From the holdings of the Department of Special Collections , Princeton University Library, Princeton, NJ

These documents are either in the public domain, or can only be used for educational and research purposes (Fair use) as per U.S. Copyright law (text below). By accessing this file, all users agree that their use falls in the public domain or within fair use as defined by the copyrightlaw. We do not charge any permission or usage fees for the publication of images of material inour collections, including those provided by Princeton University Library, via our website, catalog, or directly from staff.For more information regarding copyright, credit, and citation please review the information onthe Copyright, Credit and Citation Guidelines page of our website.
https://library.princeton.edu/special-collections/policies/copyright-credit-and-citation-guidelines. If you have any questions, including how to order higher-quality images from the collection, contact Special Collections Public Services via our Ask Us! Form. https://library.princeton.edu/special-collections/ask-us

---

Doctoral Dissertations, 2011-2026 Mathematics

2013

Galois Closures for Rings

Biesel, Owen Douglass

Princeton, NJ : Princeton University

---

http://arks.princeton.edu/ark:/88435/dsp01dz010q138

U.S. Copyright law: The copyright law of the United States (Title 17, §108, United States Code) governs the making of photocopies or other reproductions of copyrighted material. Under certain conditions specified in the law, libraries and archives are authorized to furnish a photocopy or other reproduction. One of these specified conditions is that the photocopy or reproduction is not to be used for any purpose other than private study, scholarship, or research. If a user makes a request for, or later uses, a photocopy or reproduction for purposes in excess of fair use that user may be liable for copyright infringement. This institution reserves the right to refuse to accept a copying order if, in its judgment, fulfillment of the order would involve a violation of copyright law. https://www.copyright.gov/title17/title17.pdf

Galois Closures for Rings

Owen Biesel

A Dissertation
Presented to the Faculty
of Princeton University
in Candidacy for the Degree
of Doctor of Philosophy

Recommended for Acceptance
by the Department of
Mathematics
Adviser: Manjul Bhargava

June 2013

© Copyright by Owen Biesel, 2013.

All Rights Reserved

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 of A over R is an $A^{\otimes n}$-algebra B equipped with an R-algebra homomorphism $(A^{\otimes n})^G \to R$ satisfying certain properties. Being a G-closure commutes with base change, and reduces to being the normal closure of a finite separable field extension if G is the corresponding Galois group. We describe G-closures of finite étale algebras over connected rings in terms of the corresponding finite sets with continuous actions by the fundamental group. If 2 is invertible, then A_n-closures of free extensions correspond to square roots of the discriminant, and if 2 is a non-zerodivisor, then D_4-closures of quartic monogenic extensions correspond to roots of the resolvent cubic.

Acknowledgements

First, I would like to thank my Ph.D. advisor, Manjul Bhargava. His words to me were filled with encouraging suggestions and enthusiasm over my progress, and I always left his office feeling that my work was valuable and important.

I have also received overwhelming encouragement from my family and friends, who never doubted my ability to complete this project—especially my fiancée, Clara Giebel, who has stuck by me from its beginning to its end. Special thanks for helping me through difficult times go to Peter and Kelly Leibensperger; Jennifer and Joey Li; Benjamin and Sarah (and Daniel) Bratton; and my parents Douglass and Elizabeth.

I would also like to thank Kevin Wilson, Arul Shankar, Wei Ho, and Alberto Gioia for numerous helpful conversations. In addition, I would like to thank Peter Stevenhagen, Lenny Taelman, and Hendrik Lenstra of Leiden University, with whom I also had several fruitful discussions, for generously inviting me for what became my single most productive week of research to date.

S.D.G.

