Transformation Groups ©Springer Science+Business Media New York (2017)
Vol. 23, No. 1, 2018, pp. 41–69

GALOIS CLOSURE DATA FOR EXTENSIONS OF RINGS

OWEN BIESEL

624 4th Ave SE Apt. 1
Minneapolis, MN 55414, USA
owenbiesel@gmail.com

Abstract. To generalize the notion of Galois closure for separable field extensions, we devise a notion of G-closure for algebras of commutative rings $R \to A$, where A is locally free of rank n as an R-module and G is a subgroup of S_n. A *G-closure datum* for A over R is an R-algebra homomorphism $\varphi : (A^{\otimes n})^G \to R$ satisfying certain properties, and we associate to a closure datum φ a *closure algebra* $A^{\otimes n} \otimes_{(A^{\otimes n})^G} R$. This construction reproduces the normal closure of a finite separable field extension if G is the corresponding Galois group. We describe G-closure data and algebras of finite étale algebras over a general connected ring R in terms of the corresponding finite sets with continuous actions by the étale fundamental group of R. We show that if 2 is invertible, then A_n-closure data for free extensions correspond to square roots of the discriminant, and that D_4-closure data for quartic monogenic extensions correspond to roots of the cubic resolvent. This is an updated and revised version of the author's PhD thesis.

1. Introduction

In Manjul Bhargava's groundbreaking series *Higher composition laws*, he introduced an operation on rank-n $\mathbb{Z}$-algebras called *the* S_n*-closure* in order to parameterize cubic, quartic, and quintic rings (see [1, 2.1]). Later, Bhargava and Matthew Satriano extended this operation (modulo allowing torsion) in [2] to rank-n algebras over arbitrary base rings; their new S_n-closure operation reduces to the Galois closure for finite separable field extensions with associated Galois group S_n, and also commutes with base change. The paper closes by asking whether similar G-closure operations exist for other permutation groups $G \subseteq \mathrm{S}_n$. We answer Yes, provided that one is willing to parameterize such G-closures with what we call *G-closure data.*

If L is a degree-n separable extension of a field K with separable closure $\overline{K}$, we can define the Galois closure N of L to be the minimal subfield of $\overline{K}$ containing the images of all field homomorphisms $L \to \overline{K}$. Then the Galois group $G = \mathrm{Gal}(N/K)$ is a permutation group: it comes with an action on the n-element set of homomorphisms $L \to N$ over K. Choosing an ordering of these n homomorphisms, we identify G with a subgroup of S_n and can compile the n homomorphisms into

DOI: 10.1007/s00031-017-9433-x
Received March 30, 2016. Accepted January 24, 2017.
Published online July 6, 2017.
Corresponding Author: O. Biesel, e-mail: owenbiesel@gmail.com.

a single G-equivariant K-algebra homomorphism

$$L^{\otimes n} := L \otimes_K L \otimes_K \cdots \otimes_K L \to N,$$

where G acts on N by definition but on $L^{\otimes n}$ via the action of S_n on the tensor factors. In particular, we obtain a homomorphism between the G-invariants of the two K-algebras,

$$\varphi : (L^{\otimes n})^G \to N^G = K.$$

We will later see that this homomorphism is a *G-closure datum* for L over K, because of where it sends certain elements of $(L^{\otimes n})^G$. For each element $\ell \in L$, denote the kth elementary symmetric polynomial in the elements

$$\begin{aligned} \ell^{(1)} &= \ell \otimes 1 \otimes 1 \otimes \cdots \otimes 1, \\ \ell^{(2)} &= 1 \otimes \ell \otimes 1 \otimes \cdots \otimes 1, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ \ell^{(n)} &= 1 \otimes 1 \otimes \cdots \otimes 1 \otimes \ell \end{aligned}$$

by $e_k(\ell)$. Then $\varphi(e_k(\ell))$ is the kth elementary symmetric polynomial in the n conjugates of ℓ in N. In particular, φ sends $e_1(\ell)$ to the sum of ℓ's n conjugates, that is, the trace of ℓ. And $\varphi(e_n(\ell))$ is the product of ℓ's n conjugates, the norm of ℓ.

More generally, if ℓ is an element of L, we can regard multiplication by ℓ as a K-linear map $L \to L$. This linear map corresponds to an $n \times n$ matrix M_ℓ with entries in K, for each choice of K-basis for L. The characteristic polynomial of M_ℓ is independent of this choice of basis, so its coefficients are elements of K that depend only on ℓ. Write this characteristic polynomial as

$$\mathrm{p}_\ell(\lambda) := \det(\lambda I - M_\ell) = \lambda^n - s_1(\ell)\lambda^{n-1} + s_2(\ell)\lambda^{n-2} - \cdots + (-1)^n s_n(\ell).$$

Then the homomorphism $\varphi : (L^{\otimes n})^G \to K$ sends $e_k(\ell)$ to $s_k(\ell)$ for each $k \in \{1, \ldots, n\}$; this is the defining feature of a closure datum.

Namely, the concept of characteristic polynomial extends to the following setting: let R be a ring and A a rank-n R-algebra, i.e., an algebra that is locally free of rank n as an R-module. (Note: in this paper all rings and algebras are commutative by assumption; thus an R-algebra is just a ring A with a ring homomorphism $R \to A$.) Then for each $a \in A$, the multiplication-by-a homomorphism $A \to A$ locally corresponds to action of an $n \times n$-matrix on R^n, and the characteristic polynomials of these matrices glue to a well-defined polynomial with coefficients in R, which we again write as

$$\mathrm{p}_a(\lambda) = \lambda^n - s_1(a)\lambda^{n-1} + s_2(a)\lambda^{n-2} - \cdots + (-1)^n s_n(a).$$

Then a *G-closure datum for A over R* is an R-algebra homomorphism $\varphi\colon (A^{\otimes n})^G \to R$ that sends $e_k(a)$ to $s_k(a)$ for each $a \in A$ and each $k \in \{1, \ldots, n\}$.

A given ring R and algebra A may have G-closure data for only some groups G; we will see in Theorem 4.5 that if $K \hookrightarrow L$ is a finite separable field extension, the only closure data are the above φ for various orderings of $\mathrm{Hom}_K(L,N)$, along with their restrictions to the algebras of invariants under larger subgroups of S_n.

Now given such a $\varphi : (L^{\otimes n})^G \to K$ coming from a finite separable field extension $K \hookrightarrow L$ with Galois closure N, consider the following commutative square:

$$\begin{tikzcd}
(L^{\otimes n})^G \arrow[r, "\varphi"] \arrow[d] & K \arrow[d] \\
L^{\otimes n} \arrow[r] & N
\end{tikzcd}.$$

In fact, the square is a tensor product diagram, that is, $L^{\otimes n} \otimes_{(L^{\otimes n})^G} K \cong N$. In general, given a G-closure datum φ for A over R, we will associate to it the *closure algebra* $A^{\otimes n} \otimes_{(A^{\otimes n})^G} R$, thus generalizing the normal closure in the case of fields.

The organization and main results of this paper are as follows.

In Section 2, we phrase the definition of closure datum in terms of the canonical *Ferrand homomorphism* associated to a rank-n algebra, and we show that our notion of closure algebra generalizes the "S_n-closure" in the sense of Bhargava and Satriano in [2].

Theorem 1.1 (proven as Example 2.5)**.** *Let R be a ring and A a rank-n R-algebra. The Ferrand homomorphism $\Phi_{A/R}\colon (A^{\otimes n})^{\mathrm{S}_n} \to R$ is the unique S_n-closure datum for A over R, and its associated closure algebra is Bhargava and Satriano's S_n-closure of A over R.*

In Section 3, we consider the various ways of producing some closure data from others, by varying the group, base ring, or algebra. In particular, a G-closure datum induces an H-closure datum for each subgroup H of S_n containing G. The motivating examples of closure data, those homomorphisms $\varphi\colon (L^{\otimes n})^G \to K$ that arise from finite separable field extensions $K \hookrightarrow L$ with Galois group G, are always *minimal* in the sense that they are not induced by a closure datum for any smaller group than G. In Section 4 we show that for finite étale algebras over connected rings, the minimal closure data are all of this form:

Theorem 1.2 (proven as Theorem 4.5)**.** *Let R be a connected ring with étale fundamental group π_R. Let A be a rank-n étale R-algebra with corresponding π_R-set X, and let G be the image of π_R in $\mathrm{Bij}(X,X)$. Let H be a subgroup of S_n. Then minimal H-closure data for A over R are in one-to-one correspondence with bijections $f : \{1,\dots,n\} \xrightarrow{\sim} X$ such that $f^{-1}Gf = H$, up to precomposing f by permutations in H.*

In Section 5 we consider the case of product algebras, and show that having a closure datum on each factor gives closure data on the product:

Theorem 1.3 (proven as Theorems 5.1 and 5.5)**.** *Let R be a ring, and let A_i be an R-algebra of rank n_i for each $i \in \{1,\dots,k\}$, each with a G_i-closure datum φ_i and associated closure algebra B_i. Let $n = n_1 + \cdots + n_k$ and $A = A_1 \times \cdots \times A_k$, an R-algebra of rank n, and set $B = B_1 \otimes \cdots \otimes B_k$. Then for each subgroup $H \subseteq \mathrm{S}_n$ such that $H \cap \mathrm{S}_{n_i} = G_i$—where we regard S_{n_i} as a subgroup of S_n via its action* *on $\{n_1 + \cdots + n_{i-1} + 1, \ldots, n_1 + \cdots + n_{i-1} + n_i\}$—there is an H-closure datum for A whose associated closure algebra is $B^{|H|/|G_1|\cdots|G_k|}$.*

In Section 6 we use the results of [4] to classify A_n-closure data. Namely, for each rank-n R-algebra A there is a rank-2 R-algebra $\Delta_{A/R}$ such that A_n-closure data for A over R are in one-to-one correspondence with R-algebra homomorphisms $\Delta_{A/R} \to R$. The main theorem of that section is an analogue of the classical criterion that the Galois group of a field extension (in characteristic not 2) is contained in A_n if and only if its discriminant is a square:

Theorem 1.4 (proven as Theorem 6.5)**.** *Let R be a ring in which 2 is a unit, and let A be an R-algebra equipped with an R-module basis of size $n \geq 2$. Then A_n-closure data for A over R correspond to square roots in R of the discriminant of A with respect to that basis.*

Finally, in Section 7 we explore the case of *monogenic* algebras, i.e., those rank-n R-algebras of the form $A \cong R[x]/(f(x))$. Cataloguing the G-closure data for such an A over R is analogous to identifying the Galois group of f. We show first that if G is an intransitive permutation group, then every G-closure datum for A over R yields a nontrivial factorization of f; thus if f is irreducible then all closure data are with respect to transitive subgroups of S_n:

Theorem 1.5 (proven as Theorem 7.4)**.** *Let $f(x)$ be a monic degree-n polynomial with coefficients in a ring R, and let $n_1, n_2, \ldots, n_k$ be natural numbers whose sum is n. Then $\mathrm{S}_{n_1} \times \cdots \times \mathrm{S}_{n_k}$-closure data of $A = R[x]/(f(x))$ correspond to factorizations of f into monic factors $f_1(x), \ldots, f_k(x)$ of degrees $n_1, \ldots, n_k$, resepctively.*

Given such a factorization $f(x) = f_1(x) \ldots f_k(x)$, set $A_i = R[x]/(f_i(x))$ and denote its S_{n_i}-closure algebra by B_i. Then the $\mathrm{S}_{n_1} \times \cdots \times \mathrm{S}_{n_k}$-closure algebra associated to this factorization is isomorphic to $B_1 \otimes \cdots \otimes B_k$.

Finally, we show that under mild hypotheses on R and G, the G-closure data for A over R correspond to homomorphisms $(R[x]^{\otimes n})^G \to R$ sending each $e_k(x)$ to $s_k(a)$, where $a \in A$ corresponds to the element $x \in R[x]/(f(x))$. We then use this correspondence to show that D_4-closure data for a quartic polynomial f correspond bijectively to roots of f's *cubic resolvent*, with no assumptions on the base ring R:

Theorem 1.6 (proven as Theorem 7.14)**.** *Let R be a ring and let $A = R[x]/(f(x))$ be a monogenic rank-4 R-algebra. Then D_4-closure data for A over R correspond to roots of f's cubic resolvent in R.*

Remark 1.7. This paper is a condensed version of the author's PhD thesis [3] under Manjul Bhargava, and as such, the thanks expressed there to him and everyone else who provided invaluable support to that project still apply. However, the sections on universally norm-preserving homomorphisms and product algebras in this paper are new, and nearly every definition, statement, and proof has been revised from its original version. The author would therefore like to thank Maarten Derickx, Bas Edixhoven, Riccardo Ferrario, Alberto Gioia, Hendrik Lenstra, Lenny Taelman, and the two anonymous referees for their many helpful insights during this revision process.

2. The Ferrand homomorphism and closure data

We begin by reviewing the context in which our variant on Galois closures makes sense:

Definition 2.1. Let R be a ring, M an R-module, and n a natural number. We say that M is *locally free of rank* n if the unit ideal of R is generated by the set of all $r \in R$ such that the localization M_r is free of rank n as an R_r-module. Such a module is automatically projective and finitely generated. An *R-algebra of rank* n is an R-algebra that is locally free of rank n as an R-module.

