J. Noncommut. Geom. 9 (2015), 567–602
DOI 10.4171/JNCG/201

Journal of Noncommutative Geometry

Galois bimodules and integrality of PI comodule algebras over invariants

Pavel Etingof

Abstract. Let A be a comodule algebra for a finite dimensional Hopf algebra K over an algebraically closed field k, and let A^K be the subalgebra of invariants. Let Z be a central subalgebra in A, which is a domain with quotient field Q. Assume that $Q \otimes_Z A$ is a central simple algebra over Q, and either A is a finitely generated torsion-free Z-module and Z is integrally closed in Q, or A is a finite projective Z-module. Then we show that A and Z are integral over the subring of central invariants $Z \cap A^K$. More generally, we show that this statement is valid under the same assumptions if Z is a reduced algebra with quotient ring Q, and $Q \otimes_Z A$ is a semisimple algebra with center Q. In particular, the statement holds for a coaction of K on a prime PI algebra A whose center Z is an integrally closed finitely generated domain over k. For the proof, we develop a theory of Galois bimodules over semisimple algebras finite over the center.

Mathematics Subject Classification (2010). 16T20.

Keywords. Coaction, comodule algebra, center, invariants, integrality.

1. Introduction

The goal of this paper is to prove a noncommutative analogue (for PI algebras) of Skryabin's integrality theorem for coactions of a finite dimensional Hopf algebra K on a commutative algebra A. In [12], Theorem 2.5 and Proposition 2.7, Skryabin showed under a very minor assumption (that A has no nonzero nilpotent K-costable ideals, which is not needed in positive characteristic) that such an algebra A is integral over its invariants A^K. This is a generalization of the classical theorem of E. Noether saying that a commutative algebra is integral over its invariants under a finite group action. [1]

We extend Skryabin's result to the case when A is a noncommutative PI algebra over an algebraically closed field k, under some assumptions. Namely, let $Z \subset A$ be

[1] Skryabin's result is a generalization of Noether's theorem because an action of a finite group G on A is the same thing as a coaction on A of the Hopf algebra $\mathrm{Fun}(G)$ of functions on G with values in the ground field.

a central subalgebra which is a domain, such that A is a finitely generated Z-module. We show in Theorem 3.1 that if (I) $Q \otimes_Z A$ is a central simple algebra over Q (where Q is the quotient field of Z), and (II) A is a projective Z-module, or A is a torsion free Z-module and Z is integrally closed in Q, then Z and hence A is integral over $Z \cap A^K$. In particular, we show that this property holds for a coaction of K on a prime PI algebra A whose center Z is an integrally closed finitely generated domain over k. [2] Further, we show that the degree of Q over Q^K (the field of quoteints of $Z \cap A^K$) divides the dimension of K (Proposition 3.9).

We also generalize these results to the case when Z is not necessarily a domain. Namely, we show in Theorem 5.1 that the same integrality result holds if Z is a reduced algebra, and $Q \otimes_Z A$ is a semisimple algebra with center Q. Finally, in Proposition 5.4 we generalize the divisibility result of Proposition 3.9.

Skryabin's proof is based on the freeness theorem for finite dimensional Hopf algebras over coideal subalgebras, which he uses to show that A has invariant characteristic polynomials. Our proof is ideologically similar to Skryabin's proof. Namely, we show that the coefficients of the minimal polynomial and the characteristic polynomial of the operator of right multiplication by $z \in Z$ on $Q \otimes_Z A$ belong to Z and are K-invariant. However, in the noncommutative setting the coaction does not give rise to coideal subalgebras, so we use a different method, based on minimal polynomials. [3]

Namely, we develop a theory of *Galois bimodules* over fields and, more generally, over central simple algebras and semisimple algebras finite over the center, which may be of independent interest. For an algebra A, a Galois A-bimodule of rank d is an A-bimodule P which is free of rank d on each side, and satisfies the equation $P \otimes_A P \cong P^d$. We prove a classification theorem for Galois bimodules over a field L (Theorem 2.31) which says that such a bimodule is simply a multiple of $L \otimes_F L$, where F is the center of P, i.e. the largest subalgebra of L over which P is linear. Similarly, we show that any Galois bimodule over a central simple algebra B over a field L is a rational multiple of $B \otimes_F B$ (Proposition 2.37). The same statement holds more generally (for connected Galois bimodules) if B is a semisimple algebra which is finite over its center (Proposition 4.6). [4]

The theory of Galois bimodules is applied to the problem of invariants in the

[2] In the case when K is basic (i.e., K^* is pointed), similar (but not equivalent) results were obtained by A. Totok in [15], Theorem 2.5. Also, some results about integrality and finiteness of noncommutative module algebras over invariants are obtained in [1].

[3] We expect, however, that by using the results of [13] on projectivity and freeness over comodule algebras, one can obtain different proofs of our results, which are more direct generalizations of the arguments of [12].

[4] We also introduce the notion of a weakly Galois bimodule, replacing the condition that $P \otimes_A P = P^d$ by a weaker condition that $P \otimes_A P$ is contained in P^N for some N, and show that much of the theory of Galois bimodules in fact goes through for weakly Galois bimodules. Finally, we study quasi-Galois bimodules over commutative semisimple algebras L, i.e. bimodules P finite on both sides and such that $P \otimes_L P \cong P^d$, and provide their classification (Theorem 4.2).

following way. We show that the Hopf coaction of K on A makes the tensor product [5] $Q \otimes_Z A \otimes K$ into a Galois bimodule over the algebra $Q \otimes_Z A$. This allows us to establish the invariance of the characteristic polynomials of the right action of $z \in Z$ on $Q \otimes_Z P$ and thus obtain the desired integrality result (Theorem 3.1, Theorem 5.1). [6]

We also relate Galois bimodules to tensor subcategories of the tensor category of bimodules over a field studied in [7] and of the tensor category of bimodules over a central simple algebra, and explain that these subcategories are twisted forms of categories of bimodules over semisimple algebras in the sense of [2].

Finally, our approach motivates the definition of a new invariant of a Hopf coaction on a central simple algebra — its Galois group. It would be interesting to study this invariant further.

The paper is organized as follows. In Section 2 we develop the theory of Galois and weakly Galois bimodules over fields and central simple algebras, and obtain the classification of Galois bimodules. In Section 3, we apply the theory of Section 2 to prove the integrality theorem (Theorem 3.1) in the case when Z is a domain, and discuss various consequences and examples. In Section 4 we develop the theory of Galois bimodules over semisimple algebras finite over the center, and obtain their classification. In Section 5 we apply the results of Section 4 to obtain integrality (Theorem 5.1) in the case when Z is a reduced algebra. Finally, in Section 6 we discuss the connection of the theory of Galois bimodules for fields with tensor subcategories of the category of bimodules over fields discussed in [7].

Acknowledgements. This work was partially supported by the NSF grant DMS-1000113. The author is very grateful to Chelsea Walton for introducing him to this field, for many useful discussions and ideas that inspired this work, and for helpful comments on this paper.

2. Galois bimodules

2.1. Bimodules. Let P be a bimodule over a unital ring A. Then we have a homomorphism $\phi_P : A^{op} \to \mathrm{End}_A(P)$ induced by the right action of A. We will denote ϕ_P just by ϕ, when no confusion is possible.

Assume from now on that P is free of rank $d \geq 1$ as a left module. Then, fixing an identification $P \cong A^d$ as left modules, we can view ϕ_P as a homomorphism $A \to \mathrm{Mat}_d(A)$.

[5] Throughout the paper, $\otimes$ without subscript will denote the tensor product over the ground field k.

[6] When we pass from A to the associated Galois bimodule, we forget almost everything about the coaction, but remember just enough to study the invariants of the coaction in the center of A.

Definition 2.1. We say that P is *linear* over a central subring $k \subset A$ if the left and right action of k coincide on P. The *center* of P is the set $\mathcal{Z}(P)$ of $z \in A$ such that $zx = xz$ for all $x \in P$, i.e. such that $\phi_P(z) = z \cdot \mathrm{Id}$.

Remark 2.2. 1. An A-bimodule linear over k is the same thing as a left module over $A \otimes_k A^{\mathrm{op}}$.

2. $\mathcal{Z}(P) \subset A$ is the maximal central subring of A over which P is linear. Indeed, if $z \in \mathcal{Z}(P)$ then for any $x \in P$, $a \in A$, $(az)x = a(zx) = a(xz) = (ax)z = z(ax) = (za)x$, hence $za = az$ since P is free over A. Thus z belongs to the center of A.

Let P be a bimodule over a field L which has dimension d as a left and right L-vector space.

Definition 2.3. We say that P is *split* if for each $a \in L$, the eigenvalues of $\phi_P(a)$ are contained in L. In this case, we say that P is *split separable* if in addition the matrices $\phi_P(a)$ are diagonalizable for all a.

Given an algebra A and an automorphism $g \in \mathrm{Aut}(A)$, let Ag denote the A-bimodule which is A as a left A-module, while the right A-action is multiplication twisted by g: $a \circ x \circ b = axg(b)$ for $a, x, b \in A$.

Lemma 2.4. *An L-bimodule P is split if and only if it has a finite filtration whose successive quotients are of the form Lg, where $g \in \mathrm{Aut}(L)$. Moreover, a split L-bimodule P is separable if and only if it is semisimple as a bimodule.*

Proof. Assume P is split. Then there exists a basis $v_1, \dots, v_d$ of P as a left vector space in which $\phi_P(a)$ are upper triangular for all $a \in L$. Let $\mathbf{F}_i P$ be the span of $v_1, \dots, v_i$. Then $\mathbf{F}_\bullet$ is a bimodule filtration, and $\mathbf{F}_{i+1}P/\mathbf{F}_i P$ is L with the usual left action of L and right action given by some field embedding $g_i : L \to L$. Since P has dimension d as a right vector space, these embeddings are all isomorphisms. Thus, $\mathbf{F}_{i+1}P/\mathbf{F}_i P = Lg_i$ for some $g_i \in \mathrm{Aut}(L)$. Conversely, it is clear that any bimodule having a filtration with successive quotients Lg is necessarily split.

Now, if P is separable, then the basis $\{v_i\}$ can be chosen in such a way that the matrices $\phi_P(a)$ are diagonal, so we get that $P = \oplus_i Lg_i$, i.e. P is semisimple. Conversely, if P is semisimple then the filtration $\mathbf{F}_\bullet$ must split, which implies that P is separable. The lemma is proved. □

2.2. Galois and weakly Galois bimodules.

Definition 2.5. A *weakly Galois bimodule* over A of rank $d \geq 1$ is an A-bimodule P such that $P \cong A^d$ as a left and right A-module, and $P \otimes_A P$ is contained in P^N as an A-bimodule for some N. If moreover $P \otimes_A P \cong P^d$ as an A-bimodule, then we call P a *Galois bimodule* of rank d.

Example 2.6. 1. A^d is a Galois A-bimodule of rank d.

2. If every right-invertible element of A is left-invertible, and if P is a Galois A-bimodule of rank 1 then $P = A$. Indeed, $\phi : A \to A$ is a homomorphism which makes A into a free right module of rank 1 over itself. This means that ϕ is injective. Fix a generator $x \in A$ of this module. Then for any $y \in A$ there exists $a_y \in A$ such that $y = x\phi(a_y)$. In particular, $1 = x\phi(a_1)$, hence x is right invertible and thus invertible. So the equality $xy = x\phi(a_{xy})$ implies $y = \phi(a_{xy})$, i.e. ϕ is surjective, and hence an automorphism. Moreover, since P is a Galois bimodule, $\phi^2 = \phi$ modulo inner automorphisms, hence ϕ is inner and we can assume that $\phi = \mathrm{Id}$, as claimed.

3. If A is a commutative algebra, and B is an A-algebra which is free of rank d as an A-module (e.g. if B is a field extension of degree d of a field A) then $B \otimes_A B$ is a Galois bimodule over B of rank d.

4. Let $G \subset \mathrm{Aut}(A)$ be a finite subgroup, let $n_g > 0$ be integers, and let $P = \oplus_{g\in G}(Ag)^{n_g}$. Then P is a weakly Galois A-bimodule of rank $d = \sum_{g\in G} n_g$. Moreover, if all n_g are equal, then P is a Galois A-bimodule.

Lemma 2.7. (i) *Suppose that B is an extension of A such that B is isomorphic to A^n as an A-bimodule (for instance, if $A \subset B$ is a field extension of degree n). In this case, if P is a Galois (respectively, weakly Galois) bimodule of rank d over A, then $B \otimes_A P \otimes_A B$ is a Galois (respectively, weakly Galois) bimodule of rank dn over B.*

(ii) *If P is a Galois (respectively, weakly Galois) bimodule over A of rank d linear over k, and B is another k-algebra, then $P \otimes_k B$ is a Galois (respectively, weakly Galois) bimodule over $A \otimes_k B$ of rank d. For instance, for $B = \mathrm{Mat}_m(k)$, we have that $P \otimes_k B = \mathrm{Mat}_m(P)$ is a (weakly) Galois bimodule over B.*

(iii) *If B is a central simple algebra with center A and $\dim_A B = m^2$, then the restriction to A of any Galois (respectively, weakly Galois) B-bimodule P of rank d is a Galois (respectively, weakly Galois) bimodule of rank dm^2.*

Proof. (i) Let P be a Galois (respectively, weakly Galois) A-bimodule of rank d. Then it is clear that under the assumptions of (i), $B \otimes_A P \otimes_A B$ is free as a left and right B-module of rank dn. Also

$$B \otimes_A P \otimes_A B \otimes_B B \otimes_A P \otimes_A B = (B \otimes_A P \otimes_B P \otimes_A B)^n,$$

which equals $(B \otimes_A P \otimes_A B)^{dn}$ (respectively, is contained in $(B \otimes_A P \otimes_A B)^{Nn}$ for some N), as desired.

(ii) This follows from the fact that $(P \otimes_k B) \otimes_{A\otimes_k B} (P \otimes_k B) = (P \otimes_A P)_{\otimes_k} B$.

(iii) We have $B \otimes_A B^{op} \cong \mathrm{End}_A(B)$, so any B-bimodule linear over A is a multiple of B. In particular, $B \otimes_A B = B^{m^2}$ as a B-bimodule. Thus, $P \otimes_A P = P \otimes_B B \otimes_A B \otimes_B P = (P \otimes_B P)^{m^2}$, which implies the statement. □

2.3. Galois bimodules coming from Hopf coactions. Let K be a finite dimensional Hopf algebra over an algebraically closed field k with coproduct Δ, counit ε, and antipode S. Let A be a (unital) k-algebra. Recall ([10]) that A is called a *right K-comodule algebra* if it is equipped with a coaction map $\rho : A \to A \otimes K$ which is an algebra homomorphism, and such that it equips A with a structure of a K-comodule, i.e.,

$$(\rho \otimes 1)(\rho(a)) = (1 \otimes \Delta)(\rho(a)),\ (1 \otimes \varepsilon)(\rho(a)) = a,\ a \in A.$$

Now suppose that A is an algebra with a coaction of a finite dimensional Hopf algebra K of dimension d. So we have a coaction map $\rho : A \to A \otimes K$. This map equips the tensor product $P := A \otimes K$ with a structure of an A-bimodule, via $a \circ x \circ b := (a \otimes 1)x\rho(b), a, b \in A, x \in P$.

