Galois Closures of Non-commutative Rings and an Application to Hermitian Representations

Wei Ho[1] and Matthew Satriano[2,*]

[1]Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA and [2]Pure Mathematics, University of Waterloo, 200 University Avenue West, Waterloo, ON N2L 3G1, Canada

Correspondence to be sent to: e-mail: msatrian@uwaterloo.ca

Galois closures of commutative rank n ring extensions were introduced by Bhargava and the 2nd author. In this paper, we generalize the construction to the case of non-commutative rings. We show that noncommutative Galois closures commute with base change and satisfy a product formula. As an application, we give a uniform construction of many of the representations arising in arithmetic invariant theory, including many Vinberg representations.

1 Introduction

In the last fifteen years, there have been many beautiful applications given by interpreting orbit spaces of representations as moduli spaces of arithmetic or algebraic objects, such as ideal classes of low-rank rings or Selmer elements of elliptic curves. Many of the representations that arise seem to be closely related to one another, and in some cases, they can be formally related to one another by a process called Hermitianization; see [1, 2, 11]. In this paper, we construct such representations via a uniform approach. Our method relies on a seemingly unrelated problem: defining Galois closures of possibly noncommutative rings.

Galois closures of commutative rank n ring extensions were studied in [5], building on previous work of Grothendieck [6, Exposé 4], Katz–Mazur [9, Section 1.8.2], and Gabber [7, Section 5.2]. Given a morphism $R \to A$ of commutative rings realizing A as a free R-module of rank n, the *Galois closure* $G(A/R)$ is defined as the quotient $A^{\otimes n}/I_{A/R}$, where $I_{A/R}$ is an ideal generated by relations coming from characteristic polynomials. More precisely, given $a \in A$, consider the R-linear endomorphism of A given by multiplication by a and let $T^n + \sum_{j=1}^{n}(-1)^j s_{A,j}(x)T^{n-j}$ be its characteristic polynomial. Let $a^{(i)} \in A^{\otimes n}$ denote $1 \otimes \cdots \otimes a \otimes \cdots 1$, where a is in the i-th tensor factor, and let e_j denote the j-th elementary symmetric function. Then the ideal $I_{A/R}$ is generated by the relations

$$e_j\big(a^{(1)}, a^{(2)}, \ldots, a^{(n)}\big) - s_{A,j}(a),$$

as a runs through all elements of A. Then $G(A/R)$ is an R-algebra equipped with a natural S_n-action, and the elements $a^{(1)}, a^{(2)}, \ldots, a^{(n)}$ behave as if they are "Galois conjugates." One key property is that $G(A/R)$ commutes with base change on R. This construction has since been generalized by Gioia to so-called intermediate Galois closure [8] as well as by Biesel to Galois closures associated to subgroups of S_n [3].

We now describe the connection between Galois closures of noncommutative algebras and problems in arithmetic invariant theory. In this paper, we obtain many of the representations with arithmetic applications by the following uniform construction: let A be a possibly noncommutative degree n R-algebra and let $G(A/R)$ be its Galois closure, as we define in Section 2, which comes with a natural S_n-action. For an n-dimensional $m \times m \times \cdots \times m$ array with entries in $G(A/R)$, there are two natural S_n-actions: one on $G(A/R)$ and the other permuting the coordinates of the n-dimensional array. The subspace where these two actions coincide has a natural action of the matrix ring $\mathrm{Mat}_m(A) \otimes G(A/R)$; we refer to this as the associated *Hermitian representation* $\mathcal{H}_{A,m}$. See Section 4 for lists of representations obtained in this manner that have arisen in arithmetic invariant theory. We hope that our uniform construction of these representations $\mathcal{H}_{A,m}$, with just the input of a degree n R-algebra A and a positive integer m, will also give a systematic approach to studying the moduli problems related to the orbit spaces of the Hermitian representations.

For n and m sufficiently small, these Hermitian representations were studied explicitly in previous work [1, 2, 11]. Galois closures were not needed in these previous papers for two main reasons. First, when m is small, the entries of the elements in the Hermitian representation may be defined over A itself. And second, when n is small, the Galois closure $G(A/R)$ is quite simple; for example, when

A is a quadratic algebra ($n = 2$), the Galois closure $G(A/R)$ is isomorphic to A (see Proposition 3.2). Similarly, when A is a decomposable cubic algebra, for example, $A = R \times B$ for B quadratic, then $G(A/R) \simeq B^{\oplus 3}$ (see Proposition 3.6), so $m \times m \times m$ arrays Hermitian with respect to $A = R \times B$ may be viewed as an m-tuple of $m \times m$ matrices Hermitian with respect to B (see Example 4.7). Thus, the need for Galois closures in describing Hermitian representations does not arise until one considers $m \geq 3$ and indecomposable cubic algebras A, such as the matrix ring $\text{Mat}_3(R)$.

The aforementioned Proposition 3.6 and Example 4.7 are both specific cases of more general results as we now discuss. In Section 2.3, we prove the following product formula, which allows one to calculate the Galois closure of decomposable algebras in terms of the Galois closures of its components.

Theorem (Product formula).   For $1 \leq i \leq k$, let A_i be a degree n_i R-algebra. Then

$$G(A_1 \times \cdots \times A_k/R) \simeq \big(G(A_1/R) \otimes \cdots \otimes G(A_k/R)\big)^N,$$

where N is the multinomial coefficient $\binom{n}{n_1,\ldots,n_k}$.

As a consequence, in Theorem 4.5, we may write the Hermitian representation of a decomposable algebra in terms of the Hermitian representations of its components.

Theorem (Product formula for Hermitianizations).   For $1 \leq i \leq k$, let A_i be a degree n_i R-algebra, and let $A = \prod_{i=1}^{k} A_i$. Then for any positive integer m, we have $\mathcal{H}_{A,m} \simeq \mathcal{H}_{A_1,m} \otimes \cdots \otimes \mathcal{H}_{A_k,m}$.

We also prove that taking Galois closures commutes with base change.

Theorem (Base change).   Let A be a degree n R-algebra and let S be a commutative R-algebra. The base change map yields an isomorphism

$$G(A/R) \otimes_R S \simeq G\big((A \otimes_R S)/S\big).$$

In this paper, all the algebras we consider are associative, but we believe it would be useful to generalize these ideas to non-associative algebras such as cubic Jordan algebras as well, especially as Jordan algebras have already been crucially used in basic examples of Hermitianization.

2 Galois Closures of Non-commutative Rings

In this section, we define the *Galois closure* for certain classes of (possibly noncommutative) rings and discuss several properties. When A is commutative, it recovers the construction in [5].

2.1 Degree n algebras

We first define a degree n algebra over a commutative ring R. We use the following notion: a morphism $f \colon M \to N$ of R-modules is *universally injective* if for every commutative R-algebra S, the induced map $f \otimes 1 \colon M \otimes_R S \to N \otimes_R S$ is injective. For example, if f is split, then f is universally injective.

Definition 2.1. Let A be a central R-algebra that is free of finite rank as an R-module. Let R' be a finitely generated commutative R-algebra such that $R \to R'$ is universally injective, with a universally injective R-algebra homomorphism $\iota \colon A \to \mathrm{Mat}_n(R')$. We say that the triple (A, R', ι) is a *degree n R-algebra* if for all $a \in A$, the characteristic polynomial

$$P_{A,a}(T) = \det\left(T - \iota(a)\right) = T^n - s_{A,1}(a)T^{n-1} + \cdots + (-1)^n s_{A,n}(a) \tag{2.2}$$

lives in $R[T]$, in other words, $s_{A,i}(a) \in R$ for $1 \leq i \leq n$. We frequently suppress R' and ι from the notation if they are unambiguous and refer to A itself as a degree n R-algebra.

For a degree n R-algebra (A, R', ι), we refer to $\mathrm{Tr}(a) := s_{A,1}(a)$ and $\mathrm{N}(a) := s_{A,n}(a)$ as the *trace* and *norm* of $a \in A$, respectively. It is immediate from the definition that $s_{A,j}(ra) = r^j s_{A,j}(a)$ for all $r \in R$ and $a \in A$; in particular, the trace is additive and the norm is multiplicative.

Remark 2.3. If $R' = R$, clearly the required property $P_{A,a}(T) \in R[T]$ is automatically satisfied.

Remark 2.4. Let (A, R', ι) be a degree n R-algebra and let $\psi \colon \mathrm{Mat}_n(R') \to \mathrm{Mat}_n(R')$ be conjugation by an element of $\mathrm{GL}_n(R')$. Then $(A, R', \psi\iota)$ is a degree n R-algebra and all the characteristic polynomials $P_{A,a}(T)$ for the two algebras coincide.

Example 2.5 (Left multiplication). Let A be a central R-algebra that is free of finite rank n as an R-module. Then we can view A as a degree n R-algebra as follows. Choose a basis $u_1, \ldots, u_n$ for A over R. Left multiplication by elements $a \in A$ induces a natural

map $\iota\colon A \to \mathrm{Mat}_n(R)$. Then ι is clearly injective since $a \cdot 1 \neq 0$ if $a \neq 0$. It is in fact universally injective by the same observation, since $u_1, \ldots, u_n$ is also a basis for $A \otimes_R S$ over S, for any commutative R-algebra S.

Example 2.6 (Split algebra of any degree).   For any $n \geq 1$, we may view R^n as a degree n R-algebra by left multiplication as in Example 2.5. In this case, the element $a = (r_1, \ldots, r_n)$ has characteristic polynomial $P_{R^n,a}(T) = \prod_{i=1}^n (T - r_i)$.

Example 2.7 (Trivial algebra of any degree).   For any $n \geq 1$, we may view R as a degree n algebra over itself by choosing $\iota\colon R \to \mathrm{Mat}_n(R)$ as the diagonal embedding of R. Then $P_{R,a}(T) = (T - a)^n$ for any $a \in R$. Although seemingly trivial, this example plays a useful role.

More generally, for any degree n algebra (A, R', ι) and integer $m \geq 1$, we may also give A the structure of a degree mn algebra via the diagonal block map $(\iota, \ldots, \iota)\colon A \to \mathrm{Mat}_{mn}(R')$. The characteristic polynomials are m-th powers of the original characteristic polynomials.

Example 2.8 (Matrix algebras).   If $A = \mathrm{Mat}_n(R)$, then taking ι to be the identity map gives A the structure of a degree n algebra.

Example 2.9 (Central simple algebras).   If A is a central simple algebra over a field F, then there exists a splitting field K over F such that $A \otimes_F K \simeq \mathrm{Mat}_n(K)$, where n is the square root of the rank of A as a F-vector space. We thus have an injection $\iota\colon A \to \mathrm{Mat}_n(K)$, and it is universally injective because ι is split. The polynomials $P_{A,a}$ agree with the *reduced characteristic polynomial* of a central simple algebra A, and it is well known that the coefficients lie in F (see, e.g., [4, Section IV.2]). In this way, we may view A as an algebra of degree equal to the square root of the rank of A (which is the typical definition of the degree of a central simple algebra).

Remark 2.10.   One may generalize the definition of degree n algebra to *locally* free R-modules of finite rank by requiring a universally injective homomorphism to an endomorphism algebra of a rank n vector bundle over R' instead. The definitions of and theorems for Galois closures will also generalize in a similar way, but we focus on the case of free R-modules in the rest of the paper for simplicity.

We next introduce products of degree n R-algebras.

Definition 2.11. Let (A_1, R_1, ι_1) and (A_2, R_2, ι_2) be R-algebras of degrees n_1 and n_2, respectively. We define the product $(A_1, R_1, \iota_1) \times (A_2, R_2, \iota_2)$ to be the degree $n_1 + n_2$ R-algebra $A = A_1 \times A_2$ with the universally injective composition

$$\iota \colon A_1 \times A_2 \xrightarrow{(\iota_1, \iota_2)} \operatorname{Mat}_{n_1}(R_1) \times \operatorname{Mat}_{n_2}(R_2) \hookrightarrow \operatorname{Mat}_{n_1}(R_1 \times R_2)$$
$$\times \operatorname{Mat}_{n_2}(R_1 \times R_2) \hookrightarrow \operatorname{Mat}_{n_1 + n_2}(R_1 \times R_2),$$

where the last injection is given by block diagonals. If $a_i \in A_i$ has characteristic polynomials P_{A_i, a_i} for $i \in \{1, 2\}$, then the characteristic polynomial of $a = (a_1, a_2) \in A_1 \times A_2$ is clearly the product $P_{A,a}(T) = P_{A_1, a_1}(T) P_{A_2, a_2}(T) \in R[T]$.