Recall from [4, Def. 2.6] that for each pair (R, A) with R a ring and A an R-algebra of rank n, there is a canonical R-algebra homomorphism $(A^{\otimes n})^{\mathrm{S}_n} \to R$, which is denoted $\Phi_{A/R}$ and called the *Ferrand homomorphism* for A over R. Together, the Ferrand homomorphisms for various R and A have these properties:

(1) For each ring R and R-algebra A of rank n, and for each $a \in A$, we have

$$\Phi_{A/R}(a \otimes \cdots \otimes a) = \mathrm{Nm}_{A/R}(a),$$

the norm of a, i.e., the element of R such that for every $a_1 \wedge \cdots \wedge a_n \in \bigwedge^n A$, we have

$$(aa_1) \wedge (aa_2) \wedge \cdots \wedge (aa_n) = \mathrm{Nm}_{A/R}(a)(a_1 \wedge \cdots \wedge a_n).$$

(2) The Ferrand homomorphisms *commute with base change*: if R is a ring and A is an R-algebra of rank n, and if furthermore R' is any R-algebra and we denote the rank-n R'-algebra $R' \otimes_R A$ by A', then the following square of R'-algebra homomorphisms commutes:

$$\begin{tikzcd}
R' \otimes_R (A^{\otimes n})^{\mathrm{S}_n} \arrow[r, "\sim"] \arrow[d, "\mathrm{id}_{R'} \otimes \Phi_{A/R}"'] & (A'^{\otimes_{R'} n})^{\mathrm{S}_n} \arrow[d, "\Phi_{A'/R'}"] \\
R' \otimes_R R \arrow[r, "\sim"] & R'
\end{tikzcd} .$$

Properties 1 and 2 above uniquely identify the Ferrand homomorphisms through the machinery of *polynomial laws.* A polynomial law from one R-module M to another N is a family of functions $f_S \colon S \otimes_R M \to S \otimes_R N$ for each R-algebra S, such that for all R-algebra homomorphisms $S \to T$, the square of functions formed by f_S, f_T, and the base change homomorphisms $S \otimes_R M \to T \otimes_R M$ and $S \otimes_R N \to T \otimes_R N$ commutes. In [9], Norbert Roby shows that homogeneous degree-n polynomial laws $f \colon M \to N$ (those for which $f_S(s \cdot m) = s^n \cdot f_S(m)$ for all R-algebras S and elements $s \in S$ and $m \in S \otimes_R M$) correspond to R-module homomorphisms $\Gamma^n_R(M) \to N$ with $\Gamma^n_R(M)$ the n-graded component of the *divided powers algebra* of M. In [10] Roby also shows that if M and N are R-algebras and the functions $f_S \colon S \otimes_R M \to S \otimes_R N$ are multiplicative, then $\Gamma^n_R(M) \to N$ is an algebra homomorphism.

A general presentation of $\Gamma^n_R(M)$ is somewhat involved, but if M is flat then by [5, 5.5.2.5 on p. 123] we have $\Gamma^n_R(M) \cong (M^{\otimes_R n})^{\mathrm{S}_n}$. The homomorphism

$\varphi\colon (M^{\otimes n})^{\mathrm{S}_n} \to N$ corresponding to a homogeneous degree-n polynomial law $(f_S\colon S \otimes_R M \to S \otimes_R N)_{S \in R\text{-}\mathbf{Alg}}$ is defined by the property that for every R-algebra S, the base change

$$\mathrm{id}_S \otimes \varphi : ((S \otimes_R M)^{\otimes_S n})^{\mathrm{S}_n} \cong S \otimes_R (M^{\otimes_R n})^{\mathrm{S}_n} \to S \otimes_R N$$

sends each element of the form $m \otimes \cdots \otimes m$ to $f_S(m)$.

The quintessential example of a multiplicative degree-n homogeneous polynomial law is the family of norm maps $\mathrm{Nm}_{S \otimes_R A/S}\colon S \otimes_R A \to S$ for a rank-n R-algebra A; in fact, according to [11] these are in some sense the only examples. Thus we obtain a unique R-algebra homomorphism $(A^{\otimes n})^{\mathrm{S}_n} \to R$ satisfying properties 1 and 2, and this is Ferrand's original construction of the Ferrand homomorphisms in [6].

As a consequence of this abstract characterization of the Ferrand homomorphisms, we find that for each element a of a rank-n R-algebra A, the Ferrand homomorphism $\Phi_{A/R}$ applied coefficientwise to $(x-a) \otimes (x-a) \otimes \cdots \otimes (x-a)$ gives the characteristic polynomial $\mathrm{p}_a(x) := \mathrm{Nm}_{A[x]/R[x]}(x-a)$ of a. In other words,

Lemma 2.2. *Denote the coefficient of $(-1)^k x^{n-k}$ in $(x-a) \otimes \cdots \otimes (x-a)$ by $e_k(a)$, the k-th elementary symmetric polynomial evaluated in the n elements $a^{(1)} = a \otimes 1 \otimes \cdots \otimes 1$ up to $a^{(n)} = 1 \otimes \cdots \otimes 1 \otimes a$ in $A^{\otimes n}$. And denote the coefficient of $(-1)^k x^{n-k}$ in $\mathrm{Nm}_{A[x]/R[x]}(x-a) = \mathrm{p}_a(x)$ by $s_k(a) \in R$. Then*

$$\Phi_{A/R}\big(e_k(a)\big) = s_k(a).$$

Remark 2.3. Note that by [12, Cor. 3.13(1)], which implies that elements of the form $e_k(a)$ generate $(A^{\otimes n})^{\mathrm{S}_n}$ as an R-algebra, the fact that $\Phi_{A/R}$ sends each $e_k(a)$ to $s_k(a)$ uniquely characterizes the Ferrand homomorphism among all R-algebra homomorphisms $(A^{\otimes n})^{\mathrm{S}_n} \to R$. The definition of closure datum given in the introduction is thus equivalent to the following:

Definition 2.4. Let R be a ring and A a rank-n R-algebra. A *closure datum for A over R* is a pair (G, φ), where G is a subgroup of S_n and φ is an R-algebra homomorphism $(A^{\otimes n})^G \to R$ that extends the Ferrand homomorphism $\Phi_{A/R}\colon (A^{\otimes n})^{\mathrm{S}_n} \to R$.

If (G, φ) is a closure datum for A over R, then we also say that φ is a *G-closure datum for A over R*. Furthermore, given a G-closure datum φ, we denote the R-algebra given by the tensor product

$$A^{\otimes n} \bigotimes_{(A^{\otimes n})^G} R \;\cong\; A^{\otimes n}/\big(\alpha - \varphi(\alpha) : \alpha \in (A^{\otimes n})^G\big)$$

by $A^{\otimes n}/\varphi$ and call it the *G-closure* (or *closure algebra*) of A over R associated with φ.

Example 2.5 (see Theorem 1.1)**.** There is exactly one S_n-closure for each rank-n R-algebra A: the one associated with $\Phi_{A/R}$ itself. Its associated R-algebra is

$$\begin{aligned} A^{\otimes n}/\Phi_{A/R} &\cong A^{\otimes n}/\big(\alpha - \Phi_{A/R}(\alpha) : \alpha \in (A^{\otimes n})^{\mathrm{S}_n}\big) \\ &= A^{\otimes n}/\big(e_k(a) - s_k(a) : a \in A \text{ and } k \in \{1, \ldots, n\}\big), \end{aligned}$$

where we have used the fact that the $e_k(a)$ generate $(A^{\otimes n})^{\mathrm{S}_n}$ from Remark 2.3 to simplify the ideal presentation. This last quotient is exactly the S_n-closure of A over R defined by Bhargava and Satriano in [2].

3. Relationships between closure data

In this section we demonstrate some ways of obtaining one closure datum from another, either by replacing the group with a larger subgroup of S_n, changing the base from R to an arbitrary R-algebra R', or pulling back closure data for B to closure data for A along certain R-algebra homomorphisms $A \to B$.

3.1. Inducing closure data

Varying the group gives us the most elementary means of producing new closure data:

Proposition 3.1. *Let R be a ring and A an R-algebra of rank n. If (G, φ) is a closure datum for A over R, and H is a subgroup of S_n containing G, then $(H, \varphi|_{(A^{\otimes n})^H})$ is also a closure datum for A over R.*

Proof. The only criterion to check is that $\varphi|_{(A^{\otimes n})^H}$ restricts to the Ferrand homomorphism on $(A^{\otimes n})^{\mathrm{S}_n}$, but this is true because φ does. □

We say that the G-closure datum φ *induces* the H-closure datum $\varphi|_{(A^{\otimes n})^H}$ for each H containing G. In particular, the property of a given R-algebra having a G-closure is upward-closed with respect to G. For this reason, "having a G-closure" can be thought of as roughly corresponding to "having Galois group contained in G"—the analogue of *the* Galois group, then, is a minimal group G for which a G-closure datum exists. The following definition enriches this idea with the closure data:

Definition 3.2. A closure datum (G, φ) for an R-algebra A of rank n is called *minimal* if it is not induced by any other closure datum, i.e., if the homomorphism $\varphi\colon (A^{\otimes n})^G \to R$ cannot be extended to a homomorphism $(A^{\otimes n})^H \to R$ for any smaller subgroup $H \subsetneq G$.

For a given ring and algebra, is there always a unique minimal closure datum? The answer is typically "No" for trivial reasons: if (G, φ) is a closure datum for an R-algebra A of rank n, and $\sigma \in \mathrm{S}_n$ is any permutation, then $(\sigma G \sigma^{-1}, \varphi \circ (\mathrm{id}_A)^{\otimes \sigma^{-1}})$ is another closure datum. (Here $(\mathrm{id}_A)^{\otimes \sigma^{-1}}$ is the automorphism of $A^{\otimes n}$ sending $a^{(i)}$ to $a^{(\sigma^{-1}(i))}$. It restricts to a map $(A^{\otimes n})^{\sigma G \sigma^{-1}} \to (A^{\otimes n})^G$.) This describes an action of S_n on the set of closure data for a given R-algebra, and the resulting action groupoid gives us a notion of two closure data being isomorphic:

Definition 3.3. Let R be a ring and A an R-algebra of rank n. An *isomorphism of closure data* $(G, \varphi) \to (H, \psi)$ for A over R is a permutation $\sigma \in \mathrm{S}_n$ for which $H = \sigma G \sigma^{-1}$ and for which $\psi = \varphi \circ (\mathrm{id}_A)^{\otimes \sigma^{-1}}$.

Remark 3.4. The question we should be asking, then, is whether every pair of minimal closure data is isomorphic in this sense. We will show in Section 4 that this is the case if the ring is connected and the algebra is étale. There are also more examples; for instance, every free quadratic R-algebra has this property if and only if R is a domain, as we will show in Remark 7.6.

The question of how unique minimal closure data need be has also been taken up by Riccardo Ferrario for rank-4 algebras in [7], where he exhibits an example of a quartic algebra with multiple minimal closure data with respect to groups that are not even conjugate. On the positive side, Maarten Derickx shows in forthcoming work that if R is a characteristic-zero integrally closed domain, then for every finite-rank R-algebra A the groups with minimal closure data for A over R are all conjugate. He also shows that this can fail in positive characteristic.

Note that with this definition of (iso)morphism of closure data, the operation of taking the closure associated to a closure datum is then a functor:

Proposition 3.5. *Let R be a ring and A an R-algebra of rank n. Let $\sigma\colon (G,\varphi) \to (H,\psi)$ be an isomorphism of closure data for A over R. Then the automorphism $(\mathrm{id}_A)^{\otimes\sigma}$ of $A^{\otimes n}$ descends to an R-algebra isomorphism $A^{\otimes n}/\varphi \xrightarrow{\sim} A^{\otimes n}/\psi$ of the associated closure algebras.*

Proof. That $\sigma\colon (G,\varphi) \to (H,\psi)$ is an isomorphism of closure data reflects the commutativity of the following diagram:

$$\begin{tikzcd}
& A^{\otimes n} \arrow[rr, "(\mathrm{id}_A)^{\otimes\sigma}", "\sim"'] & & A^{\otimes n} \\
(A^{\otimes n})^G \arrow[ur, hook] \arrow[rr, "(\mathrm{id}_A)^{\otimes\sigma}", "\sim"'] \arrow[dr, "\varphi"] & & (A^{\otimes n})^H \arrow[ur, hook] \arrow[dr, "\psi"] & & . \\
& R \arrow[rr, equal] & & R
\end{tikzcd}$$

Therefore we obtain the desired isomorphism of the associated closure algebras

$$A^{\otimes n}/\varphi = A^{\otimes n} \bigotimes_{(A^{\otimes n})^G} R \xrightarrow{\sim} A^{\otimes n} \bigotimes_{(A^{\otimes n})^H} R = A^{\otimes n}/\psi. \quad \square$$

Remark 3.6. Note that for a fixed ring R with rank-n algebra A, and for a fixed subgroup $G \subseteq \mathrm{S}_n$, the set of G-closure data for A over R carries a natural action by $\{\sigma \in \mathrm{S}_n : \sigma G \sigma^{-1} = G\}$, the normalizer $\mathrm{N}_{\mathrm{S}_n}(G)$ of G. Those σ that belong to G itself act trivially on the set of G-closure data, but induce generally non-trivial automorphisms of the associated closure algebras. To summarize, for a fixed ring R and rank-n algebra A:

- The set of all closure data for A over R has a natural S_n-action.
- For a fixed group $G \subseteq \mathrm{S}_n$, the set of G-closure data for A over R carries a natural action by the group $\mathrm{N}_{\mathrm{S}_n}(G)/G$. The orbits of this action are precisely the isomorphism classes of G-closure data.
- For each G-closure datum φ, the associated closure algebra $A^{\otimes n}/\varphi$ carries a natural action by G.

