \Gamma$ and note that $\gamma = \mu(\gamma \otimes 1)(1 \otimes \gamma)\sigma$ so that $(1 \otimes \gamma)\sigma : A \to A \otimes A$ is nonzero. Thus there exists $\gamma' \in \Gamma$ such that

$$\mathrm{pr}_{\gamma'} \lambda_\Gamma (1 \otimes \gamma)\sigma = \mu(1 \otimes \gamma')(1 \otimes \gamma)\sigma = \delta_{1,\gamma'\gamma}$$

is nonzero. This means $1 = \gamma'\gamma$ and $\gamma'(\gamma\gamma') = \gamma'$ so $\gamma\gamma' = 1$ by Lemma 5.3(b). Finally, (iv) $\Rightarrow$ (i) is the last part of Lemma 5.3. □

Corollary 5.10. *Let A, B and C be separable rings in $\mathcal{K}$ with $A \cong B \times C$, and suppose B is indecomposable. If $F_A(A) \cong \mathbb{1}_A^{\times d}$, then B is quasi-Galois. In particular, being quasi-Galois is stable under passing to indecomposable ring factors.*

Proof. Consider the decomposition $A\text{-Mod}_{\mathcal{K}} \cong B\text{-Mod}_{\mathcal{K}} \times C\text{-Mod}_{\mathcal{K}}$, under which $F_A(A)$ corresponds to $(F_B(B \times C), F_C(B \times C))$ and $\mathbb{1}_A^{\times d}$ corresponds to $(\mathbb{1}_B^{\times d}, \mathbb{1}_C^{\times d})$. Given that $\mathbb{1}_B$ is indecomposable and $F_B(B)$ is a ring factor of $\mathbb{1}_B^{\times d}$ in $B\text{-Mod}_{\mathcal{K}}$, we know $F_B(B) \cong \mathbb{1}_B^{\times t}$ for some $1 \le t \le d$. The result now follows from Theorem 5.9. □

6. Splitting rings

Definition 6.1. Let A and B be separable rings of finite degree in $\mathcal{K}$. We say B *splits* A if $F_B(A) \cong \mathbb{1}_B^{\times \deg(A)}$ in $B\text{-Mod}_{\mathcal{K}}$. We call an indecomposable ring B a *splitting ring* of A if B splits A and any ring morphism $C \to B$, where C is an indecomposable ring splitting A, is an isomorphism.

Remark 6.2. Let A be a separable ring in $\mathcal{K}$ with $\deg(A) = d$. The ring $A^{[d]}$ in $\mathcal{K}$ splits A by Proposition 3.5(a). Moreover, if B is a separable indecomposable ring in $\mathcal{K}$, then B splits A if and only if B is an $A^{[d]}$-algebra. This follows immediately from Proposition 4.2.

Remark 6.3. Let A be a separable ring in $\mathcal{K}$ with $\deg(A) = d$. The ring $A^{[d]}$ in $\mathcal{K}$ splits itself by Proposition 3.5(a), (b) and Corollary 3.7:

$$F_{A^{[d]}}(A^{[d]}) \cong (F_{A^{[d]}}(A))^{[d]} \cong (\mathbb{1}_{A^{[d]}}^{\times d})^{[d]} \cong \mathbb{1}_{A^{[d]}}^{\times d!}.$$

Lemma 6.4. *Let A be a separable ring in $\mathcal{K}$ that splits itself. If A_1 and A_2 are indecomposable ring factors of A, then any ring morphism $A_1 \to A_2$ is an isomorphism.*

Proof. Let A_1 and A_2 be indecomposable ring factors of A and suppose there is a ring morphism $f : A_1 \to A_2$. We know $F_{A_1}(A) \cong \mathbb{1}_{A_1}^{\times \deg(A)}$ because A splits itself. Meanwhile, $F_{A_1}(A_2)$ is a ring factor of $F_{A_1}(A)$, so that $F_{A_1}(A_2) \cong \mathbb{1}_{A_1}^{\times d}$ for some $d \geq 0$. In fact, $d = \deg(A_2) \geq 1$ by Proposition 3.5(c). Proposition 4.2 shows there exists a ring morphism $g : A_2 \to A_1$. Note that A_1 and A_2 are quasi-Galois by Corollary 5.10, so that the ring morphisms $gf : A_1 \to A_1$ and $fg : A_2 \to A_2$ are isomorphisms by Proposition 5.8(b). □

Definition 6.5. We say $\mathcal{K}$ is *nice* if for every separable ring A of finite degree in $\mathcal{K}$, there are indecomposable rings $A_1, \ldots, A_n$ in $\mathcal{K}$ such that $A \cong A_1 \times \cdots \times A_n$.

Example 6.6. Let G be a group and $\Bbbk$ a field. The categories $\Bbbk G$-mod, $\mathrm{D}^b(\Bbbk G\text{-mod})$ and $\Bbbk G$-stab (see Section 10) are nice categories. More generally, $\mathcal{K}$ is nice if it satisfies Krull–Schmidt.

Example 6.7. Let X be a noetherian scheme and let $\mathrm{D}^{\mathrm{perf}}(X)$ be the derived category of perfect complexes over X with left derived tensor product. By Example 7.4 and Proposition 7.12, $\mathrm{D}^{\mathrm{perf}}(X)$ is nice.

Lemma 6.8. *Suppose $\mathcal{K}$ is nice and let A, B be separable rings of finite degree in $\mathcal{K}$. If B is indecomposable and there exists a ring morphism $A \to B$ in $\mathcal{K}$, then there exists a ring morphism $C \to B$ for some indecomposable ring factor C of A.*

Proof. Since $\mathcal{K}$ is nice, we can write $A \cong A_1 \times \cdots \times A_n$ with A_i indecomposable for $1 \leq i \leq n$. If there exists a ring morphism $A \to B$ in $\mathcal{K}$, Proposition 4.2 shows that $\mathbb{1}_B$ is a ring factor of $F_B(A) \cong F_B(A_1) \times \cdots \times F_B(A_n)$. Since $\mathbb{1}_B$ is indecomposable, it is a ring factor of some $F_B(A_i)$ with $1 \leq i \leq n$ by Proposition 2.1. □

Proposition 6.9. *Suppose $\mathcal{K}$ is nice and let A be a separable ring of finite degree in $\mathcal{K}$. An indecomposable ring B in $\mathcal{K}$ is a splitting ring of A if and only if B is a ring factor of $A^{[\deg(A)]}$. In particular, any separable ring in $\mathcal{K}$ has a splitting ring and at most finitely many.*

Proof. Let $d := \deg(A)$ and suppose B is a splitting ring of A. By Remark 6.2, B is an $A^{[d]}$-algebra. Hence, there exists a ring morphism $C \to B$ for some indecomposable ring factor C of $A^{[d]}$ by Lemma 6.8. Now, $A^{[d]}$ splits A, so C splits A and the ring morphism $C \to B$ is an isomorphism. Conversely, suppose B is an indecomposable ring factor of $A^{[d]}$, so B splits A. Let C be an indecomposable separable ring splitting A and suppose there is a ring morphism $C \to B$. As before, C is an $A^{[d]}$-algebra and there exists a ring morphism $B' \to C$ for some indecomposable ring factor B' of $A^{[d]}$. The composition $B' \to C \to B$ is an isomorphism by Remark 6.3 and Lemma 6.4. In other words, B is a ring factor of the indecomposable ring C, so that $C \cong B$. $\square$