Proposition 2.8. *P is a Galois bimodule over A of rank d. Moreover, one has $\mathcal{Z}(P) = \mathcal{Z}(A)^K$, where $\mathcal{Z}(A)^K := \mathcal{Z}(A) \cap A^K$ is the subalgebra of central invariants of A.*

Proof. This is well known, but we will give a proof for reader's convenience.

It is clear that $P \cong A^d$ as a left A-module. Let us show that this is also the case as a right module. To this end, define the linear map $\psi : A \otimes K \to A \otimes K$ by $\psi(a \otimes y) = (1 \otimes y)\rho(a)$. Then

$$\psi(a_1 \otimes y)\rho(a_2) = (1 \otimes y)\rho(a_1)\rho(a_2) = (1 \otimes y)\rho(a_1a_2) = \psi(a_1a_2 \otimes y),$$

which shows that ψ is a homomorphism of right modules, where the target module is just the tensor product of A with the vector space K. So it is enough to show that ψ is an isomorphism. To do so, define another map $\xi : A \otimes K \to A \otimes K$ by

$$\xi(a \otimes y) = (1 \otimes y)(1 \otimes S^{-1})(\rho(a)).$$

Then it is easy to check that ξ is the inverse of ψ, which implies that ψ is an isomorphism.

Finally, let us show that $P \otimes_A P$ is isomorphic to P^d. Actually, the coaction gives rise to an explicit isomorphism. Consider the linear map $\tau : P \otimes_A P \to P \otimes K = A \otimes K \otimes K$ defined by the formula

$$\tau(a_1 \otimes y_1 \otimes a_2 \otimes y_2) := (a_1 \otimes y_1)\rho(a_2) \otimes y_2.$$

It is easy to see that this map is well defined, is an isomorphism, and commutes with the left action of A in the first component. Identifying $P \otimes_A P$ with $A \otimes K \otimes K$ using τ, we can transport the A-bimodule structure of $P \otimes_A P$ to $A \otimes K \otimes K$, and the transported structure is given by

$$a \circ x \circ b = (ax \otimes 1 \otimes 1)(1 \otimes \Delta)(\rho(b)),\ x \in A \otimes K \otimes K, a, b \in A.$$

So it remains to note that $K \otimes K$ is isomorphic to $K \otimes K_{\mathrm{vect}}$ as a right K-module, where K_{vect} is K with the trivial action of K.

The last statement follows directly from the definitions. □

2.4. Basic facts from Galois theory. Recall the basic setup of Galois theory ([9]). Let $L \supset F$ be a normal algebraic field extension, i.e. L is the splitting field over F of a family of polynomials. Let F_{perf} be the perfect closure of F in L, i.e. the field of elements whose p^n-th power is in F for some n if $\text{char} F = p$ (in characteristic zero, by definition $F_{\text{perf}} = F$). Let L_{sep} be the field of separable elements in L over F, i.e. those whose minimal polynomials are separable (have a nonzero derivative). Then L is a separable extension of F_{perf} (see [9], Chapter 5, Proposition 6.11), and a purely inseparable extension of L_{sep}, and $[L : F_{\text{perf}}] = [L_{\text{sep}} : F]$. Moreover, this number (finite or infinite) equals the order of the Galois group $G = \text{Gal}(L/F)$, which is the group of automorphisms of L which acts trivially on F. One has $L^G = F_{\text{perf}}$, $GL_{\text{sep}} = L_{\text{sep}}$, and $L_{\text{sep}}^G = F$.

2.5. Galois and weakly Galois bimodules over fields.

Proposition 2.9. *Let P be a bimodule over a field L which is finite dimensional on both sides and such that $P \otimes_L P$ is contained in a multiple of P. Then the right and left dimensions of P coincide, so that P is a weakly Galois L-bimodule.*

Proof. Let $\dim_L P = d$, $\dim P_L = d'$. The bimodule P has finite length (which is $\leq \min(d, d')$). Let $\{R_m\}$ be the simple composition factors of P, and let r_-, r_+ be the minimal and maximal ratio of the right dimension and the left dimension among the R_m. Since $P \otimes_L P$ is contained in P^N, the bimodule $P^{\otimes s}$ is contained in $P^{N^{s-1}}$, so the ratio r_s of the right dimension to the left dimension of $P^{\otimes s}$ satisfies the inequalities $r_- \leq r_s \leq r_+$. But $r_s = (d'/d)^s$. Thus, $r_- \leq (d'/d)^s \leq r_+$. This implies that $d' = d$. □

Let P be a weakly Galois bimodule of rank d over a field L. Let $\phi = \phi_P : L \to \text{Mat}_d(L)$ be the corresponding right action map. For each $a \in L$, let $\mu_a(t) = \sum_{i=0}^{d_a} c_i(a) t^i$ be the minimal polynomial of the matrix $\phi(a)$ over L ($c_{d_a} = 1$).

Proposition 2.10. *The coefficients of $\mu_a(t)$ belong to $\mathcal{Z}(P)$.*

Proof. Let us view ϕ as a map $L \to \text{Mat}_d(k) \otimes_k L$. Applying ϕ in the second component to the identity

$$\mu_a(\phi(a)) = \sum_{i=0}^{d_a} (1 \otimes c_i(a)) \phi(a)^i = 0,$$

we have

$$\sum_{i=0}^{d_a} (1 \otimes \phi(c_i(a)))(1 \otimes \phi)(\phi(a))^i = 0.$$

On the other hand, $\phi_{P \otimes_L P}(a) = (1 \otimes \phi)(\phi(a))$ so since $P \otimes_L P$ is contained in P^N, we see that the matrix $(1 \otimes \phi)(\phi(a))$ is conjugate to the restriction of $\text{Id}_N \otimes \phi(a)$ to

an invariant subspace. This implies that

$$\sum_{i=0}^{d_a}(1\otimes 1\otimes c_i(a))(1\otimes\phi)(\phi(a))^i=0.$$

So, subtracting, we get

$$\sum_{i=0}^{d_a-1}(1\otimes(\phi(c_i(a))-1\otimes c_i(a)))(1\otimes\phi)(\phi(a))^i=0 \tag{2.1}$$

(note that the terms corresponding to $i=d_a$ cancel since $c_{d_a}(a)=1$).

Let $C=L\phi(L)$ be the subalgebra of $\mathrm{Mat}_d(L)$ generated by L and $\phi(L)$. Then C is a commutative algebra over the field $\phi(L)$, and equation (2.1) can be viewed as an identity in $\mathrm{Mat}_d(k)\otimes_k C\subset \mathrm{Mat}_d(k)\otimes_k \mathrm{Mat}_d(k)\otimes_k L$.

Since $\mu_a(t)$ has degree d_a, the matrices $\phi(a)^i\in \mathrm{Mat}_d(k)\otimes_k L$ for $i=0,\dots,d_a-1$ are linearly independent over L. This implies that the matrices $(1\otimes\phi)(\phi(a)^i)\in \mathrm{Mat}_d(k)\otimes_k\phi(L)$ for $i=0,\dots,d_a-1$ are linearly independent over $\phi(L)$, hence over C. However, equation (2.1) provides a linear relation between them over C. So this relation must be trivial, which implies that $\phi(c_i(a))=1\otimes c_i(a)$ for all i, as desired. □

Proposition 2.11. *If P is a weakly Galois L-bimodule, then L is an algebraic extension of the center $\mathcal{Z}(P)$.*

Proof. Proposition 2.10 implies that for every $a\in L$, $\phi(a)$ satisfies a monic polynomial equation over $\mathcal{Z}(P)$, namely the equation $\mu_a(t)=0$. Hence, a itself satisfies the same equation. Thus, L is an algebraic extension of $\mathcal{Z}(P)$. □

Proposition 2.12. *If L has characteristic zero or $p>d$, then the matrix $\phi_P(a)$ is semisimple for all $a\in L$, i.e., its minimal polynomial μ_a has distinct roots (over an extension of L).*

Proof. Let $\mathcal{Z}=\mathcal{Z}(P)$, and consider the subfield F of $\phi(L)$ generated over $\mathcal{Z}=\phi(\mathcal{Z})$ by $\phi(a)$. Then by Proposition 2.10, $F=\mathcal{Z}[t]/(\mu_a(t))$, so it is a finite field extension of $\mathcal{Z}$ of degree $\le d$. Since we are in characteristic zero or $p>d$, this extension is separable, so μ_a has distinct roots and $\phi(a)$ is semisimple. □

Remark 2.13. Proposition 2.12 is false in positive characteristic if p divides d. For example, let $\mathcal{Z}=k(t)$, where k has characteristic p, let $L=\mathcal{Z}[u]/(u^p-t)$, and let $P=L\otimes_{\mathcal{Z}}L$. Then $\phi_P(u)$ is the operator of multiplication by x in $L[x]/(x^p-t)$, which is not semisimple, since $(x-u)^p=0$ but $x-u\neq 0$. The extension $L/\mathcal{Z}$ is not separable in this case.

2.6. Split Galois and weakly Galois bimodules over fields.

Proposition 2.14. (i) *If P is a split weakly Galois L-bimodule then L is a normal extension of $\mathcal{Z}(P)$.*

(ii) *Let L be a finite field extension of F. The Galois L-bimodule $L \otimes_F L$ is split if and only if L is a normal extension of F.*

(iii) *In characteristic 0 or $p > d$ all split weakly Galois L-bimodules of rank d are separable.*

Proof. (i) By Proposition 2.10, the minimal polynomial of $\phi(a) \in \phi(L)$ over $\mathcal{Z}(P)$ is μ_a. Hence, the minimal polynomial of $a \in L$ over $\mathcal{Z}(P)$ is also μ_a (as $\phi : L \to \phi(L)$ is an isomorphism). Thus, L is the minimal common splitting field for the polynomials $\mu_a, a \in L$, so it is a normal extension.

(ii) It is clear that the center of the L-bimodule $L \otimes_F L$ is F, so the "only if" part follows from (i). To prove the "if" part, note that the eigenvalues of $\phi(a)$ for $a \in L$ are the roots of the minimal polynomial of a over F. Since L is normal, all the roots of this polynomial are in L, i.e. $L \otimes_F L$ is a split Galois bimodule.

(iii) This follows from Proposition 2.12. □

Now we will describe the structure of split Galois and weakly Galois bimodules. Recall Example 2.6(4). Given a finite subgroup $G \subset \mathrm{Aut}(L)$ and integers $n_g > 0$, define the split separable weakly Galois L-bimodule

$$P(\mathbf{n}, L, G) := \oplus_{g \in G} (Lg)^{n_g},$$

of rank $d = \sum_{g \in G} n_g$ (where $\mathbf{n} : G \to \mathbb{Z}$ is given by $\mathbf{n}(g) = n_g$). It is clear that $\mathcal{Z}(P(\mathbf{n}, L, G)) = L^G$. If $n_g = 1$, then $P(\mathbf{n}, L, G)$ is a Galois L-bimodule, and we will denote it by $P(L, G)$. It is easy to see that $P(L, G) \cong L \otimes_{L^G} L$.

Proposition 2.15. *(i) All split separable weakly Galois L-bimodules P of rank d are of the form $P = P(\mathbf{n}, L, G)$ with $\sum_{g \in G} n_g = d$. This L-bimodule is Galois if and only if $n_g = r$ is a constant function, with $r|G| = d$. Moreover, the group G is completely determined by P.*

(ii) Let P be a split Galois (respectively, weakly Galois) L-bimodule, and let $\mathrm{gr}(P)$ be its associated graded bimodule under the socle filtration (as an L-bimodule). Then $\mathrm{gr}(P)$ is a split separable Galois (respectively, weakly Galois) bimodule, and it has the form given in (i).

Proof. (i) By Lemma 2.4, $P \cong \oplus_{i=1}^{d} Lg_i$ for some $g_i \in \mathrm{Aut}(L)$. Let G be the set of all g_i. Since $P \otimes_L P$ is contained in P^N, for any i, j there is an m such that $g_i \circ g_j = g_m$. This means that the set G of all the g_i inside $\mathrm{Aut}(L)$ is closed under composition, so it is a finite subgroup[7]. For each $g \in G$, let $n_g > 0$ be the

[7]It is clear that a finite subset G of any group which is closed under multiplication is a subgroup. Indeed, if $g \in G$ then by the pigeonhole principle $g^m = g^n$ for some $m > n$, so $g^{m-n} = 1$ and $g^{m-n-1} = g^{-1}$.

multiplicity of g among the g_i. Then $P = P(\mathbf{n}, L, G)$, where $\mathbf{n} = (n_g)$, which proves the first statement.

Now assume that P is Galois of rank d. Then the element $\mathbf{p} := \sum_{g\in G} n_g g$ satisfies the relation $\mathbf{p}^2 = d\mathbf{p}$. Also, since $\sum_g n_g = d$, we get $\mathbf{p}(\sum_g g) = d(\sum_g g)$. Thus by the Frobenius–Perron theorem, there exists a positive integer r such that $\sum n_g g = r \sum_g g$, so $n_g = r$, $P = P(L, G)^r$.

The group G is the group of all $g \in \mathrm{Aut}(L)$ such that Lg occurs in P, so it is completely determined by P. Part (i) is proved.

(ii) By Lemma 2.4, $\mathrm{gr}(P)$ is a split separable Galois (respectively, weakly Galois) L-bimodule, and (i) applies. □

Remark 2.16. Over a field of characteristic $p > 0$, a split Galois bimodule may fail to be separable (=semisimple). An example of such a Galois L-bimodule P is given in Remark 2.13. This bimodule has length p, and all its composition factors are copies of the trivial bimodule L.

2.7. Behavior of split weakly Galois bimodules under field extensions. Note that if a Galois bimodule P over L is split, and if E is a finite field extension of L, then the bimodule $Q := E \otimes_L P \otimes_L E$, which is a Galois E-bimodule by Lemma 2.7(i), does not have to be split, even if E is Galois over L.

Example 2.17. Let $L = \mathbb{C}(t)$ and $G = \mathbb{Z}/2$ acting on L by $t \mapsto -t$. Let

$$E := L[u]/(u^2 - 1 - t).$$

Take the Galois bimodule $P := P(L, G)$ over L, of rank 2. Then Q has rank 4. Consider the eigenvalues of the 4 by 4 matrix $\phi_Q(u)$. They are $\pm\sqrt{1+t}$ and $\pm\sqrt{1-t}$, and the last two don't belong to E. Thus, Q is not split over E.