3.2. Universally norm-preserving homomorphisms

We can also produce closure data by pulling it back along *universally norm-preserving* R-algebra homomorphisms:

Definition 3.7. Let R be a ring and A and B be R-algebras of rank n. An R-algebra homomorphism $f\colon A \to B$ is called *norm-preserving* if for all $a \in A$, we have $\mathrm{Nm}_A(a) = \mathrm{Nm}_B(f(a))$. We say that f is *universally* norm-preserving if for every R-algebra S, the S-algebra homomorphism $\mathrm{id}_S \otimes f : S \otimes_R A \to S \otimes_R B$ is norm-preserving.

Here are two alternative characterizations of universally norm-preserving homomorphisms:

Lemma 3.8. *Let R be a ring and $f\colon A \to B$ a homomorphism of R-algebras of rank n. The following are equivalent:*

(1) *The homomorphism f is universally norm preserving.*
(2) *The following triangle of R-algebra homomorphisms commutes:*

$$\begin{tikzcd}
(A^{\otimes n})^{\mathrm{S}_n} \arrow[rr, "(f^{\otimes n})^{\mathrm{S}_n}"] \arrow[dr, "\Phi_A"'] & & (B^{\otimes n})^{\mathrm{S}_n} \arrow[dl, "\Phi_B"] \\
& R &
\end{tikzcd}.$$

(3) *The homomorphism f preserves characteristic polynomials, i.e., for all $a \in A$, we have $\mathrm{p}_{f(a)}(\lambda) = \mathrm{p}_a(\lambda)$, or equivalently, $s_k(f(a)) = s_k(a)$ for all $k \in \{1, \dots, n\}$.*

Proof. See [4, Prop. 7.1]. □

Proposition 3.9. *Let R be a ring and A and B be R-algebras of rank n. If $f\colon A \to B$ is a universally norm-preserving homomorphism and (G, φ) is a closure datum for B, then $(G, \varphi \circ (f^{\otimes n})^G)$ is a closure datum for A.*

Furthermore, the homomorphism of R-algebras $f^{\otimes n}\colon A^{\otimes n} \to B^{\otimes n}$ descends to a homomorphism of the G-closures $A^{\otimes n}/(\varphi \circ (f^{\otimes n})^G) \to B^{\otimes n}/\varphi$.

Proof. We just need to check that $\varphi \circ (f^{\otimes n})^G$, restricted to $(A^{\otimes n})^{\mathrm{S}_n}$, is the Ferrand homomorphism Φ_A. This restriction is $\varphi|_{(B^{\otimes n})^{\mathrm{S}_n}} \circ (f^{\otimes n})^{\mathrm{S}_n} = \Phi_B \circ (f^{\otimes n})^{\mathrm{S}_n}$, which equals Φ_A since f is universally norm-preserving. That the described homomorphism of G-closures exists is elementary. □

3.3. Base extension of closure data

Finally, base change preserves closure data and commutes with forming the closure algebra:

Proposition 3.10. *Let R be a ring and A an R-algebra of rank n. Let R' be any R-algebra, and $A' = R' \otimes_R A$ the resulting R'-algebra of rank n. If (G, φ) is a closure datum for A over R, then (G, φ') is a closure datum for A' over R', where φ' is the composite homomorphism*

$$\varphi' \colon (A'^{\otimes_{R'} n})^G \cong R' \otimes_R (A^{\otimes n})^G \xrightarrow{\mathrm{id}_{R'} \otimes \varphi} R' \otimes_R R \cong R'.$$

Furthermore, the canonical isomorphism $R' \otimes_R A^{\otimes n} \cong A'^{\otimes_{R'} n}$ descends to an isomorphism $R' \otimes_R (A^{\otimes n}/\varphi) \cong A'^{\otimes_{R'} n}/\varphi'$.

Proof. First, note that because A is locally free as an R-module, the isomorphism between $A'^{\otimes_{R'} n}$ and $R' \otimes_R (A^{\otimes n})$ does indeed restrict to one $(A^{\otimes_{R'} n})^G \cong R' \otimes_R (A^{\otimes n})^G$ by [4, Prop. 3.5], so the definition of φ' makes sense. Then to check that (G, φ') is a closure datum for A' over R' is to check that φ' restricts to $\Phi_{A'/R'}$. But this holds because $\Phi_{A'/R'} \cong \mathrm{id}_{R'} \otimes \Phi_{A/R}$, and φ restricts to $\Phi_{A/R}$.

The claim that $R' \otimes_R (A^{\otimes n}/\varphi) \cong A'^{\otimes_{R'} n}/\varphi'$ is easily checked using the presentation of the G-closure as a tensor product:

$$R' \otimes_R \left(A^{\otimes n} \bigotimes_{(A^{\otimes n})^G} R \right) \cong (R' \otimes_R A^{\otimes n}) \bigotimes_{R' \otimes_R (A^{\otimes n})^G} (R' \otimes_R R) \cong A'^{\otimes_{R'} n} \bigotimes_{(A'^{\otimes_{R'} n})^G} R';$$

the tensor product on the left is $R' \otimes_R (A^{\otimes n}/\varphi)$, and the one on the right is $A'^{\otimes_{R'} n}/\varphi'$. □

Note that in the special case $G = \mathrm{S}_n$, this provides a much simpler proof of [2, Thm. 1].

Remark 3.11. Let R be a ring, let A an R-algebra of rank n, let G be a subgroup of S_n. Let R' be an arbitrary R-algebra and $A' = R' \otimes_R A$ the resulting R'-algebra of rank n, and consider the set of G-closure data for A' over R' as R' varies. We have the following bijections, natural in R', making this functor representable:

$$\begin{aligned}
&\{G\text{-closure data for } A' \text{ over } R'\} \\
&\quad \longleftrightarrow \{(A'^{\otimes_{R'} n})^{\mathrm{S}_n}\text{-algebra homomorphisms } (A'^{\otimes_{R'} n})^G \to R'\} \\
&\quad \longleftrightarrow \{R'\text{-algebra homomorphisms } (A'^{\otimes_{R'} n})^G \otimes_{(A'^{\otimes_{R'} n})^{\mathrm{S}_n}} R' \to R'\} \\
&\quad \longleftrightarrow \{R'\text{-algebra homomorphisms } R' \otimes_R ((A^{\otimes n})^G \otimes_{(A^{\otimes n})^{\mathrm{S}_n}} R) \to R'\} \\
&\quad \longleftrightarrow \{R\text{-algebra homomorphisms } (A^{\otimes n})^G \otimes_{(A^{\otimes n})^{\mathrm{S}_n}} R \to R'\}.
\end{aligned}$$

In particular, setting $R' = (A^{\otimes n})^G \otimes_{(A^{\otimes n})^{\mathrm{S}_n}} R$, we find that A' has a canonical G-closure datum corresponding to the identity map on R'. This G-closure datum is universal: every G-closure datum for every base extension of A can be obtained via base extension from this G-closure datum for A' over R'.

The special case of $G = \mathrm{A}_n$ is particularly nice: the resulting R-algebra $\Delta_{A/R} = (A^{\otimes n})^{\mathrm{A}_n} \otimes_{(A^{\otimes n})^{\mathrm{S}_n}} R$ is the discriminant algebra for A over R defined in [4], which we can now interpret as the universal R-algebra such that base-changing to it gives A an A_n-closure. We explore A_n-closure data further in Section 6.

Letting R' vary again, we find through similar reasoning that if $H \subseteq G$ are subgroups of S_n and φ is a G-closure datum for A over R, then R-algebra homomorphisms $(A^{\otimes n})^H \otimes_{(A^{\otimes n})^G} R \to R'$ correspond to the set of H-closure data on A' over R' inducing the closure datum (G, φ') of Proposition 3.10.

In particular, we can now give an interpretation to the closure algebra associated with a given closure datum (G, φ) for A over R: the closure algebra

$$A^{\otimes n}/\varphi = A^{\otimes n} \otimes_{(A^{\otimes n})^G} R$$

is the universal R-algebra for which base changing to it gives A a 1-closure datum inducing the given G-closure datum. If we think of a G-closure datum as partial factorization information for each characteristic polynomial of elements of A—a more precise version of this idea is found in Theorem 7.4—then the G-closure algebra is the universal algebra over which every characteristic polynomial splits completely in a way respecting this partial information.

4. Étale algebras

In this section, we will consider closure data for *finite étale* algebras, namely locally free algebras for which the trace form $(a, a') \mapsto \mathrm{Tr}(aa')$ is non-degenerate. Examples include the *trivial* étale algebras, of the form $R \to R^X := \prod_{x \in X} R$ for some finite set X, as well as finite separable field extensions. First, we recall a lemma characterizing finite étale algebras as those which are étale-locally trivial:

Lemma 4.1 ([2, Lem. 15])**.** *Let R be a ring and A an R-algebra finitely generated as an R-module. Then A is étale of rank n if and only if there is an étale cover $R \to S$ such that $S \otimes_R A \cong S^n$ as S-algebras.*

(An R-algebra S forms an étale cover of R if S is étale over R and $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is surjective, but we will not need this definition in order to apply Lemma 4.1.)

Thus is it helpful to first consider the Ferrand homomorphism and closure data for trivial algebras:

Lemma 4.2. *If R is a ring and X is an n-element set, then the Ferrand homomorphism of the trivial rank-n R-algebra R^X*

$$\Phi_{R^X/R} \colon ((R^X)^{\otimes n})^{\mathrm{S}_n} \cong R^{X^n/\mathrm{S}_n} \to R$$

is the projection onto the factor indexed by the orbit of bijections $\mathrm{Bij}(\{1, \dots, n\}, X)$*.*

Proof. See [6, Ex. 3.1.3(b)]. We could alternatively deduce this result from Proposition 5.3, by choosing an arbitrary bijection $\pi \colon X \to \{1, \dots, n\}$ and pulling back the canonical 1-closure datum on R^n to R^X and then restricting it to $((R^X)^{\otimes n})^{\mathrm{S}_n}$. □

To understand closure data for finite étale algebras, then, it will be helpful to understand closure data for trivial étale algebras.

Lemma 4.3. *Let R be a ring, X a finite set of cardinality n, and G a subgroup of S_n. Then G-closure data for R^X over R correspond bijectively to R-algebra homomorphisms $R^I \to R$, where I is the set of G-orbits of* $\mathrm{Bij}(\{1, \dots, n\}, X)$ *under the action of G by precomposition. Furthermore, every G-closure of R^X is isomorphic to $R^{|G|}$ as an R-algebra.*

Proof. Recall from Remark 3.11 that G-closure data for R^X over R correspond to R-algebra homomorphisms

$$((R^X)^{\otimes n})^G \bigotimes_{((R^X)^{\otimes n})^{\mathrm{S}_n}} R \to R.$$

We can write $(R^X)^{\otimes n}$ as $R^{\mathrm{Map}(\{1,\dots,n\},X)}$, with G acting on the set of basis idempotents $\{\mathrm{e}_f \mid f \colon \{1, \dots, n\} \to X\}$ via $\sigma \cdot \mathrm{e}_f = \mathrm{e}_{f \circ \sigma^{-1}}$. The G-invariants, then, have an R-basis of idempotents $\mathrm{e}_O = \sum_{f \in O} \mathrm{e}_f$ for each G-orbit O of $\mathrm{Map}(\{1, \dots, n\}, X)$.

By Lemma 4.2, the Ferrand homomorphism $R^{\mathrm{Map}(\{1,\ldots,n\},X)/\mathrm{S}_n} \to R$ is the projection onto the factor indexed by $\mathrm{Bij}(\{1,\ldots,n\},X)$. Hence every e_O in the ring $R^{\mathrm{Map}(\{1,\ldots,n\},X)/G}$ with $O \not\subseteq \mathrm{Bij}(\{1,\ldots,n\},X)$ is sent to zero in the tensor product. So G-closure data for R^X over R are parametrized by homomorphisms to R from

$$R^{\mathrm{Map}(\{1,\ldots,n\},X)/G}/\big(\mathrm{e}_O : O \not\subseteq \mathrm{Bij}(\{1,\ldots,n\},X)\big) = R^{\mathrm{Bij}(\{1,\ldots,n\},X)/G} = R^I.$$

Now we show that each G-closure algebra of R^X is isomorphic to $R^{|G|}$. Choose a homomorphism $R^I \to R$; this partitions $\mathrm{Spec}(R)$ into $|I|$ disjoint affine open subsets on which the map is a projection. Then working locally, assume we have the G-closure datum corresponding to the projection $R^I \to R$ indexed by the Oth factor for some G-orbit $O \subseteq \mathrm{Bij}(\{1,\ldots,n\},X)$. Then the associated closure algebra is

$$R^{\mathrm{Map}(\{1,\ldots,n\},X)} \bigotimes_{R^{\mathrm{Map}(\{1,\ldots,n\},X)/G}} R \cong R^O,$$

and since G acts freely on $\mathrm{Bij}(\{1,\ldots,n\},X)$, we have $|O| = |G|$ and $R^O \cong R^{|G|}$. In the general case, we find that $\mathrm{Spec}(R)$ is a disjoint union of open subsets on which the closure algebra is trivial; the closure algebra is hence globally trivial as well. □

Corollary 4.4. *Let R be a ring and A a rank-n étale R-algebra. Then for every closure datum (G,φ) for A over R, the associated closure algebra $A^{\otimes n}/\varphi$ is a rank-$|G|$ étale R-algebra.*

Proof. By Lemma 4.1, there is an étale cover $R \to S$ such that $S \otimes_R A \cong S^n$ as S-algebras. By Proposition 3.10, we obtain a G-closure datum φ_S for $S \otimes_R A$ over S, for which the associated closure $(S \otimes_R A)^{\otimes_S n}/\varphi_S$ is isomorphic to $S \otimes_R (A^{\otimes n}/\varphi)$. But by Lemma 4.3, the associated G-closure of $S \otimes_R A \cong S^n$ is isomorphic to $S^{|G|}$. Therefore $S \otimes_R (A^{\otimes n}/\varphi) \cong S^{|G|}$, so by Lemma 4.1 again $A^{\otimes n}/\varphi$ is an étale R-algebra of rank $|G|$. □

In case R is a *connected* ring, that is, R contains exactly two idempotents 0 and 1, then for each choice of homomorphism $R \to K$ with K a separably closed field, there is a profinite group π_R called the *étale fundamental group* of R, and a contravariant equivalence of categories

$$\{\text{finite étale } R\text{-algebras}\} \longleftrightarrow \{\text{finite sets with a continuous } \pi_R\text{-action}\}$$

sending an étale algebra A to the finite π_R-set $\mathrm{Hom}_R(A,K)$; see [8] for more details. In this setting, we have the following interpretation of closure data and closure algebras in terms of the corresponding π_R-sets:

Theorem 4.5 (see Theorem 1.2)**.** *Let R be a connected ring with étale fundamental group π_R. Let A be a rank-n étale R-algebra with corresponding π_R-set X, and let G be the image of π_R in* $\mathrm{Bij}(X,X)$. *Let H be a subgroup of* S_n. *Then H-closure data for A over R are in one-to-one correspondence with bijections $f : \{1,\ldots,n\} \xrightarrow{\sim} X$ such that $f^{-1}Gf \subseteq H$, up to precomposing f by permutations in H.*

Furthermore, if B is the finite étale algebra corresponding to the π_R-set G, then every H-closure of A over R is isomorphic to $B^{|H|/|G|}$.