Corollary 6.10. *Suppose $\mathcal{K}$ is nice and B is a separable indecomposable ring of finite degree in $\mathcal{K}$. Then B is quasi-Galois in $\mathcal{K}$ if and only if there exists a nonzero separable ring A of finite degree in $\mathcal{K}$ such that B is a splitting ring of A.*

Proof. Suppose B is indecomposable and quasi-Galois of degree t, so $B^{[2]} \cong \mathbb{1}_B^{\times(t-1)}$ as B-algebras. Then, B is a splitting ring for B because B is a ring factor of $B^{[t]}$:

$$B^{[t]} \cong (B^{[2]})^{[t-1]} \cong (\mathbb{1}_B^{\times(t-1)})^{[t-1]} \cong B^{\times(t-1)!}.$$

Now suppose B is a splitting ring for some A in $\mathcal{K}$, say with $\deg(A) = d > 0$. Seeing how $F_B(B)$ is a ring factor of

$$F_B(A^{[d]}) \cong F_B(A)^{[d]} \cong (\mathbb{1}_B^{\times d})^{[d]} = \mathbb{1}_B^{\times d!},$$

we know $F_B(B) \cong \mathbb{1}_B^{\times t}$ for some $t > 0$. By Theorem 5.9, B is quasi-Galois. $\square$

7. Tensor triangular geometry

Definition 7.1. A *tt-category* $\mathcal{K}$ is an essentially small, idempotent-complete tensor-triangulated category. In particular, $\mathcal{K}$ comes equipped with a symmetric monoidal structure $(\otimes, \mathbb{1})$ such that $x \otimes - : \mathcal{K} \to \mathcal{K}$ is exact for all objects x in $\mathcal{K}$. A *tt-functor* $\mathcal{K} \to \mathcal{L}$ is an exact symmetric monoidal functor.

Throughout the rest of this paper, $(\mathcal{K}, \otimes, \mathbb{1})$ will denote a tt-category.

Remark 7.2. Balmer [2011] proved in that extension along a separable ring object A preserves the triangulation: $(A\text{-Mod}_{\mathcal{K}}, \otimes_A, \mathbb{1}_A)$ is a tt-category, extension-of-scalars F_A becomes a tt-functor and U_A is exact.

Definition 7.3. We briefly recall some tt-geometry and refer the reader to [Balmer 2005] for precise statements and motivation. The *spectrum* $\mathrm{Spc}(\mathcal{K})$ of a tt-category $\mathcal{K}$ is the set of all prime thick $\otimes$-ideals $\mathcal{P} \subsetneq \mathcal{K}$. The *support* of an object x in $\mathcal{K}$ is $\mathrm{supp}(x) = \{\mathcal{P} \in \mathrm{Spc}(\mathcal{K}) \mid x \notin \mathcal{P}\} \subset \mathrm{Spc}(\mathcal{K})$. The complements of these supports $\mathcal{U}(x) := \mathrm{Spc}(\mathcal{K}) - \mathrm{supp}(x)$ form an open basis for the *Zariski topology* on $\mathrm{Spc}(\mathcal{K})$.

Example 7.4. Let X be a noetherian scheme. Then $(\mathrm{D}^{\mathrm{perf}}(X), \otimes^{\mathrm{L}}_{\mathcal{O}_X})$ is a tt-category with spectrum $\mathrm{Spc}(\mathrm{D}^{\mathrm{perf}}(X))$ homeomorphic to X; see [op. cit., Theorem 6.3].

Remark 7.5. The spectrum is functorial. In particular, every tt-functor $F : \mathcal{K} \to \mathcal{L}$ induces a continuous map

$$\mathrm{Spc}(F) : \mathrm{Spc}(\mathcal{L}) \to \mathrm{Spc}(\mathcal{K}).$$

Moreover, for all $x \in \mathcal{K}$, we have

$$(\mathrm{Spc}\, F)^{-1}(\mathrm{supp}_{\mathcal{K}}(x)) = \mathrm{supp}_{\mathcal{L}}(F(x)) \subset \mathrm{Spc}\,\mathcal{L}.$$

Let A be a separable ring in $\mathcal{K}$. We will consider the continuous map

$$f_A := \mathrm{Spc}(F_A) : \mathrm{Spc}(A\text{-Mod}_{\mathcal{K}}) \to \mathrm{Spc}(\mathcal{K})$$

induced by the extension-of-scalars $F_A : \mathcal{K} \to A\text{-Mod}_{\mathcal{K}}$.

Theorem 7.6 [Balmer 2016b, Theorem 3.14]. *Let A be a separable ring of finite degree in $\mathcal{K}$. Then*

$$\mathrm{Spc}((A \otimes A)\text{-Mod}_{\mathcal{K}}) \underset{f_2}{\overset{f_1}{\rightrightarrows}} \mathrm{Spc}(A\text{-Mod}_{\mathcal{K}}) \xrightarrow{f_A} \mathrm{supp}_{\mathcal{K}}(A) \tag{7.7}$$

is a coequalizer, where f_1, f_2 are the maps induced by extension-of-scalars along the morphisms $1 \otimes \eta$ and $\eta \otimes 1 : A \to A \otimes A$ respectively. In particular, the image of f_A is $\mathrm{supp}_{\mathcal{K}}(A) \subset \mathrm{Spc}(\mathcal{K})$.

Definition 7.8. We call a tt-category $\mathcal{K}$ *local* if $x \otimes y = 0$ implies that x or y is $\otimes$-nilpotent for all $x, y \in \mathcal{K}$. The *local category $\mathcal{K}_{\mathcal{P}}$ at the prime $\mathcal{P} \in$* $\mathrm{Spc}(\mathcal{K})$ is the idempotent completion of the Verdier quotient $\mathcal{K}/\mathcal{P}$. We write $q_{\mathcal{P}}$ for the canonical tt-functor $\mathcal{K} \twoheadrightarrow \mathcal{K}/\mathcal{P} \hookrightarrow \mathcal{K}_{\mathcal{P}}$.

Proposition 7.9 [Balmer 2014, Theorem 3.8]. *Suppose A is a separable ring in $\mathcal{K}$. If the ring $q_{\mathcal{P}}(A)$ has finite degree in $\mathcal{K}_{\mathcal{P}}$ for every $\mathcal{P} \in \mathrm{Spc}(\mathcal{K})$, then A has finite degree and*

$$\deg_{\mathcal{K}}(A) = \max_{\mathcal{P} \in \mathrm{Spc}(\mathcal{K})} \deg_{\mathcal{K}_{\mathcal{P}}}(q_{\mathcal{P}}(A)).$$

Proposition 7.10 [Balmer 2014, Corollary 3.12]. *Let $\mathcal{K}$ be a local tt-category and suppose A, B are separable rings of finite degree in $\mathcal{K}$. Then* $\deg(A \times B) = \deg(A) + \deg(B)$.

Lemma 7.11 [Balmer 2014, Theorem 3.7]. *Let A and B be separable rings in $\mathcal{K}$ and suppose* $\mathrm{supp}(A) \subseteq \mathrm{supp}(B)$. *Then* $\deg_{B\text{-Mod}_{\mathcal{K}}}(F_B(A)) = \deg_{\mathcal{K}}(A)$.