Contents

Abstract iii

Acknowledgements iv

1 Introduction **1**

1.1 What is the Galois closure of a ring extension? 1

1.2 Notation and conventions 10

2 Existence and uniqueness of S_n-closures **14**

2.1 G-closures and normative homomorphisms 15

2.2 Generators for $(A^{\otimes d})^{S_d}$ when A is locally free 17

2.3 The determinant as a polynomial law 21

3 The interactions of G-closures **29**

3.1 Base extension of G-closures 29

3.2 Induction of G-closures 31

3.3 Universal algebras for G-closures 32

4 G-closures of étale extensions **34**

4.1 G-closures of trivial étale algebras 34

4.2 G-closures of étale extensions are étale 40

4.3 G-closures and fundamental groups 42

4.4 G-closures of field extensions 45

5 G-closures of monogenic extensions **48**

5.1 G-closures of extensions with degree ≤ 2 49

5.2 G-closures for intransitive G 51

5.3 An alternative description of G-closures 55

5.4 A_n-closures 58

5.5 D_4-closures 61

6 A_n-closures revisited **67**

6.1 A_n-closures and discriminants 68

6.2 A_n-closures and the quadratic criterion 73

A Appendix **78**

A.1 Multisets 78

A.2 Polynomial laws 80

A.3 Polynomial laws for locally free modules 87

A.4 Algebras and multiplicative polynomial laws 99

Chapter 1

Introduction

1.1 What is the Galois closure of a ring extension?

In this thesis, we ask the question: What is a natural analogue of the familiar Galois closure operation for separable field extensions, that holds for some class of "ring extensions"? M. Bhargava and M. Satriano give a partial answer in [2]; their "S_n-closure" is a functor that commutes with base change and reduces to the Galois closure for finite separable field extensions with Galois group S_n. The paper closes by asking whether similar "G-closures" exist for other permutation groups $G \subseteq S_n$. We answer Yes.

To begin, we review Galois closures for fields from a slightly unusual perspective. If L is a separable extension of a field K with separable closure $\bar{K}$, we can define the Galois closure N of L to be the minimal subfield of $\bar{K}$ containing the images of all field homomorphisms $L \to \bar{K}$. The extension of K-algebras $L \subseteq N$ enjoys the following properties:

- If $n = \dim_K L$, then there are exactly n K-algebra homomorphisms from L to N. (In the following, we will denote the n-element set of them by $S_{L/K} := \mathrm{Hom}_K(L, N)$.)

- The Galois group $G = \mathrm{Gal}(N/K) := \mathrm{Aut}_K(N)$ permutes these homomorphisms faithfully, realizing G as a permutation group, a subgroup of $\mathrm{Bij}(S_{L/K}, S_{L/K})$.

- Each element of N fixed by the action of G belongs to the subfield K.

We can neatly combine these three facts in the following way: first fix an ordering of $S_{L/K}$ as $\{\pi_1, \ldots, \pi_n\}$, so that $S_{L/K}$ is identified with the set $\{1, \ldots, n\}$, and G with a subgroup of S_n. Then the n homomorphisms $\pi_1, \ldots, \pi_n : L \to N$ may be compiled into a single K-algebra homomorphism $\Phi : L^{\otimes n} \to N$ sending $\ell^{(i)} \mapsto \pi_i(\ell)$, where $\ell^{(i)}$ is the pure tensor $1 \otimes \ldots \otimes 1 \otimes \ell \otimes 1 \otimes \ldots \otimes 1$, with the ℓ in the ith tensor factor. If v is an element of $L^{\otimes n}$ fixed by the permutation action of G on the tensor factors, then its image in N is fixed by the automorphism action of G, and is hence an element of K. Thus the homomorphism $\Phi : L^{\otimes n} \to N$ restricts to a K-algebra homomorphism $\varphi : (L^{\otimes n})^G \to K$, where $(L^{\otimes n})^G \subseteq L^{\otimes n}$ is the subalgebra of elements fixed by the action of G.

We can even say where φ sends certain elements of $(L^{\otimes n})^G$. For each element $\ell \in L$, denote the kth elementary symmetric polynomial in $\ell^{(1)}, \ldots, \ell^{(n)}$ by $e_k(\ell)$. Then $\varphi(e_k(\ell))$ is the kth elementary symmetric polynomial in the n conjugates $\pi_1(\ell)$, $\ldots$, $\pi_n(\ell)$ 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 with entries in K, for each choice of K-basis for L. The characteristic polynomial of M is independent of this choice of basis, so its coefficients are elements of K that depend only on ℓ. Write this characteristic polynomial as

$$\det(\lambda I - M) = \lambda^n - s_1(\ell)\lambda^{n-1} + s_2(\ell)\lambda^{n-2} - \ldots + (-1)^n s_n(\ell).$$

Then the homomorphism $\varphi : (L^{\otimes n})^G \to K$ sends $e_k(\ell)$ to $s_k(\ell)$.