This happens because E is not Galois over L^G (it has degree 4 over L^G, while the Galois closure has degree 8) and the automorphism g of L given by $g(t) = -t$ does not lift to E. More precisely, we have the following result.

Proposition 2.18. *Let $G \subset \mathrm{Aut}(L)$ be a finite subgroup, and E a normal extension of L. Then:*

(i) *The weakly Galois E-bimodule $Q = E \otimes_L P(\mathbf{n}, L, G) \otimes_L E$ is split if and only if E is a normal extension of the center $\mathcal{Z}(P(\mathbf{n}, L, G)) = L^G$.*

(ii) *In this case, $\mathrm{gr}(Q) = P(r\mathbf{n}, E, G')$, where $G' = \mathrm{Gal}(E/L^G)$ and $r = [E : E_{\mathrm{sep}}]$, so that we have an exact sequence*

$$1 \to \mathrm{Gal}(E/L) \to G' \to G \to 1,$$

and where we denote the pullback of $\mathbf{n}$ to G' also by $\mathbf{n}$. Moreover, if E is separable over L, we have $Q = P(\mathbf{n}, E, G')$.

Proof. (i) The bimodule $P(\mathbf{n}, L, G)$ contains $P(L, G)$ and is contained in its multiple. Also, we have

$$E \otimes_L P(L, G) \otimes_L E = E \otimes_L L \otimes_{L^G} L \otimes_L E = E \otimes_{L^G} E,$$

so (i) follows from Proposition 2.14(ii).

To prove (ii), note that Q has a filtration with successive quotients $Eg \otimes_L E$, $g \in G$ (n_g copies of each), and $Eg \otimes_L E$ has a filtration whose successive quotients are Eh, where $h \in g \cdot \mathrm{Gal}(E/L)$ (each occurring r times). This implies the statement on the structure of $\mathrm{gr}(Q)$. Finally, if E is separable over L, then Q is separable too, and thus $Q = P(\mathbf{n}, E, G')$. □

2.8. General weakly Galois bimodules. Let L be a field and P be a weakly Galois L-bimodule of rank d.

Theorem 2.19. (i) *Let E be the smallest field extension of L that contains all the eigenvalues of $\phi(a) := \phi_P(a)$, $a \in L$. Then E is a finite extension of L and a normal extension of $\mathcal{Z}(P)$.*

(ii) *$E \otimes_L P \otimes_L E$ is a split weakly Galois E-bimodule of rank $d[E : L]$, which is Galois if so is P.*

(iii) *We have* $\mathrm{gr}(E \otimes_L P \otimes_L E) = P(\mathbf{n}, E, G)$, *where G is a finite subgroup of* $\mathrm{Aut}(E)$ *containing $H := \mathrm{Gal}(E/L)$ as a (not necessarily normal) subgroup.*

(iv) *P contains a copy of the trivial bimodule L.*

(v) *If F is any finite extension of L then $\mathcal{Z}(F \otimes_L P \otimes_L F) = \mathcal{Z}(P)$. In particular, $\mathcal{Z}(F \otimes_L P(\mathbf{n}, L, G) \otimes_L F) = L^G$.*

(vi) *The center $\mathcal{Z}(\mathrm{gr}(E \otimes_L P \otimes_L E))$ is $L^G := L \cap E^G = E^G$.*

(vii) *P is split if and only if* $\mathrm{Gal}(E/L)$ *is normal in G.*

Proof. (i) Consider the commutative finite dimensional L-algebra $C = L\phi(L) \subset \mathrm{Mat}_d(L)$. Let $a_1, \dots, a_s \in L$ be such that $\phi(a_1), \dots, \phi(a_s)$ are generators of C over L. Consider the field E_* obtained from L by adding the eigenvalues of $\phi(a_i)$, $i = 1, \dots, s$. Then E_* is finite over L, and there exists a basis $\mathcal{B}$ of E_*^d over E_* in which the matrices $\phi(a_i)$ are upper triangular. In this basis, the matrix $\phi(a)$ is upper triangular for all $a \in L$, since it is a polynomial of $\phi(a_i)$ over L. Thus, E_* contains all the eigenvalues of $\phi(a)$, so $E_* = E$, and hence E is finite over L.

It is clear that E is a normal extension of $\mathcal{Z}(P)$, since it is the splitting field of the minimal polynomials of $\phi(a)$ for $a \in L$, which according to Proposition 2.10 have coefficients in $\mathcal{Z}(P)$.

(ii) By Lemma 2.7(i), $E \otimes_L P \otimes_L E$ is a weakly Galois E-bimodule. Let $\lambda_j : L \to E$, $j = 1, \dots, d$, be the eigenvalue homomorphisms for ϕ, i.e. $\lambda_j(a)$ are the diagonal entries of $\phi(a)$ in the basis $\mathcal{B}$. Since E is normal over $\mathcal{Z}(P)$, for any i, there exists an automorphism $g_i \in \mathrm{Gal}(E/\mathcal{Z}(P))$ such that $\lambda_i(a) = g_i a$ for any $a \in L$. This implies that $E^{\lambda_i} \otimes_L E = Eg_i \otimes_L E$, which means that the associated

graded bimodule $\mathrm{gr}(E \otimes_L P \otimes_L E)$ of $E \otimes_L P \otimes_L E$ under the socle filtration is the direct sum of bimodules Eg_ih, where h runs through $\mathrm{Gal}(E/L)$. This implies that $E \otimes_L P \otimes_L E$ is a split weakly Galois E-bimodule, which is Galois if so is P, proving (ii).

(iii) Given (ii), Proposition 2.15 applied to $\mathrm{gr}(E \otimes_L P \otimes_L E)$ implies that the set G of elements g_ih must form a finite subgroup of $\mathrm{Gal}(E/\mathcal{Z}(P))$ containing $H := \mathrm{Gal}(E/L)$, and $\mathrm{gr}(E \otimes_L P \otimes_L E) = P(\mathbf{n}, E, G)$. Thus (iii) is proved.

(iv) By (iii), for some $i = i_0$, $\lambda_i|_L$ has to be the identity. Let us take a common eigenvector $v \in P$ of $\phi(a)$ with eigenvalue $\lambda_{i_0}(a) = a$: $\phi(a)v = av$ for all $a \in L$. Then $Lv \subset P$ is a subbimodule isomorphic to L. This proves (iv).

(v) Note first that $E \otimes_L P \otimes_L E$ contains P as an L-bimodule, so $L \cap \mathcal{Z}(E \otimes_L P \otimes_L E) = \mathcal{Z}(P)$. Also note that by (iv), $E \otimes_L P \otimes_L E$ has a subbimodule isomorphic to $E \otimes_L E$. Hence $\mathcal{Z}(E \otimes_L P \otimes_L E) \subset L$, which implies that $\mathcal{Z}(E \otimes_L P \otimes_L E) = \mathcal{Z}(P)$, as desired.

(vi) This follows from (iii).

(vii) If P is split, Proposition 2.18 implies that $\mathrm{Gal}(E/L)$ is normal in G. Conversely, if $\mathrm{Gal}(E/L)$ is normal in G, we see that L is a Galois extension of L^G, and $\mathrm{Gal}(L/L^G) = G/\mathrm{Gal}(E/L)$, so the statement follows. □

Example 2.20. If P has the same dimension over L as a right and left vector space but is not weakly Galois, then there may be no extension E such that $E \otimes_L P \otimes_L E$ is split. For example, consider $L = \mathbb{C}(t)$ and $P = L \oplus L$, with the left and right actions defined by

$$(f \circ (a, b) \circ g)(t) = (f(t)a(t)g(t^2), f(t^2)b(t)g(t)),$$

Then P is 3-dimensional over L on both sides, and the maps λ_i are defined by $\lambda_1(t) = t^2$, $\lambda_2(t) = t^{1/2}$, $\lambda_3(t) = -t^{1/2}$. So the splitting field E has to contain $t^{1/2^n}$ for all n and therefore cannot be finite over L. Note that $\mathcal{Z}(P) = \mathbb{C}$, so L is a transcendental extension of $\mathcal{Z}(P)$.

Corollary 2.21. *Let P be a Galois bimodule over a field L of degree d.*

(i) *Some power $\chi_a^{N_a}$ of the characteristic polynomial χ_a of $\phi_P(a)$, $a \in L$ is a power of its minimal polynomial μ_a. In characteristic zero or $p > d$, one may take $N_a = 1$, and in characteristic p in general, one may take $N_a = p^s$ for some $s = s_a$ such that p^s divides $[L : \mathcal{Z}(P)]$.*[8]

(ii) *The coefficients $C_i(a)$ of $\chi_a^{N_a}$ belong to $\mathcal{Z}(P)$.*

Proof. To prove (i), let $P_* = E \otimes_L P \otimes_L E$, where E is the splitting field from Proposition 2.19, and let $D = [E : L]$. Then for $a \in L$ the characteristic polynomial of $\phi_{P_*}(a)$ is the D-th power of the characteristic polynomial of $\phi_P(a)$. Also, the minimal polynomials of $\phi_P(a)$ and $\phi_{P_*}(a)$ coincide. So it suffices to check that

[8] We will show later in Corollary 2.32 that in fact one can always take $N_a = 1$, but this is a more difficult result.

some power of the characteristic polynomial of $\phi_{P_*}(a)$ is a power of its minimal polynomial. But by Proposition 2.19, P_* is split, and $\mathrm{gr}(P_*) = P(E,G)^r$. So the characteristic polynomial $\chi_a^*(t)$ of $\phi_{P_*}(a)$ can be written in the form

$$\chi_a^*(t) = \prod_{g\in G}(t - ga)^r,$$

while the minimal polynomial is

$$\mu_a(t) = \prod_{b\in O(a)}(t-b)^{N_a}$$

where $O(a)$ is the orbit of a under the action of G, and $N_a = 1$ for characteristic zero or $p > d$ and a power of p dividing $[L : \mathcal{Z}(P)]$ in characteristic p in general. This shows that $\chi_a^*(t)^{N_a} = \mu_a(t)^K$, where $K = r \cdot |\mathrm{Stab}_G(a)|$, and $\mathrm{Stab}_G(a)$ is the stabilizer of a in G. Thus (i) is proved.

(ii) follows from (i) and Proposition 2.10. □

2.9. Finiteness over the center. Let P be a weakly Galois bimodule over a field L of rank d.

Proposition 2.22. *If* $\mathrm{char}L = 0$, *or* $\mathrm{char}L > d$ *then* L *is a finite extension of* $\mathcal{Z}(P)$ *of degree* $\leq d$, *whose degree divides* d *if* P *is a Galois bimodule.*[9]

Proof. The result follows Proposition 2.11 and the Primitive Element Theorem ([9]), since by Proposition 2.10 and Corollary 2.21(i), every element of L satisfies a polynomial equation over $\mathcal{Z}(P)$ of degree $\leq d$, which has degree dividing d if P is Galois (namely, the equation $\mu_a(t) = 0$). □

Corollary 2.23. *In characteristic zero or* $p > d$, *any weakly Galois bimodule of rank* d *is semisimple as a bimodule.*

Proof. Any weakly Galois L-bimodule is a bimodule over the algebra $L \otimes_{\mathcal{Z}(P)} L$, which by Proposition 2.22 is a finite dimensional semisimple algebra. □

2.10. Galois bimodules containing $L \otimes_{\mathcal{Z}(P)} L$.

Proposition 2.24. *Let* P *be a bimodule over a field* L, *finite dimensional as a left vector space, such that* P^N *contains* $L \otimes_{\mathcal{Z}(P)} L$ *for some* N. *Then* $L \otimes_{\mathcal{Z}(P)} L$ *is in fact a direct summand in* P^N, *and moreover in* P.

[9] It will be shown later in Proposition 2.30, Proposition 2.24, Theorem 2.31 that this result is in fact valid in any characteristic.

Proof. It is clear that $[L : \mathcal{Z}(P)] < \infty$. Thus, $L \otimes_{\mathcal{Z}(P)} L$ is a Frobenius algebra, so it is an injective module over itself. Hence the inclusion of $L \otimes_{\mathcal{Z}(P)} L$ into P^N splits, so $L \otimes_{\mathcal{Z}(P)} L$ is a direct summand in P^N. Furthermore, $L \otimes_{\mathcal{Z}(P)} L$ is a finite dimensional commutative algebra, so it has multiplicity free decomposition into indecomposable projective modules. Hence $L \otimes_{\mathcal{Z}(P)} L$ is a direct summand in P, as desired. □

Proposition 2.25. *Suppose that P be a Galois L-bimodule containing $L \otimes_{\mathcal{Z}(P)} L$ as a direct summand.*[10] *Then P is a multiple of $L \otimes_{\mathcal{Z}(P)} L$.*

Proof. Let $[L : \mathcal{Z}(P)] = m < \infty$. We have $P = (L \otimes_{\mathcal{Z}(P)} L)^r \oplus M$, where $r \geq 1$, and M does not have direct summands of the form $L \otimes_{\mathcal{Z}(P)} L$. We have $\dim M = d - rm$ as a left and a right vector space. Since $P \otimes_L P \cong P^d$, and since

$$L \otimes_{\mathcal{Z}(P)} L \otimes_L M \cong M \otimes_L L \otimes_{\mathcal{Z}(P)} L \cong (L \otimes_{\mathcal{Z}(P)} L)^{d-rm},$$

we have

$$P \otimes_L P \cong (L \otimes_{\mathcal{Z}(P)} L)^{r^2 m + 2r(d-rm)} \oplus M \otimes_L M \cong P^d \cong (L \otimes_{\mathcal{Z}(P)} L)^{rd} \oplus M^d.$$

Since $L \otimes_{\mathcal{Z}(P)} L$ is a commutative algebra and hence has a multiplicity free decomposition into projective modules over itself, M^d does not contain $L \otimes_{\mathcal{Z}(P)} L$ as a direct summand. This implies that $rd \geq r^2 m + 2r(d - rm)$, i.e., $r^2 m \geq rd$, or $rm \geq d$ (as $r \geq 1$). Hence $M = 0$, which implies the result.[11] □

2.11. Purely inseparable weakly Galois bimodules.

Definition 2.26. A split weakly Galois L-bimodule P of rank d is said to be *purely inseparable* if $\mathrm{gr}(P) = L^d$.

Let P be a split weakly Galois L-bimodule of rank d. Then $\mathrm{gr}(P)$ is separable, so by Proposition 2.15, $\mathrm{gr}(P) = P(\mathbf{n}, L, G) = \oplus_{g \in G} (Lg)^{n_g}$, where $G \subset \mathrm{Aut}(L)$ is a finite subgroup and $n_g > 0$. Let $F = L^G$.