Proposition 7.12. *Suppose the spectrum* $\mathrm{Spc}(\mathcal{K})$ *of $\mathcal{K}$ is noetherian. Then $\mathcal{K}$ is nice. That is, any separable ring A of finite degree in $\mathcal{K}$ has a decomposition $A \cong A_1 \times \ldots \times A_n$ where $A_1, \ldots, A_n$ are indecomposable rings in $\mathcal{K}$.*

Proof. Let A be a separable ring of finite degree in $\mathcal{K}$. We prove that any ring decomposition of A in $\mathcal{K}$ has at most finitely many nonzero ring factors. Suppose there is a sequence of nontrivial decompositions $A = A_1 \times B_1$, $B_1 = A_2 \times B_2, \ldots,$ with $B_n = A_{n+1} \times B_{n+1}$ for $n \geq 1$. By Proposition 7.10, we know

$$\deg(q_{\mathcal{P}}(B_n)) \geq \deg(q_{\mathcal{P}}(B_{n+1}))$$

for every $\mathcal{P} \in \operatorname{Spc}(\mathcal{K})$. We note that $\deg(q_{\mathcal{P}}(B_n)) \geq i$ if and only if $\mathcal{P} \in \operatorname{supp}(B_n^{[i]})$, so we get $\operatorname{supp}(B_n^{[i]}) \supseteq \operatorname{supp}(B_{n+1}^{[i]})$ for every $i \geq 0$. Since $\operatorname{Spc}(\mathcal{K})$ is noetherian, we can find $k \geq 1$ with $\operatorname{supp}(B_n^{[i]}) = \operatorname{supp}(B_{n+1}^{[i]})$ for every $i \geq 0$ and $n \geq k$. In particular, $\deg(q_{\mathcal{P}}(B_k)) = \deg(q_{\mathcal{P}}(B_{k+1}))$ for every $\mathcal{P} \in \operatorname{Spc}(\mathcal{K})$, so $q_{\mathcal{P}}(A_{k+1}) = 0$ for all $\mathcal{P} \in \operatorname{Spc}(\mathcal{K})$. By Proposition 7.9, we conclude $A_{k+1} = 0$, a contradiction. □

8. Rings of constant degree

Definition 8.1. We say a separable ring A in $\mathcal{K}$ has *constant degree* $d \in \mathbb{N}$ if the degree $\deg_{\mathcal{K}_{\mathcal{P}}} q_{\mathcal{P}}(A)$ equals d for every $\mathcal{P} \in \operatorname{supp}(A) \subset \operatorname{Spc}(\mathcal{K})$.

Lemma 8.2. *Let A be a separable ring of degree d in $\mathcal{K}$. Then A has constant degree if and only if* $\operatorname{supp}(A^{[d]}) = \operatorname{supp}(A)$.

Proof. Note that $\operatorname{supp}(A^{[2]}) \subseteq \operatorname{supp}(A)$ because $A \otimes A \cong A \times A^{[2]}$ in $\mathcal{K}$. Hence $\operatorname{supp}(A^{[d]}) \subseteq \operatorname{supp}(A)$. Now, let $\mathcal{P} \in \operatorname{supp}(A)$. Then $q_{\mathcal{P}}(A)$ has degree d if and only if $q_{\mathcal{P}}(A^{[d]}) \neq 0$, in other words $\mathcal{P} \in \operatorname{supp}(A^{[d]})$. □

Lemma 8.3. *Let A be a separable ring in $\mathcal{K}$ and suppose $F : \mathcal{K} \to \mathcal{L}$ is a tt-functor with $F(A) \neq 0$. If A has constant degree d, then $F(A)$ has constant degree d. Conversely, if $F(A)$ has constant degree d and* $\operatorname{supp}(A) \subset \operatorname{im}(\operatorname{Spc}(F))$, *then A has constant degree d.*

Proof. We first note that $\deg(F(A)) \leq \deg(A)$ by Proposition 3.5(b). Now, if A has constant degree d, then

$$\begin{aligned}\operatorname{supp}_{\mathcal{L}}(F(A)^{[d]}) &= \operatorname{supp}_{\mathcal{L}}(F(A^{[d]})) = \operatorname{Spc}(F)^{-1}(\operatorname{supp}_{\mathcal{K}}(A^{[d]})) \\ &= \operatorname{Spc}(F)^{-1}(\operatorname{supp}_{\mathcal{K}}(A)) = \operatorname{supp}_{\mathcal{L}}(F(A)) \neq \varnothing,\end{aligned}$$

which shows $F(A)$ has constant degree d. Conversely, suppose $F(A)$ has constant degree d and $\operatorname{supp}(A) \subset \operatorname{im}(\operatorname{Spc}(F))$. In particular, $\operatorname{supp}(A^{[d+1]}) \subset \operatorname{im}(\operatorname{Spc}(F))$, so

$$\varnothing = \operatorname{supp}(F(A^{[d+1]})) = \operatorname{Spc}(F)^{-1}(\operatorname{supp}(A^{[d+1]}))$$

implies $\operatorname{supp}(A^{[d+1]}) = \varnothing$. Thus A has degree d. Moreover, seeing how

$$\begin{aligned}\operatorname{Spc}(F)^{-1}(\operatorname{supp}_{\mathcal{K}}(A^{[d]})) &= \operatorname{supp}_{\mathcal{L}}(F(A)^{[d]}) \\ &= \operatorname{supp}_{\mathcal{L}}(F(A)) = \operatorname{Spc}(F)^{-1}(\operatorname{supp}_{\mathcal{K}}(A)),\end{aligned}$$

we can conclude $\operatorname{supp}_{\mathcal{K}}(A^{[d]}) = \operatorname{supp}_{\mathcal{K}}(A)$. □

Proposition 8.4. *Let A be a separable ring in $\mathcal{K}$. Then A has constant degree d if and only if there exists a separable ring B in $\mathcal{K}$ with* $\operatorname{supp}(A) \subset \operatorname{supp}(B)$ *and such that $F_B(A) \cong \mathbb{1}_B^{\times d}$. In particular, if A is quasi-Galois in $\mathcal{K}$ with group Γ, then A has constant degree $|\Gamma|$ in $\mathcal{K}$.*

Proof. If A has constant degree d, we can let $B := A^{[d]}$ and use Proposition 3.5(a). On the other hand, if A and B are separable rings in $\mathcal{K}$ with $\operatorname{supp}(A) \subset \operatorname{supp}(B)$, then Theorem 7.6 and Lemma 8.3 show that A has constant degree d whenever $F_B(A)$ has constant degree d. $\square$

Proposition 8.5. *Let A be a separable ring of constant degree in $\mathcal{K}$ with connected support* $\operatorname{supp}(A) \subset \operatorname{Spc}(\mathcal{K})$. *If B and C are nonzero rings in $\mathcal{K}$ such that $A = B \times C$, then B and C have constant degree and* $\operatorname{supp}(A) = \operatorname{supp}(B) = \operatorname{supp}(C)$.

Proof. Given that A has constant degree d, we claim that for every $1 \le n \le d$,

$$\operatorname{supp}(A) = \operatorname{supp}(B^{[n]}) \sqcup \operatorname{supp}(C^{[d-n+1]}).$$

Fix $1 \le n \le d$ and suppose $\mathcal{P} \in \operatorname{supp}(B^{[n]}) \cap \operatorname{supp}(C^{[d-n+1]})$, so $\deg(q_{\mathcal{P}}(B)) \ge n$ and $\deg(q_{\mathcal{P}}(C)) \ge d-n+1$. By Proposition 7.10, $\deg(q_{\mathcal{P}}(A)) \ge d+1$, which is a contradiction. So far we've proven $\operatorname{supp}(A) \supset \operatorname{supp}(B^{[n]}) \sqcup \operatorname{supp}(C^{[d-n+1]})$. Now, if $\mathcal{P} \in \operatorname{supp}(A) - \operatorname{supp}(B^{[n]})$, we get $\deg(q_{\mathcal{P}}(A)) = d$ and $\deg(q_{\mathcal{P}}(B)) \le n-1$. It follows that $\deg(q_{\mathcal{P}}(C)) \ge d-n+1$, so $\mathcal{P} \in \operatorname{supp}(C^{[d-n+1]})$ and the claim follows.