Now consider the following diagram:

$$\begin{array}{ccc} (L^{\otimes n})^G & \xrightarrow{\varphi} & K \\ \downarrow & & \downarrow \\ L^{\otimes n} & \xrightarrow{\Phi} & N \end{array}$$

This square commutes because φ is the restriction of Φ. In fact, the square is a tensor product diagram, that is, $L^{\otimes n} \bigotimes_{(L^{\otimes n})^G} K \cong N$.

This isomorphism is a special case of our first theorem. A bit of terminology will make this theorem simpler to state: Let L be a degree-n extension of a field K, and let f be a K-algebra homomorphism whose domain is a subalgebra of $L^{\otimes n}$. Call f *normative* if $f(e_k(\ell))$ is defined and equals $s_k(\ell)$ for each element $\ell \in L$ and $k \in \{1, \ldots, n\}$. Then, for example, the above homomorphisms $\Phi : L^{\otimes n} \to N$ and $\varphi : (L^{\otimes n})^G \to K$ are both normative.

Theorem 1. *Let K be a field, and let L be a degree-n separable field extension of K with Galois closure N and Galois group $G = \mathrm{Gal}(N/K)$. Regard G as a group of permutations of $S_{L/K}$, and let H be a subgroup of S_n. Then there exists a normative K-algebra homomorphism $f : (L^{\otimes n})^H \to K$ if and only if H contains G for some identification of $\{1, \ldots, n\}$ with $S_{L/K}$. For each such f, the resulting tensor product is isomorphic to a power of N as a K-algebra: $L^{\otimes n} \bigotimes_{(L^{\otimes n})^H} K \cong N^{|H|/|G|}$.*

This theorem motivates a generalization of Galois closure, but first we need to generalize some of the component ingredients. If R is ring (commutative with identity), define a *degree-n extension of R* to be an R-algebra A such that A is locally free of rank n as an R-module. (An R-module M is locally free of rank n if there exist elements $r_1, \ldots, r_k$ of R that together generate the unit ideal of R, and such that M_{r_i} is isomorphic to $R_{r_i}^n$ as an R_{r_i}-module. Each locally free module of rank n is automatically projective and finitely presented—see [7, 4.6].)

If A is a degree-n extension of R, then for each $a \in A$ and $k \in \{1, \ldots, n\}$, the definition of $e_k(a) \in A^{\otimes n}$ generalizes verbatim as the kth elementary symmetric polynomial in the n elements $\{a^{(i)}\}$ of $A^{\otimes n}$. We can also generalize the definition of $s_k(a)$ to this new context: multiplication by a is an R-linear map whose characteristic polynomial is well-defined for each free localization A_{r_i}, and each coefficient patches together to give a characteristic polynomial defined over R. Again, if f is an R-algebra homomorphism defined on a subalgebra of $A^{\otimes n}$, we call f *normative* if f sends $e_k(a) \mapsto s_k(a)$ for each element $a \in A$ and $k \in \{1, \ldots, n\}$.

However, switching categories from fields to rings gives us many more morphisms, and it would be desirable for a notion of Galois closure to commute with base change. From this perspective, the ordinary notion of Galois closure for fields is slightly defective: under base extension, the degree of the Galois closure will change if the corresponding Galois group changes. So for each potential Galois group $G \subseteq S_n$, we will fix a notion of G-closure that does commute with base change.

Definition 2. *Let R be a ring and A a degree-n extension of R. Let G be a subgroup of S_n. Then a* G-closure of A over R *is an $A^{\otimes n}$-algebra B equipped with a normative R-algebra homomorphism $\varphi : (A^{\otimes n})^G \to R$, such that the resulting square of R-algebra homomorphisms*

$$\begin{array}{ccc} (A^{\otimes n})^G & \xrightarrow{\varphi} & R \\ \downarrow & & \downarrow \\ A^{\otimes n} & \longrightarrow & B \end{array}$$

(commutes and) is a tensor product diagram, i.e. $B \cong A^{\otimes n} \bigotimes_{(A^{\otimes n})^G} R$ as $A^{\otimes n}$-algebras.