Proof. Recall that H-closure data for A over R correspond to homomorphisms

$$(A^{\otimes n})^H \bigotimes_{(A^{\otimes n})^{\mathrm{S}_n}} R \to R,$$

and thus to π_R-equivariant maps

$$\{*\} \to X^n/H \times_{X^n/\mathrm{S}_n} \{*\},$$

that is, π_R-invariant elements of X^n/H whose images in X^n/S_n are the class of bijections $\mathrm{Bij}(\{1,\dots,n\},X)$. These in turn correspond to the π_R-invariant (i.e., G-invariant, since the action is via $\pi_R \twoheadrightarrow G$) H-orbits of $\mathrm{Bij}(\{1,\dots,n\},X)$. Write such an H-orbit as fH for some bijection $f:\{1,\dots,n\} \xrightarrow{\sim} X$; then the condition that fH be G-invariant is the equality $GfH = fH$, or the containment $Gf \subseteq fH$. Thus we may say that fH is a G-invariant H-orbit if and only if $f^{-1}Gf \subseteq H$. Therefore H-closure data correspond to bijections f (up to precomposition by elements of H) such that $f^{-1}Gf \subseteq H$, as desired.

Now given such a G-invariant H-orbit O of $\mathrm{Bij}(\{1,\dots,n\},X)$, giving a π_R-equivariant function $\{*\} \to X^n/H$, we find that the π_R-set corresponding to the associated H-closure algebra is

$$X^n \times_{X^n/H} \{*\} = O.$$

Now the action of π_R on $\mathrm{Bij}(\{1,\dots,n\},X)$ is via G, and the G-action on $\mathrm{Bij}(\{1,\dots,n\},X)$ is free, so as a π_R-set it is isomorphic to a disjoint union of copies of G. Then so is the G-invariant subset O, and by comparing cardinalities we find that $O \cong \coprod_{|H|/|G|} G$ as π_R-sets. Therefore the H-closure algebra corresponding to O is isomorphic to $B^{|H|/|G|}$, as claimed. □

Remark 4.6. Note that if $H \subseteq K$ are subgroups of S_n, then induction of H-closure data to K-closure data sends the H-orbit of a bijection $f\colon \{1,\dots,n\} \xrightarrow{\sim} X$ to the larger K-orbit of f. Then for each bijection f, there is a smallest subgroup $G_f \subseteq \mathrm{S}_n$ for which f gives a G_f-closure datum, namely $G_f = f^{-1}Gf$, and this G_f-closure datum is therefore minimal. Two bijections $f, f' : \{1,\dots,n\} \xrightarrow{\sim} X$ give the same minimal closure datum if and only if $G_f = G_{f'}$ and $fG_f = f'G_{f'}$, which implies that $Gf = Gf'$, so f and f' are related via postcomposition by an element of G. Thus the minimal closure data for A over R are in bijection with the G-orbits of $\mathrm{Bij}(\{1,\dots,n\},X)$. Since the action of S_n on these is transitive, all the minimal closure data are isomorphic, as we claimed in Section 3. Note also that the closure algebras associated to the minimal closure data are all isomorphic to B, the étale algebra corresponding to the finite π_R-set G, as in the usual Galois theory of projective separable ring extensions.

5. Product algebras

In this section, we consider the closure data that arise on product algebras $A_1 \times \cdots \times A_k$ given closure data on each A_i. Our first main theorem is as follows, and covers the case of Theorem 1.3 where H is the product of the factor groups G_i:

Theorem 5.1. *Let R be a ring, and let A_i be an R-algebra of rank n_i for each $i \in \{1, \dots, k\}$, each with a closure datum (G_i, φ_i). Set*

- $n := \sum_{i=1}^k n_i$.
- $A := \prod_{i=1}^k A_i$, *an R-algebra of rank n.*
- $G := \prod_{i=1}^k G_i$, *considered as a subgroup of S_n via the action of each G_i on the n_i-element set $\{n_1 + \cdots + n_{i-1} + 1, \dots, n_1 + \cdots + n_{i-1} + n_i\}$.*
- $\varphi\colon (A^{\otimes n})^G \to R$ *equal to the composite*

$$(A^{\otimes n})^G \cong \bigotimes_{i=1}^k (A^{\otimes n_i})^{G_i} \twoheadrightarrow \bigotimes_{i=1}^k (A_i^{\otimes n_i})^{G_i} \xrightarrow{\bigotimes_{i=1}^k \varphi_i} R.$$

Then (G, φ) is a closure datum for A over R.

Furthermore, the R-algebra homomorphism $A^{\otimes n} \cong \bigotimes_{i=1}^k A^{\otimes n_i} \to \bigotimes_{i=1}^k A_i^{\otimes n_i}$ descends to an isomorphism $A^{\otimes n}/\varphi \cong \bigotimes_{i=1}^k (A_i^{\otimes n_i}/\varphi_i)$.

Proof. First we show that φ restricts to the Ferrand homomorphism $(A^{\otimes n})^{\mathrm{S}_n} \to R$. Let $a = (a_1, \dots, a_k) \in A$, and consider the image of $(x-a)^{\otimes n}$ under $\varphi \otimes \mathrm{id}_{R[x]}$. We find

$$(x-a)^{\otimes n} = \bigotimes_{i=1}^k (x-a)^{\otimes n_i} \longmapsto \bigotimes_{i=1}^k (x-a_i)^{\otimes n_i} \longmapsto \prod_{i=1}^k \mathrm{p}_{a_i}(x) = \mathrm{p}_a(x),$$

so looking at each coefficient of x^{n-k}, we have that φ sends $e_k(a)$ to $s_k(a)$ as desired. (That the characteristic polynomial $\mathrm{p}_a(x)$ of $a \in A$ factors as the product of each characteristic polynomial $\mathrm{p}_{a_i}(x)$ of $a_i \in A_i$ is easy to check locally when each A_i has an R-basis: then $a = (a_1, \dots, a_k)$ acts block diagonally.)

Next we show that the closure algebra associated to (G, φ) is the tensor product of all the $A_i^{\otimes n_i}/\varphi_i$. Note that

$$(A^{\otimes G})^n = (A^{\otimes n_1} \otimes \cdots \otimes A^{\otimes n_k})^{G_1 \times \cdots \times G_k} \cong (A^{\otimes n_1})^{G_1} \otimes \cdots \otimes (A^{\otimes n_k})^{G_k},$$

since the natural map is easily checked to be an isomorphism whenever A is a free R-module. So we obtain

$$A^{\otimes n} \bigotimes_{(A^{\otimes n})^G} R \cong \left(\bigotimes_{i=1}^k A^{\otimes n_i}\right) \bigotimes_{\bigotimes_{i=1}^k (A^{\otimes n_i})^{G_i}} R \cong \bigotimes_{i=1}^k \left(A^{\otimes n_i} \bigotimes_{(A^{\otimes n_i})^{G_i}} R\right).$$

Then all we must show is that $A^{\otimes n_i} \otimes_{(A^{\otimes n_i})^{G_i}} R$ is isomorphic to $A_i^{\otimes n_i} \otimes_{(A_i^{\otimes n_i})^{G_i}} R = A_i^{\otimes n_i}/\varphi_i$. Indeed, if we let $\mathrm{e}_i \in A$ be the element $(0, \dots, 0, 1, 0, \dots, 0)$ with a 1 in the ith place, then $\mathrm{e}_i \otimes \cdots \otimes \mathrm{e}_i \in (A^{\otimes n_i})^{G_i}$ is sent to 1 in R. Hence for each element $a \in I := \{(a_1, \dots, a_n) \in A : a_i = 0\}$, the image of $a^{(j)}$ in $A^{\otimes n_i} \otimes_{(A^{\otimes n_i})^{G_i}} R$ is equal to that of $a^{(j)} \cdot (\mathrm{e}_i \otimes \cdots \otimes \mathrm{e}_i) = 0$. Therefore

$$A^{\otimes n_i} \bigotimes_{(A^{\otimes n_i})^{G_i}} R \cong (A/I)^{\otimes n_i} \bigotimes_{(A^{\otimes n_i})^{G_i}} R \cong A_i^{\otimes n_i} \bigotimes_{(A^{\otimes n_i})^{G_i}} R.$$

Last, observe that the two maps defining the tensor product

$$(A^{\otimes n_i})^{G_i} \to A^{\otimes n_i} \to A_i^{\otimes n_i} \quad \text{and} \quad (A^{\otimes n_i})^{G_i} \to (A_i^{\otimes n_i})^{G_i} \to R$$

both factor through $(A_i^{\otimes n_i})^{G_i}$; we may therefore substitute it in the base of the tensor product:

$$A_i^{\otimes n_i} \bigotimes_{(A^{\otimes n_i})^{G_i}} R \cong A_i^{\otimes n_i} \bigotimes_{(A_i^{\otimes n_i})^{G_i}} R = A_i^{\otimes n_i}/\varphi_i.$$

Thus $A^{\otimes n}/\varphi = \bigotimes_{i=1}^{k}(A_i^{\otimes n_i}/\varphi_i)$ as desired. □

Remark 5.2. Note that even if all the closure data (G_i, φ_i) in Theorem 5.1 are minimal, the resulting closure datum on the product may or may not be. One need not look farther than classical Galois theory for examples: let $R = \mathbb{Q}$ and consider the product of $A_1 = \mathbb{Q}[\sqrt{2}]$ and $A_2 = \mathbb{Q}[\sqrt{3}]$. Neither admits a 1-closure datum, so the Ferrand homomorphisms $\Phi_{A_1/R}$ and $\Phi_{A_2/R}$ are minimal S_2-closure data for them, and in this case, the $\mathrm{S}_2 \times \mathrm{S}_2$-closure datum for $A_1 \times A_2$ of Theorem 5.1 is minimal. (To see this, look at the corresponding $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-sets: $A_1 \times A_2$ corresponds to a disjoint union of two two-element sets and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on them via $\mathrm{S}_2 \times \mathrm{S}_2$.

However, if we consider the product $A_1 \times A_1$, the resulting $\mathrm{S}_2 \times \mathrm{S}_2$-closure datum is *not* minimal, since the corresponding Galois action is via the simultaneous action of S_2 on the disjoint union of two copies of the two-element set corresponding to A_1: the diagonal copy of S_2 inside $\mathrm{S}_2 \times \mathrm{S}_2$. In future work we hope to characterize exactly when the product closure datum of Theorem 5.1 is minimal in general.

Note that Theorem 5.1 implies that a universally norm-preserving homomorphism from a rank-n algebra A to a product of lower rank algebras $\prod_{i=1}^{k} B_i$ (with each B_i of rank n_i) produces a $\prod_{i=1}^{k} \mathrm{S}_{n_i}$-closure datum for A. We might ask whether all $\prod_{i=1}^{k} \mathrm{S}_{n_i}$-closure data arise in this way. Theorem 7.4 shows that the answer is yes if A is monogenic. We can also see elementarily that $1 = \mathrm{S}_1 \times \cdots \times \mathrm{S}_1$-closures arise in this way via the following proposition:

Proposition 5.3. *Let R be a ring and A an R-algebra of rank n. Let $f_1, \dots, f_n$ be R-algebra homomorphisms from A to R; we can compile these into two single R-algebra homomorphisms*

$$\bigotimes_{i=1}^{n} f_i \colon A^{\otimes n} \to R : a^{(i)} \mapsto f_i(a) \textit{ for each } i \in \{1, \dots, n\},$$

$$\prod_{i=1}^{n} f_i \colon A \to R^n : a \mapsto (f_1(a), \dots, f_n(a)).$$

Then $\bigotimes_i f_i$ is a 1-closure datum for A over R if and only if $\prod_i f_i$ is a universally norm-preserving homomorphism from A to R^n.