The following gives some further properties of product R-algebras.

Lemma 2.12. Let A_i be a degree n_i R-algebra for $1 \le i \le k$ and endow $A = \prod_{i=1}^{k} A_i$ with its associated structure as a degree $n := \sum_{i=1}^{k} n_i$ R-algebra.

1. If $a = (a_1, \dots, a_k) \in A$, then

$$s_{A,m}(a) = \sum_{\substack{0 \le m_i \le n_i \\ m_1 + \cdots + m_k = m}} \prod_{i=1}^{k} s_{A_i, m_i}(a_i),$$

where we set $s_{A_i, 0}(a_i) = 1$.

2. If $a = (0, \dots, 0, a_j, 0, \dots 0)$, then

$$s_{A,m}(a) = s_{A_j, m}(a_j).$$

Proof. We first show (1). We use the notation $[T^j]Q$ to denote the T^j-coefficient of a polynomial $Q(T)$. As $P_{A,a}(T) = \prod_j P_{A_j, a_j}(T)$, we have

$$[T^{n-m}]P_{A,a} = \sum_{\substack{0 \le m_i \le n_i - m_i \\ m_1 + \cdots + m_k = n - m}} \prod_j [T^{m_i}]P_{A_i, a_i}.$$

Since the indices of the summation satisfy $0 \le m_i \le n_i$, replacing m_i by $n_i - m_i$ changes the above sum to

$$[T^{n-m}]P_{A,a} = \sum_{\substack{0 \le m_i \le n_i \\ \sum (n_i - m_i) = n - m}} \prod_i [T^{n_i - m_i}]P_{A_i, a_i} = \sum_{\substack{0 \le m_i \le n_i \\ \sum m_i = m}} \prod_j [T^{n_i - m_i}]P_{A_i, a_i}$$

and multiplying by $(-1)^m = \prod_i (-1)^{m_i}$ gives the result.

For (2), we know that for all $i \neq j$, we have $P_{A_i,0}(T) = T^{n_i}$ and so $s_{A_i,m_i}(a) = \delta_{m_i,0}$. Thus, by (1) we see $s_{A,m}(a) = s_{A_j,m}(a_j)$.   ∎

2.2   Galois closures

We now define the Galois closure for a degree n R-algebra A. For an element $a \in A$, let $a^{(i)}$ denote $1 \otimes \cdots \otimes a \otimes \cdots \otimes 1 \in A^{\otimes n}$, where a is in the i-th tensor factor. Then consider the left ideal $I_{A/R}$ in $A^{\otimes n}$ generated by the elements

$$e_j(a^{(1)}, a^{(2)}, \ldots, a^{(n)}) - s_j(a) \tag{2.13}$$

for every $a \in A$ and $1 \leq j \leq n$, where e_j denotes the j-th elementary symmetric function and $s_j(a) = s_{A,j}(a) \cdot (1 \otimes \cdots \otimes 1)$.

Definition 2.14.   The *Galois closure* of a degree n R-algebra A is defined to be the left $A^{\otimes n}$-module

$$G(A/R) := A^{\otimes n}/I_{A/R}. \tag{2.15}$$

Remark 2.16.   If A is a commutative ring of rank n over R, and if we endow A with the degree n algebra structure via left multiplication as in Example 2.5, then it is immediate from the definition that the Galois closure $G(A/R)$ agrees with the S_n-closure introduced in [5].

Remark 2.17.   Unlike the case of commutative rings considered in [5], here $G(A/R)$ does not necessarily have a natural ring structure since $I_{A/R}$ is not necessarily a two-sided ideal. In fact, in many cases of interest (e.g., if A is the ring of $n \times n$ matrices $\mathrm{Mat}_n(R)$ for $n \geq 3$), if we were to replace $I_{A/R}$ by the two-sided ideal generated by the elements (2.13), the expression (2.15) would become 0.

Remark 2.18.   If (A, R', ι) is a degree n algebra and B is an R-algebra with a universally injective homomorphism $B \to A$, then (B, R', ι) inherits the structure of a degree n algebra. Then since $I_{B/R} \subset I_{A/R}$, there is a well-defined homomorphism $G(B/R) \to G(A/R)$ of left $B^{\otimes n}$-modules.

Remark 2.19.   Let (A, R', ι) be a degree n R-algebra and let R'' be a commutative R'-algebra. Let $\psi : \mathrm{Mat}_n(R') \to \mathrm{Mat}_n(R'')$ be the induced morphism. If $\psi\iota : A \to \mathrm{Mat}_n(R'')$ is universally injective, for example, if $R' \to R''$ is universally injective, then $(A, R'', \psi\iota)$ is

a degree n R-algebra. In this case, the characteristic polynomials $P_{A,a}$ for (A, R', ι) and $(A, R'', \psi \iota)$ are the same, so the associated Galois closures agree.

By definition, the module $G(A/R)$ has n distinct A-actions (one on each tensor factor). We denote the i-th action of $a \in A$ on an element $b \in G(A/R)$ as $a \cdot_i b$. Furthermore, the natural action of S_n on $A^{\otimes n}$ induces an S_n-action on $G(A/R)$ with the following property: for all $\sigma \in S_n$, $a \in A$, and $b \in G(A/B)$, we have $\sigma(a \cdot_i b) = a \cdot_{\sigma(i)} \sigma(b)$. This gives $G(A/R)$ the structure of a left module over the twisted group ring $A^{\otimes n} * S_n$ (or equivalently, an S_n-equivariant left $A^{\otimes n}$-module).

2.3   Key properties: base change and the product formula

The focus of this subsection is to prove two main properties of Galois closures: they commute with base change and they satisfy a product formula. Our 1st step is to show that the left ideal $I_{A/R}$ is generated by the expressions (2.13) for basis elements.

Proposition 2.20.   Let A be a degree n R-algebra. If $u_1, \ldots, u_m$ is a basis for A over R, then $I_{A/R}$ is the left $A^{\otimes n}$-ideal generated by the expressions

$$e_j\big(a^{(1)}, a^{(2)}, \ldots, a^{(n)}\big) - s_j(a)$$

for $a \in \{u_1, \ldots, u_m\}$.

Proof.   By definition, there is a finitely generated commutative R-algebra R' and a universally injective R-algebra morphism $\iota \colon A \to \mathrm{Mat}_n(R')$ such that $P_{A,a}(T) = \det(T - \iota(a)) \in R[T]$ for all $a \in A$. We then have

$$\det\big(1 - \iota(a)T\big) = \sum_{j=0}^{n} (-1)^j s_{A,j}(a) T^j. \tag{2.21}$$

As shown in [5, Lemma 11], for a noncommutative polynomial ring $\mathbb{Z}\langle X, Y \rangle$ over $\mathbb{Z}$ generated by X and Y, there is a unique sequence $\{f_d(X, Y)\}_{d=0}^{\infty}$ of homogeneous degree d polynomials in $\mathbb{Z}\langle X, Y \rangle$ such that

$$\big(1 - (X + Y)T\big) = (1 - XT)(1 - YT) \prod_{d=0}^{\infty} \big(1 - f_d(X, Y)XYT^{d+2}\big)$$

in $\mathbb{Z}\langle X, Y \rangle[[T]]$. In particular, for any $a, b \in A$, letting $x = \iota(a)$ and $y = \iota(b)$, we have

$$1 - (x + y)T = (1 - xT)(1 - yT) \prod_{d=0}^{k-2} \big(1 - f_d(x, y)xyT^{d+2}\big) \mod T^{k+1}. \tag{2.22}$$

Taking determinants of both sides of (2.22) and equating the coefficients of T^k, equation (2.21) yields an expression for $s_{A,k}(a + b)$ in terms of $s_{A,k}(a)$, $s_{A,k}(b)$, and $s_{A,i}(q_j(a,b))$ for $i < k$, where the q_j are noncommutative polynomials. In the case where A is the split degree n algebra R^n as in Example 2.6, the $s_{A,k}$ are the elementary symmetric functions e_k.

Combining the above with the observation that $s_{A,i}(ra) = r^i s_{A,i}(a)$ for all $r \in R$, we see by induction on k that $s_{A,k}(a)$ is expressible in terms of the $s_{A,j}(u_\ell)$ for $j \leq k$. Since the elementary symmetric functions e_k satisfy these same relations (since they correspond to the special case where $A = R^n$), we conclude that $I_{A/R}$ is generated by the expressions $e_j(a^{(1)}, a^{(2)}, \ldots, a^{(n)}) - s_j(a)$ for $a \in \{u_1, \ldots, u_m\}$.   ∎

Next, we show that if A is a degree n R-algebra, and $R \to S$ is a map of commutative rings, then $A \otimes_R S$ carries a natural degree n S-algebra structure.

Lemma 2.23.   Let R be a commutative ring and S a commutative R-algebra. If (A, R', ι) is a degree n R-algebra, then $(A \otimes_R S, R' \otimes_R S, \iota \otimes 1)$ is a degree n S-algebra.

Proof.   By definition, ι is universally injective, so $\iota \otimes 1 \colon A \otimes_R S \to \mathrm{Mat}_n(R' \otimes_R S)$ is as well. It remains to prove that if $b \in A \otimes_R S$, then the characteristic polynomial of $(\iota \otimes 1)(b)$ lives in $S[T]$. The proof of Proposition 2.20 yields an integral polynomial expression for the characteristic polynomial of $x + y$ in terms of the characteristic polynomials of x and y. Since b is a sum of pure tensors, we are therefore reduced to the case where b is a pure tensor itself, for example, $b = a \otimes c$ for $a \in A$ and $c \in S$. Then $(\iota \otimes 1)(b)$ is the product of $\iota(a) \otimes 1$ and the scalar $c \in S$. So $s_{A \otimes_R S, i}(b) = c^i s_{A,i}(a)$. Since (A, R', ι) is a degree n R-algebra, we have $s_{A,i}(a) \in R$, and hence $s_{A \otimes_R S, i}(b) \in S$, as desired.   ∎

Remark 2.24.   While proving Lemma 2.23, we showed that $s_{A \otimes_R S, i}(a \otimes c) = c^i s_{A,i}(a)$ for all $a \in A$ and $c \in S$.

The map $A \to A \otimes_R S$ induces a map $A^{\otimes n} \to (A \otimes_R S)^{\otimes n}$. This latter morphism sends $I_{A/R}$ into $I_{(A \otimes_R S)/S}$ by Remark 2.24, and hence induces a map $G(A/R) \otimes_R S \to G((A \otimes_R S)/S)$, which we refer to as the *base change map*. Note that $(A \otimes_R S)^{\otimes n} \simeq A^{\otimes n} \otimes_R S$ acts on both $G(A/R) \otimes_R S$ and $G((A \otimes_R S)/S)$.

Theorem 2.25. (Base change).   Let A be a degree n R-algebra and let S be a commutative R-algebra. The base change map yields an isomorphism

$$G(A/R) \otimes_R S \simeq G((A \otimes_R S)/S)$$

of left modules over $(A \otimes_R S)^{\otimes n} * S_n$.

Proof. Let $\epsilon_j(a) := e_j(a^{(1)}, a^{(2)}, \ldots, a^{(n)}) - s_j(a)$. If $u_1, \ldots, u_m$ is a basis for A over R, then the $u_\ell \otimes 1$ gives a basis for $A \otimes_R S$ over S. Proposition 2.20 implies that $I_{A/R}$ is generated by the expressions $\epsilon_j(u_\ell)$ and $I_{(A \otimes_R S)/S}$ is generated by the expressions $\epsilon_j(u_\ell \otimes 1) = \epsilon_j(u_\ell) \otimes 1$. Hence, $I_{(A \otimes_R S)/S}$ is the extension of the ideal $I_{A/R}$. Consequently, the base change map is an isomorphism $G(A/R) \otimes_R S \simeq G((A \otimes_R S)/S)$. $\blacksquare$

We next compute the Galois closure of a product in terms of the Galois closures of the factors.