This notion of G-closure does commute with base change:

Theorem 3. *Let A be a degree-n extension of a ring R, and let R' be an arbitrary R-algebra. Then $A' := R' \otimes_R A$ is a degree-n extension of R'. If G is a subgroup of*

S_n and (B, φ) is a G-closure of A over R, then $B' := R' \otimes_R B$ is naturally equipped with the structure of being a G-closure of A' over R'.

And with this definition of G-closure, we can restate Theorem 1 more simply: Let $K \subseteq L$ be a degree-n field extension, and let N be the Galois closure of L, with Galois group $\mathrm{Gal}(N/K) \subseteq \mathrm{Bij}(S_{L/K}, S_{L/K})$. Then for each subgroup H of S_n, an H-closure of L exists if and only if H contains $\mathrm{Gal}(N/K)$ for some identification of $\{1, \ldots, n\}$ with $S_{L/K}$. If this condition holds, the underlying K-algebra of the H-closure is isomorphic to an appropriate power of N.

Definition 2 thus provides an answer to M. Bhargava and M. Satriano's Question 5 of [2]: Given a ring R and a permutation group $G \subseteq S_n$, what is a natural class of degree-n extensions of R, for which there is a notion of G-closure that commutes with base change and reduces to the correct power of the normal closure for separable field extensions? The answer given here is the class of extensions $R \to A$ equipped with the structure of a normative homomorphism $(A^{\otimes n})^G \to R$.

It is helpful not just to have a definition of G-closure, but also a description of when two G-closures should be regarded as the same. The following definition-theorem defines morphisms of G-closures and asserts that they are all isomorphisms:

Theorem 4. *Let A be a degree-n extension of a ring R, and let G be a subgroup of S_n. Let (B, φ) and (B', φ') be two G-closures of A over R. Define a* morphism of G-closures $(B, \varphi) \to (B', \varphi')$ *to be an $A^{\otimes n}$-algebra homomorphism $B \to B'$ and an equality $\varphi = \varphi'$. Every morphism of G-closures is an isomorphism, and such a morphism is unique if it exists; in other words, the category of G-closures of A over R is (essentially) discrete.*

In effect, this discreteness is due to the fact that the underlying $A^{\otimes n}$-algebra B of a G-closure (B, φ) is determined up to unique isomorphism by $\varphi : (A^{\otimes n})^G \to R$: From such a normative R-algebra homomorphism, we may form the canonical surjection

$A^{\otimes n} \to A^{\otimes n} \bigotimes_{(A^{\otimes n})^G} R$, which is uniquely isomorphic to B as an $A^{\otimes n}$-algebra. Therefore normative R-algebra homomorphisms $\varphi : (A^{\otimes n})^G \to R$ parametrize isomorphism classes of G-closures of A over R.

Theorem 5. *Let A be a degree-n extension of a ring R. Let G be a subgroup of S_n. There is a natural one-to-one correspondence between normative R-algebra homomorphisms $(A^{\otimes n})^G \to R$ and isomorphism classes of G-closures of A over R, given by*

$$\varphi : (A^{\otimes n})^G \to R \quad \longmapsto \left(A^{\otimes n} \bigotimes_{(A^{\otimes n})^G} R \ , \ \varphi \right).$$

Because of this parametrization, we can immediately see that if $G \subseteq H$ are subgroups of S_n, and a degree-n extension $R \to A$ has a G-closure, then A also has an H-closure: Merely take the normative homomorphism $\varphi : (A^{\otimes n})^G \to R$ and restrict it further to a homomorphism $(A^{\otimes n})^H \to R$; the latter corresponds to an isomorphism class of H-closures of A over R. So G-closures for small subgroups $G \subseteq S_n$ should exist less often than for larger subgroups $H \subseteq S_n$. Rarest of all should be a 1-closure, where 1 is the trivial subgroup of S_n, while an S_n-closure should exist if any G-closure does. In fact, S_n-closures are marvelously ubiquitous:

Theorem 6. *Let R be a ring and let A be a degree-n extension of R. There exists a unique normative R-algebra homomorphism $\varphi_0 : (A^{\otimes n})^{S_n} \to R$. Hence an S_n-closure of A over R exists, and it is unique up to unique isomorphism.*

In [6, 3.1.2], D. Ferrand constructed the homomorphism φ_0 of Theorem 6 as a homomorphism to R from the divided power algebra $\Gamma_n(A)$, which is canonically isomorphic to $(A^{\otimes n})^{S_n}$ because A is flat (see, for example, [4, 5.5.2.5]). We therefore call this R-algebra homomorphism *the Ferrand map*. The unique S_n-closure is constructed in [6, 5.2], a comment by O. Gabber, though no properties are proven there. We cover the arguments necessary to construct the S_n-closure and prove its uniqueness in Chapter 2.