Lemma 2.27. (i) *The L-bimodule $L \otimes_F P \otimes_F L$ embeds into P^N for some N.*

(ii) *The restriction of P to F is a purely inseparable weakly Galois F-bimodule of rank $d|G|$.*

Proof. (i) One has $L \otimes_F L = \oplus_{g \in G} Lg$. Now, for each $g \in G$ pick an eigenvector $v_g \in P$ of the operators $\phi(a)$ with eigenvalues $g(a)$. Then $\oplus_{g \in G} L v_g = \oplus_{g \in G} Lg = L \otimes_F L$. Thus, $L \otimes_F L \subset P$, so $L \otimes_F P = L \otimes_F L \otimes_L P \subset P \otimes_L P \subset P^n$, and similarly $L \otimes_F P \otimes_F L \subset P^{n^2}$.

(ii) We have $P \otimes_F P = P \otimes_L L \otimes_F P \subset P \otimes_L P^n \subset P^{n^2}$. This implies that $P|_F$ is a weakly Galois F-bimodule of rank $d|G|$. Moreover, $P|_F$ is split, and $\mathrm{gr}(P|_F) = L^d = F^{d|G|}$, as desired. □

[10] It follows from Proposition 2.24 and Proposition 2.30 below that in fact any Galois L-bimodule has this property.

[11] This proof is based on the idea of "projectivity defect", [4], Section 2.5.

2.12. The restricted Lie algebra of derivations attached to a purely inseparable weakly Galois L-bimodule. This and the next subsection are devoted to studying the structure of purely inseparable weakly Galois bimodules. This is nontrivial only in characteristic $p > 0$, as in characteristic zero by Proposition 2.12, all purely inseparable weakly Galois L-bimodules are multiples of L.

Let $\mathrm{char} L = p > 0$. Let M be an extension of the trivial L-bimodule L by itself. Such extensions are classified by $\mathrm{Ext}^1_{\mathrm{L-bimod}}(L, L) = \mathrm{Der}(L)$, the space of derivations of L. For a derivation D of L, denote by $M(D)$ the corresponding bimodule. Namely, $M(D) = L[x]/x^2$, and the left action of L is as usual, while the right action is given by $v \circ a = v(a + xD(a))$ (such bimodules appear in [8] and are called "self-representations of fields"). It is easy to see that the bimodules $M(D_1)$ and $M(D_2)$ are isomorphic if and only if there exists $a \in L^\times$ such that $aD_1 = D_2$.

Now let P be a purely inseparable weakly Galois L-bimodule. Let us say that a derivation $D : L \to L$ is P-compatible if $M(D)$ is a subbimodule of P (or, equivalently, of some multiple of P, as $M(D)$ has length 2). Let $\mathcal{D}(P)$ be the set of all P-compatible derivations. Clearly, it is a vector space over L under left multiplication.

Proposition 2.28. (i) *$\mathcal{D}(P)$ is finite dimensional over L.*

(ii) *$\mathcal{D}(P)$ is closed under commutator.*

(iii) *$\mathcal{D}(P)$ is closed under taking p-th powers. Thus, $\mathcal{D}(P)$ is a finite-dimensional restricted L-Lie ring of derivations of L in the sense of Jacobson* [8].

Proof. (i) Consider the socle filtration of P: $\mathbf{F}_1P \subset \mathbf{F}_2P \subset \cdots$, where $\mathbf{F}_1P$ is the maximal semisimple subbimodule, $\mathbf{F}_2P/\mathbf{F}_1P$ is the maximal semisimple subbimodule of $P/\mathbf{F}_1P$, etc. Then any inclusion of $M(D)$ into P is actually an inclusion into $\mathbf{F}_2P$. Now, the bimodule $\mathbf{F}_2P$ is an extension of $V_2 = \mathbf{F}_2P/\mathbf{F}_1P \cong L^{m_2}$ by $V_1 = \mathbf{F}_1P \cong L^{m_1}$. Thus, it defines a linear map $\xi : \mathrm{Hom}(V_1, V_2) \to \mathrm{Ext}^1_{\mathrm{L-bimod}}(L, L) = \mathrm{Der}(L)$. It is clear that $M(D)$ is contained in P if and only if $D \in \mathrm{Im}(\xi)$. Thus, $\mathcal{D}(P) = \mathrm{Im}(\xi)$, so $\mathcal{D}(P)$ is finite dimensional.

(ii) Let $X, Y \in \mathrm{Der}(L)$. Consider the tensor product $M(X) \otimes_L M(Y) \otimes_L M(X) \otimes_L M(Y)$. This product is isomorphic to $L[x_1, y_1, x_2, y_2]/(x_1^2 = y_1^2 = x_2^2 = y_2^2 = 0)$ with the usual left action of L, and right action given by

$$\begin{aligned} v \circ a &= v \cdot (\mathrm{Id} + x_1X)(\mathrm{Id} + y_1Y)(\mathrm{Id} + x_2X)(\mathrm{Id} + y_2Y)(a) \\ &= v(a + (x_1 + x_2)Xa + (y_1 + y_2)Ya \\ &\qquad + (x_1 + x_2)(y_1 + y_2)XYa + x_2y_1[Y, X]a + \cdots). \end{aligned}$$

Now consider the 2-dimensional subspace N in this product spanned by $v_1 = x_1x_2y_1y_2$ and $v_2 = (x_1 - x_2)(y_1 - y_2)$. Then from the last formula we get $v_1 \circ a = v_1a$, and $v_2 \circ a = v_2a + v_1[X, Y]a$. Thus, $N = M([X, Y])$.

Now assume that $X, Y \in \mathcal{D}(P)$. Then $M(X) \otimes_L M(Y) \otimes_L M(X) \otimes_L M(Y)$ and hence N is contained in $P^{\otimes 4}$, which is contained in a multiple of P, since

P is a weakly Galois bimodule. Hence $N = M([X,Y])$ is contained in P, so $[X,Y] \in \mathcal{D}(P)$, as desired.

(iii) Consider the tensor power $M(D)^{\otimes 2p-1}$. This is the algebra

$$L[x_1,\dots,x_{2p-1}]/(x_i^2 = 0, i = 1,\dots,2p-1)$$

with the usual left action of L and right action given by

$$v \circ a = v \prod_{i=1}^{2p-1} (\mathrm{Id} + x_i D)(a) = v \sum_{j=0}^{2p-1} e_j(x_1,\dots,x_{2p-1}) D^j(a),$$

where e_j are the elementary symmetric functions. Consider the vectors $v_1 = e_{2p-1}$ and $v_2 = e_{p-1}$. Since $\sum_{i=0}^{2p-1} e_i t^i = \prod_{k=1}^{2p-1}(1 + t x_k)$, we have

$$e_i e_j = \binom{i+j}{j} e_{i+j},$$

so $e_{p-1}e_j = \binom{p-1+j}{j} e_{p-1+j} = \frac{p(p+1)\cdots(p+j-1)}{j!} e_{p-1+j}$. This means that $e_{p-1}e_j = 0$ for $j = 0,\dots,p-1$, but $e_{p-1}e_p = e_{2p-1}$. So we get $v_1 \circ a = v_1 a$ and $v_2 \circ a = v_2 a + v_1 D^p a$. Thus, $M(D^p)$ is contained in $M(D)^{\otimes 2p-1}$. Thus, if $M(D)$ is contained in P, then $M(D^p)$ is contained in $P^{\otimes 2p-1}$, which is a multiple of P. Thus, $M(D^p)$ is contained in P and hence $D^p \in \mathcal{D}(P)$, as desired. □

2.13. The containment theorem for purely inseparable weakly Galois L-bimodules.

Theorem 2.29. *Let P be a purely inseparable weakly Galois L-bimodule of rank d. Then L is a finite purely inseparable extension of $\mathcal{Z}(P)$. Moreover, P contains the bimodule $L \otimes_{\mathcal{Z}(P)} L$.*

Proof. The theorem is trivial in characteristic zero, so we will assume that $\mathrm{char} L = p > 0$.

We will prove the theorem by induction in the length $\ell(P)$ of the socle filtration of P, starting from the trivial case $\ell = 1$.

By Jacobson's theorem [8], if $\mathcal{D}$ is a finite dimensional restricted L-Lie ring of derivations of L, then $[L : L^{\mathcal{D}}] < \infty$. Therefore, Proposition 2.28 implies that L is a finite extension of the field of invariants $F := L^{\mathcal{D}(P)}$, of exponent 1 (i.e., $L^p \subset F$). Let $[L : F] = p^m$ and $L = F(x_1,\dots,x_m)$, where $x_i^p = \alpha_i \in F$. Define derivations $D_1,\dots,D_m$ of L over F by $D_i(x_j) = \delta_{ij}$.

Let D be a derivation of L such that $D^p = 0$. Consider the L-bimodule $M(D)^{\otimes p-1}$, and consider the subbimodule $Q(D)$ in it generated by 1. As explained

in the proof of Proposition 2.28, this subbimodule is spanned over L by e_i, $i = 0, \dots, p-1$ (where $e_0 = 1$), and the right action is defined by

$$v \circ a = v \sum_{i=0}^{p-1} e_i D^i(a).$$

Note that $e_i = \frac{u^i}{i!}$, where $u = e_1$, so $Q(D) = L[u]/(u^p)$, and we can rewrite the last formula as

$$v \circ a = v \exp(uD(a)).$$

Thus, $Q(D_1) \otimes_L \cdots \otimes_L Q(D_m) = L[u_1, \dots, u_m]/(u_1^p = \cdots = u_m^p = 0)$, with the usual left action of L and the right action given by $v \circ a = v\gamma(a)$, where $\gamma(x_i) = x_i + u_i$. Thus, $Q(D_1) \otimes_L \dots \otimes_L Q(D_m) \cong L \otimes_F L$ as L-bimodules, Now, $Q(D_i)$ is contained in a tensor power of P. Hence, $Q(D_1) \otimes_L \dots \otimes_L Q(D_m) \otimes_L P$ is contained in a tensor power of P. Therefore, since P is a weakly Galois bimodule, $Q(D_1) \otimes_L \dots \otimes_L Q(D_m) \otimes_L P$ is contained in a multiple of P, i.e. $L \otimes_F P$ is contained in P^N for some N. Hence, $P \otimes_F P = P \otimes_L L \otimes_F P \subset P \otimes_L P^N \subset P^{nN}$. This implies that $P|_F$ is a purely inseparable weakly Galois F-bimodule with the same center $\mathcal{Z}(P)$.

Moreover, we have $\ell(P|_F) < \ell(P)$. Indeed, if $\mathbf{F}_\bullet$ is the socle filtration of P then by construction $\mathbf{F}_2 P|_F$ is semisimple (i.e., isomorphic to a multiple of F).

Thus, by the induction assumption, F is a finite purely inseparable extension of $\mathcal{Z}(P)$. It follows that L is a finite purely inseparable extension of $\mathcal{Z}(P)$.

So to complete the induction and prove the theorem, it remains to show that P contains $L \otimes_{\mathcal{Z}(P)} L$.

We have seen that $L \otimes_F L$ embeds into a tensor power, hence a multiple of P. Since P is weakly Galois, this means that $L \otimes_F P \otimes_F L = L \otimes_F L \otimes_L P \otimes_L L \otimes_F L$ embeds into a multiple of P. But by the induction assumption, P contains $F \otimes_{\mathcal{Z}(P)} F$, hence $L \otimes_F P \otimes_F L$ contains $L \otimes_{\mathcal{Z}(P)} L$. Hence $L \otimes_{\mathcal{Z}(P)} L$ is contained in P^N for some N. Thus, by Proposition 2.24, $L \otimes_{\mathcal{Z}(P)} L$ is actually a direct summand in P. The theorem is proved. □

2.14. The classification theorem for Galois bimodules over a field.

Proposition 2.30. *Let P be a weakly Galois L-bimodule. Then the bimodule $L \otimes_{\mathcal{Z}(P)} L$ is contained in P^N for some N. In particular, $[L : \mathcal{Z}(P)] < \infty$.*

Proof. First assume that P is split. Let G be the set of $g \in \mathrm{Aut}(L)$ such that Lg occurs in $\mathrm{gr}(P)$, and let $F = L^G$. Then by Lemma 2.27(ii), $P|_L$ is a purely inseparable weakly Galois F-bimodule, with the same center as P. So by Theorem 2.29 it contains $F \otimes_{\mathcal{Z}(P)} F$. This means that $L \otimes_F P \otimes_F L$ contains $L \otimes_{\mathcal{Z}(P)} L$. But we know from Lemma 2.27(i) that $L \otimes_F P \otimes_F L$ embeds into a multiple of P. Thus, $L \otimes_{\mathcal{Z}(P)} L$ embeds into a multiple of P.

Now consider the general case. Let E be the extension of Theorem 2.19, such that the E-bimodule $E \otimes_L P \otimes_L E$ is split. Then, as we have just shown, a multiple of $E \otimes_L P \otimes_L E$ contains $E \otimes_{\mathcal{Z}(P)} E$, which in turn contains $L \otimes_{\mathcal{Z}(P)} L$. But as an L-bimodule, $E \otimes_L P \otimes_L E$ is a multiple of P. So we get that $L \otimes_{\mathcal{Z}(P)} L$ is contained in a multiple of P, as desired. □

Now we are ready to prove the main theorem about Galois bimodules.

Theorem 2.31. *Let L be a field. Then any Galois L-bimodule P of rank d is a multiple of $L \otimes_{\mathcal{Z}(P)} L$. In particular, $[L : \mathcal{Z}(P)]$ is finite and divides d.*

Proof. By Proposition 2.30, $L \otimes_{\mathcal{Z}(P)} L$ is contained in P^N for some N. By Proposition 2.24, this means that $L \otimes_{\mathcal{Z}(P)} L$ is a direct summand in P. By Proposition 2.25, this means that P is a multiple of $L \otimes_{\mathcal{Z}(P)} L$, which implies the theorem. □

Corollary 2.32. *In Corollary 2.21, one may take $N_a = 1$. Thus, if P is a Galois L-bimodule, then the characteristic polynomial of $\phi_P(a)$ is a power of its minimal polynomial, and the coefficients $C_i(a)$ of this characteristic polynomial are in $\mathcal{Z}(P)$.*

Proof. By Theorem 2.31, we only need to show that the statement holds for $P = L \otimes_{\mathcal{Z}(P)} L$. But in this case the minimal polynomial μ_a and the characteristic polynomial χ_a of $\phi(a)$ are just the minimal and characteristic polynomials of the operator M_a of multiplication by a in L, regarded as a $\mathcal{Z}(P)$-vector space. So, it is clear that $\chi_a = \mu_a^r$, where $r = [L : \mathcal{Z}(P)(a)]$. □

2.15. Galois bimodules over matrix algebras and central simple algebras. Let L be a field.

Proposition 2.33. *There is a natural bijection between isomorphism classes of Galois bimodules over L of rank d and isomorphism classes of Galois bimodules over $\mathrm{Mat}_m(L)$ of rank d, defined by $P \mapsto \mathrm{Mat}_m(P)$ as in Lemma 2.7(ii). The center is preserved under this bijection.*

Proof. We only need to construct the inverse. Suppose that Q is a Galois bimodule for $\mathrm{Mat}_m(L)$ of rank d. Define the L-bimodules $\bar{Q}_{ij} = E_{ii} Q E_{jj}$, where E_{pq} are the elementary matrices. Clearly, these bimodules are all isomorphic, so we'll call them $\bar{Q}$. We clearly have $\bar{Q} \otimes_L \bar{Q} = \bar{Q}^d$, and also $m\bar{Q} = \oplus_i \bar{Q}_{ij} = QE_{jj}$, which is of dimension dm over L on the right. Hence $\bar{Q}$ is of dimension d over L on the right, and similarly on the left. The assignment $Q \mapsto \bar{Q}$ is inverse to $P \mapsto \mathrm{Mat}_m(P)$, as desired.