Theorem 2.26 (Product formula). For $1 \leq j \leq k$, let A_j be a degree n_j R-algebra and endow $A = A_1 \times \cdots \times A_k$ with the associated structure of a degree $n = \sum_{i=1}^k n_i$ R-algebra. Then we have an isomorphism of left $(A^{\otimes n} * S_n)$-modules

$$G(A/R) \simeq \left(G(A_1/R) \otimes \cdots \otimes G(A_k/R) \right)^N, \tag{2.27}$$

where N is the multinomial coefficient $\binom{n}{n_1, \ldots, n_k}$. As a representation of S_n, the right-hand side of (2.27) is the induced representation from $S_{n_1} \times \cdots \times S_{n_k}$ acting on $G(A_1/R) \otimes \cdots \otimes G(A_k/R)$, and the $A^{\otimes n}$-action on the right-hand side of (2.27) is given by n_i actions of A on each $G(A_i/R)$.

Proof. Since $A = \prod_j A_j$, there exist idempotents ε_j in the center $Z(A)$ of A for $1 \leq j \leq k$, such that $A_j = \varepsilon_j A = A \varepsilon_j$ and $\varepsilon_i \varepsilon_j = \delta_{i,j} \varepsilon_j$, where δ is the Kronecker delta function. Let $[k] = \{1, 2, \cdots, k\}$ and for every n-tuple $\underline{i} = (i_1, \cdots, i_n) \in [k]^n$, let $A_{\underline{i}} := A_{i_1} \otimes A_{i_2} \otimes \cdots \otimes A_{i_n}$. Then

$$A^{\otimes n} = \prod_{\underline{i} \in [k]^n} A_{\underline{i}}.$$

This product decomposition corresponds to the idempotents $\varepsilon_{\underline{i}} \in Z(A^{\otimes n})$ defined by

$$\varepsilon_{\underline{i}} = \varepsilon_{i_1} \otimes \varepsilon_{i_2} \otimes \cdots \otimes \varepsilon_{i_n} = \varepsilon_{i_1}^{(1)} \varepsilon_{i_2}^{(2)} \cdots \varepsilon_{i_n}^{(n)}.$$

Notice that if $J \subseteq A^{\otimes n}$ is a left ideal, then $\varepsilon_{\underline{i}} J = J \varepsilon_{\underline{i}}$ is a left ideal, which can be identified with a left ideal $J_{\underline{i}}$ of $A_{\underline{i}}$. Moreover, $J = \prod_{\underline{i}} J_{\underline{i}}$. In particular,

$$I_{A^{\otimes n}/R} = \prod_{\underline{i} \in [k]^n} I_{\underline{i}}.$$

Our 1st goal is to show that $I_{\underline{i}} = A_{\underline{i}}$ unless $\#\{\ell \mid i_\ell = j\} = n_j$ for every j, that is, unless $A_{\underline{i}} \simeq A_{i_1}^{\otimes n_1} \otimes A_{i_2}^{\otimes n_2} \otimes \cdots A_{i_k}^{\otimes n_k}$. Let $\underline{i}$ be an n-tuple for which this does not hold;

then there is some j with $\#\{\ell \mid i_\ell = j\} < n_j$. By Lemma 2.12 (2), we know that $s_{A,n_j}(\varepsilon_j) = s_{A_j,n_j}(1) = 1$. So, the n_j-th elementary symmetric function in the $\varepsilon_j^{(\ell)}$ equals 1 in the module $G(A/R)$, that is,

$$1 - \sum_{1 \leq r_1 < r_2 < \cdots < r_{n_j} \leq n} \varepsilon_j^{(r_1)} \varepsilon_j^{(r_2)} \cdots \varepsilon_j^{(r_{n_j})} \in I_{A^{\otimes n}/R}.$$

Since j occurs fewer than n_j times in the n-tuple $\underline{i}$, we see $\varepsilon_{\underline{i}} \varepsilon_j^{(r_1)} \varepsilon_j^{(r_2)} \cdots \varepsilon_j^{(r_{n_j})} = 0$ for every summand above, and so $\varepsilon_{\underline{i}} \in \varepsilon_{\underline{i}} I_{A^{\otimes n}/R} = I_{\underline{i}}$, that is, we have $I_{\underline{i}} = A_{\underline{i}}$, as desired.

Next let $\underline{i} \in [k]^n$ such that $A_{\underline{i}} \simeq A_{i_1}^{\otimes n_1} \otimes A_{i_2}^{\otimes n_2} \otimes \cdots A_{i_k}^{\otimes n_k}$. We show in this case that $A_{\underline{i}}/I_{\underline{i}} \simeq G(A_1/R) \otimes G(A_2/R) \otimes \cdots G(A_k/R)$. To do so, it is enough to consider the specific case where $\underline{i} = (i_1, \cdots, i_n)$ is equal to $(\underbrace{1, 1, \cdots, 1}_{n_1}, \cdots, \underbrace{k, k, \cdots, k}_{n_k})$, since this is the case up to permutation. First note that A is generated by elements of the form $a_j \varepsilon_j$ where $a_j \in A_j$ and $1 \leq j \leq n$. So, by Theorem 2.25, we know that $I_{A^{\otimes n}/R}$ is generated as a left ideal by elements of the form

$$s_{A,m}(a_j \varepsilon_j) - \sum_{1 \leq r_1 < r_2 < \cdots < r_m \leq n} (a_j \varepsilon_j)^{(r_1)} (a_j \varepsilon_j)^{(r_2)} \cdots (a_j \varepsilon_j)^{(r_m)},$$

and so $I_{\underline{i}}$ is generated by the above elements after left multiplying by $\varepsilon_{\underline{i}}$. First notice that by Lemma 2.12 (2) we know $s_{A,m}(a_j \varepsilon_j) = s_{A_j,m}(a_j)$, which is 0 if $m > n_j$. Next note that $i_\ell = j$ if and only if $n_1 + n_2 + \cdots + n_{j-1} + 1 \leq \ell \leq n_1 + n_2 + \cdots + n_j$. So, multiplying the above expression by $\varepsilon_{\underline{i}}$ is 0 if $m > n_j$, and otherwise we obtain

$$s_{A_j,m}(a_j) - \sum_{n_1 + \cdots + n_{j-1} + 1 \leq r_1 < r_2 < \cdots < r_m \leq n_1 + \cdots + n_j} \varepsilon_{\underline{i}} a_j^{(r_1)} a_j^{(r_2)} \cdots a_j^{(r_m)}$$

that is nothing more than

$$s_{A_j,m}(a_j) - \underbrace{\varepsilon_1 \otimes \cdots \varepsilon_1}_{n_1} \otimes \cdots \otimes \sum_{1 \leq r_1 < r_2 < \cdots < r_m \leq n_j} a_j^{(r_1)} a_j^{(r_2)} \cdots a_j^{(r_m)} \otimes \cdots \otimes \underbrace{\varepsilon_k \otimes \cdots \varepsilon_k}_{n_k}.$$

This shows $I_{\underline{i}} = I_{A_1^{\otimes n_1}/R} \otimes \cdots \otimes I_{A_k^{\otimes n_k}/R}$ and therefore $A_{\underline{i}}/I_{\underline{i}} \simeq G(A_1/R) \otimes G(A_2/R) \otimes \cdots G(A_k/R)$ as desired. ∎

3   Examples of Galois Closures

In this section, we give many examples of Galois closures.

3.1   Trivial algebras

As in Example 2.7, for any $n \geq 1$, we may view the R-algebra $A = R$ as a degree n algebra with characteristic polynomial $P_{R,r}(T) = (T - r)^n$. It is easy to check that $I_{A/R} = 0$, so the Galois closure $G(A/R)$ is isomorphic to R itself. The S_n-action is trivial, and the n A-actions are all the same, namely the usual multiplication by elements of $A = R$. This seemingly trivial example plays a role in many of the examples in Section 4.4.

3.2   Quadratic algebras

Suppose A is a degree 2 R-algebra. Then every element $a \in A$ satisfies an equation of the form

$$a^2 - \mathrm{Tr}(a)a + \mathrm{N}(a) = 0, \tag{3.1}$$

where $\mathrm{Tr}(a)$ and $\mathrm{N}(a)$ are the trace and norm, respectively, of a. Let $\overline{a} := \mathrm{Tr}(a) - a$, which one should think of as the conjugate of a. It is easy to check that $a\overline{a} = \overline{a}a = \mathrm{N}(a)$ and $\overline{ab} = \overline{b}\overline{a}$.

The Galois closure $G(A/R)$ is the quotient of $A \otimes A$ by the left ideal $I_{A/R}$, generated by the elements

$$a \otimes 1 + 1 \otimes a - \mathrm{Tr}(a)(1 \otimes 1) \quad \text{and} \quad a \otimes a - \mathrm{N}(a)(1 \otimes 1)$$

for all $a \in A$. We will show that $G(A/R)$ is isomorphic to A in this case. We first give A the structure of a left $(A^{\otimes 2} * S_2)$-module as follows: given $b \in A$ and a pure tensor $a_1 \otimes a_2 \in A^{\otimes 2}$, let $(a_1 \otimes a_2) \cdot b := a_1 b \overline{a}_2$. If $\sigma \in S_2$ denotes the nontrivial element, then the S_2-action on A is given by $\sigma(b) := \overline{b}$.

Proposition 3.2.   If A is a degree 2 R-algebra, then the morphism $\varphi \colon A \otimes A \to A$ given by $\varphi(b \otimes c) = b\overline{c}$ induces an isomorphism

$$G(A/R) \simeq A$$

of left $(A^{\otimes 2} * S_2)$-modules.

Proof.   One easily checks that φ is well defined and a morphism of left $(A^{\otimes 2} * S_2)$-modules. It is clear that $\varphi(I_{A/R}) = 0$, so we obtain an induced map $\overline{\varphi} \colon G(A/R) \to A$. Note that $\varphi(a \otimes 1) = a$ for all $a \in A$, so $\overline{\varphi}$ is surjective.

Since $\overline{\varphi}$ is a morphism of left $(A^{\otimes 2} * S_2)$-modules, to complete the proof, it is enough to show $\overline{\varphi}$ is an isomorphism of R-modules. Consider the R-module morphism $\psi : A \to G(A/R)$ given by $\psi(a) = a^{(1)} = a \otimes 1$. It is injective since $\overline{\varphi}\psi(a) = a$. It is surjective because

$$b \otimes c = b^{(1)}c^{(2)} = b \cdot_1 c^{(2)} = b \cdot_1 (\mathrm{Tr}(c)(1 \otimes 1) - c^{(1)}) = \mathrm{Tr}(c)b^{(1)} - (bc)^{(1)}$$

for all $b, c \in A$, that is, $G(A/R)$ is generated as an R-module by the image of elements of the form $a^{(1)}$ for $a \in A$. ∎

Remark 3.3. Proposition 3.2 generalizes the fact that a separable degree 2 field extension L/K is already Galois and hence its Galois closure is L. Note that in the case of quadratic R-algebras, since $G(A/R) \simeq A$, the Galois closure inherits a ring structure.

3.3 Cubic algebras built from smaller-degree algebras

We give some examples of $G(A/R)$ where A has degree 3 but is the product of smaller degree algebras. These Galois closures may be easily computed using the product formula (Theorem 2.26), but in this section, we show how to work with them explicitly.