In Chapter 3, we prove Theorem 3 and other facts relating G-closures between different groups G or different extensions. We also give a formula for the universal algebra over which a given extension has a G-closure for a given group G; homomorphisms from this algebra to R correspond to G-closures of A over R.

Chapter 4 develops the theory of G-closures of étale extensions, and parametrizes G-closures of étale algebras over connected rings R in terms of the fundamental group of the scheme $\mathrm{Spec}(R)$. In particular, we prove Theorem 1, that G-closures of finite separable field extensions reduce to (powers of) the usual Galois closure.

For *monogenic* extensions, those of the form $R \to R[x]/(m(x))$ where m is a monic polynomial of degree n, there is a simpler presentation of the G-closure which we explore in Chapter 5. (In particular, this applies to every free extension of degree up to 2.) There we show that if $|G|$ is a non-zerodivisor, then G-closures of $R[x]/(m(x))$ over R are parametrized by homomorphisms $(R[x]^{\otimes n})^G \to R$ sending $e_k(x)$ to $s_k(x)$—a considerable simplification, since $(R[x]^{\otimes n})^G$ often has a simple presentation as an $(R[x]^{\otimes n})^{S_n} = R[e_1(x), \ldots, e_n(x)]$-algebra. We give such a presentation for the family of subgroups $A_n \subseteq S_n$ and for the subgroup $D_4 \subseteq S_4$. For the latter, the main theorem is the following, which nicely generalizes a classical criterion for discerning the Galois group of a field extension:

Theorem 7. *Let R be a ring in which 2 is a non-zerodevisor, and let $m(x)$ be a monic quartic polynomial over R. There is a D_4-closure of $R[x]/(m(x))$ if and only if the resolvent cubic of $m(x)$ has a root in R.*

We continue the thread of A_n-closures in Chapter 6. By Theorem 1, the classical notion corresponding to "having an A_n-closure" is "having a Galois group contained in A_n." A related classical criterion is that in characteristic other than 2, the discriminant of a degree-n Galois extension is a square in K if and only if the Galois group is contained in A_n. The theorem below is a generalization of this criterion to A_n-closures for ring extensions.

To state the theorem, we need an appropriate generalization of the condition "characteristic other than 2." Let p be an element of a ring R. Call p *primoid* if whenever a, b are elements of R and p^2 divides ab, then a or b is divisible by p. This condition holds, for example, whenever p is prime or a unit, or more generally, whenever p is a power of a prime non-zerodivisor.

Theorem 8. *Let R be a ring in which 2 is a primoid non-zerodivisor. Let A be an extension of R that is free of rank n as an R-module. Then the isomorphism classes of A_n-closures of A over R are in one-to-one correspondence with the square roots of the discriminant of A over R.*

In Chapter 6, we give an example of a ring extension whose discriminant is square, but which does not (and should not) have an A_n-closure. We also describe a more general quadratic criterion for deciding when a free rank-n extension has an A_n-closure, which holds for arbitrary R. For example, a degree-3 monogenic extension $R \to R[x]/(x^3 - sx^2 + tx - u)$ has an A_3-closure if and only if R has a solution γ to the quadratic equation

$$\gamma^2 - (st - 3u)\gamma + (t^3 - 6stu + s^3u + 9u^2) = 0.$$

There are many avenues left to explore. For example, in Chapter 6 we make use of a construction sending a degree-n extension $R \to A$ to the universal R-algebra over which A has an A_n-closure, namely $(A^{\otimes n})^{A_n} \bigotimes_{(A^{\otimes n})^{S_n}} R$. In forthcoming work with A. Gioia, we show that this R-algbera is a discriminant algebra of A in the sense of [5], and is a much simpler construction than the ones presented there and in [8] and [14]. Discriminant algebras, and similar "cubic resolvent algebras," have already been useful in parametrizing low-degree extensions of $\mathbb{Z}$ (see, for example, [1]); it is possible that the universal algebras constructed in Section 3.3 will allow more general parametrizations of low-degree extensions for arbitrary base rings.