Proof. First, note that the characteristic polynomial for an element $(r_1, \dots, r_n)$ of R^n is $\prod_{i=1}^{n}(x - r_i)$, so the s_k of this tuple is the kth elementary symmetric polynomial in the r_i. Then $\prod_i f_i$ being universally norm-preserving is equivalent to the kth elementary symmetric polynomial in the $f_i(a)$ always equaling $s_k(a)$. But $\bigotimes_i f_i$ sends $e_k(a)$ to the kth elementary symmetric polynomial in the $f_i(a)$, so $\prod_i f_i$ being universally norm-preserving is equivalent to $\bigotimes_i f_i$ sending each $e_k(a)$ to $s_k(a)$. This is in turn equivalent to $\bigotimes_i f_i$ restricting to Φ_A on $(A^{\otimes n})^{\mathrm{S}_n}$ by Remark 2.3. □

Remark 5.4. In particular, the n projections $\pi_1, \ldots, \pi_n \colon R^n \to R$ give a canonical 1-closure datum for R^n over R, thereby inducing a canonical G-closure datum for each subgroup $G \subseteq \mathrm{S}_n$. Furthermore, if $\prod_i f_i \colon A \to R^n$ is universally norm-preserving, then $\bigotimes_i f_i$ is the 1-closure datum for A obtained via $\prod_i f_i$ from the canonical 1-closure datum for R^n. Then given any G-closure datum φ for A over R, we can interpret the G-closure algebra $A^{\otimes n}/\varphi$ as the universal R-algebra R' such that $A' := R' \otimes_R A$ gains a universally norm-preserving homomorphism to R'^n for which the base change of φ is the pullback of the canonical G-closure datum on R'^n.

Our second main theorem of this section shows that if we replace G in Theorem 5.1 with a larger group H (while keeping $H \cap \mathrm{S}_{n_i}$ equal to G_i) then the induced closure algebra is just a power of the G-closure algebra, generalizing [2, Thm. 6] that

$$A^{\otimes n}/\Phi_A \cong \Big(\bigotimes_{i=1}^{k} A_i^{\otimes n_i}/\Phi_{A_i}\Big)^{\binom{n}{n_1, n_2, \ldots, n_k}}.$$

Theorem 5.5 (see Theorem 1.3). *In the setting of Theorem* 5.1*, let $H \subseteq \mathrm{S}_n$ be a subgroup such that $H \cap \mathrm{S}_{n_i} = G_i$, where we regard S_{n_i} as a subgroup of S_n via its action on $\{n_1 + \cdots + n_{i-1} + 1, \ldots, n_1 + \cdots + n_{i-1} + n_i\}$. Then $H \supseteq G$, and the induced H-closure datum $\varphi|_{(A^{\otimes n})^H}$ has associated closure algebra*

$$A^{\otimes n}/(\varphi|_{(A^{\otimes n})^H}) \cong \big(A^{\otimes n}/\varphi\big)^{(H:G)} \cong \Big(\bigotimes_{i=1}^{k} A_i^{\otimes n_i}/\varphi_i\Big)^{(H:G)}.$$

Proof. Again, for $i \in \{1, \ldots, k\}$ denote by e_i the idempotent $(0, \ldots, 0, 1, 0, \ldots, 0) \in A = \prod_{j=1}^{k} A_j$ with a 1 in the ith place. Let e be the idempotent of $A^{\otimes n}$ given by

$$e = \mathrm{e}_1 \otimes \cdots \otimes \mathrm{e}_1 \otimes \mathrm{e}_2 \otimes \cdots \otimes \mathrm{e}_2 \otimes \cdots \otimes \mathrm{e}_k \otimes \cdots \otimes \mathrm{e}_k,$$

with n_i tensor factors of each e_i. Then e is G-invariant, so the H-orbit $\{h.e : h \in H\}$ of e will be in natural bijection with the set H/G of left cosets of G in H. Let $\tilde{e}$ be the sum of all the elements of this orbit; then $\tilde{e}$ is H-invariant and sent to 1 under $\varphi|_{(A^{\otimes n})^H}$.

Now the $|H/G|$ idempotents $\{h.e : h \in H\}$ map to idempotents of the H-closure $A^{\otimes n}/\varphi|_{(A^{\otimes n})^H}$ that are permuted transitively by the action of H, and moreover these idempotents are orthogonal and have sum 1. Therefore $A^{\otimes n}/\varphi|_{(A^{\otimes n})^H}$ splits as a product of $|H/G|$ isomorphic factors. We claim that the factor corresponding to the idempotent e is canonically isomorphic to $A^{\otimes n}/\varphi$. Indeed, we are comparing the two quotients

$$A^{\otimes n}/(e - 1, y - \varphi(y) : y \in (A^{\otimes n})^H) \quad \text{and} \quad A^{\otimes n}/(x - \varphi(x) : x \in (A^{\otimes n})^G).$$

The right-hand ideal clearly contains the left-hand ideal; we show conversely that everything in the right-hand ideal is already zero in the left-hand quotient. Let $x \in (A^{\otimes n})^G$. By working locally, we may assume that the A_i are all free, and by expanding x, we may assume x is a sum over the G-orbit of a pure tensor with each tensor factor a basis element of some A_i. Let y be the corresponding H-orbit sum. There are two cases, according as $x \cdot e = x$ (when, in order, the tensor factors of x consist of n_1 from A_1, n_2 from A_2, etc.) or $x \cdot e = 0$. In the former case, we have $y \cdot e = x$ as well, since e annihilates every term of $y - x$. Then $\varphi(x) = \varphi(y \cdot e) = \varphi(y)\varphi(e) = \varphi(y)$, so in $\big(A^{\otimes n}/\varphi|_{(A^{\otimes n})^H}\big)/(e-1)$ we have

$$\varphi(x) = \varphi(y) = y = y \cdot 1 = y \cdot e = x.$$

In the case that $x \cdot e = 0$, then $\varphi(x) = \varphi(x) \cdot 1 = \varphi(x)\varphi(e) = \varphi(x \cdot e) = 0$. And in $A^{\otimes n}/\varphi|_{(A^{\otimes n})^H}/(e-1)$ we thus have

$$\varphi(x) = 0 = x \cdot e = x \cdot 1 = x.$$

Therefore the ideal $(x - \varphi(x) : x \in (A^{\otimes n})^G)$ is equal to $(y - \varphi(y) : y \in (A^{\otimes n})^H) + (e-1)$ as claimed. So $A^{\otimes n}/\varphi|_{(A^{\otimes n})^H}$ is isomorphic to a product of $|H/G|$ copies of $A^{\otimes n}/\varphi$. □

6. $\mathbf{A}_n$-closure data

Recall from Remark 3.11 that if A is a rank-n algebra over R, then A_n-closure data for A over R correspond to R-algebra homomorphisms to R from the *discriminant algebra*

$$\Delta_{A/R} := (A^{\otimes n})^{\mathrm{A}_n} \bigotimes_{(A^{\otimes n})^{\mathrm{S}_n}} R.$$

The discriminant algebra is always a rank-2 algebra over the base ring, and furthermore there is a canonical isomorphism

$$\textstyle\bigwedge^n A \xrightarrow{\sim} \bigwedge^2 \Delta_{A/R}$$

sending $a_1 \wedge \cdots \wedge a_n$ to $1 \wedge \dot\gamma(a_1, \dots, a_n)$, where $\dot\gamma(a_1, \dots, a_n)$ is the image in $\Delta_{A/R}$ of the A_n-invariant element $\gamma(a_1, \dots, a_n) = \sum_{\sigma \in \mathrm{A}_n} a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(n)}$ of $(A^{\otimes n})^{\mathrm{A}_n}$. This isomorphism respects the discriminant bilinear forms on $\bigwedge^n A$ and $\bigwedge^2 \Delta_{A/R}$; see [4, Thm. 4.1] for proofs of all the above statements.

If A is not merely locally free as an R-module, but free with R-basis $(\theta_1, \dots, \theta_n)$, then $\bigwedge^n A$ is free with generator $\theta_1 \wedge \cdots \wedge \theta_n$. Therefore $\bigwedge^2 \Delta_A$ is free with generator $1 \wedge \dot\gamma(\theta_1, \dots, \theta_n)$, and hence Δ_A itself has R-basis $(1, \dot\gamma(\theta_1, \dots, \theta_n))$. We can thus present $\Delta_{A/R}$ abstractly as an R-algebra $R[y]/(q(y))$, where q is a monic quadratic polynomial, the characteristic polynomial of $\dot\gamma(\theta_1, \dots, \theta_n)$ in $\Delta_{A/R}$. Futhermore, the discriminant of q is the same as the discriminant of A with respect to its basis $(\theta_1, \dots, \theta_n)$. So A_n-closures of A over R correspond to R-algebra homomorphisms $R[y]/(q(y)) \to R$, i.e., roots of q in R.

Example 6.1. Let R be a ring with elements $a, b \in R$, and let A be the R-algebra $R[x]/(x^3 + ax + b)$ with R-basis $(1, x, x^2)$. Then $\Delta_{A/R}$ has R-basis $(1, \dot{\gamma}(1, x, x^2))$. Since the sum and product of $\dot{\gamma}(1, x, x^2)$ and $\dot{\gamma}(1, x^2, x)$ are both in R, we have a monic quadratic polynomial of which $\dot{\gamma}(1, x, x^2)$ is a root, and which must therefore be its characteristic polynomial:

$$y^2 - \big(\dot{\gamma}(1, x, x^2) + \dot{\gamma}(1, x^2, x)\big)y + \big(\dot{\gamma}(1, x, x^2)\dot{\gamma}(1, x^2, x)\big).$$

We can compute these coefficients with the Ferrand homomorphism $(A^{\otimes 3})^{\mathrm{S}_3} \to R$:

$$\begin{aligned}\dot{\gamma}(1, x, x^2) + \dot{\gamma}(1, x^2, x) &= \Phi_{A/R}(\gamma(1, x, x^2) + \gamma(1, x^2, x)) = 3b,\\ \dot{\gamma}(1, x, x^2)\dot{\gamma}(1, x^2, x) &= \Phi_{A/R}(\gamma(1, x, x^2)\gamma(1, x^2, x)) = a^3 + 9b^2.\end{aligned}$$

(See [4, Example 5.6] for the full and more general computation.) Then $\Delta_{A/R} \cong R[y]/(y^2 - (3b)y + (a^3 + 9b^2))$, so A_3-closure data for A over R correspond to roots of $y^2 - (3b)y + (a^3 + 9b^2)$ in R. In particular, if an A_3-closure datum exists then the discriminant $(3b)^2 - 4(a^3 + 9b^2) = -4a^3 - 27b^2$ is a square in R.

Example 6.2. Consider the degree-2 separable extension $\mathbb{F}_4$ over $\mathbb{F}_2$. Since any quadratic algebra is canonically isomorphic to its discriminant algebra ([4, Prop. 5.1]), there exists an $\mathrm{A}_2 = 1$-closure datum if and only if there is a map $\mathbb{F}_4 \to \mathbb{F}_2$, which there is not, even though the discriminant of $\mathbb{F}_4$ over $\mathbb{F}_2$ is 1, a square. This is consistent with the Galois group of $\mathbb{F}_4$ over $\mathbb{F}_2$ being S_2.

On the other hand, the cubic $\mathbb{F}_2$-algebra $\mathbb{F}_8 \cong \mathbb{F}_2[x]/(x^3+x+1)$ has discriminant algebra $\mathbb{F}_2[y]/(y^2 - (3 \cdot 1)y + (1^3 + 9 \cdot 1^2)) = \mathbb{F}_2[y]/(y^2 - y)$, which does admit a map to $\mathbb{F}_2$. Therefore $\mathbb{F}_8$ has an $\mathrm{A}_3 = \mathrm{C}_3$-closure datum, which is consistent with having Galois group C_3.

Note that this criterion for A to have an A_n-closure datum, namely that there is an R-algebra homomorphism $\Delta_{A/R} \to R$, works equally well in every characteristic. In this respect, the discriminant algebra is a better quadratic resolvent than testing whether the discriminant is a square, which for field extensions only works in characteristic other than 2. However, the square-discriminant test does work in a slightly larger generality: when 2 is a *primoid non-zerodivisor.*

Definition 6.3. Let p be an element of a ring R. We say that p is *primoid* if whenever p^2 divides a product ab, then p divides a or b.

For example, units and prime elements are primoid. More generally, every power of a prime non-zerodivisor is primoid. The utility of this notion is that the quadratic formula works over a ring R if $2 \in R$ is a primoid non-zerodivisor:

Lemma 6.4. *Let R be a ring, and let $x \in R$ be a solution to the equation $x^2 + bx + c = 0$ for fixed $b, c \in R$. Then $2x + b$ is a square root of the equation's discriminant $b^2 - 4c$. If 2 is a primoid non-zerodivisor in R, then this assignment $x \mapsto 2x + b$ forms a one-to-one correspondence between the solutions to $x^2 + bx + c = 0$ and the square roots of the discriminant.*

Proof. That $2x+b$ is a square root of the discriminant is straightforward: $(2x+b)^2 = 4x^2+4bx+b^2 = 4(-bx-c)+4bx+b^2 = b^2-4c$. Conversely, suppose that 2 is a primoid non-zerodivisor and that d is a square root of b^2-4c. We show that d can be uniquely written as $2x+b$ for some solution x to $x^2+bx+c=0$. Consider that $(d+b)(d-b) = d^2-b^2 = -4c$, so since 2 is primoid we must have $2|(d+b)$ or $2|(d-b)$. Then we conclude that since the difference between $d+b$ and $d-b$ is a multiple of 2, both are multiples of 2. In particular, $d-b$ can be written uniquely as $2x$ for some x, since 2 is a non-zerodivisor. And for that x, we have $4(x^2+bx+c) = (2x)^2+2b(2x)+4c = (d-b)^2+2b(d-b)+4c = d^2-b^2+4c = 0$, so $x^2+bx+c=0$ as desired. □

Theorem 6.5 (see Theorem 1.4)**.** *Let R be a ring in which* 2 *is a primoid non-zerodivisor (e.g., a unit), and let A be an R-algebra equipped with an R-module basis of size $n \geq 2$. Then A_n-closure data for A over R correspond to square roots in R of the discriminant of A with respect to that basis.*

Proof. We know that A_n-closure data for A correspond to roots in R of a quadratic polynomial whose discriminant equals that of A with respect to the given basis. But since 2 is a primoid non-zerodivisor, roots of such a quadratic polynomial correspond to square roots of its discriminant, and thus square roots of the discriminant of A. □

Example 6.6. To see that the primoid hypothesis in Theorem 6.5 is necessary, consider the ring $R = \mathbb{Z}[\sqrt{5}]$ and $A = R[x]/(x^2-x-1)$. The discriminant of A over R is $(-1)^2-4(1)(-1) = 5$, a square in R. But A does not have an $\mathrm{A}_2 = 1$-closure as it does not admit a homomorphism to R; the golden ratio is not a $\mathbb{Z}$-linear combination of 1 and $\sqrt{5}$. This is because 2 is not primoid in R: we have $(1+\sqrt{5})(1-\sqrt{5}) = -4$, a multiple of 2^2, but neither factor is a multiple of 2.