Assuming A has connected support, we note that for every $1 \le n \le d$, either $\operatorname{supp}(B^{[n]}) = \operatorname{supp}(A)$ or $\operatorname{supp}(B^{[n]}) = \varnothing$. In particular, taking $n = \deg(B)$ and then $n = 1$ shows that $\operatorname{supp}(A) = \operatorname{supp}(B^{[\deg(B)]}) = \operatorname{supp}(B)$. Similarly, we see $\operatorname{supp}(A) = \operatorname{supp}(C^{[\deg(C)]}) = \operatorname{supp}(C)$ by letting $n = d+1-\deg(C)$ and then $n = 1$. In other words, $\operatorname{supp}(A) = \operatorname{supp}(B) = \operatorname{supp}(C)$ and B, C have constant degree. $\square$

9. Quasi-Galois theory and tensor triangular geometry

Let A be a separable ring in $\mathcal{K}$ and suppose Γ is a finite group of ring automorphisms of A. Then, Γ acts on $A\text{-Mod}_{\mathcal{K}}$ (see Remark 1.14) and therefore on the spectrum $\operatorname{Spc}(A\text{-Mod}_{\mathcal{K}})$.

Theorem 9.1. *Suppose A is quasi-Galois in $\mathcal{K}$ with group Γ. Then,*

$$\operatorname{supp}(A) \cong \operatorname{Spc}(A\text{-Mod}_{\mathcal{K}})/\,\Gamma.$$

Proof. Diagram (5.2) yields a diagram of topological spaces

$$\begin{tikzcd}
 & \operatorname{Spc}(A\text{-Mod}_{\mathcal{K}}) & \\
\operatorname{Spc}((A\otimes A)\text{-Mod}_{\mathcal{K}}) \arrow[ur, shift left, "f_1"] \arrow[ur, shift right, "f_2"'] \arrow[rr, "\cong", "l"'] & & \operatorname{Spc}(\prod_{\gamma\in\Gamma} A_\gamma\text{-Mod}_{\mathcal{K}}), \arrow[ul, shift left, "g_1"] \arrow[ul, shift right, "g_2"']
\end{tikzcd}$$

where f_1, f_2, g_1, g_2 and l are the maps induced by extension-of-scalars along the morphisms $1 \otimes \eta$, $\eta \otimes 1$, φ_1, φ_2 and λ respectively (in the notation of Definition 5.1). That is, $g_1, g_2 : \bigsqcup_{\gamma\in\Gamma} \operatorname{Spc}(A_\gamma\text{-Mod}_{\mathcal{K}}) \to \operatorname{Spc}(A\text{-Mod}_{\mathcal{K}})$ are continuous maps such that $g_1 \operatorname{incl}_\gamma$ is the identity and $g_2 \operatorname{incl}_\gamma$ is the action of γ on $\operatorname{Spc}(A\text{-Mod}_{\mathcal{K}})$. Now, the coequalizer (7.7) turns into

$$\bigsqcup_{\gamma\in\Gamma} \operatorname{Spc}(A_\gamma\text{-Mod}_{\mathcal{K}}) \underset{g_2}{\overset{g_1}{\rightrightarrows}} \operatorname{Spc}(A\text{-Mod}_{\mathcal{K}}) \xrightarrow{f_A} \operatorname{supp}(A),$$

which shows $\operatorname{supp}(A) \cong \operatorname{Spc}(A\text{-Mod}_{\mathcal{K}})/\,\Gamma$. □

Remark 9.2. Let A be a ring in $\mathcal{K}$. We call A *nil-faithful* if $F_A(f) = 0$ implies f is $\otimes$-nilpotent for any morphism f in $\mathcal{K}$. By [Balmer 2016b, Proposition 3.15], A is nil-faithful if and only if $\operatorname{supp}(A) = \operatorname{Spc}(\mathcal{K})$. If A is nil-faithful and quasi-Galois in $\mathcal{K}$ with group Γ, Theorem 9.1 recovers $\operatorname{Spc}(\mathcal{K})$ as the Γ-orbits of $\operatorname{Spc}(A\text{-Mod}_{\mathcal{K}})$.

The following is a tensor-triangular version of Lemma 6.4.

Lemma 9.3. *Let A be a separable ring in $\mathcal{K}$ that splits itself. If A_1 and A_2 are indecomposable ring factors of A, then* $\operatorname{supp}(A_1) \cap \operatorname{supp}(A_2) = \varnothing$ *or* $A_1 \cong A_2$.

Proof. Let A_1 and A_2 be indecomposable ring factors of A and suppose A splits itself. We know $F_{A_1}(A) \cong \mathbb{1}_{A_1}^{\times \deg(A)}$ and hence $F_{A_1}(A_2) \cong \mathbb{1}_{A_1}^{\times t}$ for some $t \geq 0$. In fact, $t = 0$ only if $\operatorname{supp}(A_1 \otimes A_2) = \operatorname{supp}(A_1) \cap \operatorname{supp}(A_2) = \varnothing$. If $t > 0$, we can find a ring morphism $A_2 \to A_1$ by Proposition 4.2. Now Lemma 6.4 shows this is an isomorphism. □

Proposition 9.4. *Suppose $\mathcal{K}$ is nice. Let A be a separable ring in $\mathcal{K}$ with connected support* $\operatorname{supp}(A)$ *and constant degree. Then the splitting ring A^* of A is unique up to isomorphism and* $\operatorname{supp}(A) = \operatorname{supp}(A^*)$.

Proof. Let $d := \deg(A)$. Recall that by Proposition 6.9, the splitting rings of A are exactly the indecomposable ring factors of $A^{[d]}$. We now prove that any two indecomposable ring factors, say A_1 and A_2, of $A^{[d]}$ are isomorphic. Note that $\operatorname{supp}(A) = \operatorname{supp}(A^{[d]})$ is connected and $A^{[d]}$ has constant degree $d!$ by Remark 6.3, so that $\operatorname{supp}(A) = \operatorname{supp}(A_1) = \operatorname{supp}(A_2)$ by Proposition 8.5. Now, Lemma 9.3 shows A_1 and A_2 are isomorphic. □

Remark 9.5. In what follows, we consider a separable ring A in $\mathcal{K}$ and assume the spectrum $\operatorname{Spc}(A\text{-Mod}_{\mathcal{K}})$ is connected, which implies that A is indecomposable. Moreover, if the tt-category $A\text{-Mod}_{\mathcal{K}}$ is *rigid*, $\operatorname{Spc}(A\text{-Mod}_{\mathcal{K}})$ is connected if and only if A is indecomposable, see [Balmer 2007, Theorem 2.11]. We note that many tt-categories are rigid, including all examples given in this paper.