The simplest case of a decomposable degree 3 R-algebra is $A = R \times R \times R$. Each element $a = (r_1, r_2, r_3) \in A$ satisfies the polynomial

$$a^3 - ta^2 + sa - n1_A = 0, \tag{3.4}$$

where the *trace* $\mathrm{Tr}(a)$ is $s_{A,1}(a) = t = r_1 + r_2 + r_3$, the *spur* $\mathrm{Spr}(a)$ is $s_{A,2}(a) = s = r_1r_2 + r_1r_3 + r_2r_3$, the *norm* $\mathrm{N}(a)$ is $s_{A,3}(a) = n = r_1r_2r_3$, and 1_A denotes the multiplicative identity element $(1,1,1)$ in A.

We claim that $G(A/R)$ is isomorphic to $R^{\oplus 6}$ as left $(A^{\otimes 3} * S_3)$-modules, where the left $(A^{\otimes 3} * S_3)$-module structure on $R^{\oplus 6}$ is given as follows. We index each of the six copies of R in $R^{\oplus 6}$ by the six permutations of $\{1, 2, 3\}$. The three actions of $(r_1, r_2, r_3) \in A$ on $(c_{ijk})_{\{i,j,k\}=\{1,2,3\}} \in R^{\oplus 6}$ are as follows:

$$(r_1, r_2, r_3) \cdot_1 (c_{ijk})_{\{i,j,k\}=\{1,2,3\}} := (r_i c_{ijk})_{\{i,j,k\}=\{1,2,3\}}$$
$$(r_1, r_2, r_3) \cdot_2 (c_{ijk})_{\{i,j,k\}=\{1,2,3\}} := (r_j c_{ijk})_{\{i,j,k\}=\{1,2,3\}}$$
$$(r_1, r_2, r_3) \cdot_3 (c_{ijk})_{\{i,j,k\}=\{1,2,3\}} := (r_k c_{ijk})_{\{i,j,k\}=\{1,2,3\}}.$$

The action of $\sigma \in S_3$ on $R^{\oplus 6}$ is the standard action on the indices, that is, $\sigma((c_{ijk})_{ijk}) = (c_{\sigma(i),\sigma(j),\sigma(k)})_{ijk}$. Then we define the morphism $\varphi \colon A^{\otimes 3} \to R^{\oplus 6}$ of left $A^{\otimes 3}$-modules by linearly extending

$$\varphi\big((b_1, b_2, b_3) \otimes (c_1, c_2, c_3) \otimes (d_1, d_2, d_3)\big) = (b_i c_j d_k)_{\{i,j,k\}=\{1,2,3\}}.$$

It is easy to check that the image of $I_{A/R}$ is 0 in $R^{\oplus 6}$, so we obtain an induced map $\overline{\varphi} \colon G(A/R) \to R^{\oplus 6}$.

Proposition 3.5.   The map $\overline{\varphi}$ is an isomorphism of left $(A^{\otimes 3} * S_3)$-modules:

$$G(A/R) \simeq R^{\oplus 6}.$$

Proof.   This is a special case of Proposition 3.6 below, with $B = R \times R$.   ∎

We next consider the more general situation where B is a quadratic R-algebra and let $A = R \times B$. Recall from Section 3.2 that there is a trace form Tr_B and norm form N_B on B such that $b \in B$ satisfies the quadratic polynomial (3.1): $b^2 - \mathrm{Tr}_B(b)b + \mathrm{N}_B(b) = 0$. Then by the definition of the product polynomial $P_{R\times B,(r,b)}$, an element $a = (r, b) \in A$ satisfies the cubic polynomial (3.4), where $t = \mathrm{Tr}(a) = r + \mathrm{Tr}_B(b)$, $s = \mathrm{Spr}(a) = r\,\mathrm{Tr}_B(b) + \mathrm{N}_B(b)$, $n = \mathrm{N}(a) = r\,\mathrm{N}_B(b)$, and $1_A = (1, 1_B)$. Recall as well from Section 3.2 that for $b \in B$, we define $\overline{b} = \mathrm{Tr}_B(b) - b$.

We claim that the Galois closure $G(A/R)$ is isomorphic to $B^{\oplus 3}$ where we endow $B^{\oplus 3}$ with a left $(A^{\otimes 3} * S_3)$-module structure as follows. The three actions of $(r, c) \in A$ on $(b_1, b_2, b_3) \in B^{\oplus 3}$ are given by

$$(r, c) \cdot_1 (b_1, b_2, b_3) := (rb_1, cb_2, b_3\overline{c})$$

$$(r, c) \cdot_2 (b_1, b_2, b_3) := (b_1\overline{c}, rb_2, cb_3)$$

$$(r, c) \cdot_3 (b_1, b_2, b_3) := (cb_1, b_2\overline{c}, rb_3).$$

The S_3-action on $B^{\oplus 3}$ is given by

$$\sigma(b_1, b_2, b_3) := \begin{cases} (b_{\sigma^{-1}(1)}, b_{\sigma^{-1}(2)}, b_{\sigma^{-1}(3)}) & \text{if } \mathrm{sgn}(\sigma) = 1 \\ (\overline{b}_{\sigma^{-1}(1)}, \overline{b}_{\sigma^{-1}(2)}, \overline{b}_{\sigma^{-1}(3)}) & \text{if } \mathrm{sgn}(\sigma) = -1. \end{cases}$$

Then we may define a morphism $\varphi\colon A^{\otimes 3} \to B^{\oplus 3}$ of left $(A^{\otimes 3} * S_3)$-modules by linearly extending

$$\varphi\big((r_1, b_1) \otimes (r_2, b_2) \otimes (r_3, b_3)\big) = \big(r_1 b_3 \overline{b}_2, r_2 b_1 \overline{b}_3, r_3 b_2 \overline{b}_1\big).$$

An easy check shows that $\varphi(I_{A/R}) = 0$, so we obtain an induced map $\overline{\varphi}\colon G(A/R) \to B^{\oplus 3}$. We then have the following.

Proposition 3.6.   The map $\overline{\varphi}$ is an isomorphism of left $(A^{\otimes 3} * S_3)$-modules:

$$G(A/R) \simeq B^{\oplus 3}.$$

Proof.   We see that $\overline{\varphi}$ is surjective since φ is: for every $b \in B$, we have

$$\varphi\big((0, 1)^{(2)}(0, b)^{(3)}\big) = (b, 0, 0)$$

$$\varphi\big((0, \overline{b})^{(3)} - (0, 1)^{(2)}(0, \overline{b})^{(3)}\big) = (0, b, 0)$$

$$\varphi\big((0, b)^{(2)} - (0, 1)^{(2)}(0, \overline{b})^{(3)}\big) = (0, 0, b).$$

Since we know $\overline{\varphi}$ is a surjective map of left $(A^{\otimes 3} * S_3)$-modules, to prove it is an isomorphism, it is enough to show it is an isomorphism of R-modules. To do so, we need only find an R-module map $\psi\colon B^{\oplus 3} \to G(A/R)$ that is a surjective section of $\overline{\varphi}$. Then we can define ψ by $\psi(b, 0, 0) = (0, 1)^{(2)}(0, b)^{(3)}$, $\psi(0, b, 0) = (0, \overline{b})^{(3)} - (0, 1)^{(2)}(0, \overline{b})^{(3)}$, and $\psi(0, 0, b) = (0, b)^{(2)} - (0, 1)^{(2)}(0, \overline{b})^{(3)}$. It then suffices to show that $G(A/R)$ is generated as an R-module by elements of the form $(0, b)^{(2)}$, $(0, b)^{(3)}$, and $(0, 1)^{(2)}(0, b)^{(3)}$.

For any element $\alpha \in A$, the trace relation $\alpha^{(1)} + \alpha^{(2)} + \alpha^{(3)} - \mathrm{Tr}(\alpha) \in I_{A/R}$ trivially shows that any element $\alpha^{(1)} = \alpha \otimes 1 \otimes 1 \in A^{\otimes 3}$ may be written in $G(A/R)$ as an R-linear combination of 1_A, $\alpha^{(2)}$, and $\alpha^{(3)}$. In particular, any element of $G(A/R)$ may thus be written as a linear combination of elements of the form $\beta^{(2)} \gamma^{(3)}$ for $\beta, \gamma \in A$. Also, for $\beta = (r, b) \in R \times B = A$, we see that $\beta^{(i)} = r 1_A + (0, b - r)^{(i)}$, so the Galois closure $G(A/R)$ is generated as an R-module by 1_A and elements of the form $(0, b)^{(2)}$, $(0, b)^{(3)}$, and $(0, b)^{(2)}(0, b')^{(3)}$ for $b, b' \in B$.

We claim that for $b, b' \in B$, we can write $(0, b)^{(2)}(0, b')^{(3)}$ in the form $(0, 1)^{(2)}(0, b'')^{(3)}$ with $b'' \in B$; specifically, $b'' = b' \overline{b}$. First, expanding the equation $(b + 1)^2 - \mathrm{Tr}_B(b + 1)(b + 1) - \mathrm{N}_B(b + 1) = 0$ yields

$$\mathrm{N}_B(b + 1) - \mathrm{N}_B(b) - 1 = \mathrm{Tr}_B(b). \tag{3.7}$$

Next, the trace and spur relations tell us

$$
\begin{aligned}
(0,b)^{(2)}(0,b)^{(3)} &= \mathrm{N}_B(b) - (0,b)^{(1)}(0,b)^{(2)} - (0,b)^{(1)}(0,b)^{(3)} \\
&= \mathrm{N}_B(b) + (0,b) \cdot_1 \left((0,b)^{(1)} - \mathrm{Tr}_B(b)\right) \\
&= \mathrm{N}_B(b) + \left(0, b^2 - \mathrm{Tr}_B(b)b\right)^{(1)} \\
&= \mathrm{N}_B(b) - (0, \mathrm{N}_B(b))^{(1)} = \mathrm{N}_B(b)\left(1_A - (0,1)^{(1)}\right) \\
&= \mathrm{N}_B(b)(-1_A + (0,1)^{(2)} + (0,1)^{(3)}),
\end{aligned}
$$

where the last equality holds because $\mathrm{Tr}_A(0,1) = \mathrm{Tr}_B(1_B) = 2$. Applying this equation once to left-hand side and twice to the right-hand side of

$$
(0,b+1)^{(2)}(0,b+1)^{(3)} = (0,b)^{(2)}(0,b)^{(3)} + (0,b)^{(2)}(0,1)^{(3)} + (0,1)^{(2)}(0,b)^{(3)} + (0,1)^{(2)}(0,1)^{(3)}
$$

and making use of (3.7) implies

$$
(0,b)^{(2)}(0,1)^{(3)} + (0,1)^{(2)}(0,b)^{(3)} = -\mathrm{Tr}_B(b)\left(1_A + (0,1)^{(2)} + (0,1)^{(3)}\right) \tag{3.8}
$$

that simplifies to

$$
(0,b)^{(2)}(0,1)^{(3)} = -\mathrm{Tr}_B(b)\left(1 \otimes (1,0) \otimes (1,0)\right) + (0,1)^{(2)}(0,\overline{b})^{(3)}.
$$

Acting on the left by $(0,b')^{(3)}$ shows that $(0,b)^{(2)}(0,b')^{(3)} = (0,1)^{(2)}(0,b'\overline{b})^{(3)}$, that is, we have shown that $(0,b)^{(2)}(0,b')^{(3)}$ is of the form $(0,1)^{(2)}(0,b'')^{(3)}$.

So far, we have shown that $G(A/R)$ is generated as an R-module by 1_A and elements of the form $(0,b)^{(2)}$, $(0,b)^{(3)}$, and $(0,1)^{(2)}(0,b')^{(3)}$. It remains to remove 1_A from our generating set. We have shown above that $(0,b)^{(2)}(0,b)^{(3)} = \mathrm{N}_B(b)(-1_A + (0,1)^{(2)} + (0,1)^{(3)})$. Substituting in $b = 1$ shows that $(0,1)^{(2)}(0,1)^{(3)} = -1_A + (0,1)^{(2)} + (0,1)^{(3)}$. Therefore, 1_A is also a linear combination of elements of the form $(0,b)^{(2)}$, $(0,b)^{(3)}$, and $(0,1)^{(2)}(0,b)^{(3)}$. This concludes the proof. ∎

Remark 3.9.   As a consequence of Proposition 3.6, we see that $G(A/R)$ inherits a ring structure when $A = R \times B$ with B a degree 2 R-algebra. This is not true more generally for indecomposable degree 3 R-algebras, for example, for the case $A = \mathrm{Mat}_3(R)$ considered in Section 3.4.