7. Monogenic algebras

Definition 7.1. Let R be a ring and A an R-algebra. We say that A is *monogenic of rank n* if there exists an isomorphism $A \cong R[x]/(f(x))$ for some monic degree-n polynomial $f(x)$. In particular, a monogenic rank-n R-algebra is necessarily *free* of rank n as an R-module.

Remark 7.2. There is also a weaker notion of "monogenic," meaning just that A is generated by a single element as an R-algebra, but if A is a rank-n R-algebra then these two notions are equivalent. Indeed, suppose A has rank n and is generated as an R-algebra by a single element a. Then we have a surjective R-algebra homomorphism $R[x] \twoheadrightarrow A$ sending $x \mapsto a$, and since a is a root of its characteristic polynomial $\mathrm{p}_a(x)$, this map descends to a surjection $R[x]/(\mathrm{p}_a(x)) \twoheadrightarrow A$. Locally, this is a surjective homomorphism of free rank-n modules, hence must be (locally and globally) an isomorphism. So $R[x]/(\mathrm{p}_a(x)) \cong A$.

Remark 7.3. Note that given any element $a \in A$, not necessarily a generator, we still obtain a well-defined algebra homomorphism $R[x]/(\mathrm{p}_a(x)) \to A$. By [4, Example 7.2], this homomorphism is universally norm-preserving. Therefore G-closure data for A pull back to G-closure data for $R[x]/(\mathrm{p}_a(x))$. This may be viewed as a kind of obstruction to the existence of G-closure data for A over R; there cannot be any unless $R[x]/(\mathrm{p}_a(x))$ has one too for every $a \in A$. For this reason, criteria for monogenic algebras to admit G-closure data are useful even if one is interested in algebras that are not necessarily monogenic.

7.1. Intransitive closure data

In this section we consider closure data for a monogenic algebra when the subgroup of S_n is of the form $\mathrm{S}_{n_1} \times \cdots \times \mathrm{S}_{n_k}$, with each S_{n_i} acting on $\{1, \ldots, n\}$ by permuting the n_i elements

$$\{n_1 + \cdots + n_{i-1} + 1, \ldots, n_1 + \cdots + n_{i-1} + n_i\}$$

as in Theorem 5.1. We find that such closure data correspond to factorizations of the defining polynomial of the monogenic algebra.

Theorem 7.4 (see Theorem 1.5)**.** *Let $f(x)$ be a monic degree-n polynomial with coefficients in a ring R, and let $n_1, n_2, \ldots, n_k$ be natural numbers whose sum is n. Then $\mathrm{S}_{n_1} \times \cdots \times \mathrm{S}_{n_k}$-closure data of $A = R[x]/(f(x))$ correspond to factorizations of f into monic factors $f_1(x), \ldots, f_k(x)$ of degrees $n_1, \ldots, n_k$, resepctively.*

Given such a factorization $f(x) = f_1(x) \ldots f_k(x)$, set $A_i = R[x]/(f_i(x))$. Then the $\mathrm{S}_{n_1} \times \cdots \times \mathrm{S}_{n_k}$-closure algebra associated to this factorization is isomorphic to the tensor product $\bigotimes_{i=1}^k A_i^{\otimes n_i}/\Phi_{A_i}$.

Proof. To produce a $\prod_i \mathrm{S}_{n_i}$-closure datum from a factorization, consider the R-algebra homomorphism $A \to \prod_{i=1}^k A_i : x \mapsto (x, \ldots, x)$. It is a universally norm-preserving homomorphism because the characteristic polynomial of $(x, \ldots, x)$ in $\prod_{i=1}^k A_i$ is the product $f_1(x) \ldots f_k(x) = f(x)$, which is the characteristic polynomial of x in A. Therefore the $\prod_i \mathrm{S}_{n_i}$-closure datum on $\prod_{i=1}^k A_i$ from Theorem 5.1 pulls back to a $\prod_i \mathrm{S}_{n_i}$-closure datum on A.

Now we must show that every $\prod_i \mathrm{S}_{n_i}$-closure datum on A arises in this way. Given a homomorphism $\varphi : (A^{\otimes n})^{\prod_i \mathrm{S}_{n_i}} \to R$ restricting to the Ferrand homomorphism, consider for each $i \in \{1, \ldots, k\}$ the image under $\varphi \otimes \mathrm{id}_{R[\lambda]}$ of the $\prod_i \mathrm{S}_{n_i}$-invariant element

$$1^{\otimes n_1} \otimes \cdots \otimes 1^{\otimes n_{i-1}} \otimes (\lambda - x)^{\otimes n_i} \otimes 1^{\otimes n_{i+1}} \otimes \cdots \otimes 1^{\otimes n_k};$$

this is a monic degree-n_i polynomial in $R[\lambda]$ which we denote by $f_i(\lambda)$. Then because the product of these k invariant elements is $(\lambda - x)^{\otimes n}$ and is sent to $f(\lambda)$, we therefore have a factorization $f(\lambda) = \prod_{i=1}^k f_i(\lambda)$. To see that this factorization gives rise to the closure datum $\varphi : (A^{\otimes n})^{\prod_i \mathrm{S}_{n_i}} \cong \bigotimes_i (A^{\otimes n_i})^{\mathrm{S}_{n_i}} \to R$, we show that φ's ith component $(A^{\otimes n_i})^{\mathrm{S}_{n_i}} \to R$ factors via $(A_i^{\otimes n_i})^{\mathrm{S}_{n_i}}$. By the fundamental theorem of elementary symmetric polynomials, it is sufficient to check the images of each element of the form $e_\ell(x) \in (A^{\otimes n_i})^{\mathrm{S}_{n_i}}$ for $\ell \in \{1, \ldots, n_i\}$. We may check these simultaneously by adjoining an auxiliary indeterminate λ and considering the single element $(\lambda - x)^{\otimes n_i} = \sum_{\ell=1}^{n_i} (-1)^\ell \lambda^\ell e_\ell(x)$. Applying the homomorphism $(A^{\otimes n_i})^{\mathrm{S}_{n_i}} \twoheadrightarrow (A_i^{\otimes n_i})^{\mathrm{S}_{n_i}} \to R$ coefficientwise, this element is sent to the characteristic polynomial of x in A_i, namely $f_i(\lambda)$. But this is equal, by definition of f_i, to the image of $(\lambda - x)^{\otimes n_i}$ under φ's ith component $(A^{\otimes n_i})^{\mathrm{S}_{n_i}} \to R$. Thus we recover φ as the $\prod_i \mathrm{S}_{n_i}$-closure datum corresponding to the factorization $f = \prod_i f_i$.

Now we check that given such a factorization $f(x) = f_1(x) \dots f_k(x)$, the corresponding $\prod_i \mathrm{S}_{n_i}$-closure algebra is isomorphic to $\bigotimes_i A_i^{\otimes n_i}/\Phi_{A_i}$. Let φ be the associated closure datum

$$(A^{\otimes n})^{\prod_i \mathrm{S}_{n_i}} \cong \bigotimes_{i=1}^{k} (A^{\otimes n_i})^{\mathrm{S}_{n_i}} \twoheadrightarrow \bigotimes_{i=1}^{k} (A_i^{\otimes n_i})^{\mathrm{S}_{n_i}} \to R.$$

We have the isomorphism

$$A^{\otimes n}/\Phi_A = A^{\otimes n} \bigotimes_{(A^{\otimes n})^{\prod_i \mathrm{S}_{n_i}}} R \cong \bigotimes_{i=1}^{k} A^{\otimes n_i} \bigotimes_{(A^{\otimes n_i})^{\mathrm{S}_{n_i}}} R,$$

where for each $i \in \{1, \dots, k\}$ the map $(A^{\otimes n_i})^{\mathrm{S}_{n_i}} \to R$ is the composite

$$(A^{\otimes n_i})^{\mathrm{S}_{n_i}} \twoheadrightarrow (A_i^{\otimes n_i})^{\mathrm{S}_{n_i}} \xrightarrow{\Phi_{A_i}} R$$

Note that this homomorphism tensored with $R[\lambda]$ sends the element

$$\prod_{j=1}^{n_i} (\lambda - x^{(j)}) = (\lambda - x) \otimes \cdots \otimes (\lambda - x) \mapsto \mathrm{Nm}_{A_i[\lambda]}(\lambda - x) = f_i(\lambda),$$

and thus in $A^{\otimes n_i} \otimes_{(A^{\otimes n_i})^{\mathrm{S}_{n_i}}} R$ we find that each $f_i(x^{(j)}) = \prod_{j'} (x^{(j)} - x^{(j')}) = 0$. Therefore we have

$$A^{\otimes n_i} \bigotimes_{(A^{\otimes n_i})^{\mathrm{S}_{n_i}}} R \cong A_i^{\otimes n_i} \bigotimes_{(A^{\otimes n_i})^{\mathrm{S}_{n_i}}} R.$$

Now the two homomorphisms from $(A^{\otimes n_i})^{\mathrm{S}_{n_i}}$ in the tensor product both factor through its quotient $(A_i^{\otimes n_i})^{\mathrm{S}_{n_i}}$, so we obtain

$$A_i^{\otimes n_i} \bigotimes_{(A^{\otimes n_i})^{\mathrm{S}_{n_i}}} R \cong A_i^{\otimes n_i} \bigotimes_{(A_i^{\otimes n_i})^{\mathrm{S}_{n_i}}} R = A_i^{\otimes n_i}/\Phi_{A_i}.$$

Thus $A^{\otimes n}/\varphi \cong \bigotimes_{i=1}^{k} A_i^{\otimes n_i}/\Phi_{A_i}$ as desired. □

Corollary 7.5. *If a polynomial $f(x) \in R[x]$ is irreducible, then every $G \subseteq \mathrm{S}_n$ for which $R[x]/(f(x))$ has a G-closure datum acts transitively on $\{1, \dots, n\}$.*

Remark 7.6. Recall the question of whether the minimal closure data for a given algebra are isomorphic. This holds for all free quadratic R-algebras if and only if R is a domain, as we claimed in Remark 3.4. Namely, suppose that R is a domain and A is a free quadratic R-algebra. Then $A/R \cong \bigwedge^2 A$ is also free, so we can choose a basis for A of the form $\{1, a\}$, so that $A \cong R[x]/(x^2 - bx + c)$ for some $b, c \in R$. If the S_2-closure datum of A is minimal, then it is the unique closure datum for A over R, so the minimal closure data are trivially isomorphic. Otherwise, there is a $1 = \mathrm{S}_1 \times \mathrm{S}_1$-closure datum for A over R, corresponding to a factorization of $x^2 - bx + c$ into linear factors over R. If we have two such factorizations

$$x^2 - bx + c = (x-r)(x-s) = (x-t)(x-u),$$

then we have $rs = c = tu = t(b-t) = t(r+s-t)$, so $(r-t)(s-t) = 0$. So since R is a domain, we must have $r = t$ (and $s = u$) or $s = t$ (and $r = u$); either way, the two factorizations correspond to isomorphic closure data.

Conversely, if $rs = 0$ in R with r and s nonzero, then we have

$$(x-r)(x-s) = x\bigl(x-(r+s)\bigr),$$

factorizations which correspond to two non-isomorphic 1-closure data for the algebra $R[x]/(x^2-(r+s)x)$ over R.

Remark 7.7. More generally, isomorphic $\mathrm{S}_{n_1} \times \cdots \times \mathrm{S}_{n_k}$-closure data correspond to factorizations that differ only in the order of factors of the same degree. The group of such reorderings is exactly the quotient by $\mathrm{S}_{n_1} \times \cdots \times \mathrm{S}_{n_k}$ of its normalizer in S_n—see Remark 3.6.

7.2. Parameterizing G-closure data

Note that in the case of monogenic algebras, Theorem 6.5 gives us the following criterion for a monogenic rank-n algebra to have an A_n-closure datum:

Theorem 7.8. *Let R be a ring in which 2 is a primoid non-zerodivisor, and let $A = R[x]/(f(x))$ be a monogenic rank-n R-algebra. Then A_n-closure data for A over R correspond to square roots of the discriminant of f.*

We wish to produce similar parameterizations of monogenic algebras' closure data for other groups than A_n, where closure data for A over R correspond to solutions in R of certain polynomial equations whose coefficients depend on A. The main goal of this section is Lemma 7.13, which abstractly allows one to produce such a parameterization whenever the pair (ring R, group G) forms a "benign pair," to be defined below.