Proposition 9.6. *Suppose $\mathcal{K}$ is nice. Let A be a separable ring in $\mathcal{K}$ and suppose* $\operatorname{Spc}(A\text{-Mod}_{\mathcal{K}})$ *is connected. Let B be an A-algebra with* $\operatorname{supp}(A) = \operatorname{supp}(B)$. *If B*

is quasi-Galois in $\mathcal{K}$ *with group* Γ, *then* B *splits* A. *In particular*, *the degree of* A *in* $\mathcal{K}$ *is constant.*

Proof. If B is quasi-Galois in $\mathcal{K}$ for some group Γ, then all of its indecomposable ring factors are also quasi-Galois by Corollary 5.10. What is more, $\operatorname{supp}(B) = f_A(\operatorname{Spc}(A\text{-Mod}_{\mathcal{K}}))$ is connected, so the indecomposable ring factors of B have support equal to $\operatorname{supp}(B)$ by Proposition 8.5. It thus suffices to prove the proposition when B is indecomposable. Now, $F_A(B)$ is quasi-Galois by Lemma 5.7 and $\operatorname{supp}(F_A(B)) = f_A^{-1}(\operatorname{supp}(B)) = \operatorname{Spc}(A\text{-Mod}_{\mathcal{K}})$ is connected. By Corollary 2.4, $\bar{B}$ is an indecomposable ring factor of $F_A(B)$, and all ring factors of $F_A(B)$ have equal support by Proposition 8.5. In fact, Lemma 9.3 shows that $F_A(B) \cong \bar{B}^{\times t}$ for some $t \geq 1$. Forgetting the A-action, we get $A \otimes B \cong B^{\times t}$ in $\mathcal{K}$ and $F_B(A \otimes B) \cong F_B(B^{\times t}) \cong \mathbb{1}_B^{\times dt}$ in B-$\mathrm{Mod}_{\mathcal{K}}$, where $d := \deg(B)$. On the other hand, $F_B(A \otimes B) \cong F_B(A) \otimes_B \mathbb{1}_B^{\times d} \cong (F_B(A))^{\times d}$. It follows that $F_B(A) \cong \mathbb{1}_B^{\times t}$, with $t = \deg(A)$ by Lemma 7.11. $\square$

Theorem 9.7 (Quasi-Galois closure). *Suppose* $\mathcal{K}$ *is nice. Let* A *be a separable ring of constant degree in* $\mathcal{K}$ *and suppose* $\operatorname{Spc}(A\text{-Mod}_{\mathcal{K}})$ *is connected. The splitting ring* A^* *is the quasi-Galois closure of* A. *That is*, A^* *is quasi-Galois in* $\mathcal{K}$, $\operatorname{supp}(A) = \operatorname{supp}(A^*)$ *and for any* A*-algebra* B *that is quasi-Galois in* $\mathcal{K}$ *with* $\operatorname{supp}(A) = \operatorname{supp}(B)$, *there exists a ring morphism* $A^* \to B$.

Proof. Corollary 6.10 and Proposition 9.4 show that A^* is quasi-Galois in $\mathcal{K}$ and $\operatorname{supp}(A) = \operatorname{supp}(A^*)$. Suppose there is an A-algebra B as above. By Proposition 9.6, B splits A, so there exists a ring morphism $A^{[\deg(A)]} \to B$. The result now follows because $A^{[\deg(A)]} \cong A^* \times \cdots \times A^*$ by Proposition 9.4. $\square$

Remark 9.8. By Proposition 9.6, the assumption that A has constant degree is necessary for the existence of a quasi-Galois closure A^* of A with $\operatorname{supp}(A) = \operatorname{supp}(A^*)$.

10. Some modular representation theory

Let G be a finite group and $\Bbbk$ a field with characteristic $p > 0$ dividing $|G|$. We write $\Bbbk G$-mod for the category of finitely generated left $\Bbbk G$-modules. This category is nice, idempotent-complete and symmetric monoidal: the tensor is $\otimes_{\Bbbk}$ with diagonal G-action, and the unit is the trivial representation $\mathbb{1} = \Bbbk$.

We will also work in the bounded derived category $\mathrm{D}^b(\Bbbk G\text{-mod})$ and stable category $\Bbbk G$-stab, which are nice tt-categories. The spectrum $\operatorname{Spc}(\mathrm{D}^b(\Bbbk G\text{-mod}))$ of the derived category is homeomorphic to the homogeneous spectrum $\operatorname{Spec}^h(H^\bullet(G,\Bbbk))$ of the graded-commutative cohomology ring $H^\bullet(G,\Bbbk)$. Accordingly, the spectrum $\operatorname{Spc}(\Bbbk G\text{-stab})$ of the stable category is homeomorphic to the projective support variety $\mathcal{V}_G(\Bbbk) := \operatorname{Proj}(H^\bullet(G,\Bbbk))$; see [Benson et al. 1997].

Notation 10.1. Let $H \leq G$ be a subgroup. The $\Bbbk G$-module $A_H = A_H^G := \Bbbk(G/H)$ is the free $\Bbbk$-module with basis G/H and left G-action given by $g \cdot [x] = [gx]$ for every $[x] \in G/H$. The $\Bbbk G$-linear map $\mu : A_H \otimes_\Bbbk A_H \to A_H$ is given by

$$\gamma \otimes \gamma' \mapsto \begin{cases} \gamma & \text{if } \gamma = \gamma', \\ 0 & \text{if } \gamma \neq \gamma', \end{cases} \quad \text{for all } \gamma, \gamma' \in G/H.$$

We define $\eta : \mathbb{1} \to A_H$ by sending $1 \in \Bbbk$ to $\sum_{\gamma \in G/H} \gamma \in \Bbbk(G/H)$.

We will write $\mathcal{K}(G)$ to denote any of $\Bbbk G$-mod, $\mathrm{D}^b(\Bbbk G\text{-mod})$ or $\Bbbk G$-stab and consider the object A_H in each of these categories.

Proposition 10.2 [Balmer 2015, Proposition 3.16 and Theorem 4.4]. *Let $H \leq G$ be a subgroup. Then,*

(a) *The triple (A_H, μ, η) is a commutative separable ring object in $\mathcal{K}(G)$.*

(b) *There is an equivalence of categories*

$$\Psi_H^G : \mathcal{K}(H) \xrightarrow{\simeq} A_H\text{-Mod}_{\mathcal{K}(G)}$$

sending $V \in \mathcal{K}(H)$ to $\Bbbk G \otimes_{\Bbbk H} V \in \mathcal{K}(G)$ with A_H-action

$$\varrho : \Bbbk(G/H) \otimes_\Bbbk (\Bbbk G \otimes_{\Bbbk H} V) \to \Bbbk G \otimes_{\Bbbk H} V$$

given for $\gamma \in G/H$, $g \in G$ and $v \in V$ by $\gamma \otimes g \otimes v \to \begin{cases} g \otimes v & \text{if } g \in \gamma, \\ 0 & \text{if } g \notin \gamma. \end{cases}$

(c) *The following diagram commutes up to isomorphism*:

$$\begin{tikzcd} & \mathcal{K}(G) \arrow[dl, "\mathrm{Res}_H^G"'] \arrow[dr, "F_{A_H}"] & \\ \mathcal{K}(H) \arrow[rr, "\Psi_H^G", "\simeq"'] & & A_H\text{-Mod}_{\mathcal{K}(G)}. \end{tikzcd}$$

So, every subgroup $H \leq G$ provides an indecomposable separable ring A_H in $\mathcal{K}(G)$, along which extension-of-scalars becomes restriction to the subgroup.

Proposition 10.3. *The ring A_H has degree $[G : H]$ in* $\Bbbk G$-mod *and* $\mathrm{D}^b(\Bbbk G\text{-mod})$.