The fact that the center is preserved is clear. □

Corollary 2.34. *Any Galois bimodule over* $\mathrm{Mat}_m(L)$ *is a multiple of*

$$\mathrm{Mat}_m(L \otimes_{\mathcal{Z}(P)} L).$$

Proof. This follows from Proposition 2.33 and Theorem 2.31. □

Definition 2.35. We will say that a Galois bimodule over $\mathrm{Mat}_m(L)$ is *split* if so is the corresponding L-bimodule under the bijection of Proposition 2.33.

Now assume that B is a central simple algebra over L of dimension m^2, and let P be a Galois bimodule over B of rank d. Recall that by restricting from B to L, by Lemma 2.7(iii) P is automatically a Galois L-bimodule of rank dm^2, with the same center.

Proposition 2.36. *There exists a normal extension* K *of* $\mathcal{Z}(P)$ *finite over* L *which is a splitting field for the algebra* B *and contains the eigenvalues of* $\phi_P(a)$ *for all* $a \in L$. *Moreover,* $K \otimes_L P \otimes_L K$ *is a split Galois bimodule over* $\mathrm{Mat}_m(K)$ *of rank* $d[K : L]$.

Proof. Let S be a finite extension of L which splits B, and let E be the extension of Theorem 2.19. Let K be the normal closure over $S \cdot E$ over E. Then by Theorem 2.19, Proposition 2.18 and Proposition 2.33, the K-bimodule $K \otimes_L P \otimes_L K$ is a split Galois bimodule over $\mathrm{Mat}_m(K)$ of rank $d[K : L]$. □

Corollary 2.37. *If* P *is a Galois bimodule over* B, *then* P^{m^2} *is a multiple of* $B \otimes_{\mathcal{Z}(P)} B$.

Proof. By Proposition 2.36 and Proposition 2.34, the Galois $\mathrm{Mat}_m(K)$-bimodule $K \otimes_L P \otimes_L K$ has the form $\mathrm{Mat}_m(K \otimes_{\mathcal{Z}(P)} K)^r$. So $K \otimes_L P^{m^2} \otimes_L K$ has the form $(\mathrm{Mat}_m(K) \otimes_{\mathcal{Z}(P)} \mathrm{Mat}_m(K))^r$, which as a B-bimodule is $(B \otimes_{\mathcal{Z}(P)} B)^{rn^2}$, where $n = [K : L]$. On the other hand,

$$K \otimes_L P^{m^2} \otimes_L K = P^{m^2 n^2}$$

as a B-bimodule. So we get that $P^{m^2} = (B \otimes_{\mathcal{Z}(P)} B)^r$, as desired. □

3. Invariants of K-comodule algebras finite over center

3.1. The main theorem. Let K be a finite dimensional Hopf algebra over an algebraically closed field k. Let A be a (right) K-comodule algebra. We are interested in the K-invariants A^K of A, i.e., the space of elements $a \in A$ such that $\rho(a) = a \otimes 1$.[12]

[12] We note that many authors call these elements coinvariants and denote the space of such elements by $A^{\mathrm{co}K}$.

Suppose that Z is a central k-subalgebra of A (not necessarily K-costable[13]) which is an integral domain, and let Q be the quotient field of Z.

Consider the following (redundant) list of assumptions on A and Z:

(1) A is finitely generated as a Z-module.

(2) $Q \otimes_Z A$ is a central simple algebra with center Q.

(3) A is a torsion-free Z-module.

(4) Z is integrally closed (in Q).

(5) A is a projective Z-module.

Our main result is the following theorem.

Theorem 3.1. (i) *Under assumptions (1)–(4), Z and hence A are integral over $Z \cap A^K$.*

(ii) *The conclusion of (i) also holds if conditions (3), (4) are replaced with condition (5). In particular, it holds if A is an Azumaya algebra over Z.*

(iii) *If in addition Z is a finitely generated algebra over k, then in the situation of (i) and (ii), A and Z are finitely generated modules over $Z \cap A^K$, and thus A is a finitely generated module over A^K (on both sides).*

(iv) *If Z is a finitely generated algebra over k then in the situation of (i) or (ii), so is $Z \cap A^K$.*

Theorem 3.1 is proved in the next subsection. We note that the proof of (i) uses only the material up to Proposition 2.10, and the proof of (ii) only uses the material up to Corollary 2.21 (inclusively). Parts (iii) and (iv) follow easily.

Remark 3.2. It is well known that a coaction of a noncommutative Hopf algebra K on an algebra A does not have to preserve its center. The classical example is $K = A = k[G]$ being the group algebra of a nonabelian finite group G, coacting on itself by its coproduct.

Remark 3.3. If A is commutative, conditions (1)–(4) imply that $A = Z$. Indeed, if A is torsion-free and finite over Z, and coincides with Z after localization, then A is contained in the integral closure of Z, which is Z if Z is integrally closed. Also, it is clear that (1), (2) and (5) imply that $A = Z$ if A is commutative.

Also note that the algebra A is necessarily a PI algebra, since by (2) and either (3) or (5) it embeds into the central simple algebra $Q \otimes_Z A$.

Remark 3.4. In the case $A = Z$ Theorem 3.1 says that Z is integral over Z^K, which is finitely generated as a Z^K-module if Z is finitely generated over k. This is a result of Skryabin ([12]) in the case of Z being a domain (Skryabin proves the result more generally, when Z has no nilpotent K-costable ideals, and always in positive characteristic).

[13] A K-costable subspace of a K-comodule is the same thing as a subcomodule.

Example 3.5. Let A be a flat family of finite dimensional algebras parametrized by an irreducible affine algebraic variety X over k, such that the fiber A_x is a matrix algebra for a generic point $x \in X$ ("flat family" means that A is projective over $Z := \mathcal{O}(X)$). Suppose a finite dimensional Hopf algebra K coacts on A, not necessarily preserving Z. Then conditions (1), (2), (5) are satisfied, and parts (ii), (iii), (iv) of Theorem 3.1 apply. Also, these statements apply to the case when $A = \mathrm{Mat}_m(Z)$, where Z is a finitely generated integral domain over k. This is an interesting example even if Z is a polynomial algebra.

Corollary 3.6. *Let Z be a finitely generated integrally closed domain over k, and A be a prime PI algebra with center Z and a coaction of K. Then Z and A are finitely generated modules over $Z \cap A^K$, and A is a finite module over A^K on both sides. Moreover, in this case $Z \cap A^K$ is a finitely generated k-algebra.*

Proof. Condition (1) of Theorem 3.1 is satisfied by [11], Proposition 13.6.11. Condition (2) holds by Posner's theorem, [11], Theorem 13.6.5. Condition (3) holds because A is prime. Condition (4) is one of the assumptions. So Theorem 3.1 applies. □

3.2. Proof of Theorem 3.1. Let us prove (i). Let $Q = Q_Z$ be the field of quotients of Z. Consider the tensor product $Q \otimes_Z P$. This is a left module over the algebra $B := Q \otimes_Z A$, which is a central simple algebra over Q by (2), of rank m^2 for some m. Consider the right action of Z on $Q \otimes_Z P$. This action defines a homomorphism $\psi_P : Z \to \mathrm{End}_Q(Q \otimes_Z P) \cong \mathrm{Mat}_{dm^2}(Q)$.

We claim that for any nonzero $z \in Z$, the matrix $\psi_P(z)$ is invertible. Indeed, let $x \in Q \otimes_Z P$ be such that $\psi_P(z)x = xz = 0$. Let $x = w^{-1}y$, where $w \in Z$, $w \neq 0$, and $y \in P$. Hence, yz is a torsion element of P, i.e. $z'yz = 0$ in P for some nonzero $z' \in Z$. But by (3) (or by (5)), A is torsion-free over Z, which implies that P is torsion-free over Z on each side. So we get that $yz = 0$ and hence $y = 0$ and $x = 0$, as desired.

Thus, we see that the right action of Z on $Q \otimes_Z P$ naturally extends to a right action of Q, i.e. $Q \otimes_Z P$ is a Q-bimodule. Hence, $Q \otimes_Z P$ is a bimodule over the central simple algebra B, and

$$Q \otimes_Z P = Q \otimes_Z P \otimes_Z Q = B \otimes_A P \otimes_A B.$$

Now, let $\dim K = d$. By Proposition 2.8, $P := A \otimes K$ is a Galois bimodule over A of rank d. This implies by Lemma 2.7(i) that $P_{\mathrm{loc}} := Q \otimes_Z P = B \otimes_A P \otimes_A B$ is a Galois bimodule over B of rank d, and hence by restriction (Lemma 2.7(iii)) a Galois bimodule over Q of rank dm^2, with the same center.

By Proposition 2.10, this implies that the coefficients of the minimal polynomial μ_a of $\phi_P(a)$ for all $a \in Q$ are in $\mathcal{Z}(P_{\mathrm{loc}})$.

Now we will use the following well known lemma.

Lemma 3.7. *Let Z be an integrally closed domain with field of quotients Q, and M a finitely generated Z-module. Let $b : M \to M$ be an endomorphism. Then the coefficients of the minimal polynomial and the coefficients of the characteristic polynomial of b on $Q \otimes_Z M$ belong to Z.*

Proof. Let $m_1, \dots, m_n$ be generators of M. Then $b(m_i) = \sum b_{ij} m_j$ for some $b_{ij} \in Z$. Let $B = (b_{ij})$, and let χ_B be the characteristic polynomial of B. Then by the Hamilton-Cayley theorem, $\chi_B(b) = 0$. So the eigenvalues of b on $Q \otimes_Z M$ (which are elements of $\bar{Q}$) are integral over Z. Hence the coefficients of the minimal polynomial μ_b and the characteristic polynomial χ_b of b (which may have lower degree than χ_B) are integral over Z (as they are polynomials of the eigenvalues). Since these coefficients are in Q and since Z is integrally closed, they are in Z, as desired. □

We can now apply Lemma 3.7 to $M = P$ as a left Z-module, and $b = \psi_P(z)$. Then we get that the coefficients of the minimal polynomial of $\psi_P(z)$ belong to Z.

Moreover, if $z \in Z$ is central for P_{loc} then by (3) it is also central for P (indeed, since P is torsion-free over Z, the map $P \to P_{\mathrm{loc}}$ is an embedding of Z-bimodules).

Thus, the coefficients of the minimal polynomial of $\psi_P(z)$ belong to $Z \cap \mathcal{Z}(P)$. By Proposition 2.8, this means that these coefficients belong to $Z \cap A^K$. Hence Z is integral over $Z \cap A^K$ (as z is annihilated by the minimal polynomial of $\psi_P(z)$). Thus, (i) is proved.

Now we prove (ii). We use Corollary 2.21(ii) to conclude that the coefficients of some power of the characteristic polynomial of $\psi_P(z)$ in $\mathrm{End}_Q(Q \otimes_Z P) \cong \mathrm{Mat}_{dm^2}(Q)$ belong to $F := \mathcal{Z}(P_{\mathrm{loc}}) \subset Q$.[14]

Since condition (5) is satisfied, the module P is locally free as a left Z-module, so the matrix $\psi_P(z)$ actually has coefficients in Z. This implies that the coefficients of the characteristic polynomial of $\psi_P(z)$ belong to $Z \cap F = Z \cap A^K$ (as by (5) any element of Z central in P_{loc} is also central in P). Thus, Z is integral over $Z \cap A^K$, and (ii) is proved.

Part (iii) follows from (i) and (ii) and the standard fact that if $R \subset S$ is an integral extension of k-algebras, and S is finitely generated as a k-algebra, then S is a finitely generated R-module.

Finally, part (iv) follows from part (iii) and the Artin–Tate lemma: if $B \subset C$ are commutative k-algebras and C is finitely generated over k and finite as a module over B, then B is a finitely generated k-algebra.

Theorem 3.1 is proved.

Remark 3.8. 1. Note that if $Z = Q$ is a field and A a central simple algebra over Z, then (i) follows immediately from Proposition 2.8 and Proposition 2.10, by regarding $A \otimes K$ as a Galois Z-bimodule.

2. The coefficients of the minimal polynomial of a square matrix over Z (unlike

[14] In fact, Corollary 2.32 (which is more difficult to prove than Corollary 2.21) says that the coefficients of the characteristic polynomial itself are in F, but we don't need it here.

those of its characteristic polynomial) do not have to be in Z if Z is not integrally closed. For instance, take the 5 by 5 matrix over $Z := \mathbb{C}[x^2, x^3]$ given by $a_{12} = 1$, $a_{21} = x^2$, $a_{34} = 1$, $a_{45} = 1$, $a_{53} = x^3$, and the rest of the entries are zero. Then the minimal polynomial is $(t^3 - x^3)(t + x)$, whose coefficients are not in Z. This is why we used characteristic polynomials rather than minimal polynomials in the proof of Theorem 3.1(ii).

3.3. Divisibility.

Proposition 3.9. *In the situation Theorem 3.1 (i) or (ii), the degree of Q over the field of quotients Q^K of $Z \cap A^K$ divides the dimension of K.*

Proof. By Proposition 2.36, for a suitable extension E of Q, the bimodule $E \otimes_Q P_{\mathrm{loc}} \otimes_Q E = E \otimes_Z P \otimes_Z E$ is a split Galois bimodule over $\mathrm{Mat}_m(E)$ of rank $d[E : Q]$, where $d = \dim(K)$. Hence by Proposition 2.33, it corresponds to a split Galois bimodule P' over E of the same rank. The center of P' is $\mathcal{Z}(P') = \mathcal{Z}(P_{\mathrm{loc}}) = Q^K$, so by Theorem 2.31, $P' = (E \otimes_{Q^K} E)^r$, so $d[E : Q] = r[E : Q^K]$. Thus, $d = r[Q : Q^K]$ and hence $[Q : Q^K]$ divides d. □

Remark 3.10. If $\mathrm{char}L = 0$ or $\mathrm{char}L = p > d$, then there is a simpler proof of Proposition 3.9. Namely, in this case by Proposition 2.14(iii) and Proposition 2.15, $P' = P(E, G)^r$ for some finite group $G \subset \mathrm{Aut}(E)$. We have $E^G = \mathcal{Z}(P') = Q^K$, so $|G| = [E : Q^K]$ and hence $d[E : Q] = r|G| = r[E : Q^K]$. Thus $d = r[Q : Q^K]$ and hence $[Q : Q^K]$ divides d.