3.4   Endomorphism rings (or matrix algebras)

Let V be a free rank n module over R and let $A = \mathrm{End}(V)$ be the ring of R-module endomorphisms. Then as in Example 2.8, we may view A as a degree n R-algebra where for each $\alpha \in A$, the polynomial $P_{A,\alpha}(T)$ is the characteristic polynomial of α viewed as an endomorphism of V; the trace and the norm of an endomorphism coincide with their usual definitions.

Via the canonical isomorphism $A \simeq V \otimes V^*$, we have an isomorphism $A^{\otimes n} \simeq V^{\otimes n} \otimes (V^*)^{\otimes n}$. The natural left $(A^{\otimes n} * S_n)$-module structure on $A^{\otimes n}$ then induces such a structure on $V^{\otimes n} \otimes (V^*)^{\otimes n}$. Explicitly, $\sigma \in S_n$ acts on the pure tensors via

$$\sigma \left(v_1 \otimes \cdots \otimes v_n \otimes f_1 \otimes \cdots \otimes f_n \right) := v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(n)} \otimes f_{\sigma^{-1}(1)} \otimes \cdots \otimes f_{\sigma^{-1}(n)},$$

where $v_j \in V$ and $f_j \in V^*$. The i-th action of $\alpha \in A$ is given by acting on the i-th factor of V:

$$\alpha \cdot_i \left(v_1 \otimes \cdots \otimes v_n \otimes f_1 \otimes \cdots \otimes f_n \right) := v_1 \otimes \cdots \otimes \alpha(v_i) \otimes \cdots \otimes v_n \otimes f_1 \otimes \cdots \otimes f_n.$$

We next define a left $(A^{\otimes n} * S_n)$-module structure on $V^{\otimes n} \otimes \bigwedge^n(V^*)$ as follows. For $\sigma \in S_n$, let

$$\sigma \left(v_1 \otimes \cdots \otimes v_n \otimes (f_1 \wedge \cdots \wedge f_n) \right) := v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(n)} \otimes \left(f_{\sigma^{-1}(1)} \wedge \cdots \wedge f_{\sigma^{-1}(n)} \right);$$

in other words, for a form $\omega \in \bigwedge^n(V^*)$, we have

$$\sigma(v_1 \otimes \cdots \otimes v_n \otimes \omega) := \mathrm{sgn}(\sigma) v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(n)} \otimes \omega.$$

For $\alpha \in A$, the i-th A-action is given by

$$\alpha \cdot_i (v_1 \otimes \cdots \otimes v_n \otimes \omega) := v_1 \otimes \cdots \otimes \alpha(v_i) \otimes \cdots \otimes v_n \otimes \omega.$$

Let $\pi \colon (V^*)^{\otimes n} \to \bigwedge^n(V^*)$ be the natural map $\pi(f_1 \otimes \cdots \otimes f_n) = f_1 \wedge \cdots \wedge f_n$. We then obtain a map of left $(A^{\otimes n} * S_n)$-left modules given by.

$$\varphi \colon A^{\otimes n} = V^{\otimes n} \otimes (V^*)^{\otimes n} \xrightarrow{\mathrm{id} \otimes \pi} V^{\otimes n} \otimes \bigwedge^n (V^*). \tag{3.10}$$

Explicitly, if $u_1, \ldots, u_n$ is a basis of V, then for $\alpha_1, \ldots, \alpha_n \in A = \mathrm{End}(V)$, we compute

$$\varphi(\alpha_1 \otimes \cdots \otimes \alpha_n) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma)\alpha_1(u_{\sigma(1)}) \otimes \cdots \otimes \alpha_n(u_{\sigma(n)}) \otimes (u_1^* \wedge \cdots \wedge u_n^*). \tag{3.11}$$

We show that φ induces an isomorphism between $G(A/R)$ and $V^{\otimes n} \otimes \bigwedge^n(V^*)$. First, we show that we may find a fairly simple basis for A.

Lemma 3.12.   Let V be a free rank n R-module. Then the endomorphism ring $\mathrm{End}(V)$ has a basis $\beta_1, \ldots, \beta_{n^2}$ over R where each β_i is a linear operator that is diagonalizable over R.

Proof.   After choosing an R-basis for V, we have an isomorphism $\mathrm{End}(V) \simeq \mathrm{Mat}_n(R)$. Let e_{ij} denote the matrix whose entries are all 0 except for a 1 in the (i,j)-th position. Then for $i \neq j$, the matrix $e_{ij} + e_{ii}$ is diagonalizable: if $P = e_{ii} + e_{ij} - e_{jj} + \sum_{k \neq i,j} e_{kk}$, then $P^{-1} = P$ and $P^{-1}(e_{ij}+e_{ii})P = e_{ii}$. So, we can choose our desired basis to be the n elements $e_{11}, \ldots, e_{nn}$ as well as the $n^2 - n$ elements $e_{ij} + e_{ii}$ and $e_{ji} + e_{jj}$ with $i < j$. ∎

Theorem 3.13.   Let V be a free rank n R-module and $A = \mathrm{End}(V)$. The map φ of (3.10) induces an isomorphism

$$G(A/R) \simeq V^{\otimes n} \otimes \bigwedge^n(V^*)$$

of left $(A^{\otimes n} * S_n)$-modules.

Proof.   We begin by showing that $\varphi(I_{A/R}) = 0$. That is, we show that for all $\alpha \in A$,

$$\varphi\left(\sum_{i_1 < \cdots < i_r} \alpha^{(i_1)} \cdots \alpha^{(i_r)}\right) = \varphi(s_{A,r}(\alpha)).$$

By Proposition 2.20, it suffices to prove this as α ranges over a basis of A over R. Combining this with Lemma 3.12, we may assume that α is diagonalizable over R. Choose a basis $u_1, \ldots, u_n$ of V such that $\alpha(u_i) = \lambda_i u_i$ for $\lambda_i \in R$. Let $\omega = u_1^* \wedge \cdots \wedge u_n^*$. From (3.11), we see

$$\varphi(\alpha^{(i_1)} \cdots \alpha^{(i_r)}) = \sum_{\sigma \in S_n} \lambda_{\sigma(i_1)} \cdots \lambda_{\sigma(i_r)} \mathrm{sgn}(\sigma) u_{\sigma(1)} \otimes \cdots \otimes u_{\sigma(n)} \otimes \omega.$$

Since

$$s_{A,r}(\alpha) = \sum_{i_1 < \cdots < i_r} \lambda_{i_1} \cdots \lambda_{i_r},$$

we obtain

$$\varphi\left(\sum_{i_1 < \cdots < i_r} \alpha^{(i_1)} \cdots \alpha^{(i_r)}\right) = \sum_{\sigma \in S_n} \sum_{i_1 < \cdots < i_r} \lambda_{\sigma(i_1)} \cdots \lambda_{\sigma(i_r)} \, \mathrm{sgn}(\sigma) u_{\sigma(1)} \otimes \cdots \otimes u_{\sigma(n)} \otimes \omega$$

$$= \sum_{\sigma \in S_n} \sum_{i_1 < \cdots < i_r} \lambda_{i_1} \cdots \lambda_{i_r} \, \mathrm{sgn}(\sigma) u_{\sigma(1)} \otimes \cdots \otimes u_{\sigma(n)} \otimes \omega$$

$$= s_{A,r}(\alpha) \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) u_{\sigma(1)} \otimes \cdots \otimes u_{\sigma(n)} \otimes \omega = \varphi\big(s_{A,r}(\alpha)\big),$$

where the last equality again follows from (3.11).

Having now shown that $\varphi(I_{A/R}) = 0$, we obtain an induced map $\overline{\varphi}\colon G(A/R) \to V^{\otimes n} \otimes \bigwedge^n(V^*)$. Since π is surjective, $\overline{\varphi}$ is as well. Since $\overline{\varphi}$ is a map of $(A^{\otimes n} * S_n)$-modules, to prove it is an isomorphism, it is enough to show it is an isomorphism of R-modules. To do so, we construct a surjective R-module map that is a section of $\overline{\varphi}$.

After choosing a basis of V, we may identify A with $\mathrm{Mat}_n(R)$ and use the notation e_{ij} to indicate a matrix that is 0 in all entries except 1 in the (i,j)-th position. It is clear that $G(A/R)$ is generated by (the image of) the elements $(e_{i_1 j_1})^{(1)} \cdots (e_{i_n j_n})^{(n)}$ for $1 \leq i_k, j_k \leq n$. We claim that for every function $\tau\colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, we have the following equality in $G(A/R)$:

$$\left(e_{i_1 \tau(1)}\right)^{(1)} \cdots \left(e_{i_n \tau(n)}\right)^{(n)} = \begin{cases} \mathrm{sgn}(\tau)\, (e_{i_1 1})^{(1)} \cdots (e_{i_n n})^{(n)} & \text{for } \tau \in S_n \\ 0, & \text{for } \tau \notin S_n. \end{cases} \tag{3.14}$$

Let $N_\tau = \sum_j e_{j\tau(j)}$. Then because $e_{i_k k} N_\tau = e_{i_k \tau(k)}$ and $(N_\tau)^{(1)} \cdots (N_\tau)^{(n)} = \det(N_\tau)$ in $G(A/R)$, we have

$$\left(e_{i_1 \tau(1)}\right)^{(1)} \cdots \left(e_{i_n \tau(n)}\right)^{(n)} = e_{i_1 1} \cdot_1 \cdots e_{i_n n} \cdot_n (N_\tau)^{(1)} \cdots (N_\tau)^{(n)} = \det(N_\tau)(e_{i_1 1})^{(1)} \cdots (e_{i_n n})^{(n)}.$$

Since $\det(N_\tau)$ vanishes for $\tau \notin S_n$ and is equal to $\mathrm{sgn}(\tau)$ for $\tau \in S_n$, we have (3.14). Thus, $G(A/R)$ is generated by the elements $(e_{i_1 1})^{(1)} \cdots (e_{i_n n})^{(n)}$ for $1 \leq i_k \leq n$.

Next, notice that $V^{\otimes n} \otimes \bigwedge^n(V^*)$ is a free R-module of rank n^n with basis $u_{i_1} \otimes \cdots \otimes u_{i_n} \otimes \omega$, where $1 \le i_j \le n$ and $\omega = u_1 \wedge \cdots \wedge u_n$. We can therefore define an R-module map $\psi \colon V^{\otimes n} \otimes \bigwedge^n(V^*) \to G(A/R)$ by

$$\psi\left(u_{i_1} \otimes \cdots \otimes u_{i_n} \otimes \omega\right) = \left(e_{i_1 1}\right)^{(1)} \cdots \left(e_{i_n n}\right)^{(n)}.$$

By (3.11), we see

$$\overline{\varphi}\left((e_{i_1 1})^{(1)} \cdots (e_{i_n n})^{(n)}\right) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) e_{i_1 1}\left(u_{\sigma(1)}\right) \otimes \cdots \otimes e_{i_n n}\left(u_{\sigma(n)}\right) \otimes \omega = u_{i_1} \otimes \cdots \otimes u_{i_n} \otimes \omega$$

and so ψ is a section of $\overline{\varphi}$. Since $(e_{i_1 1})^{(1)} \cdots (e_{i_n n})^{(n)}$ generate $G(A/R)$ as an R-module, it follows that ψ is surjective, hence an isomorphism of R-modules. Therefore, $\overline{\varphi}$ is an isomorphism as well. ∎

3.5   Central simple algebras

We recall some basic facts about central simple algebras. For a field F, let F^{sep} denote its separable closure. If $\mathcal{A}$ is a central simple algebra of dimension n^2 over F, then there exists an F^{sep}-vector space V of dimension n and an F^{sep}-algebra isomorphism $\mathcal{A}_{F^{\mathrm{sep}}} := \mathcal{A} \otimes_F F^{\mathrm{sep}} \simeq \mathrm{End}(V)$. Since the Galois group G of F^{sep}/F acts continuously on $\mathcal{A}_{F^{\mathrm{sep}}}$, we obtain an induced action on $\mathrm{End}(V)$. In particular, Galois descent implies that giving a central simple algebra of dimension n^2 over F is equivalent to giving a continuous G-action on $\mathrm{End}(V)$ over F^{sep}.