Proof. Seeing how the fiber functor $\mathrm{Res}_{\{1\}}^G$ is conservative, we get

$$\deg_{\Bbbk G\text{-mod}}(A_H) = \deg_{\Bbbk\text{-mod}}(\mathrm{Res}_{\{1\}}^G(A_H)) = [G : H].$$

The degree of A_H in $\mathrm{D}^b(\Bbbk G\text{-mod})$ is computed in [Balmer 2014, Corollary 4.5]. □

Lemma 10.4. *Let $\mathcal{K}(G)$ denote* $\mathrm{D}^b(\Bbbk G\text{-mod})$ *or* $\Bbbk G$-stab *and consider subgroups $K \leq H \leq G$. Then* $\mathrm{supp}(A_H) = \mathrm{supp}(A_K) \subset \mathrm{Spc}(\mathcal{K}(G))$ *if and only if every elementary abelian p-subgroup of H is conjugate in G to a subgroup of K.*

Proof. This follows from [Evens 1991, Theorem 9.1.3], seeing how $\mathrm{supp}(A_H) = (\mathrm{Res}^G_H)^*(\mathrm{Spc}(\mathcal{K}(H)))$ can be written as a union of disjoint pieces coming from conjugacy classes in G of elementary abelian p-subgroups of H. $\square$

Notation 10.5. For any two subgroups $H, K \leq G$, we write ${}_H[g]_K$ for the equivalence class of $g \in G$ in $H - G/K$, just $[g]$ if the context is clear. We will write $H^g := g^{-1}Hg$ for the conjugate subgroups of H.

Remark 10.6. Let $H, K \leq G$ be subgroups and choose a complete set $T \subset G$ of representatives for $H\backslash G/K$. Consider the Mackey isomorphism of G-sets,

$$\coprod_{g\in T} G/(K \cap H^g) \xrightarrow{\cong} G/K \times G/H,$$

sending $[x] \in G/(K \cap H^g)$ to $([x]_K, [xg^{-1}]_H)$. The corresponding ring isomorphism

$$\tau : A_K \otimes A_H \xrightarrow{\cong} \prod_{g\in T} A_{K\cap H^g}$$

in $\mathcal{K}(G)$ [Balmer 2016b, Construction 4.1] is given for $g \in T$ and $x, y \in G$ by

$$\mathrm{pr}_g\, \tau([x]_K \otimes [y]_H) = \begin{cases} [xk]_{K\cap H^g} & \text{if } {}_H[g]_K = {}_H[y^{-1}x]_K, \\ 0 & \text{otherwise,} \end{cases}$$

with $k \in K$ such that $y^{-1}xkg^{-1} \in H$. This yields an A_K-algebra structure on $A_{K\cap H^t}$ for every $t \in T$, given by

$$A_K \xrightarrow{1\otimes\eta} A_K \otimes A_H \cong \prod_{g\in T} A_{K\cap H^g} \xrightarrow{\mathrm{pr}_t} A_{K\cap H^t},$$

which sends $[x]_K \in G/K$ to

$$\sum_{[k]\in K/K\cap H^t} [xk]_{K\cap H^t} \in A_{K\cap H^t}.$$

In the notation of Proposition 10.2(b), this just means $A_{K\cap H^t} = \Psi^G_K(A^K_{K\cap H^t})$ in $A_K\text{-Mod}_{\mathcal{K}(G)}$. In other words, τ defines an isomorphism

$$F_{A_K}(A_H) \cong \Psi^G_K\Big(\prod_{g\in T} A^K_{K\cap H^g}\Big)$$

of rings in $A_K\text{-Mod}_{\mathcal{K}(G)}$.

Lemma 10.7. *Let $H < G$. Suppose $x, g_1, g_2, \ldots, g_n \in G$ and $1 \leq i \leq n$. Then*

$${}_H[x]_{H\cap H^{g_1}\cap\cdots\cap H^{g_n}} = {}_H[g_i]_{H\cap H^{g_1}\cap\cdots\cap H^{g_n}}$$

if and only if ${}_H[x] = {}_H[g_i]$.

Proof. It suffices to prove that for $x, y \in G$, we have ${}_H[x]_{H^y} = {}_H[y]_{H^y}$ if and only if ${}_H[x] = {}_H[y]$. This follows because for $[x] = [y]$ in $H - G/H^y$, there are $h, h' \in H$ with $x = hy(y^{-1}h'y) = hh'y$. ☐

Notation 10.8. We fix a subgroup $H < G$ and a complete set $S \subset G$ of representatives for $H - G/H$. Likewise, if $g_1, g_2, \ldots, g_n \in G$ we will write $S_{g_1,g_2,\ldots,g_n} \subset G$ to denote some complete set of representatives for $H - G/H \cap H^{g_1} \cap \cdots \cap H^{g_n}$.

Recall that $\mathcal{K}(G)$ can denote $\Bbbk G$-mod, $\mathrm{D}^b(\Bbbk G\text{-mod})$ or $\Bbbk G$-stab.

Lemma 10.9. *Let $1 \le n < [G : H]$. There is an isomorphism of rings*

$$A_H^{[n+1]} \cong \prod_{g_1,\ldots,g_n} A_{H \cap H^{g_1} \cap \cdots \cap H^{g_n}}$$

in $\mathcal{K}(G)$, where the product runs over all $g_1 \in S$ and $g_i \in S_{g_1,\ldots,g_{i-1}}$ for $2 \le i \le n$ with ${}_H[1], {}_H[g_1], \ldots, {}_H[g_n]$ distinct in $H \backslash G$.

Proof. By Remark 10.6, we know that

$$A_H \otimes A_H \cong \prod_{g \in S} A_{H \cap H^g} = A_H \times \prod_{\substack{g \in S \\ {}_H[g] \ne {}_H[1]}} A_{H \cap H^g},$$

so Proposition 2.1 shows

$$A_H^{[2]} \cong \prod_{\substack{g \in S \\ {}_H[g] \ne {}_H[1]}} A_{H \cap H^g} \quad \text{in } \mathcal{K}(G).$$

Now suppose

$$A_H^{[n]} \cong \prod_{g_1,\ldots,g_{n-1}} A_{H \cap H^{g_1} \cap \cdots \cap H^{g_{n-1}}}$$

for some $1 \le n < [G : H]$, where the product runs over all $g_1 \in S$ and $g_i \in S_{g_1,\ldots,g_{i-1}}$ for $2 \le i \le n-1$ with ${}_H[1], {}_H[g_1], \ldots, {}_H[g_{n-1}]$ distinct in $H \backslash G$. Then

$$A_H^{[n]} \otimes A_H \cong \prod_{g_1,\ldots,g_{n-1}} A_{H \cap H^{g_1} \cap \cdots \cap H^{g_{n-1}}} \otimes A_H \cong \prod_{g_1,\ldots,g_{n-1}} \prod_{g_n \in S_{g_1,\ldots,g_{n-1}}} A_{H \cap H^{g_1} \cap \cdots \cap H^{g_n}},$$

again by Remark 10.6. We note that every $g_n \in S_{g_1,\ldots,g_{n-1}}$ with either ${}_H[g_n] = {}_H[1]$ or ${}_H[g_n] = {}_H[g_i]$ for $1 \le i \le n-1$ provides a copy of $A_H^{[n]}$. By Lemma 10.7, this happens exactly n times. Hence,

$$A_H^{[n]} \otimes A_H \cong \big(A_H^{[n]}\big)^{\times n} \times \prod_{g_1,\ldots,g_n} A_{H \cap H^{g_1} \cap \cdots \cap H^{g_n}},$$

where the product runs over all $g_1 \in S$ and $g_i \in S_{g_1,\ldots,g_{i-1}}$ for $2 \le i \le n$ with distinct ${}_H[1], {}_H[g_1], \ldots, {}_H[g_n]$ in $H \backslash G$. The lemma follows by Proposition 3.5(a). ☐

Corollary 10.10. *Let $d := [G : H]$. There is an isomorphism of rings*

$$A_H^{[d]} \cong \big(A_{\mathrm{norm}_H^G}\big)^{\times k(G,H)}, \quad \text{where } k(G, H) = \frac{d!}{[G : \mathrm{norm}_H^G]},$$

in $\Bbbk G$-mod *and* $\mathrm{D}^b(\Bbbk G\text{-mod})$. *Here*, $\mathrm{norm}_H^G := \bigcap_{g\in G} g^{-1}Hg$ *is the normal core of* H *in* G.