Recall that an R-module M is called *faithful* if no nonzero element of R acts as zero on M, and that an R-algebra B is faithful as an R-module if and only if the structure map $R \to B$ is injective.

Definition 7.9. Let R be a ring and G a subgroup of S_n for a fixed natural number n. We say that the pair (R, G) is *benign* if for every R-algebra B with an action of G by R-algebra homomorphisms, and for every R-algebra homomorphism $B^G \to R$, the resulting tensor product $B \otimes_{B^G} R$ is a faithful R-algebra.

Lemma 7.10. *Either of the following two conditions is sufficient for the pair (R, G) to be a benign pair:*

(1) *R is reduced.*
(2) *$|G|$ is a non-zerodivisor in R.*

Proof. Recall that given a homomorphism of rings $f : A \to B$, the corresponding map of schemes $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective if and only if the kernel of f consists of nilpotents. Then if R is reduced, injectivity of $R \to B \otimes_{B^G} R$ is equivalent to surjectivity of $\operatorname{Spec}(B \otimes_{B^G} R) \to \operatorname{Spec}(R)$. But this is guaranteed by surjectivity of $\operatorname{Spec}(B) \to \operatorname{Spec}(B^G)$, because $B^G \to B$ is injective and surjectivity of morphisms of schemes is preserved under base change.

Now suppose instead that $|G|$ is a non-zerodivisor in R. Then consider the B^G-module homomorphism $B \to B^G$ sending $b \mapsto \sum_{g \in G} g.b$. On elements b that are already fixed by G, each term in the sum is just b again, so the composite

$$B^G \to B \to B^G$$

is multiplication by $|G|$. After base changing along the given R-algebra homomorphism $B^G \to R$, then, we find that the composite

$$R \to B \otimes_{B^G} R \to R$$

is multiplication by $|G|$, which is injective since $|G|$ is a non-zerodivisor. Therefore the map $R \to B \otimes_{B^G} R$ must be injective as well. □

If (R, G) is a benign pair with $G \subseteq \mathrm{S}_n$, then for every rank-n R-algebra A with a G-closure datum φ, we find that the homomorphism $R \to A^{\otimes n}/\varphi$ is injective. Not every pair is benign, however, and not every closure algebra is faithful:

Example 7.11. Let $R = \mathbb{Z}/(9)$ and $G = \mathrm{A}_3$. Then the R-algebra $A = R[x]/(x^3)$ has a G-closure datum φ for which the map $R \to A^{\otimes 3}/\varphi$ sends 3 to 0.

Namely, since 2 is a unit in R we have a correspondence between A_3-closure data for A over R and square roots in R of the discriminant of A, which vanishes. If we choose the square root 3 of 0 in R, the corresponding A_3-closure datum sends $\gamma(1, x, x^2) - \gamma(1, x^2, x)$ to $3 \in R$, and since the sum $\gamma(1, x, x^2) + \gamma(1, x^2, x)$ must be sent to zero by Example 6.1, we find that $\gamma(1, x, x^2) \mapsto 6$ and $\gamma(1, x^2, x) \mapsto 3$.

Then in the closure algebra $A^{\otimes 3}/\varphi$, we find that

$$\begin{aligned}\gamma(1, x^2, x) &= 1 \otimes x^2 \otimes x + x^2 \otimes x \otimes 1 + x \otimes 1 \otimes x^2 \\ &= (1 \otimes x^2 \otimes 1)(-x \otimes 1 \otimes 1 - 1 \otimes x \otimes 1) \\ &\quad + x^2 \otimes x \otimes 1 \\ &\quad + (x \otimes 1 \otimes 1)(-x \otimes 1 \otimes 1 - 1 \otimes x \otimes 1)^2,\end{aligned}$$

using the relation $x \otimes 1 \otimes 1 + 1 \otimes x \otimes 1 + 1 \otimes 1 \otimes x = \operatorname{Tr}_A(x) = 0$,

$$\begin{aligned}&= -x \otimes x^2 \otimes 1 + x^2 \otimes x \otimes 1 + x \otimes x^2 \otimes 1 + 2x^2 \otimes x \otimes 1 \\ &= 3x^2 \otimes x \otimes 1.\end{aligned}$$

Therefore $3 = 3x^2 \otimes x \otimes 1$. Multiplying both sides by $x^2 \otimes x \otimes 1$, we find that $3x^2 \otimes x \otimes 1 = 0$. Thus by transitivity, $3 = 0$ in the closure algebra.

Remark 7.12. Even though the pair (R, S_n) is not always benign, the S_n-closure of a rank-n R-algebra A is always faithful. If we use the Ferrand homomorphism to equip the R-module $\bigwedge^n A$ with an $(A^{\otimes n})^{\mathrm{S}_n}$-module structure, then the defining surjection $A^{\otimes n} \to \bigwedge^n A$ is actually a $(A^{\otimes n})^{\mathrm{S}_n}$-module homomorphism by [4, Lem. 4.2]. Then tensoring with R over $(A^{\otimes n})^{\mathrm{S}_n}$ gives a surjection

$$A^{\otimes n}/\Phi_A \;=\; A^{\otimes n} \bigotimes_{(A^{\otimes n})^{\mathrm{S}_n}} R \;\twoheadrightarrow\; \textstyle\bigwedge^n A \displaystyle\bigotimes_{(A^{\otimes n})^{\mathrm{S}_n}} R \cong \textstyle\bigwedge^n A.$$

Since $\bigwedge^n A$ is a locally free R-module of rank 1, it is faithful, and therefore $A^{\otimes n}/\Phi_A$ must be too.

But supposing that the pair (R, G) *is* benign, then we obtain the following parameterization of G-closure data for monogenic R-algebras:

Lemma 7.13. *Let R be a ring and A be a monogenic R-algebra with generator a. Given a closure datum (G, φ) for A over R, we may compose φ with the projection $(R[x]^{\otimes n})^G \to (A^{\otimes n})^G$ to obtain an R-algebra homomorphism $(R[x]^{\otimes n})^G \to R$ such that $e_k(x) \mapsto s_k(a)$ for all $k \in \{1, \ldots, n\}$.*

If G is a subgroup of S_n for which (R, G) is benign, then this operation forms a one-to-one correspondence between G-closure data for A over R and such homomorphisms $(R[x]^{\otimes n})^G \to R$.

In particular, if we can present $(R[x]^{\otimes n})^G$ as an algebra over $(R[x]^{\otimes n})^{\mathrm{S}_n}$, then G-closure data for A over R will correspond to solutions in R of a list of polynomial equations, the way A_n-closure data correspond to square roots of the discriminant. In the next section, we will do just that in the case $G = \mathrm{D}_4 = \langle (13), (1234) \rangle \subseteq \mathrm{S}_4$. Since the publication of this argument in the author's PhD thesis, Riccardo Ferrario has produced similar results in [7] for the cases $\mathrm{V}_4 = \langle (12)(34), (13)(24) \rangle$ and $\mathrm{C}_4 = \langle (1234) \rangle$. The parameterization of V_4-closure data is very similar to the one that follows for D_4—they correspond to *splittings* of the cubic resolvent instead of roots—but so far there is no nice interpretation for the parameterization of C_4-closure data.

Proof of Lemma 7.13. Suppose that (G, φ) is a closure datum for A over R. Then under the composite $(R[x]^{\otimes n})^G \to (A^{\otimes n})^G \to R$, we have $e_k(x) \mapsto e_k(a) \mapsto s_k(a)$.

Now conversely, suppose that $(R[x]^{\otimes n})^G \to R$ is an R-algebra homomorphism sending $e_k(x)$ to $s_k(a)$ for all $k \in \{1, \ldots, n\}$, and use the hypothesis that (R, G) is a benign pair to obtain that the resulting tensor product

$$T := R[x]^{\otimes n} \bigotimes_{(R[x]^{\otimes n})^G} R$$

is a faithful R-algebra. We will fill in the two dashed arrows in the following commutative diagram:

$$\begin{tikzcd}
(R[x]^{\otimes n})^G \arrow[r, two heads] \arrow[d, hook] \arrow[rr, bend left] & (A^{\otimes n})^G \arrow[r, dashed] \arrow[d, hook] & R \arrow[d, hook] \\
R[x]^{\otimes n} \arrow[r, two heads] \arrow[rr, bend right, two heads] & A^{\otimes n} \arrow[r, dashed] & T
\end{tikzcd} .$$

For the existence of the lower dashed arrow, notice that for each $i \in \{1, \dots, n\}$, the image of $\mathrm{p}_a(x^{(i)})$ under the map $R[x]^{\otimes n} \to T$ is

$$\begin{aligned}\mathrm{p}_a(x^{(i)}) &= \sum_{k=0}^{n} (-1)^k s_k(a)(x^{(i)})^{n-k} \\ &= \sum_{k=0}^{n} (-1)^k e_k(x)(x^{(i)})^{n-k} = \prod_{j=1}^{n} (x^{(i)} - x^{(j)}) = 0,\end{aligned}$$

so each component of the map factors through the projection

$$R[x] \twoheadrightarrow A \cong R[x]/(\mathrm{p}_a(x)).$$

Then the existence of the upper dashed arrow follows elementarily: we have the composite $(A^{\otimes n})^G \hookrightarrow A^{\otimes n} \to T$, and by the commutativity of the rest of the diagram its image is contained in the subring R. Thus we obtain the existence of a (necessarily unique) map $(A^{\otimes n})^G \to R$ commuting with the maps from $(R[x]^{\otimes n})^G$. In particular, this map is a G-closure datum for A over R, because $e_k(x)$ in $(R[x]^{\otimes n})^G$ is sent to $e_k(a)$ in $(A^{\otimes n})^G$ and $s_k(a)$ in R. □

7.3. D$_4$-closure data

A classical result of Galois theory is that the Galois group of a separable irreducible quartic polynomial

$$f(x) = x^4 - s_1 x^3 + s_2 x^2 - s_3 x + s_4$$

is contained in the permutation group $\mathrm{D}_4 = \langle (13), (1234) \rangle \subseteq \mathrm{S}_4$ if and only if that polynomial's *cubic resolvent*

$$m(y) = y^3 - (s_2)y^2 + (s_1 s_3 - 4s_4)y - (s_1^2 s_4 - 4s_2 s_4 + s_3^2)$$

has a root in the base field. In this section, we prove the following generalization:

Theorem 7.14 (see Theorem 1.6)**.** *Let R be a ring and let $A = R[x]/(f(x))$ be a monogenic rank-4 R-algebra. Then D_4-closure data for A over R correspond to roots of f's cubic resolvent in R.*

We will do so by first giving generators and relations for $(R[x]^{\otimes 4})^{\mathrm{D}_4}$ as an algebra over $(R[x]^{\otimes 4})^{\mathrm{S}_4}$, and then using this presentation to show that if R is reduced, then D_4-closure data of $R[x]/(f(x))$ correspond to roots in R of the cubic resolvent of $f(x)$. Finally, we will carefully lift the condition that R be reduced.

Lemma 7.15. *The ring $(\mathbb{Z}[x]^{\otimes 4})^{\mathrm{D}_4}$ is a free $(\mathbb{Z}[x]^{\otimes 4})^{\mathrm{S}_4}$-module with basis $\{1, \Lambda, \Lambda^2\}$, where $\Lambda = x^{(1)}x^{(3)} + x^{(2)}x^{(4)}$.*

Proof. First, we fix some helpful notation. We will write x_1, x_2, x_3, x_4 for the four conjugates $x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}$ in $R[x]^{\otimes 4}$, identifying the latter R-algebra with $R[x_1, x_2, x_3, x_4]$. If $p \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{\mathrm{D}_4}$, then we denote the polynomial $(14).p =$

$(23).p$ in $\mathbb{Z}[x_1,x_2,x_3,x_4]$ by p', and the polynomial $(12).p = (34).p$ by p''. Each transposition permutes $\{p,p',p''\}$:

$$\begin{gathered}(23) \text{ and } (14) \text{ interchange } p \leftrightarrow p' \text{ and fix } p'',\\ (12) \text{ and } (34) \text{ interchange } p \leftrightarrow p'' \text{ and fix } p',\\ (13) \text{ and } (24) \text{ interchange } p' \leftrightarrow p'' \text{ and fix } p.\end{gathered}$$

If $p \in \mathbb{Z}[x_1,x_2,x_3,x_4]^{\mathrm{D}_4}$ and any two of $\{p,p',p''\}$ are equal, then we have $p \in \mathbb{Z}[x_1,x_2,x_3,x_4]^{\mathrm{S}_4}$. In particular, Λ, Λ', and Λ'' are all distinct:

$$\begin{aligned}\Lambda - \Lambda' &= (x_1-x_4)(x_3-x_2),\\ \Lambda - \Lambda'' &= (x_1-x_2)(x_3-x_4),\\ \Lambda' - \Lambda'' &= (x_1-x_3)(x_2-x_4).\end{aligned}$$

First, we show that 1, Λ, and Λ^2 are $\mathbb{Z}[x_1,x_2,x_3,x_4]^{\mathrm{S}_4}$-linearly independent. Suppose $q\Lambda^2+r\Lambda+s=0$, with $q,r,s \in \mathbb{Z}[x_1,x_2,x_3,x_4]^{\mathrm{S}_4}$. Then $0 = q\Lambda'^2+r\Lambda'+s = q\Lambda''^2+r\Lambda''+s$, so

$$0 = \frac{q(\Lambda'^2-\Lambda''^2)+r(\Lambda'-\Lambda'')}{\Lambda'-\Lambda''} = q(\Lambda'+\Lambda'')+r = -q\Lambda + (r+q(\Lambda+\Lambda'+\Lambda'')).$$

Therefore $0 = -q\Lambda' + (r+q(\Lambda+\Lambda'+\Lambda'')) = -q\Lambda'' + (r+q(\Lambda+\Lambda'+\Lambda''))$, so $q(\Lambda'-\Lambda'')=0$, and $q=0$. Then $0 = q(\Lambda'+\Lambda'')+r$ implies that $r=0$, and $0 = q\Lambda^2+r\Lambda+s$ implies that $s=0$.