In what follows, we endow $\mathcal{A}$ with the degree n F-algebra structure from Example 2.9, namely choose a finite Galois extension K/F, a K-algebra isomorphism $\iota' \colon \mathcal{A} \otimes_F K \xrightarrow{\simeq} \mathrm{Mat}_n(K)$, and let ι be the embedding map $\mathcal{A} \to \mathrm{Mat}_n(K)$. Lemma 2.23 tells us that $\mathcal{A} \otimes_F K$ inherits a degree n K-algebra structure. As we will see momentarily, this is *not* the degree n K-algebra structure on $\mathrm{Mat}_n(K)$ defined in Example 2.8; nonetheless, $\mathcal{A} \otimes_F K$ and $\mathrm{Mat}_n(K)$ do have isomorphic Galois closures, as we will see in the course of proving the following result.

Lemma 3.15.   We have

$$G(\mathcal{A}/F) \otimes_F F^{\mathrm{sep}} \simeq G(\mathcal{A}_{F^{\mathrm{sep}}}/F^{\mathrm{sep}}) \simeq V^{\otimes n} \otimes \bigwedge^n V^*.$$

Proof.   Throughout the proof, we endow $\mathcal{A} \otimes_F K$ with its degree n K-algebra structure coming from Lemma 2.23. By the base change Theorem 2.25, it is enough to show that if we endow $\mathrm{Mat}_n(K)$ with the degree n K-algebra structure coming from Example 2.8, then $\iota' \colon \mathcal{A} \otimes_F K \to \mathrm{Mat}_n(K)$ induces an isomorphism of Galois closures.

Recall that the degree n K-algebra structure on $\mathcal{A} \otimes_F K$ is induced from the map $\iota \otimes 1 \colon \mathcal{A} \otimes_F K \to \mathrm{Mat}_n(K) \otimes_F K \simeq \mathrm{Mat}_n(K \otimes_F K)$. Let $\eta \colon \mathrm{Mat}_n(K \otimes_F K) \to \mathrm{Mat}_n(K)$ be the map induced from the K-algebra morphism $K \otimes_F K \to K$ sending $\alpha \otimes \beta$ to $\alpha\beta$. We claim that $\eta \circ (\iota \otimes 1) = \iota'$. Indeed, let $a \in \mathcal{A}$, $\alpha \in K$, and $\iota'(a) = (Q_{ij}) \in \mathrm{Mat}_n(K)$. Since ι' is a K-algebra map, we have $\iota'(a \otimes \alpha) = (Q_{ij}\alpha)$. On the other hand, $(\iota \otimes 1)(a \otimes \alpha) = (Q_{ij}) \otimes \alpha \in \mathrm{Mat}_n(K) \otimes_F K$ that is identified with the matrix $(Q_{ij} \otimes \alpha) \in \mathrm{Mat}_n(K \otimes_F K)$. This maps under η to $(Q_{ij}\alpha) = \iota'(a \otimes \alpha)$, which proves our claim. It then follows immediately from Remark 2.19 that ι' induces an isomorphism of Galois closures. ∎

In light of Lemma 3.15, by Galois descent, $G(\mathcal{A}/F)$ determines and is determined by a continuous G-action on $V^{\otimes n} \otimes \bigwedge^n(V^*)$. The following result shows how to obtain this G-action in terms of the one on $\mathrm{End}(V)$, that is, how to determine $G(\mathcal{A}/F)$ in terms of $\mathcal{A}$.

Proposition 3.16.   With notation as above, let $\varphi \colon G \to \mathrm{Aut}(\mathrm{End}(V))$ be the continuous Galois action corresponding to the central simple algebra $\mathcal{A}$, and let $\pi \colon V^{\otimes n} \otimes (V^*)^{\otimes n} \to V^{\otimes n} \otimes \bigwedge^n(V^*)$ be the natural projection. Then for every $\sigma \in G$, the automorphism $\varphi(\sigma)^{\otimes n}$ of $\mathrm{End}(V)^{\otimes n} \simeq V^{\otimes n} \otimes (V^*)^{\otimes n}$ preserves $\ker \pi$, thereby inducing an automorphism $\psi(\sigma)$ of $V^{\otimes n} \otimes \bigwedge^n(V^*)$. The resulting map $\psi \colon G \to \mathrm{Aut}(V^{\otimes n} \otimes \bigwedge^n(V^*))$ gives the Galois action corresponding to $G(\mathcal{A}/F)$.

Proof.   By Theorem 2.25, we know that tensoring the surjection $\mathcal{A} \to G(\mathcal{A}/F)$ with F^{sep} yields the surjection $\mathcal{A}_{F^{\mathrm{sep}}}^{\otimes n} \to G(\mathcal{A}_{F^{\mathrm{sep}}}/F^{\mathrm{sep}})$. As a result, the continuous G-action on $G(\mathcal{A}_{F^{\mathrm{sep}}}/F^{\mathrm{sep}})$ is induced from that on $\mathcal{A}_{F^{\mathrm{sep}}}^{\otimes n}$. The G-action on $\mathcal{A}_{F^{\mathrm{sep}}}^{\otimes n}$ is nothing more than the one obtained from $\mathcal{A}_{F^{\mathrm{sep}}}$ by tensoring n times, that is, $\sigma \in G$ acts on $\mathcal{A}_{F^{\mathrm{sep}}}^{\otimes n}$ by $\varphi(\sigma)^{\otimes n}$. Finally, as noted above, the G-action on $G(\mathcal{A}_{F^{\mathrm{sep}}}/F^{\mathrm{sep}})$ is induced from that on $\mathcal{A}_{F^{\mathrm{sep}}}^{\otimes n}$. Hence, each $\varphi(\sigma)^{\otimes n}$ preserves $I_{\mathcal{A}_{F^{\mathrm{sep}}}/F^{\mathrm{sep}}} = \ker \pi$ and the resulting action on $G(\mathcal{A}_{F^{\mathrm{sep}}}/F^{\mathrm{sep}})$ is given by $\psi(\sigma)$. ∎

Let us next consider a large class of explicit examples that includes all central simple algebras over number fields (see, e.g., [10, Chapter 15] for further details). Let K/F be a Galois extension having a cyclic Galois group of order n with generator σ. For

$\gamma \in F^*$, one may define an associative F-algebra

$$\mathcal{A}(K/F, \sigma, \gamma) := (K \oplus uK \oplus \cdots u^{n-1}K)/(u^n = \gamma; \alpha u = u\sigma(\alpha) \, \forall \, \alpha \in K). \qquad (3.17)$$

The Albert–Brauer–Hasse–Noether theorem combined with the Grunwald–Wang theorem implies that if F is a number field, then every central simple algebra over F is a cyclic algebra, that is, of the form (3.17). If $\gamma \in N_{K/F}(K^*)$, then $\mathcal{A}(K/F, \sigma, \gamma)$ is isomorphic to $\mathrm{Mat}_n(F)$. If $\gamma \in F^*$ modulo $N_{K/F}(K^*)$ has order exactly n (i.e., $\gamma^n \in N_{K/F}(K^*)$ and $\gamma^d \notin N_{K/F}(K^*)$ for all d dividing n), then $\mathcal{A}(K/F, \sigma, \gamma)$ is a division algebra.

Now fix a central simple algebra $\mathcal{A}$ over F of the form (3.17). Since K splits $\mathcal{A}$, we have an injection of $\mathcal{A}$ into $\mathcal{A} \otimes_F K \simeq \mathrm{Mat}_n(K)$; explicitly $\mathcal{A}$ may be identified with the subring of $\mathrm{Mat}_n(K)$ consisting of elements of the form

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & \cdots & \gamma\sigma^{n-1}(x_3) \\ \vdots & \vdots & \vdots & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}.$$

Since $\mathcal{A}_K \simeq \mathrm{Mat}_n(K)$, the central simple algebra $\mathcal{A}$ corresponds to a Galois action on $\mathrm{Mat}_n(K)$, which we now describe explicitly. Fix an n-dimensional K-vector space V and basis $u_1, \ldots, u_n$ of V to identify $\mathrm{End}(V) = \mathrm{Mat}_n(K)$. Recall the notation that e_{ij} (or $e_{i,j}$) refers to the $n \times n$ matrix whose only nonzero entry is a 1 in the (i,j)-th position. For all $\alpha \in K$, the action of $\mathrm{Gal}(K/F) = \langle \sigma \rangle$ is given by

$$\sigma(\alpha e_{ij}) := \begin{cases} \sigma(\alpha)e_{i+1,j+1}, & i,j < n \\ \sigma(\alpha)e_{11}, & i = j = n \\ \sigma(\alpha)\gamma e_{1,j+1}, & i = n, j < n \\ \sigma(\alpha)\gamma^{-1}e_{i+1,1}, & i < n, j = n. \end{cases}$$

In other words, σ acts as usual on K, and it adds 1 to both of the i and j indices, multiplying by γ or γ^{-1} whenever the i or j index, respectively, overflows. Written in

matrix form, we have

$$\sigma: (\alpha_{ij})_{i,j} \longmapsto \begin{pmatrix} \sigma(\alpha_{nn}) & \gamma\sigma(\alpha_{n1}) & \gamma\sigma(\alpha_{n2}) & \cdots & \gamma\sigma(\alpha_{n,n-1}) \\ \gamma^{-1}\sigma(\alpha_{1n}) & \sigma(\alpha_{11}) & \sigma(\alpha_{21}) & \cdots & \sigma(\alpha_{2,n-1}) \\ \gamma^{-1}\sigma(\alpha_{2n}) & \sigma(\alpha_{21}) & \sigma(\alpha_{22}) & \cdots & \sigma(\alpha_{3,n-1}) \\ \vdots & \vdots & \vdots & & \vdots \\ \gamma^{-1}\sigma(\alpha_{n-1,n}) & \sigma(\alpha_{n-1,1}) & \sigma(\alpha_{n-1,2}) & \cdots & \sigma(\alpha_{n-1,n-1}) \end{pmatrix}.$$

The induced action on $V^{\otimes n} \otimes \bigwedge^n V^* = G(\mathcal{A}_K/K)$ given by Proposition 3.16 is as follows: let $u_{n+1} := u_1$ and $\omega = u_1^* \wedge \cdots \wedge u_n^*$. Then for $1 \le i_j \le n$, we have

$$\sigma: \alpha u_{i_1} \otimes \cdots \otimes u_{i_n} \otimes \omega \longmapsto \sigma(\alpha)\gamma^{r-1}(-1)^{n-1} u_{i_1+1} \otimes \cdots \otimes u_{i_n+1} \otimes \omega,$$

where r is the number of j such that $i_j = n$.

Example 3.18. Let $F/\mathbb{Q}$ be a field that does not contain a square root of -1 and let $K = F(i)$. Then $\sigma(i) = -i$ and let $\overline{\alpha} := \sigma(\alpha)$. If $\gamma \in F^*$ is not of the form $a^2 + b^2$ for $a, b \in F$, then $\mathcal{A}(K/F, \sigma, \gamma)$ is a division algebra, whose elements are explicitly represented by matrices of the form

$$\begin{pmatrix} x_0 & \gamma\overline{x}_1 \\ x_1 & \overline{x}_0 \end{pmatrix}$$

with $x_i \in K$. For example, when $F = \mathbb{R}$ and $\gamma = -1$, this gives the usual matrix representation of the Hamiltonian quaternions $\mathbb{H}$.