3.4. Examples.

Example 3.11. Condition (2) cannot be removed to allow semisimple (rather than simple) algebras over Q. Indeed, take $Z = \mathbb{C}[t]$ and $A = \mathbb{C}[t] \oplus \mathbb{C}[t]$, containing Z as the diagonal. Consider the action of $G = \mathbb{Z}/2$ on A by $g(f_1(t), f_2(t)) = (f_1(-t), f_2(1 - t))$ for the generator $g \in G$ (which corresponds to a coaction of $\mathrm{Fun}(G)$). Then $Z \cap A^G = \mathbb{C}$ (it consists of polynomials f such that $f(t) = f(-t) = f(1 - t)$).

However, there is a generalization of Theorem 3.1 in which Z is a reduced algebra (not necessarily a domain), Q is its total quotient ring, and $Q \otimes_Z A$ is a semisimple algebra with center Q (see Theorem 5.1).

Example 3.12. Condition (4) cannot be removed. Indeed, take $A = \mathbb{C}[x, y]$ and $Z = \{f \in A | f(0, y) = f(1, y)\}$. Define an action of $G = \mathbb{Z}/2$ on A by $(gf)(x, y) = f(x, x - y)$ for the generator g of G. Then $Z \cap A^G$ consists of polynomials f such that $f(0, -y) = f(0, y) = f(1, y) = f(1, 1 - y) = f(0, 1 - y)$. For such f, we have that $f(0, y)$ is constant. Therefore, A and Z cannot be finite modules over $Z \cap A^G$.

Also, condition (3) cannot be removed. Namely, let R be any commutative algebra over k with generators $x_1, \ldots, x_n$, $A = k[x_1, \ldots, x_n, t] \oplus R$, and $Z \subset A$

be the image of $k[x_1,\dots,x_n,t]$ under the map $k[x_1,\dots,x_n,t] \to A$ given by $x_i \mapsto (x_i, x_i)$, $t \mapsto (t,0)$. Suppose that K coacts on R and coacts trivially on $k[x_1,\dots,x_n,t]$; then it coacts diagonally on A and conditions (1), (2), (4) (although not (3)) are satisfied. Yet, the invariants in $Z = k[x_1,\dots,x_n,t]$ are those elements whose images in R are invariant under the coaction of K on R. So if A is integral over its invariants, then so must be R. But it is known that there exist finitely generated commutative k-algebras with a coaction of K which are not integral over their invariants, see [16].

Example 3.13. If A is a deformation of an algebra A_0 satisfying the conditions of Theorem 3.1 with a coaction of K, A does not have to be finite over A^K, even if $Z \subset A_0$ is finitely generated. Indeed, let $K = H^*$, where H is the Nichols Hopf algebra of dimension 16 over $\mathbb{C}$ generated by a grouplike element g such that $g^2 = 1$ and skew-primitive elements x_i, $i = 0,1,2$, such that $gx_i = -x_i g$, $x_i x_j = -x_j x_i$, $x_i^2 = 0$, and $\Delta(x_i) = 1 \otimes x_i + x_i \otimes g$. Let B be any $\mathbb{C}$-algebra. Define a right B-linear action of H on B^2 with right B-basis e_1, e_2 by

$$g(e_1) = e_1,\ g(e_2) = -e_2,\ x_i(e_1) = 0,\ x_0(e_2) = e_1, x_1(e_2) = xe_1,\ x_2(e_2) = ye_1,$$

where $x, y \in B$ are any elements. Now consider the corresponding adjoint action of H on $A := \mathrm{End}(B^2)_B = \mathrm{Mat}_2(B)$, via

$$a \circ M = a_{(1)} M S(a_{(2)})$$

(using Sweedler's notation). Then it is easy to show that A^K is the set of matrices $b \cdot \mathrm{Id}$, where $b \in Z_{x,y}$, and $Z_{x,y}$ is the centralizer of x, y in B.

Now take B to be the Weyl algebra generated by x, y with the defining relation $[y,x] = 1$. Then we get that $Z_{x,y} = \mathbb{C}$, so the invariants A^K in A are trivial, and hence A is not finite over A^K.

Note, however, that A can be viewed as a deformation of an algebra A_0 satisfying the conditions of Theorem 3.1, with finitely generated Z. Namely, we can consider the filtration on A given by $\deg(bE_{ij}) = i - j + \deg(b)$, where E_{ij} are the elementary matrices and $\deg(b)$ is the Bernstein filtration degree of $b \in B$ defined by $\deg(x) = \deg(y) = 1$. This filtration is preserved by H, and $A_0 = \mathrm{gr}(A) = \mathrm{Mat}_2(\mathbb{C}[x,y])$ satisfies conditions (1), (2) and (5), for $Z = \mathbb{C}[x,y]$. Also, we may consider the reductions of A modulo primes p, and these reductions satisfy (1), (2), and (5) for $Z = k[x^p, y^p]$.

Thus, this is an example of a situation when the invariants of A_0 don't lift to the deformation.

We note that such a thing could not happen for a coaction on B itself: it is shown in [5] that any action of a finite dimensional Hopf algebra H on B preserving the Bernstein filtration necessarily factors through a finite group algebra and hence B is finite as a module over B^K, where $K = H^*$. Also nothing like this can happen for a semisimple $H = K^*$ since it is known that in this case a Noetherian algebra A is a Noetherian A^K-module ([10], Theorem 4.4.2).

Remark 3.14. Taking B to be the algebra of matrices of any size N and x, y generic elements of this algebra, we get an example when $H = K^*$ is fixed and the dimension of A^K is 1, but the dimension of A (which is a matrix algebra of size $2N$) is arbitrarily large.

Such an example is only possible for nonsemisimple H, due to the following lemma.

Lemma 3.15. *Let $H = K^*$ be a semisimple Hopf algebra over an algebraically closed field k, and A be a semisimple H-module algebra. Then* $\dim A^K \cdot \dim H \geq \dim A$.

Proof. Consider the algebra $H\#A$. This algebra is semisimple ([10], Theorem 7.4.2(2)). Let us decompose A as an $H\#A$-module: $A = \oplus n_i V_i$, where V_i are the simple $H\#A$-modules, and $n_i \geq 0$. Then $A^K = \mathrm{End}_{H\#A}(A) = \oplus_i \mathrm{Mat}_{n_i}(k)$, so $\dim A^K = \sum_i n_i^2$. Also, if $d_i = \dim V_i$, then we have $\dim H \dim A = \sum d_i^2$ and $\dim A = \sum n_i d_i$. Thus, the result follows from the Cauchy–Schwarz inequality. □

Example 3.16. ([6]) The following example of an inner faithful coaction of a non-basic finite dimensional Hopf algebra on a field shows that in the situation of Theorem 3.1, even when $A = Z$ is a field, the Galois Z-bimodule $P = Z \otimes K$ is not necessarily split, i.e., the eigenvalues of $\phi_P(z)$ don't necessarily belong to Z but may define a nontrivial extension of Z. In other words, Z is not necessarily a Galois extension of Z^K, and the Galois group G attached to P does not have to preserve Z.

Namely, let q be a primitive m-th root of unity, and consider the m^2n-dimensional generalized Taft algebra $K = T_{m,n}$ generated by g, x such that $g^{mn} = 1$, $gx = qxg$, $x^m = g^m - 1$, $\Delta(g) = g \otimes g$, $\Delta(x) = x \otimes g + 1 \otimes x$ (where $n, m \geq 2$). Define the coaction of K on $Z = \mathbb{C}(z)$ by the formula $\rho(z) = z \otimes g + 1 \otimes x$. Then we have $\rho(z^m) = z^m \otimes g^m + 1 \otimes (g^m - 1)$, so $\rho(z^m + 1) = (z^m + 1) \otimes g^m$, and thus the invariants Z^K are generated by $u = (z^m + 1)^n$. So $[Z : Z^K] = mn$, but this is a non-Galois extension obtained by adding to $\mathbb{C}(u)$ a root of the polynomial $(t^m + 1)^n - u$. The Galois closure E of this extension is the splitting field of this polynomial, which has degree $m^n n$ over $Z^K = \mathbb{C}(u)$:

$$E = \mathbb{C}(u^{1/n})((-1 + \varepsilon^j u^{1/n})^{1/m}, j = 0, \dots, n-1),$$

where ε is a primitive n-th root of unity. The Galois group $G = \mathrm{Gal}(E/Z^K)$ is thus of order $m^n n$, and is isomorphic to $\mathbb{Z}/n \ltimes (\mathbb{Z}/m)^n$, where $\mathbb{Z}/n$ cyclically permutes the summands. The eigenvalues of $\rho(z)$ include $q^j(-1 + \varepsilon^i(1 + z^m))^{1/m}$, so they don't all lie in Z.

This is, of course, only possible because K is not basic. If K is basic, all its irreducible representations are 1-dimensional, and thus it is clear that all the eigenvalues of $\rho(z)$ have to belong to Z.

3.5. Localization and the Galois group of a coaction.

Corollary 3.17. *In the situation of Theorem 3.1, the central simple algebra $Q \otimes_Z A$ carries a coaction of K, which extends the coaction of K on A.*

Remark 3.18. This is a special case of a much more general result, [14], Theorem 2.2.

Proof. Let L be the quotient field of $Z \cap A^K$. Then we have a coaction of K on $L \otimes_{Z\cap A^K} A$ which extends the coaction of K on A. But it is easy to see that $L \otimes_{Z\cap A^K} A = Q \otimes_Z A$. Indeed, it is well known that if $U \subset Z$ are commutative domains with fields of quotients Q_U, Q_Z and Z is integral over U then $Q_U \otimes_U Z = Q_Z$.

This allows us to define, in the situation of Theorem 3.1, the Galois group of the coaction. Write Q^K for $Q \cap (Q \otimes_Z A)^K$ (we don't assume that Q is K-costable).

Definition 3.19. The *Galois group* $\mathrm{Gal}(\rho)$ of the coaction ρ is the group $G = \mathrm{Gal}(E/Q^K)$, where E is the Galois closure of Q over Q^K.

Example 3.20. 1. If a finite group Γ acts on central simple algebra A with center Z by automorphisms, then the Galois group is $G = \Gamma/\Gamma_0$, where Γ_0 is the subgroup of elements acting trivially on Z.

2. In Example 3.16, the Galois group is $G = \mathbb{Z}/n \ltimes (\mathbb{Z}/m)^n$. □

4. Galois bimodules over semisimple algebras finite over the center

4.1. Galois bimodules over commutative semisimple algebras. Now let L be a commutative semisimple algebra, i.e., a direct sum of finitely many fields of the same characteristic: $L = L_1 \oplus \cdots \oplus L_n$. Then an L-bimodule P has the form $P = \oplus_{i,j} P_{ij}$, where P_{ij} is an (L_i, L_j)-bimodule. Define the oriented incidence graph $\Gamma(P)$ of P with vertices labeled by $1, \dots, n$, and edges $i \to j$ whenever $P_{ji} \neq 0$. Let us say that P is connected if $\Gamma(P)$ is a connected graph.

For a vector $\mathbf{p} = (p_1, \dots, p_n) \in \mathbb{Z}^n_{\geq 0}$, denote by $L^{\mathbf{p}}$ the L-module $L_1^{p_1} \oplus \cdots \oplus L_n^{p_n}$.

Definition 4.1. A *quasi-Galois bimodule* over L of rank d and type $(\mathbf{p}, \mathbf{q})$ is an L-bimodule P which is isomorphic to $L^{\mathbf{p}}$ as a left L-module, to $L^{\mathbf{q}}$ as a right L-module, and such that $P \otimes_L P \cong P^d$ as a bimodule.

Clearly, a Galois L-bimodule of rank d is the same thing as a quasi-Galois L-bimodule of rank d and type $(d \cdot \mathbf{1}, d \cdot \mathbf{1})$, where $\mathbf{1} = (1, \dots, 1)$.

It is clear that any quasi-Galois L-bimodule of rank d is of the form $P = \oplus_i P^{(i)}$, where $P^{(i)}$ is a connected quasi-Galois bimodule of rank d over $L^{(i)}$, and $L = \oplus_i L^{(i)}$ (namely, $\Gamma(P^{(i)})$ are the connected components of $\Gamma(P)$). Thus it suffices to consider only connected quasi-Galois L-bimodules.

Suppose $\mathcal{Z}$ is a field, and $\psi_i : \mathcal{Z} \to L_i$ are field embeddings, such that $[L_i : \mathcal{Z}] = d_i < \infty$. Then $\mathcal{Z} \subset L$ by the diagonal embedding $z \mapsto (\psi_1(z), \dots, \psi_n(z))$. Let

$$P = \oplus_{i,j}(L_i \otimes_{\mathcal{Z}} L_j)^{a_i r_j} \tag{4.1}$$

for some positive integers a_i, r_j. It is easy to see that P is a quasi-Galois L-bimodule of rank $d = \sum_i a_i d_i r_i$ and type $(\mathbf{p}, \mathbf{q})$, where $p_i = a_i \sum_j r_j d_j$ and $q_j = r_j \sum_i a_i d_i$.

Theorem 4.2. *Let P be a connected quasi-Galois L-bimodule. Then the center $\mathcal{Z} = \mathcal{Z}(P)$ is a field, which embeds into each L_i, with $[L_i : \mathcal{Z}] = d_i < \infty$. Moreover, P has the form (4.1). In particular, if P is Galois, then it is a multiple of $L \otimes_{\mathcal{Z}} L$.*

Proof. Let d be the rank of P. We will need the following well known lemma from linear algebra.

Lemma 4.3. *Let $0 < p < m$ be positive integers, and $A \in \mathrm{Mat}_m(\mathbb{R})$ be a block matrix*

$$A = \begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix}$$

where X is of size p by p. Suppose that $A^2 = A$, the entries of X and Z are strictly positive, and the entries of Y are nonnegative. Then $Y = 0$.

Proof. For any $N \geq 2$ we have

$$A = A^N = \begin{pmatrix} X^N & \sum_i X^i Y Z^{N-1-i} \\ 0 & Z^N \end{pmatrix} = \begin{pmatrix} X & XY + YZ + (N-2)XYZ \\ 0 & Z \end{pmatrix}.$$

Thus, $XYZ = 0$. Since X, Z have positive entries and Y nonnegative entries, we have $Y = 0$, as desired. □

Lemma 4.4. *One has $P_{ij} \neq 0$ for any i, j.*

Proof. Let $[P]$ be the matrix of dimensions of P_{ij} over L_i. Then $[P]^2 = d[P]$.