Proof. From the above lemma, we know

$$A_H^{[d]} \cong \prod_{g_1,\dots,g_{d-1}} A_{H\cap H^{g_1}\cap\cdots\cap H^{g_{d-1}}},$$

where the product runs over some $g_1,\dots g_{d-1} \in G$ with

$$\{{}_H[1], {}_H[g_1], \dots, {}_H[g_{d-1}]\} = H - G.$$

This shows $A_H^{[d]} \cong A_{\mathrm{norm}_H^G}^{\times t}$ for some $t \geq 1$. Now, $\deg(A_{\mathrm{norm}_H^G}) = [G : \mathrm{norm}_H^G]$ and $\deg(A_H^{[d]}) = d!$ by Remark 6.3, so $t = d!/[G : \mathrm{norm}_H^G]$ by Lemma 3.8(c). □

Corollary 10.11. *The ring* A_H *in* $\mathrm{D}^b(\Bbbk G\text{-mod})$ *has constant degree* $[G : H]$ *if and only if* norm_H^G *contains every elementary abelian* p*-subgroup of* H. *In that case, its quasi-Galois closure is* $A_{\mathrm{norm}_H^G}$. *Furthermore,* A_H *is quasi-Galois in* $\mathrm{D}^b(\Bbbk G\text{-mod})$ *if and only if* H *is normal in* G.

Proof. By Lemma 8.2, A_H has constant degree $[G : H]$ in $\mathrm{D}^b(\Bbbk G\text{-mod})$ if and only if $\mathrm{supp}(A^{[d]}) = \mathrm{supp}(A) \subset \mathrm{Spc}(\mathrm{D}^b(\Bbbk G\text{-mod}))$. Hence, the first statement follows immediately from Lemma 10.4 and Corollary 10.10. By Proposition 6.9, the splitting ring of A_H is $A_{\mathrm{norm}_H^G}$, so the second statement is Theorem 9.7. Since A_H is an indecomposable ring, it is quasi-Galois if and only if it is its own splitting ring. Thus A_H is quasi-Galois if and only if $A_{\mathrm{norm}_H^G} \cong A_H$, which yields $\mathrm{norm}_H^G = H$ by comparing degrees. □

Remark 10.12. Let $H \leq G$ be a subgroup. Recall that $A_H \cong 0$ in $\Bbbk G$-stab if and only if p does not divide $|H|$. On the other hand, $A_H \cong \Bbbk$ in $\Bbbk G$-stab if and only if H is *strongly* p*-embedded in* G, that is p divides $|H|$ and p does not divide $|H \cap H^g|$ if $g \in G - H$.

Proposition 10.13. *Let* $H \leq G$ *and consider the ring* A_H *in* $\Bbbk G$-stab. *Then,*

(a) *The degree of* A_H *is the greatest* $0 \leq n \leq [G : H]$ *such that there exist distinct* $[g_1], \dots, [g_n]$ *in* $H\backslash G$ *with* p *dividing* $|H^{g_1} \cap \cdots \cap H^{g_n}|$.

(b) *The ring* A_H *is quasi-Galois if and only if* p *divides* $|H|$ *and* p *does not divide* $|H \cap H^g \cap H^{gh}|$ *whenever* $g \in G - H$ *and* $h \in H - H^g$.

(c) *If* A_H *has degree* n, *the degree is constant if and only if there exist distinct* $[g_1], \dots, [g_n]$ *in* $H\backslash G$ *such that* $H^{g_1} \cap \cdots \cap H^{g_n}$ *contains a* G*-conjugate of every elementary abelian* p*-subgroup of* H.
In that case, A_H *has quasi-Galois closure given by* $A_{H^{g_1}\cap\cdots\cap H^{g_n}}$.

Proof. For (a), recall that $\deg(A_H)$ is the greatest n such that $A_H^{[n]} \neq 0$, thus such that there exist distinct ${}_H[1], {}_H[g_1], \dots, {}_H[g_{n-1}]$ with $|H \cap H^{g_1} \cap \cdots \cap H^{g_{n-1}}|$ divisible by p.

To show (b), recall that $F_{A_H}(A_H) \cong \Psi_H^G\big(\prod_{g\in S} A^H_{H\cap H^g}\big)$ by Remark 10.6. It follows that $F_{A_H}(A_H) \cong \mathbb{1}_{A_H}^{\times \deg(A_H)}$ in A_H-$\mathrm{Mod}_{\Bbbk G\text{-stab}}$ if and only if

$$\prod_{g\in S} A^H_{H\cap H^g} \cong \Bbbk^{\times \deg(A_H)}$$

in $\Bbbk H$-stab. So, A_H is quasi-Galois in $\Bbbk G$-stab if and only if $A_H \neq 0$ and for every $g \in G$, either $A^H_{H\cap H^g} = 0$ or $A^H_{H\cap H^g} \cong \Bbbk$ in $\Bbbk H$-stab. By Remark 10.12, this means either p does not divide $|H \cap H^g|$, or p divides $|H \cap H^g|$ but does not divide $|H \cap H^g \cap H^{gh}|$ when $h \in H - H^g$. Equivalently, p does not divide $|H \cap H^g \cap H^{gh}|$ whenever $g \in G - H$ and $h \in H - H^g$.

For (c), suppose A_H has constant degree n. By Proposition 9.4, any indecomposable ring factor of $A_H^{[n]}$ is isomorphic to the splitting ring A_H^*, so Lemma 10.9 shows that the quasi-Galois closure is given by $A_H^* \cong A_{H^{g_1}\cap\cdots\cap H^{g_n}}$ for any distinct ${}_H[g_1], \ldots, {}_H[g_n]$ with $|H^{g_1} \cap \cdots \cap H^{g_n}|$ divisible by p. Then, $\mathrm{supp}(A_H) = \mathrm{supp}(A_H^*) = \mathrm{supp}(A_{H^{g_1}\cap\cdots\cap H^{g_n}})$ so $H^{g_1} \cap \cdots \cap H^{g_n}$ contains a G-conjugate of every elementary abelian p-subgroup of H. On the other hand, if there exist distinct $[g_1], \ldots, [g_n]$ in $H\backslash G$ such that $H^{g_1} \cap \cdots \cap H^{g_n}$ contains a G-conjugate of every elementary abelian p-subgroup of H, then $\mathrm{supp}(A_H^{[n]}) = \mathrm{supp}(A_{H^{g_1}\cap\cdots\cap H^{g_n}}) = \mathrm{supp}(A_H)$, so the degree of A_H is constant. □

Example 10.14. Let $p = 2$ and suppose $G = S_3$ is the symmetric group on 3 elements $\{1, 2, 3\}$. Consider the subgroup $H := \{(\,), (1\,2)\} \cong S_2$ of permutations fixing $\{3\}$. Its conjugate subgroups in G are the subgroups of permutations fixing $\{1\}$ and $\{2\}$ respectively, so $\mathrm{norm}_H^G = \{(\,)\}$. Now, A_H is a ring of degree 3 in $\mathrm{D}^b(\Bbbk G\text{-mod})$, and we immediately see that $\mathrm{supp}(A_H) = \mathrm{Spc}(\mathrm{D}^b(\Bbbk G\text{-mod}))$ because p does not divide $[G : H]$. Seeing how $\mathrm{supp}(A_H^{[3]}) \subset \mathrm{Spc}(\mathrm{D}^b(\Bbbk G\text{-mod}))$ contains only one point, the ring A_H does not have constant degree in $\mathrm{D}^b(\Bbbk G\text{-mod})$. On the other hand, the ring A_H considered in $\Bbbk G$-stab is quasi-Galois of degree 1, since H is strongly p-embedded in G.