To show that the elements 1, Λ, and Λ^2 also generate $\mathbb{Z}[x_1,x_2,x_3,x_4]^{\mathrm{D}_4}$ as a $\mathbb{Z}[x_1,x_2,x_3,x_4]^{\mathrm{S}_4}$-module, we use the following observation:

If $p \in \mathbb{Z}[x_1,x_2,x_3,x_4]^{\mathrm{D}_4}$, then $p' \equiv p''$ modulo either (x_1-x_3) or (x_2-x_4), so $p'-p''$ must contain factors of both (x_1-x_3) and (x_2-x_4). Since $\mathbb{Z}[x_1,x_2,x_3,x_4]$ is a unique factorization domain, we find that $p'-p''$ is a multiple of $\Lambda'-\Lambda''$. In fact, the ratio $\rho = \frac{p'-p''}{\Lambda'-\Lambda''}$ also belongs to $\mathbb{Z}[x_1,x_2,x_3,x_4]^{\mathrm{D}_4}$, since it is fixed by (13) and $(1234) = (12)(23)(34)$:

$$\rho = \frac{p'-p''}{\Lambda'-\Lambda''} \xmapsto{(13)} \frac{p''-p'}{\Lambda''-\Lambda'} = \rho,$$

$$\rho = \frac{p'-p''}{\Lambda'-\Lambda''} \xmapsto{(34)} \frac{p'-p}{\Lambda'-\Lambda} \xmapsto{(23)} \frac{p-p'}{\Lambda-\Lambda'} \xmapsto{(12)} \frac{p''-p'}{\Lambda''-\Lambda'} = \rho.$$

Thus we can apply the same procedure to ρ as we did to p; set

$$q = -\frac{\rho'-\rho''}{\Lambda'-\Lambda''}.$$

We claim that $q \in \mathbb{Z}[x_1,x_2,x_3,x_4]^{\mathrm{S}_4}$. In fact, we can write

$$\begin{aligned}-q &= \frac{\rho'-\rho''}{\Lambda'-\Lambda''}\\ &= \frac{\dfrac{p-p''}{\Lambda-\Lambda''} - \dfrac{p'-p}{\Lambda'-\Lambda}}{\Lambda'-\Lambda''}\\ &= \frac{(p-p'')(\Lambda-\Lambda')-(p-p')(\Lambda-\Lambda'')}{(\Lambda-\Lambda')(\Lambda-\Lambda'')(\Lambda'-\Lambda'')}\\ &= \frac{(p-p')\Lambda''+(p''-p)\Lambda'+(p'-p'')\Lambda}{(\Lambda-\Lambda')(\Lambda-\Lambda'')(\Lambda'-\Lambda'')}.\end{aligned}$$

Every transposition changes the sign of both the numerator and the denominator of the right-hand side, so q is fixed by the action of S_4. Now set

$$r = \rho - q(\Lambda' + \Lambda'') \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{\mathrm{D}_4}.$$

Again, we claim that $r \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{\mathrm{S}_4}$, and calculate

$$\begin{aligned} r &= \frac{p' - p''}{\Lambda' - \Lambda''} + \frac{((p - p')\Lambda'' + (p'' - p)\Lambda' + (p' - p'')\Lambda)(\Lambda' + \Lambda'')}{(\Lambda - \Lambda')(\Lambda - \Lambda'')(\Lambda' - \Lambda'')} \\ &= \frac{(p - p')\Lambda''^2 + (p'' - p)\Lambda'^2 + (p' - p'')\Lambda^2}{(\Lambda - \Lambda')(\Lambda - \Lambda'')(\Lambda' - \Lambda'')}. \end{aligned}$$

Once again, every transposition changes the sign of both numerator and denominator, so r is fixed by S_4. Finally, set

$$s = p - q\Lambda^2 - r\Lambda \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{\mathrm{D}_4}.$$

Again, we claim that $s \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{\mathrm{S}_4}$:

$$\begin{aligned} s &= p - q\Lambda^2 - r\Lambda \\ &= p + \frac{(p - p')\Lambda'' + (p'' - p)\Lambda' + (p' - p'')\Lambda}{(\Lambda - \Lambda')(\Lambda - \Lambda'')(\Lambda' - \Lambda'')}\Lambda^2 \\ &\quad - \frac{(p - p')\Lambda''^2 + (p'' - p)\Lambda'^2 + (p' - p'')\Lambda^2}{(\Lambda - \Lambda')(\Lambda - \Lambda'')(\Lambda' - \Lambda'')}\Lambda \\ &= \frac{p(\Lambda' - \Lambda'')\Lambda'\Lambda'' + p'(\Lambda'' - \Lambda)\Lambda\Lambda'' + p''(\Lambda - \Lambda')\Lambda\Lambda'}{(\Lambda - \Lambda')(\Lambda - \Lambda'')(\Lambda' - \Lambda'')}. \end{aligned}$$

Once again, the numerator and denominator each change sign under the action of any transposition, so s is fixed by $\mathbb{Z}[x_1, x_2, x_3, x_4]^{\mathrm{S}_4}$. Thus we have written $p = q\Lambda^2 + r\Lambda + s$ with $q, r, s \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{\mathrm{S}_4}$, as desired. □

Corollary 7.16. *Let R be a ring. Then*

$$(R[x]^{\otimes 4})^{\mathrm{D}_4} \cong (R[x]^{\otimes 4})^{\mathrm{S}_4}[y]/((y - \Lambda)(y - \Lambda')(y - \Lambda''))$$

as $(R[x]^{\otimes 4})^{\mathrm{S}_4}$-algebras.

Proof. The isomorphism from right to left is given by $y \mapsto \Lambda$. This homomorphism is bijective since it maps the $(R[x]^{\otimes 4})^{\mathrm{S}_4}$-module basis $\{1, y, y^2\}$ to the module basis $\{1, \Lambda, \Lambda^2\}$. □

Proof of Theorem 7.14. First we prove this in the case that R is reduced, so that (R, D_4) is a benign pair. Then by Lemma 7.13, isomorphism classes of D_4-closures of A over R correspond to R-algebra homomorphisms $(R[x]^{\otimes 4})^{\mathrm{D}_4} \to R$ sending $e_k(x) \mapsto s_k$. If we denote the R-algebra map $(R[x]^{\otimes 4})^{\mathrm{S}_4} \to R$ sending $e_k(x) \mapsto s_k$ by φ, then such homomorphisms in turn correspond to R-algebra homomorphisms to R from $(R[x]^{\otimes 4})^{\mathrm{D}_4} \otimes_{(R[x]^{\otimes 4})^{\mathrm{S}_4}} R$, which by Corollary 7.16 is

$$\begin{aligned} &R[y]/\big(y^3 - \varphi(\Lambda + \Lambda' + \Lambda'')y^2 + \varphi(\Lambda\Lambda' + \Lambda\Lambda'' + \Lambda'\Lambda'')y - \varphi(\Lambda\Lambda'\Lambda'')\big) \\ &\quad = R[y]/\big(y^3 - (s_2)y^2 + (s_1 s_3 - 4s_4)y - (s_1^2 s_4 - 4s_2 s_4 + s_3^2)\big), \end{aligned}$$

the cubic resolvent algebra.

One way of phrasing the conclusion of Lemma 7.13 is that every R-algebra homomorphism

$$(R[x]^{\otimes 4})^{\mathrm{D}_4} \bigotimes_{(R[x]^{\otimes 4})^{\mathrm{S}_4}} R \to R$$

factors through the quotient map

$$(R[x]^{\otimes 4})^{\mathrm{D}_4} \bigotimes_{(R[x]^{\otimes 4})^{\mathrm{S}_4}} R \twoheadrightarrow (A^{\otimes 4})^{\mathrm{D}_4} \bigotimes_{(A^{\otimes 4})^{\mathrm{S}_4}} R$$

to give a D_4-closure datum $(A^{\otimes 4})^{\mathrm{D}_4} \otimes_{(A^{\otimes 4})^{\mathrm{S}_4}} R \to R$. We now show that this holds even if R is not reduced.

Indeed, consider the universal monogenic rank-4 algebra $R_0 \to A_0$ given by

$$\begin{aligned} R_0 &= \mathbb{Z}[S_1, S_2, S_3, S_4], \\ A_0 &= R_0[x]/(x^4 - S_1x^3 + S_2x^2 - S_3x + S_4), \end{aligned}$$

with the S_i formal indeterminates. Then the algebra $R \to A$ is the base change of $R_0 \to A_0$ along the ring homomorphism $R_0 \to R$ sending each S_i to s_i.

What we have already shown is that if R is any *reduced* R_0-algebra, then every R_0-algebra homomorphism

$$(R_0[x]^{\otimes 4})^{\mathrm{D}_4} \bigotimes_{(R_0[x]^{\otimes 4})^{\mathrm{S}_4}} R_0 \to R$$

factors through the quotient map

$$(R_0[x]^{\otimes 4})^{\mathrm{D}_4} \bigotimes_{(R_0[x]^{\otimes 4})^{\mathrm{S}_4}} R_0 \twoheadrightarrow (A_0^{\otimes 4})^{\mathrm{D}_4} \bigotimes_{(A_0^{\otimes 4})^{\mathrm{S}_4}} R_0.$$

In particular, we can take R itself to be the tensor product

$$\begin{aligned} R :=\ & (R_0[x]^{\otimes 4})^{\mathrm{D}_4} \bigotimes_{(R_0[x]^{\otimes 4})^{\mathrm{S}_4}} R_0 \\ &\cong R_0[y]/\big(y^3 - (S_2)y^2 + (S_1S_3 - 4S_4)y - (S_1^2S_4 - 4S_2S_4 + S_3^2)\big), \end{aligned}$$

which is reduced because $y^3 - (S_2)y^2 + (S_1S_3 - 4S_4)y - (S_1^2S_4 - 4S_2S_4 + S_3^2)$ is an irreducible element of the polynomial ring $\mathbb{Z}[S_1, S_2, S_3, S_4, y]$—if it were not, every cubic resolvent would have a root, and every separable quartic polynomial would have Galois group contained in D_4.

Therefore $\mathrm{id}_R\colon R \to R$ factors through R's quotient $(A_0^{\otimes 4})^{\mathrm{D}_4} \otimes_{(A_0^{\otimes 4})^{\mathrm{S}_4}} R_0$, so the quotient map must in fact be an isomorphism:

$$(R_0[x]^{\otimes 4})^{\mathrm{D}_4} \bigotimes_{(R_0[x]^{\otimes 4})^{\mathrm{S}_4}} R_0 \cong (A_0^{\otimes 4})^{\mathrm{D}_4} \bigotimes_{(A_0^{\otimes 4})^{\mathrm{S}_4}} R_0.$$

Changing base to a general ring R, then, we find that

$$(R[x]^{\otimes 4})^{\mathrm{D}_4} \bigotimes_{(R[x]^{\otimes 4})^{\mathrm{S}_4}} R \cong (A^{\otimes 4})^{\mathrm{D}_4} \bigotimes_{(A^{\otimes 4})^{\mathrm{S}_4}} R,$$

so the conclusion of Lemma 7.13 holds even if R is not reduced, and D_4-closure data for $R[x]/(f(x))$ correspond to roots of f's cubic resolvent. □

References

[1] M. Bhargava, *Higher composition laws* III: *The parametrization of quartic rings*, Ann. Math. **159** (2004), 1329–1360.

[2] M. Bhargava, M. Satriano, *On a notion of "Galois closure" for extensions of rings*, J. Eur. Math. Soc. **16** (2014), 1881–1913.

[3] O. Biesel, *Galois closures for rings*, PhD thesis, Princeton University, Princeton, NJ, 2013.

[4] O. Biesel, A. Gioia, *A new discriminant algebra construction*, Documenta Math. **21** (2016), 1051–1088.

[5] P. Deligne, *Cohomologie à supports propres*, in: *Théorie des Topos et Cohomologie Etale de Schémas*, Lecture Notes in Mathematics, Vol. 305, Springer, Berlin, 1973, pp. 250–480.

[6] D. Ferrand, *Un foncteur norme*, Bull. Soc. Math. France **126** (1998), 1–49.

[7] R. Ferrario, *Galois closures for monogenic degree-*4 *extensions of rings*, Master's thesis, Leiden University, the Netherlands, 2014.

[8] H. W. Lenstra, *Galois theory for schemes*, Leiden University course notes, available at `http://websites.math.leidenuniv.nl/algebra/GSchemes.pdf`, 2008.

[9] N. Roby, *Lois polynomes et lois formelles en théorie des modules*, Ann. Sci. École Norm. Sup. **80** (1963), 213–348.

[10] N. Roby, *Lois polynômes multiplicatives universelles*, C. R. Acad. Sci. Paris Sér. A-B **290** (1980), A869–A871.

[11] F. Vaccarino, *Homogeneous multiplicative polynomial laws are determinants*, J. Pure Appl. Algebra **213** (2009), 1283–1289.

[12] F. Vaccarino, *Moduli of linear representations, symmetric products and the noncommutative Hilbert scheme*, in: *Geometric Methods in Representation Theory*, II (M. Brion, ed.); Séminaires et Congrès 24-II (2012), pp. 435–456.