Call two vertices of $\Gamma(P)$ equivalent if they can be reached from each other by moving along the edges of $\Gamma(P)$ according to their orientation.[15] Let C_1 be an equivalence class from which one cannot reach any other one (i.e., a sink), and assume for the sake of contradiction that C_2 is another equivalence class from which there is an edge into C_1. Consider the principal submatrix A of $[P]/d$ corresponding to C_1 and C_2. Then A satisfies the conditions of Lemma 4.3. Then the conclusion of the lemma gives a contradiction with the existence of an edge from C_2 to C_1. Thus, there is only one equivalence class, which proves the lemma (in view of the identity $[P]^2 = d[P]$). □

[15] Note that since $[P]^2 = d[P]$, if a vertex $v_1 \in \Gamma(P)$ can be reached from $v_2 \in \Gamma(P)$ by an oriented path then there is actually an edge from v_2 to v_1.

Thus, we see that the matrix $[P]$ has rank 1, i.e. $[P]_{ij} = a_i b_j$ for some positive rational numbers a_i, b_j. We may scale a_i in such a way that they are positive integers with $\gcd(a_1, \dots, a_n) = 1$. Then b_j are positive integers as well. Also, since P is of rank d, we have $d = \sum_j a_j b_j$.

Now consider the L_i-bimodule P_{ii}. It has left dimension $a_i b_i$, finite right dimension, and we have $P_{ii} \otimes_{L_i} P_{ii} \subset P_{ii}^d$. Thus, by Proposition 2.9, the right dimension of P_{ii} is also $a_i b_i$, and P_{ii} is a weakly Galois L_i-bimodule.

Let $\mathcal{Z}_i$ be the center of P_{ii}. Then by Proposition 2.30, $[L_i : \mathcal{Z}_i] < \infty$.

Let $\phi_{ij} : L_j \to \mathrm{Mat}_{a_i b_j}(L_i)$ be the map defined by the right action of L_j on P_{ij}. Since $P_{ij} \otimes_{L_j} P_{ji}$ is contained in P_{ii}^d, we have

$$(1 \otimes \phi_{ij})(\phi_{ji}(z)) = \mathrm{Id}_{a_i b_j} \otimes \mathrm{Id}_{a_j b_i} \otimes z \tag{4.2}$$

for any $z \in \mathcal{Z}_i$. This means that $\phi_{ji}(z)$ is a scalar matrix, $\phi_{ji}(z) = \eta_{ji}(z)\mathrm{Id}_{a_j b_i}$, where $\eta_{ji}(z) \in L_j$. Moreover, since $P_{jj} \otimes_{L_j} P_{ji}$ is contained in P_{ji}^d, we have that $(1 \otimes \phi_{jj})(\phi_{ji}(z))$ is conjugate to restriction of $\mathrm{Id}_d \otimes \phi_{ji}(z)$ to an invariant subspace, which implies that $\eta_{ji}(z) \in \mathcal{Z}_j$. Thus, $\eta_{ji} : \mathcal{Z}_i \to \mathcal{Z}_j$, and by (4.2), $\eta_{ji} \circ \eta_{ij} = \mathrm{Id}$, so η_{ij} are isomorphisms. Finally, since $P_{\ell j} \otimes_{L_j} P_{ji}$ is contained in $P_{\ell i}^d$, we have $\eta_{\ell j} \circ \eta_{ji} = \eta_{\ell i}$.

Thus, we have a single field $\mathcal{Z}$, and embeddings $\psi_i : \mathcal{Z} \to L_i$ such that $\mathcal{Z}_i = \psi_i(\mathcal{Z})$ and $\eta_{ji} = \psi_j \circ \psi_i^{-1}$. Moreover, $\mathcal{Z} = \mathcal{Z}(P)$ (where $\mathcal{Z}$ is embedded into L by the diagonal embedding $\oplus_i \psi_i$). We will identify $\mathcal{Z}$ with $\mathcal{Z}_i$ using the maps ψ_i.

Now we see that the dimension of P_{ij} over $\mathcal{Z}$ (on either side) is $a_i b_j d_i$, which implies that the dimension of P_{ij} as a right vector space over L_j is $a_i b_j d_i / d_j$ (which is therefore an integer). Thus, P is a quasi-Galois bimodule of type $(\mathbf{p}, \mathbf{q})$, where

$$p_i = a_i \sum_j b_j, \; q_j = \frac{b_j}{d_j} \sum_i a_i d_i.$$

Now, by Proposition 2.30, P_{ii} contains $L_i \otimes_{\mathcal{Z}} L_i$. Since $P_{ii} \otimes_{L_i} P_{ij}$ is contained in P_{ij}^d, we get that P_{ij}^d contains $L_i \otimes_{\mathcal{Z}} L_j$. Now, $L_i \otimes_{\mathcal{Z}} L_j$ is a Frobenius algebra, so it is an injective module over itself. Thus, this inclusion splits and $L_i \otimes_{\mathcal{Z}} L_j$ is contained in a multiple of P_{ij} as a direct summand. Since $L_i \otimes_{\mathcal{Z}} L_j$ is a commutative algebra, it has multiplicity free decomposition into indecomposable projective modules, so is contained as a direct summand in P_{ij} itself.

To conclude the proof, we use the argument from the proof of Proposition 2.25. Let $Q = \oplus_{i,j} (L_i \otimes_{\mathcal{Z}} L_j)^{N a_i b_j / d_j}$, where N is the smallest positive integer such that the numbers $N b_j / d_j$ are integers. It is easy to check that Q is a quasi-Galois L-bimodule of rank Nd and type $(N\mathbf{p}, N\mathbf{q})$, so that

$$Q \otimes_L Q = Q^{dN} \tag{4.3}$$

and also

$$Q \otimes_L P = P \otimes_L Q = Q^d. \tag{4.4}$$

Let $Q = \oplus_k Q_k^{s_k}$, $s_k > 0$, be the decomposition of Q into indecomposable L-bimodules, let t_k be the multiplicity of Q_k in the decomposition of P, and let $t/s = t_\ell/s_\ell$ be the smallest of the rational numbers t_k/s_k. Since, as shown above, some multiple of P contains Q as a direct summand, $t > 0$. We have $P^s = Q^t \oplus M$, where M does not contain Q_ℓ as a direct summand. By (4.3) and (4.4), we have

$$Q \otimes_L M = M \otimes_L Q = Q^{d(s-tN)}. \tag{4.5}$$

Thus, we get

$$\begin{aligned} Q^{tds} \oplus M^{ds} = P^{ds^2} &= P^s \otimes_L P^s \\ &= (Q^t \oplus M) \otimes_L (Q^t \oplus M) \\ &= Q^{t^2dN+2td(s-tN)} \oplus M \otimes_L M. \end{aligned}$$

Since M does not contain Q_ℓ as a direct summand, we get

$$tds \geq t^2dN + 2td(s - tN).$$

Since $t > 0$, this gives

$$s \geq tN + 2(s - tN) = 2s - tN.$$

Thus,

$$s - tN \leq 0.$$

But we also know from (4.5) that $s - tN \geq 0$. Thus $s - tN = 0$, and hence $M = 0$. So $P^s = Q^t$, i.e. $P = \oplus_{i,j}(L_i \otimes_{\mathcal{Z}} L_j)^{a_i t b_j N/s d_j}$. This means that $r_j := \frac{t b_j N}{s d_j}$ are integers, and $P = \oplus_{i,j}(L_i \otimes_{\mathcal{Z}} L_j)^{a_i r_j}$, as claimed. The theorem is proved. □

4.2. Galois bimodules over noncommutative semisimple algebras finite over center. Let B be a semisimple algebra finite over its center, i.e. $B = \oplus_{i=1}^n B_i$, where B_i are central simple algebras over fields L_i of the same characteristic, of dimension m_i^2. Let P be a Galois B-bimodule of rank d. As in the commutative case, it suffices to consider connected bimodules, so we will assume that P is connected.

First consider the case when $B_i = \mathrm{Mat}_{m_i}(L_i)$. In this case, similarly to the case of simple algebras, we have the following proposition. Let m_* be the greatest common divisor of the m_i.

Proposition 4.5. *The center $\mathcal{Z}$ of P is a field such that $[L_i : \mathcal{Z}] < \infty$, and P is a multiple of $\oplus_{i,j}\mathrm{Mat}_{m_i \times m_j}(L_i \otimes_{\mathcal{Z}} L_j)^{m_i m_j/m_*^2}$.*

Proof. Let $L = \oplus_{i=1}^n L_i$ be the center of B. Let $F : B - \mathrm{Bimod} \to L - \mathrm{bimod}$ be the standard Morita equivalence. It is easy to see that $F(P)$ is a quasi-Galois L-bimodule of rank d. Thus, by Theorem 4.2, $F(P) = \oplus_{i,j}(L_i \otimes_{\mathcal{Z}} L_j)^{a_i r_j}$, where a_i are coprime integers. By looking at the left dimensions of P_{ij} over L_i, we get

$$\sum_j m_i m_j a_i r_j d_j = d m_i^2.$$

where $d_j = [L_j : \mathcal{Z}]$. This implies that $a_i = m_i/m_*$, and $d m_* = \sum_j m_j r_j d_j$. Also, by looking at right dimensions we have

$$\sum_i m_i m_j a_i r_j d_i = d m_j^2,$$

which implies that $r_j = r m_j/m_*$, where

$$r = \frac{d m_*}{\sum_i d_i m_i a_i} = \frac{d m_*^2}{\sum_i d_i m_i^2}.$$

is an integer. This implies the statement by applying F^{-1}. □

Now consider the general case.

Proposition 4.6. *The center $\mathcal{Z}$ of P is a field such that $[L_i : \mathcal{Z}] < \infty$, and $P^{m_*^2}$ is a multiple of $B \otimes_{\mathcal{Z}} B$.*

Proof. Let $E_i \supset L_i$ be finite dimensional commutative separable algebras (not necessarily field extensions) which split the central simple algebras B_i, i.e. $E_i \otimes_{L_i} B_i = \mathrm{Mat}_{m_i}(E_i)$. We can pick E_i in such a way that $[E_i : L_i] = D$, the same number for all i. Let $E = \oplus_i E_i$. Then $E = L^D$ as an L-module, so by Lemma 2.7(i), $E \otimes_L P \otimes_L E$ is a Galois bimodule over $E \otimes_L B = \oplus_i \mathrm{Mat}_{m_i}(E_i)$. By Proposition 4.5, $E \otimes_L P \otimes_L E$ is a multiple of $\oplus_{i,j} \mathrm{Mat}_{m_i \times m_j}(E_i \otimes_{\mathcal{Z}} E_j)^{m_i m_j/m_*^2}$, where $\mathcal{Z}$ is the center of P. This implies that the E-bimodule $(E \otimes_L P \otimes_L E)^{m_*^2}$ is a multiple of

$$\begin{aligned}\oplus_{i,j} \mathrm{Mat}_{m_i \times m_j}(E_i \otimes_{\mathcal{Z}} E_j)^{m_i m_j} &= \oplus_{i,j} \mathrm{Mat}_{m_i}(E_i) \otimes_{\mathcal{Z}} \mathrm{Mat}_{m_j}(E_j) \\ &= (E \otimes_L B) \otimes_{\mathcal{Z}} (E \otimes_L B).\end{aligned}$$

So restricting back to B, we get that $P^{D^2 m_*^2}$ is a multiple of $(B \otimes_{\mathcal{Z}} B)^{D^2}$, which shows that $P^{m_*^2}$ is a multiple of $B \otimes_{\mathcal{Z}} B$, as desired. □

Corollary 4.7. *Let P be a Galois bimodule over B. Let m be the least common multiple of the m_i. Given $a \in (a_1, \dots, a_n) \in L \subset B$, denote by $\phi_i(a)$ the i-th component of $\phi(a) = \phi_P(a)$, $\phi_i(a) \in \mathrm{Mat}_{d m_i^2}(L_i)$. Let $\chi_a \in L[t]$ be the collection*

of monic polynomials $\chi_{\phi_i(a)}(t)^{m^2/m_i^2} \in L_i[t]$ *of degree* dm^2, *where* $\chi_{\phi_i(a)}$ *is the characteristic polynomial of* $\phi_i(a)$. *Then the coefficients of* χ_a *belong to the center* $\mathcal{Z} = \mathcal{Z}(P) \subset L$.

Proof. It suffices to assume that P is connected, so we restrict ourselves to this case. Let χ_{a_j} be the characteristic polynomial of $a_i \in L_i$ acting by multiplication on L_i as a vector space over $\mathcal{Z}$. Clearly, this is a polynomial over $\mathcal{Z}$. By Proposition 4.6, we have

$$\chi_{\phi_i(a)}^{m_*^2} = \prod_{j=1}^{n} \chi_{a_j}^{m_i^2 m_j^2} = f^{m_i^2},$$

where $f = \prod_{j=1}^{n} \chi_{a_j}^{m_j^2}$. Thus,

$$\chi_{\phi_i(a)}^{m^2/m_i^2} = f^{(m/m_*)^2}.$$

This is a polynomial with coefficients in $\mathcal{Z}$, and it is independent on i, which implies that χ_a has coefficients in $\mathcal{Z}$, as desired. □

Corollary 4.8. *If* P *is a connected Galois* B*-bimodule of rank* d, *and* $d_i = [L_i : \mathcal{Z}]$, *then* $\sum_{i=1}^{n} d_i (m_i/m_*)^2$ *divides* d.

Proof. By Proposition 4.6, $P^{m_*^2} = (B \otimes_{\mathcal{Z}} B)^r$, so computing ranks over B as left modules, we get $dm_*^2 = r \sum d_i m_i^2$, which implies the statement. □

5. Generalization of Theorem 3.1

In this section we use the results of the previous section to generalize Theorem 3.1 to the situation when Z is not necessarily a domain, but a reduced algebra, i.e., one without nonzero nilpotents. Let Q be the total quotient ring of Z.

Let A be an algebra over Z with a coaction of a finite dimensional Hopf algebra K over k of dimension d. As in Section 3, consider assumptions (1)–(5) on A, Z, generalizing assumption (2) as follows:

(2) $Q \otimes_Z A$ is a semisimple algebra with center Q.

Note that (2) implies that $Q = Q_1 \oplus \ldots \oplus Q_n$, where Q_i are fields containing k. This property of Z is satisfied, for instance, if Z is Noetherian (in particular, affine).

Theorem 5.1. *Theorem 3.1 holds in this more general situation. In other words, under the conditions (1)–(4) or (1), (2), (5),* A *and* Z *are integral over* Z^K, *and if* Z *is finitely generated over* k, *then so is* Z^K, *and* Z *is a finite module over* Z^K.

In the case when A is commutative, this is again a special case of the result of [12] (for reduced agebras whose quotient rings are finite direct sums of fields).

Proof. The proof is parallel to the proof of Theorem 3.1. The proofs of (iii) and (iv) are the same, so we only comment on the proofs of (i) and (ii).

As in the proof of Theorem 3.1, let $P = A \otimes K$, and $P_{\mathrm{loc}} = Q \otimes_Z P$. This is a left module over the algebra $B := Q \otimes_Z A$, which is a semisimple algebra over Q by (2), i.e., a direct sum of central simple algebras B_i of dimensions m_i^2 over Q_i for some m_i. Consider the right action of Z on $Q \otimes_Z P$. This action defines a homomorphism $\psi_P : Z \to \mathrm{End}_Q(Q \otimes_Z P) \cong \oplus_{i=1}^n \mathrm{Mat}_{dm_i^2}(Q_i)$.