By Proposition 3.16, the action of $\mathrm{Gal}(K/F) = \langle\sigma\rangle$ on $\mathrm{Mat}_2(K)$ corresponding to $G(\mathcal{A}/F)$ is given by

$$\sigma\big((\alpha_{11}u_1 \otimes u_1 + \alpha_{12}u_1 \otimes u_2 + \alpha_{21}u_2 \otimes u_1 + \alpha_{22}u_2 \otimes u_2) \otimes \omega\big)$$
$$= -\big(\gamma^{-1}\overline{\alpha}_{11}u_2 \otimes u_2 + \overline{\alpha}_{12}u_2 \otimes u_1 + \overline{\alpha}_{21}u_1 \otimes u_2 + \gamma\overline{\alpha}_{22}u_1 \otimes u_1\big) \otimes \omega.$$

Since $G(\mathcal{A}/F)$ is the subspace of elements that are fixed by σ, it is explicitly given by the set of

$$\big(\alpha u_1 \otimes u_1 - \gamma\overline{\alpha}u_2 \otimes u_2 + \beta u_1 \otimes u_2 - \overline{\beta}u_2 \otimes u_1\big) \otimes \omega$$

with $\alpha, \beta \in K$. On the other hand, $\mathcal{A}$ is a quadratic algebra over F, so we know from Proposition 3.2 that $G(\mathcal{A}/F) \simeq \mathcal{A}$, where the left $(\mathcal{A}^{\otimes 2} * S_2)$-module structure on $\mathcal{A}$ is

described in Section 3.2. The map

$$\begin{pmatrix} \beta & \gamma\overline{\alpha} \\ \alpha & \overline{\beta} \end{pmatrix} \longmapsto \left(\alpha u_1 \otimes u_1 - \gamma\overline{\alpha} u_2 \otimes u_2 + \beta u_1 \otimes u_2 - \overline{\beta} u_2 \otimes u_1 \right) \otimes \omega$$

yields an explicit isomorphism between our two different descriptions of $G(\mathcal{A}/F)$ as a left $(\mathcal{A}^{\otimes 2} * S_2)$-module.

3.6 Group rings

An easy application of the product formula (Theorem 2.26) and our work in Sections 3.4 and 3.5 allows us to compute Galois closures of group rings. For a finite group G and a field F with characteristic prime to $|G|$, Maschke's theorem implies that the group ring $F[G]$ is semisimple, that is, has the structure of a product of central simple algebras (and thus is a degree n algebra for some integer n). One thus can compute the Galois closure of such a group ring. If all G-representations are split, the computation is easier.

Proposition 3.19.   Let G be a finite group and F a field whose characteristic is prime to $|G|$. If all G-representations are split over F, then

$$G\big(F[G]/F\big) \simeq \left(\bigotimes_{\rho} \left(V_\rho^{\otimes n_\rho} \otimes \bigwedge^{n_\rho} V_\rho^* \right) \right)^N,$$

where the tensor product varies over the irreducible representations $\rho \colon G \to V_\rho$, $n_\rho := \dim V_\rho$, and N is the multinomial coefficient $N := |G|! / \prod_\rho n_\rho!$.

Proof.   By Maschke's theorem and Artin–Wedderburn (see, e.g., [16, Chapter 6]), one has $F[G] \simeq \prod_\rho \mathrm{End}(V_\rho)$. The result then follows from Theorem 2.26 and the computation of $G(\mathrm{End}(V_\rho)/F)$ in Theorem 3.13.   ∎

4   Hermitian Representations from Galois Closures

As indicated in the introduction, one of our motivations for studying noncommutative Galois closures is related to constructing "Hermitian" representations. We describe in Section 4.1 one way to construct such representations and how Galois closures are needed.

4.1   Definitions

We would like to study representations of algebraic groups that generalize tensor products of standard representations.

A simple explicit example is the space W of $m \times m$ matrices that are *Hermitian* with respect to a quadratic algebra A over R. Using the notation for quadratic algebras from Section 3.2, these are $m \times m$ matrices $C = (c_{ij})$ such that $\overline{C} = C^t$, where $\overline{C}$ denotes the entrywise conjugate of C, that is, $c_{ij} = \overline{c_{ji}}$ for all $1 \le i, j \le m$. If A is a rank ρ free module over R, then W is a free module over R of rank $m + \rho m(m-1)/2$. Moreover, the group $\mathrm{GL}_m(A)$ naturally acts on W: for $\gamma \in \mathrm{GL}_m(A)$, we define the action of γ by $\gamma \cdot C = \gamma C \overline{\gamma}$, where $\overline{\gamma}$ is the entrywise conjugate of γ. For example, if A is simply R itself considered as a degree 2 algebra with polynomial $P_r(T) = (T - r)^2$, then we have recovered the space of symmetric $m \times m$ matrices over R with the standard action of $\mathrm{GL}_m(R)$; for $A = R^2$ as a quadratic algebra, this space is isomorphic to the space of $m \times m$ matrices over R with the standard action of $\mathrm{GL}_m(R) \times \mathrm{GL}_m(R)$. It is of course possible to define W in a basis-free manner, as we will see in more generality below.

We wish to generalize the above to a notion of a Hermitian n-dimensional $m \times \cdots \times m$ array with entries in a degree n algebra A over R. Intuitively, we would like the symmetric group S_n to act on such an array in two different ways: by an S_n-action on A and by permuting the factors, and we would like to restrict to the arrays for which these two actions agree. In general, an algebra A does not come equipped with a natural S_n-action, but its Galois closure $G(A/R)$ does. So instead we allow for entries in $G(A/R)$. We now make this definition precise.

We begin with a coordinate-free description of the representation and then give an explicit description in terms of coordinates. Let U be a free R-module of rank m. There are two natural S_n-actions on $G(A/R) \otimes_R U^{\otimes n}$, one is the left action on $G(A/R)$ and the other is a right action on $U^{\otimes n}$ given by permuting coordinates. For $\sigma \in S_n$ and $\aleph \in G(A/R) \otimes_R U^{\otimes n}$, we denote the two actions by $\sigma \cdot_1 \aleph$ and $\sigma \cdot_2 \aleph$, respectively.

Definition 4.1.   We define the *Hermitian space* $\mathcal{H}_{A,U}$ to be the subspace of $G(A/R) \otimes_R U^{\otimes n}$ where the two S_n-actions agree (up to an inverse), that is,

$$\left\{ \aleph \in G(A/R) \otimes_R U^{\otimes n} : \sigma \cdot_1 \aleph = \sigma^{-1} \cdot_2 \aleph \text{ for all } \sigma \in S_n \right\}.$$

Remark 4.2.   We have two commuting (left) S_n-actions on $G(A/R) \otimes U^{\otimes n}$, hence an action of $S_n \times S_n$. The Hermitianization $\mathcal{H}_{A,U}$ is the space of invariants for the diagonally embedded copy of S_n in $S_n \times S_n$, that is, $\mathcal{H}_{A,U} = (G(A/R) \otimes U^{\otimes n})^{S_n}$.

We have a natural action of $A \otimes_R \text{End}(U)$ on $G(A/R) \otimes_R U^{\otimes n}$, where A acts on $G(A/R)$ via the diagonal embedding of A in $A^{\otimes n}$ and $\text{End}(U)$ acts on each factor of $U^{\otimes n}$ in the standard way.

Lemma 4.3. The action of $A \otimes_R \text{End}(U)$ on $G(A/R) \otimes_R U^{\otimes n}$ commutes with the two S_n-actions on $G(A/R) \otimes_R U^{\otimes n}$. In particular, $\mathcal{H}_{A,U}$ is preserved by the action of $A \otimes_R \text{End}(U)$.

Proof. This follows from the $A \otimes_R \text{End}(U)$-action being the same on every factor A of $G(A/R)$ and every factor U of $U^{\otimes n}$ by definition. ∎

Definition 4.4. We refer to $\mathcal{H}_{A,U}$ with this action of $A \otimes \text{End}(U)$ as a *Hermitian representation*.

We next describe the Hermitian representation explicitly using coordinates. After choosing a basis for U, we may make identifications $U \simeq R^{\oplus m}$ and $A \otimes_R \text{End}(U) \simeq \text{Mat}_m(A)$. Letting $T = \{(i_1, \ldots, i_n) \mid 1 \le i_j \le m\}$, we then have

$$G(A/R) \otimes_R U^{\otimes n} \simeq G(A/R)^{\oplus T},$$

that is, elements of $G(A/R) \otimes U^{\otimes n}$ are represented as n-dimensional $m \times \cdots \times m$ arrays with entries in $G(A/R)$, where T parametrizes the coordinates of the array. The two S_n-actions can then by described as follows. The 1st S_n-action on $G(A/R)$ acts on $M \in G(A/R)^{\oplus T}$ coordinate-wise: $\sigma(M_t)_{t \in T} = (\sigma(M_t))_{t \in T}$. The 2nd S_n-action on $U^{\otimes n}$ yields an action on T via $\sigma(i_1, \ldots, i_n) := (i_{\sigma(1)}, \ldots, i_{\sigma(n)})$, which then induces an action on $G(A/R)^{\oplus T}$. The Hermitian space $\mathcal{H}_{A,U}$ is then the subspace of arrays where these two actions agree (up to an inverse).

In coordinates, the action of $A \otimes \text{End}(U)$ on $\mathcal{H}_{A,U}$ is described as follows. Let $\gamma \in A \otimes_R \text{End}(U) \simeq \text{Mat}_m(A)$ and $M = (M_t)_{t \in T} \in \mathcal{H}_{A,U}$. Then $\gamma \cdot M$ has $(i_1, \ldots, i_n)$-entry as follows:

$$(\gamma \cdot M)_{i_1 \ldots i_n} = \sum_{j_1, \ldots, j_n} \left(\gamma_{i_1 j_1} \otimes \gamma_{i_2 j_2} \otimes \cdots \otimes \gamma_{i_n j_n} \right) \cdot M_{j_1 \ldots j_n};$$

here $(\gamma_{i_1 j_1} \otimes \gamma_{i_2 j_2} \otimes \cdots \otimes \gamma_{i_n j_n}) \cdot M_{j_1 \ldots j_n}$ comes from the left action of $A^{\otimes n}$ on $G(A/R)$.

4.2 Product formula for Hermitian representations

In this subsection we show that if A is a product of degree n_i algebras, then the Hermitian representation associated to A is a tensor product of the corresponding Hermitian representations.

Theorem 4.5. (Product formula for Hermitianizations).   For $1 \leq i \leq \ell$, let A_i be a degree n_i R-algebra. If $A = A_1 \times \cdots \times A_\ell$, then $\mathcal{H}_{A,U} \simeq \mathcal{H}_{A_1,U} \otimes_R \cdots \otimes_R \mathcal{H}_{A_\ell,U}$.

Proof.   For notational simplicity, we reduce to the case $\ell = 2$. Recall from Theorem 2.26 that if A_1 and A_2 are R-algebras of degree n_1 and n_2, respectively, then the R-algebra $A = A_1 \times A_2$ has degree $n = n_1 + n_2$ and its Galois closure is given by

$$G(A/R) = \mathrm{Ind}_{S_{n_1} \times S_{n_2}}^{S_n} \left(G(A_1/R) \otimes G(A_2/R) \right).$$

Further, recall from Remark 4.2 that $\mathcal{H}_{A,U} = (G(A/R) \otimes U^{\otimes n})^{S_n}$ for the diagonally embedded copy of S_n.