Example 10.15. Let $p = 2$ and suppose $G = S_4$ is the symmetric group on 4 elements $\{1, 2, 3, 4\}$. If $H \cong S_3$ is the subgroup of permutations fixing $\{4\}$, the ring A_H in $\Bbbk G$-stab has constant degree 2. Indeed, the intersections $H \cap H^g$ with $g \in G - H$ each fix two elements of $\{1, 2, 3, 4\}$ pointwise, so p does not divide $[H : H \cap H^g]$; thus $\mathrm{supp}(A_H^{[2]}) = \mathrm{supp}(A_H)$. Furthermore, the intersections $H \cap H^{g_1} \cap H^{g_2}$ with $[1], [g_1], [g_2]$ distinct in $H\backslash G$ are trivial, so $A_H^{[3]} = 0$ in $\Bbbk G$-stab. The quasi-Galois closure of A_H in $\Bbbk G$-stab is A_{S_2}, with S_2 embedded in H.

Acknowledgement

I am very thankful to my advisor Paul Balmer for valuable ideas and instructive comments. I'd also like to thank the referee for detailed and very helpful suggestions.

References

[Auslander and Goldman 1960] M. Auslander and O. Goldman, "The Brauer group of a commutative ring", *Trans. Amer. Math. Soc.* **97** (1960), 367–409. MR

[Baker and Richter 2008] A. Baker and B. Richter, "Galois extensions of Lubin–Tate spectra", *Homology Homotopy Appl.* **10**:3 (2008), 27–43. MR Zbl

[Balmer 2005] P. Balmer, "The spectrum of prime ideals in tensor triangulated categories", *J. Reine Angew. Math.* **588** (2005), 149–168. MR Zbl

[Balmer 2007] P. Balmer, "Supports and filtrations in algebraic geometry and modular representation theory", *Amer. J. Math.* **129**:5 (2007), 1227–1250. MR Zbl

[Balmer 2011] P. Balmer, "Separability and triangulated categories", *Adv. Math.* **226**:5 (2011), 4352–4372. MR Zbl

[Balmer 2014] P. Balmer, "Splitting tower and degree of tt-rings", *Algebra Number Theory* **8**:3 (2014), 767–779. MR Zbl

[Balmer 2015] P. Balmer, "Stacks of group representations", *J. Eur. Math. Soc.* (*JEMS*) **17**:1 (2015), 189–228. MR Zbl

[Balmer 2016a] P. Balmer, "The derived category of an étale extension and the separable Neeman–Thomason theorem", *J. Inst. Math. Jussieu* **15**:3 (2016), 613–623. MR Zbl

[Balmer 2016b] P. Balmer, "Separable extensions in tensor-triangular geometry and generalized Quillen stratification", *Ann. Sci. Éc. Norm. Supér.* (*4*) **49**:4 (2016), 907–925. MR Zbl

[Balmer and Schlichting 2001] P. Balmer and M. Schlichting, "Idempotent completion of triangulated categories", *J. Algebra* **236**:2 (2001), 819–834. MR Zbl

[Balmer et al. 2015] P. Balmer, I. Dell'Ambrogio, and B. Sanders, "Restriction to finite-index subgroups as étale extensions in topology, KK-theory and geometry", *Algebr. Geom. Topol.* **15**:5 (2015), 3025–3047. MR

[Benson et al. 1997] D. J. Benson, J. F. Carlson, and J. Rickard, "Thick subcategories of the stable module category", *Fund. Math.* **153**:1 (1997), 59–80. MR Zbl

[Borceux and Janelidze 2001] F. Borceux and G. Janelidze, *Galois theories*, Cambridge Studies in Advanced Mathematics **72**, Cambridge University Press, 2001. MR Zbl

[Bourbaki 1981] N. Bourbaki, *Éléments de mathématique*, Lecture Notes in Mathematics **864**, Masson, Paris, 1981. MR Zbl

[Chase and Sweedler 1969] S. U. Chase and M. E. Sweedler, *Hopf algebras and Galois theory*, Lecture Notes in Mathematics **97**, Springer, Berlin, 1969. MR Zbl

[Chase et al. 1965] S. U. Chase, D. K. Harrison, and A. Rosenberg, "Galois theory and Galois cohomology of commutative rings", pp. 15–33 Mem. Amer. Math. Soc. No. **52**, 1965. MR Zbl

[DeMeyer and Ingraham 1971] F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings*, Lecture Notes in Mathematics **181**, Springer, Berlin, 1971. MR Zbl

[Eilenberg and Moore 1965] S. Eilenberg and J. C. Moore, "Foundations of relative homological algebra", pp. 39 Mem. Amer. Math. Soc. No. **55**, 1965. MR Zbl

[Evens 1991] L. Evens, *The cohomology of groups*, Clarendon, New York, 1991. MR Zbl

[Hess 2009] K. Hess, "Homotopic Hopf–Galois extensions: foundations and examples", pp. 79–132 in *New topological contexts for Galois theory and algebraic geometry* (*BIRS 2008*) (Banff, 2008), edited by A. Baker and B. Richter, Geom. Topol. Monogr. **16**, Geom. Topol. Publ., Coventry, 2009. MR Zbl

[Kreimer 1967] H. F. Kreimer, "A Galois theory for noncommutative rings", *Trans. Amer. Math. Soc.* **127** (1967), 29–41. MR Zbl

[Mac Lane 1998] S. Mac Lane, *Categories for the working mathematician*, 2nd ed., Graduate Texts in Mathematics **5**, Springer, New York, 1998. MR Zbl

[Neeman 2015] A. Neeman, "Separable monoids in $\mathrm{D}_{\mathrm{qc}}(X)$", *J. Reine Angew. Math.* (2015).

[Pauwels 2015] B. Pauwels, *Quasi-Galois theory in triangulated categories*, Ph.D. thesis, University of California, Los Angeles, 2015, Available at https://search.proquest.com/docview/1732406955.

[Rognes 2008] J. Rognes, "Galois extensions of structured ring spectra: Stably dualizable groups", pp. viii+137 Mem. Amer. Math. Soc. **192**, 2008. MR Zbl

[SGA 1 1971] A. Grothendieck, *Revêtements étales et groupe fondamental* (Séminaire de Géométrie Algébrique du Bois Marie 1960–1961), vol. 1960/61, Lecture Notes in Math. **224**, Springer, Berlin, 1971. MR

Communicated by Dave Benson
Received 2016-09-01 Revised 2017-05-29 Accepted 2017-07-09

bregje.pauwels@anu.edu.au *Mathematical Sciences Institute, The Australian National University, Acton ACT 2601, Australia*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2017 is US $325/year for the electronic version, and $520/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 11 No. 8 2017