We claim that for any $z \in Z$ which is not a zero divisor, the element $\psi_P(z)$ is invertible. Indeed, let $x \in Q \otimes_Z P$ be such that $\psi_P(z)x = xz = 0$. Let $x = w^{-1}y$, where $w \in Z$ (not a zero divisor), and $y \in P$. Hence, yz is a torsion element of P, i.e. $z'yz = 0$ in P for some $z' \in Z$, which is not a zero divisor. But by (3) (or by (5)), A is torsion-free over Z, which implies that P is torsion-free over Z on each side. So we get that $yz = 0$ and hence $y = 0$ and $x = 0$, as desired.

Thus, we see that the right action of Z on $Q \otimes_Z P$ naturally extends to a right action of Q, i.e. $Q \otimes_Z P$ is a Q-bimodule. Hence, $Q \otimes_Z P$ is a bimodule over the semisimple algebra B, and

$$P_{\mathrm{loc}} = Q \otimes_Z P = Q \otimes_Z P \otimes_Z Q = B \otimes_A P \otimes_A B.$$

By Proposition 2.8, $P := A \otimes K$ is a Galois bimodule over A of rank d. This implies by Lemma 2.7(i) that P_{loc} is a Galois bimodule over B of rank d.

By Corollary 4.7, for each $a \in Z$, the polynomial $\chi_a(t) \in Q[t]$ defined in Corollary 4.7 has coefficients in $\mathcal{Z}(P_{\mathrm{loc}}) = Q^K = Q \cap A^K$.

Now, since Z is integrally closed (i.e., is a normal algebra), it is a direct sum of integrally closed domains $Z_1 \oplus \ldots \oplus Z_n$. Hence, Lemma 3.7 implies that $\chi_a(t) \in Z[t]$.

Moreover, if $z \in Z$ is central for P_{loc} then by (3) it is also central for P. Thus, the coefficients of χ_a belong to $Z \cap \mathcal{Z}(P)$. By Proposition 2.8, this means that these coefficients belong to $Z \cap A^K$. Hence Z is integral over $Z \cap A^K$ (as $a \in Z$ is annihilated by the polynomial χ_a). Thus, (i) is proved.

To prove (ii), it suffices to note that by (5), for $a \in Z$ the coefficients of the polynomial $\chi_a(t)$ of Proposition 4.6 are in Z, after which the proof is the same as in (i). □

Corollary 5.2. *In the situation of Theorem 5.1, the coaction of K on A uniquely extends to $Q \otimes_Z A$.*

Proof. This follows since by Theorem 5.1, $Q \otimes_Z A = Q^K \otimes_{Z^K} A$. □

Remark 5.3. As before, this is a special case of [14], Theorem 2.2.

We also obtain the following generalization of Proposition 3.9:

Proposition 5.4. *Suppose $A = \oplus_{i=1}^n A_i$ is an indecomposable semisimple K-comodule algebra with center Q, where A_i are simple algebras of degrees m_i over fields Q_i (so that $Q = \oplus_{i=1}^n Q_i$). Let m_* be the greatest common divisor of the m_i, and $d_i = [Q_i : Q^K]$. Then $\sum_{i=1}^n d_i(m_i/m_*)^2$ divides $d = \dim K$.*

Proof. $A \otimes K$ is a Galois A-bimodule of rank d, so the statement follows from Proposition 4.8. □

Remark 5.5. Here is another proof of Proposition 5.4 in characteristic zero, using the theory of tensor categories (this approach also works in characteristic p with some complications). By Theorem 5.1, $[L_i : \mathcal{Z}] = d_i < \infty$. So, tensoring over $\mathcal{Z}$ with the algebraic closure $\overline{\mathcal{Z}}$, we obtain a semisimple algebra $\overline{A}$ with a coaction of a Hopf algebra $\overline{K}$ (both finite dimensional over $\overline{\mathcal{Z}}$). Then $\mathrm{Rep}\overline{A}$ is a semisimple indecomposable module category over $\mathrm{Rep}\overline{K}$. Thus, one can define canonical Frobenius–Perron dimensions of objects in $\mathrm{Rep}\overline{A}$, as in [3], Subsection 2.5. They are defined by the formula

$$\mathrm{FPdim}(M_i)^2 = \frac{dn_i^2}{\sum_j n_j^2},$$

where n_j is the ordinary dimension of M_j. These dimensions are known to be integers, since $\mathrm{FPdim}(M_i)^2 = \mathrm{FPdim}\underline{\mathrm{End}}(M_i)$. This implies that if n_* is the greatest common divisor of the n_i then $\frac{dn_*^2}{\sum_j n_j^2} \in \mathbb{Z}$. But $n_* = m_*$, and (n_j) is the collection where each m_i is repeated d_i times. This implies the statement.

6. The tensor category of finite dimensional L-bimodules

The theory of Galois bimodules over a field L is closely related to the theory developed in [7]. Let us discuss this connection. For simplicity, we assume that $\mathrm{char}(L) = 0$, although this discussion can be extended to positive characteristic as well (at the cost of losing semisimplicity of bimodules).

In [7], the authors consider the semisimple tensor category $L - \mathrm{bimod}_E$ of finite dimensional L-bimodules M that split over some finite Galois extension E of L (or are E-balanced, in the language of [7]), i.e., $E \otimes_L M \otimes_L E$ is a direct sum of bimodules Eg for $g \in \mathrm{Aut}(E)$. They show that the Grothendieck ring of this category tensored with $\mathbb{Q}$, $K_0(L - \mathrm{bimod}_E) \otimes \mathbb{Q}$, is naturally isomorphic to the Hecke algebra $\mathcal{H}(\mathrm{Aut}(E), H)$, where $H = \mathrm{Gal}(E/L)$ (i.e., the convolution algebra of $\mathbb{Q}$-valued H-biinvariant functions on $\mathrm{Aut}(E)$ with finite support). Thus, a Galois L-bimodule P of rank d which splits over E defines a nonnegative idempotent $e = \frac{1}{d}[P]$ in this Hecke algebra. The support of such an idempotent is a

multiplicatively closed finite subset of $\mathrm{Aut}(E)$, so it is a finite subgroup $G \subset \mathrm{Aut}(E)$ containing H. Moreover, it is easy to see as in the proof of Proposition 2.15 that the idempotent e has to be defined by the formula $e(g) = \frac{1}{|G|}$ for all $g \in G$. So $[P](g) = \frac{d}{|G|}$. For this to define an integral class, we need $r := |H|d/|G|$ to be an integer, and then $E \otimes_L P \otimes_L E = P(E,G)^r$, as explained in Proposition 2.19.

The results of Section 2 on Galois bimodules and the results of [7] can be used to prove the following result about the tensor category $L-$bimod of L-bimodules which are finite dimensional as left and right L-vector spaces, which also gives a classification of Galois L-bimodules.

Theorem 6.1. *Suppose $\mathcal{C} \subset L-$bimod is a full abelian rigid tensor subcategory, which is semisimple and has finitely many simple objects. Then there exists a unique subfield $F \subset L$ such that $[L:F] < \infty$, and $\mathcal{C} = \mathcal{C}(F,L)$ is the category of L-bimodules which are linear over F, i.e. the right and left actions of F coincide. The simple objects of this category are the simple direct summands in $L \otimes_F L$, and they split over the Galois closure E of L over F.*

Proof. Let $d(X)$ be the dimension of an L-bimodule X as a left L-vector space. Then $d : K_0(\mathcal{C}) \to \mathbb{Z}$ is a character. Let X_i be the simple objects of $\mathcal{C}$. Let $X = \oplus_i X_i$. Since $\mathcal{C}$ is a tensor category, the matrix of right multiplication by X in the basis X_i is an indecomposable nonnegative matrix. So by the Frobenius–Perron theorem there exist unique up to scaling positive real numbers r_i such that $(\sum_i r_i X_i)X = \Lambda \sum_i r_i X_i$ in $K_0(\mathcal{C}) \otimes \mathbb{R}$, where Λ is the largest positive eigenvalue of X. Computing the dimensions of both sides as a left vector space, we get that $\Lambda = d(X)$, which is an integer. This implies that the numbers r_i can be scaled to be all integers as well; let us choose them in such a way. Let $P = \oplus_i r_i X_i$. By uniqueness of r_i, we get that $P \otimes_L P = P^{d(P)}$. Thus, P is a Galois bimodule. So by Theorem 2.31, P is a multiple of $L \otimes_F L$ for some F (namely, $F = \mathcal{Z}(P)$). This implies the desired statement (as any simple F-linear L-bimodule is a quotient, hence a direct summand, of $L \otimes_F L$). □

Remark 6.2. In the tensor category $\mathcal{C}(F,L)$, one has $\mathrm{End}(\mathbf{1}) = L$, but in general it is not L-linear but only F-linear. It is a form over F, in the sense of [2], of the multifusion category of $\mathrm{Fun}(G/H,E)$-bimodules, which is associated to the natural semilinear action of $G = \mathrm{Gal}(E/F)$ on this category. The simple objects in this F-linear tensor category are then associated to orbits of G on $G/H \times G/H$, which correspond to double cosets of H in G, spanning the Hecke algebra as in [7]. Note also that this category is independent on the choice of the Galois extension E of F, as long as it contains L.

Remark 6.3. Theorem 6.1 generalizes to the case when the field L is replaced by a central simple algebra B with center L. Namely, recall that by Proposition 2.37, any Galois B-bimodule is semisimple and is a rational multiple of the bimodule $B \otimes_F B$ for a uniquely determined subfield $F \subset L$ such that $[L:F] < \infty$ (namely,

$F = \mathcal{Z}(P)$). Now, if $\mathcal{C} \subset B-$bimod is a full abelian rigid tensor subcategory, which is semisimple and has finitely many simple objects, then one shows similarly to Theorem 6.1 that there exists a unique subfield $F \subset L$ such that $[L : F] < \infty$, and $\mathcal{C} = \mathcal{C}(F, B)$ is the category of B-bimodules which are linear over F, i.e. the right and left actions of F coincide. The simple objects of this category are the simple direct summands in $B \otimes_F B$.

This is related to the results of [2] in the following way. The category $\mathcal{C}(F, B)$ is a twisted form of the category $\mathcal{C}(F, L)$ in the sense of [2]. According to [2], such twisted forms which split over the Galois extension E of F containing L correspond to elements of $H^2(G, \mathrm{Aut}_\otimes(\mathrm{Id}))$. In our situation $\mathrm{Aut}_\otimes(\mathrm{Id}) = \mathrm{Fun}(G/H, E^\times)/E^\times$, and the long exact sequence of cohomology and the Shapiro lemma imply that $H^2(G, \mathrm{Aut}_\otimes(\mathrm{Id}))$ contains the quotient $H^2(H, E^\times)/\mathrm{Im}H^2(G, E^\times)$, which parametrizes E-split central simple algebras B over L up to Morita equivalence modulo those of the form $B = L \otimes_F A$, where A is a central simple algebra over F. It is easy to show that under the correspondence of [2], the category $\mathcal{C}(F, B)$ corresponds precisely to the class of the central simple algebra B in $H^2(H, E^\times)/\mathrm{Im}H^2(G, E^\times)$.

In fact, it is easy to see explicitly that the categories $\mathcal{C}(F, B_1)$ and $\mathcal{C}(F, B_2)$ are equivalent if $B_1 = B_2 \otimes_F A$, where A is a central simple algebra over F. The equivalence is defined by the formula $M \mapsto M \otimes_F A$ for a B_2-bimodule M linear over F.

References

[1] M. S. Eryashkin, Martindale rings and H-module algebras with invariant characteristic polynomials, *Sibirsk. Mat. Zh.*, **53** (2012), no. 4, 822–838. Zbl 1260.16026 MR 3013530

[2] P. Etingof and S. Gelaki, *Descent and forms of tensor categories*, International Mathematics Research Notices, **2012** (2012) no. 13, 3040–3063. arXiv:1102.0657 Zbl 1246.18003 MR 2946231

[3] P. Etingof, D. Nikshych and V. Ostrik, Fusion categories and homotopy theory, *Quantum Topology*, **1** (2010), 209–273. arXiv:0909.3140 Zbl 1214.18007 MR 2677836

[4] P. Etingof and V. Ostrik, Finite tensor categories, *Mosc. Math. J.* **4** (2004), no. 3, 627–654. Zbl 1077.18005 MR 2119143

[5] P. Etingof and C. Walton, Semisimple Hopf actions on commutative domains, *Adv. Math.* **251** (2014), 47–61. arXiv:1301.4161 Zbl 1297.16029 MR 3130334

[6] P. Etingof and C. Walton, *Actions of finite dimensional Hopf algebras on commutative domains and their deformations*, work in progress.

[7] V. Futorny and S. Ovsienko, Galois orders in skew monoid rings, *J. of Algebra*, **324** (2010), 598–630. Zbl 1204.16010 MR 2651560

[8] N. Jacobson, Galois theory of purely inseparable fields of exponent one, *American Journal of Mathematics*, **66** (1944), 645–648. Zbl 0063.03019 MR 11079

[9] S. Lang, *Algebra*, Third addition, Springer, 2002. Zbl 0984.00001 MR 1878556

[10] S. Montgomery, *Hopf algebras and their actions on rings*, AMS, 1993. Zbl 0793.16029 MR 1243637

[11] J. McConnell and J. Robson, with the cooperation of L. Small, *Noncommutative Noetherian rings*, Graduate Studies in Mathematics, 30, AMS, 2001. Zbl 0980.16019 MR 1811901

[12] S. Skryabin, Invariants of finite Hopf algebras, *Adv. Math.*, **183** (2004) no. 2, 209–239. arXiv:math/0209046 Zbl 1052.16025 MR 2041899

[13] S. Skryabin, Projectivity and freeness over comodule algebras, *Trans. Amer. Math. Soc.*, **359** (2007) 2597–2623. arXiv:math/0610657 Zbl 1123.16032 MR 2286047

[14] S. Skryabin and F. van Oystaeyen, The Goldie Theorem for H-semiprime algebras, *Journal of Algebra*, **305** (2006) 292–320. Zbl 1109.16033 MR 2264132

[15] A. A. Totok, Actions of Hopf algebras, *Mat. Sb.*, **189** (1998) no. 1, 147–157. Zbl 0914.16019 MR 1616452
http://www.cs.nyu.edu/totok/professional/papers/actions98.pdf

[16] S. Zhu, Integrality of Module Algebras over Its Invariants, *Journal of Algebra*, **180**, (1996) no. 1, 187–205. Zbl 0845.16039 MR 1375574

Received 18 June, 2013; revised 09 May, 2014

P. Etingof, Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
E-mail: etingof@math.mit.edu