Now, in complete generality, if G is a finite group, $H \subseteq G$ is a subgroup, V is a finite-dimensional H-representation, and W is a finite-dimensional G-representation, then by the projection formula (see, e.g., [17, Tag 01E6]) we have

$$\mathrm{Ind}_H^G(V) \otimes W \simeq \mathrm{Ind}_H^G \left(V \otimes \mathrm{Res}_H^G(W) \right).$$

Taking G-invariants of both sides yields

$$\left(\mathrm{Ind}_H^G(V) \otimes W \right)^G \simeq \left(V \otimes \mathrm{Res}_H^G(W) \right)^H.$$

Applying this to the case where $G = S_n$, $H = S_{n_1} \times S_{n_2}$, $V = G(A_1/R) \otimes G(A_2/R)$, and $W = U^{\otimes n}$, we see

$$\mathcal{H}_{A,U} = \left(G(A/R) \otimes U^{\otimes n} \right)^{S_n} \simeq \left(G(A_1/R) \otimes G(A_2/R) \otimes U^{\otimes n_1} \otimes U^{\otimes n_2} \right)^{S_{n_1} \times S_{n_2}} \simeq \mathcal{H}_{A_1,U} \otimes \mathcal{H}_{A_2,U}$$

thereby proving the result.   ∎

Example 4.6.   Viewing R as a degree 1 algebra over itself, we have $\mathcal{H}_{R,U} = U$. The Hermitian representation is given by the standard action of $\mathrm{GL}(U)$ on U. Applying the product formula (Theorem 4.5) tells us that for the degree n algebra $A = R^n$, the Hermitian representation is $\mathcal{H}_{A,U} = U^{\otimes n}$ equipped with the natural action of $\mathrm{GL}(U)^n$.

Example 4.7.   If B is a quadratic R-algebra and A is the cubic algebra $R \times B$ as in Section 3.3, we conclude that $\mathcal{H}_{A,U} \simeq U \otimes \mathcal{H}_{B,U}$. With a choice of basis for the rank m free R-module U, we see that $m \times m \times m$ arrays that are Hermitian with respect to $A = R \times B$ may be viewed as an m-tuple of $m \times m$ matrices that are Hermitian with respect to B.

More generally, for a degree n R-algebra B, elements of the Hermitian space $\mathcal{H}_{R \times B, U}$ may be viewed as an m-tuple of elements of $\mathcal{H}_{B,U}$.

4.3 Example: endomorphism algebras (or matrix rings)

Let V be a rank n free R-module and let $A = \text{End}(V)$. We study the Hermitian representation $\mathcal{H}_{A,U}$, where U is a rank m free R-module.

Proposition 4.8. Let U be a rank m free R-module, V be a rank n free R-module, and $A = \text{End}(V)$. The Hermitian representation $\mathcal{H}_{A,U}$ is isomorphic to $\bigwedge^n (V \otimes U) \otimes \bigwedge^n (V^*)$.

Proof. As mentioned in Remark 4.2, we may view $\mathcal{H}_{A,U}$ as the invariant subspace of a particular S_n-action. Recall from Theorem 3.13 that $G(A/R) \simeq V^{\otimes n} \otimes \bigwedge^n (V^*)$. Since $\bigwedge^n (V^*)$ is the sign representation, our desired subspace of $G(A/R) \otimes U^{\otimes n}$ is therefore $\bigwedge^n (V^*)$ tensored with the copy of the sign representation in $V^{\otimes n} \otimes U^{\otimes n} = (V \otimes U)^{\otimes n}$. This is given by $\bigwedge^n (V \otimes U) \otimes \bigwedge^n (V^*)$.

The action of $A \otimes \text{End}(U) = \text{End}(V) \otimes \text{End}(U)$ on $\mathcal{H}_{A,U} \simeq \bigwedge^n (V \otimes U) \otimes \bigwedge^n (V^*)$ is then given by $\text{End}(U)$ acting on U and $\text{End}(V)$ acting on both V and V^*. ∎

Example 4.9. If U and V are free R-modules of ranks m and n, respectively, then with a choice of basis for each, we observe that $\mathcal{H}_{\text{End}(V),U}$ is naturally isomorphic to (a twist of) the n-th wedge product of a free R-module of rank mn, with the standard action of $\text{GL}_{mn}(R)$. In particular, we obtain some interesting representations (see Section 4.4):

dim U	dim V	$\mathcal{H}_{\text{End}(V),U}$	group
m	2	$\bigwedge^2 (2m)$	GL_{2m}
2	3	$\bigwedge^3 (6)$	GL_6
2	4	$\bigwedge^4 (8)$	GL_8
3	3	$\bigwedge^3 (9)$	GL_9.

(4.10)

Note that the 1st two cases in the table could have been computed without the definition of a Galois closure. The 1st may be visualized as Hermitian $m \times m$ matrices over the quadratic algebra $\text{Mat}_2(R)$. The 2nd may be visualized as $2 \times 2 \times 2$ cubes, Hermitian over the cubic algebra $\text{Mat}_3(R)$; the orbits of this space for $R = \mathbb{Z}$ are studied in [2], which motivated much of this paper.

4.4 Vinberg representations

In [19], Vinberg considers finite d-gradings of Lie algebras $\mathfrak{g} = \sum_{i=0}^{d-1} \mathfrak{g}_i$ and studies the representation of $G_0 \subset G$ on $\mathfrak{g}_1$, where $G_0 \subset G$ are the groups corresponding to the Lie algebras $\mathfrak{g}_0 \subset \mathfrak{g}$. The orbit spaces of many of these representations have, in recent years, been studied as moduli spaces of arithmetic or algebraic data [1, 2, 11–13, 18].

We observe that many of these representations may be viewed as Hermitian representations, as in Example 4.9. Below is a table with Vinberg's representations, coming from a d-grading on an exceptional group G, that also arise as Hermitian representations $\mathcal{H}_{A,U}$ for an m-dimensional vector space U over a field k and a degree n k-algebra A. The last column gives some recent references where the representation, corresponding moduli problem, and/or relevant arithmetic statistics problem have been studied.

	G	d	(semisimple) group	representation	m	n	A	reference
1.	$E_6^{(1)}$	2	$\mathrm{SL}_2 \times \mathrm{SL}_6$	$2 \otimes \bigwedge^3(6)$	2	4	$k \times \mathrm{Mat}_3(k)$	[1, Section 6.6.2]
2.	$E_6^{(1)}$	3	$\mathrm{SL}_3 \times \mathrm{SL}_3 \times \mathrm{SL}_3$	$3 \otimes 3 \otimes 3$	3	3	k^3	[1, ~Section 4.2]
3.	$E_7^{(1)}$	2	SL_8	$\bigwedge^4(8)$	2	4	$\mathrm{Mat}_4(k)$	[14, 18]
4.	$E_7^{(1)}$	3	$\mathrm{SL}_3 \times \mathrm{SL}_6$	$3 \otimes \bigwedge^2(6)$	3	3	$k \times \mathrm{Mat}_2(k)$	[1, Section 5.5]
5.	$E_8^{(1)}$	2	$\mathrm{SL}_2 \times E_7$	$2 \otimes 56$	2	4	$k \times \mathcal{J}$	[1, Section 6.6.3]
6.	$E_8^{(1)}$	3	SL_9	$\bigwedge^3(9)$	3	3	$\mathrm{Mat}_3(k)$	[12, 13, 15]
7.	$E_8^{(1)}$	3	$\mathrm{SL}_3 \times E_6$	$3 \otimes 27$	3	3	$k \times \mathbb{O}$	[1, Section 5.4]
8.	$F_4^{(1)}$	3	$\mathrm{SL}_3 \times \mathrm{SL}_3$	$3 \otimes \mathrm{Sym}^2(3)$	3	3	$k \times k_{[2]}$	[1, Section 5.2.1]
9.	$G_2^{(1)}$	2	$\mathrm{SL}_2 \times \mathrm{SL}_2$	$2 \otimes \mathrm{Sym}^3(2)$	2	4	$k \times k_{[3]}$	[1, Section 6.3.2]
10.	$D_4^{(3)}$	3	SL_3	$\mathrm{Sym}^3(3)$	3	3	$k_{[3]}$	[1, Section 5.2.2]

We use the notation $k_{[n]}$ to denote k as a degree n algebra (see Example 2.7). The notation $\mathbb{O}$ refers to the split octonion algebra over k, and $\mathcal{J}$ is the exceptional cubic Jordan algebra (also known as the space of Hermitian 3×3 matrices with respect to $\mathbb{O}$). In both of these cases, this algebra A is non-associative, but the Galois closure is not needed to describe the Hermitian space (see [1] for details).

There are in fact many additional cases of representations that arise from Vinberg's construction and are closely related to Hermitian representations. A simple example is that of $SL_2 \times SL_4$ acting on $2 \otimes Sym^2(4)$, which comes from a 4-grading of $E_6^{(2)}$; it is the tensor product of a 2D space and the space of Hermitian matrices over $k_{[2]}$. However, there are still numerous Vinberg representations for which we do not yet have such an interpretation.

Due to the non-associativity of general cubic Jordan algebras, our current definition of Galois closure does not apply. However, given the above connection between Vinberg representations and Galois closures, we ask the following.

Question 4.11.   Can our definition of Galois closure be extended to the case of cubic Jordan algebras (or other non-associative algebras)? If so, can any of the remaining Vinberg representations be recovered as Hermitian representations associated to such algebras?

Remark 4.12.   As mentioned in the introduction, our original motivation for this paper was to study as many representations as possible, including those arising from Vinberg theory, with a uniform method. In particular, we hope it will be possible to study the moduli problems coming from these Hermitian spaces using uniform geometric constructions via Galois closures.

References

[1] Bhargava, M. and W. Ho. "Coregular spaces and genus one curves." *Camb. J. Math.* 4, no. 1 (2016): 1–119.

[2] Bhargava, M. "Higher composition laws. I: a new view on Gauss composition, and quadratic generalizations." *Ann. of Math. (2)* 159, no. 1 (2004): 217–50.

[3] Biesel, O. "Galois closure data for extensions of rings." *Transform. Groups* 23, no. 1 (2018): 41–69.

[4]   Berhuy, G. and F. Oggier. An Introduction to Central Simple Algebras and Their Applications to Wireless Communication *Math. Surveys Monogr.* 191. Providence, RI: American Mathematical Society, 2013. With a foreword by B. A. Sethuraman.

[5]   Bhargava, M. and M. Satriano. "On a notion of "Galois closure" for extensions of rings." *J. Eur. Math. Soc. (JEMS)* 16, no. 9 (2014): 1881–913.

[6]   Chevalley, C. *Seminaire C. Chevalley: 2e Annee: 1958; Anneaux de Chow et Applications*. 11 rue Pierre Curie: Secrétariat Mathématique, 1958.

[7]   Ferrand, D. "Un foncteur norme." *Bull. Soc. Math. France* 126, no. 1 (1998): 1–49.

[8]   Gioia, A. "The Galois closure for rings and some related constructions." *J. Algebra* 446 (2016): 450–88.

[9]   Katz, N. M. and B. Mazur. *Arithmetic Moduli of Elliptic Curves. Annals of Mathematics Studies* 108. Princeton, NJ: Princeton University Press, 1985.

[10]   Pierce, R. S. *Associative Algebras*. Graduate Texts in Mathematics 88. New York-Berlin: Springer, 1982. Studies in the History of Modern Science, 9.

[11]   Pollack, A. "Lifting laws and arithmetic invariant theory." *Camb. J. Math.*, to appear.

[12]   Rains, E. and S. Sam. "Invariant theory of $\wedge^3(9)$ and genus 2 curves." *Algebra Number Theory,* to appear.

[13]   Rains, E. and S. Sam. "Vector bundles on genus 2 curves and trivectors." *Algebr. Geom.,* to appear.

[14]   Romano, B. and J. Thorne. "On the arithmetic of simple singularities of type E." *Res. Number Theory,* to appear.

[15]   Romano, B. and J. Thorne. "E_8 and the average size of the 3-Selmer group of the Jacobian of a pointed genus-2 curve." (2018): preprint https://arxiv.org/abs/1804.07702.

[16]   Serre, J.-P. "Linear representations of finite groups." *Graduate Texts in Mathematics 42.* New York-Heidelberg: Springer, 1977. Translated from the second French edition by Leonard L. Scott.

[17]   The Stacks Project Authors, *Stacks Project*, http://stacks.math.columbia.edu, 2018.

[18]   Thorne, J. A. "Vinberg's representations and arithmetic invariant theory." *Algebra Number Theory* 7, no. 9 (2013): 2331–68.

[19]   Vinberg, È. B. "The Weyl group of a graded Lie algebra." *Izv. Akad. Nauk SSSR Ser. Mat.* 40, no. 3 (1976): 488–526, 709.