But other groups besides A_n and D_4 have classical criteria for when they contain the Galois group of a field extension. For example, the Galois group of a quartic separable field extension $K \to K[x]/(m(x))$ is the Klein 4-group if and only if the resolvent cubic of m splits over K. When and how do these other criteria generalize to guarantees on the existence of G-closures?

Also, while it is known that the S_2-closure of a degree-2 extension is always isomorphic to itself, the question of when a C_3-closure of a rank-3 extension is isomorphic to itself remains open. We do not know the answer even in the case that $R = \mathbb{Z}$ and A is the ring of integers in a cubic number field.

Another big question concerns the ranks of G-closures. For étale extensions, the degree of a G-closure is always $|G|$, but in [2, Prop. 19] it is shown that the rank of the S_n-closure of a non-étale ring extension may exceed $n!$. Under what circumstances is the rank of a G-closure equal to $|G|$?

Each G-closure over R has a natural G-action as an R-algebra, given by permuting the tensor factors. A counter-result is that the G-fixed subalgebra of the G-closure need not be R: an example due to A. Gioia is that of $\mathbb{F}_2 \to \mathbb{F}_2[x]/(x^2)$, where the S_2-closure is $\mathbb{F}_2[x]/(x^2)$, but the S_2-action on it is trivial. It would be useful to find criteria for when this fundamental result of classical Galois theory carries over to the theory of G-closures.

A more abstract line of inquiry is the following: Because of Theorem 3, there is associated to each permutation group $G \subseteq S_n$ a natural functor from the category $\mathcal{C}$ of degree-n extensions (whose morphisms are tensor product squares) to the category of sets, sending each degree-n extension to its set of G-closures. Is there a natural site structure on $\mathcal{C}^{\mathrm{op}}$ making this functor a sheaf or a stack? If so, what are its properties?

And most abstract of all, why is this a good definition of G-closure? Perhaps there is a natural set of axioms that rigidly fixes Definition 2 as the "right" notion of Galois closure for rings.

1.2 Notation and conventions

Sets and multisets:

- If n is a natural number, the notation $[n]$ denotes the n-element set $\{1, \ldots, n\}$.
- If X and Y are two sets, $\mathrm{Hom}(X, Y)$ denotes the set of functions $X \to Y$, and $\mathrm{Bij}(X, Y)$ denotes the set of bijections $X \to Y$. We identify $\mathrm{Bij}([n], [n])$ with the permutation group S_n.
- If d is a natural number and G is a subset of S_d, and X is a set, then we denote by X^d/G the set of orbits of X^d under the action of G permuting the components. The orbit of an element $(x_1, \ldots, x_d)$ of X^d is written $[(x_1, \ldots, x_d)]_G$, or $[(x_1, \ldots, x_d)]$ if $G = S_d$.
- A *multiset of size d from a set X* is an element of X^d/S_d.
- The notation $\xi \sqsubseteq X$ means that ξ is a multiset from X of unspecified finite size.
- If ξ is a multiset, the notation $|\xi| = d$ means that ξ has size d.
- If $\xi \sqsubseteq X$, then for each $x \in X$, $\xi(x)$ is the natural number defined as the multiplicity with which x appears in ξ, so that $|\xi| = \sum_{x \in X} \xi(x)$. A multiset $\xi \subseteq X$ can be completely recovered from the function $X \to \mathbb{N} : x \mapsto \xi(x)$.
- Let X be a set and let $\xi \sqsubseteq X$. For each $x \in X$, we say $x \in \xi$ if $\xi(x) > 0$.
- Let X be a set and let $\xi \sqsubseteq X$. We say that ξ is *primitive* if it is not a multiple of any other multiset, i.e. if $\{\xi(x) : x \in X\}$ has no common factor except 1.
- Let A be a commutative monoid, and let $a : I \to A : i \mapsto a_i$ be a list of elements of A. For each multiset ξ from I, the element a^ξ of A is the product $\prod_{\{i : i \in \xi\}} a_i^{\xi(i)}$.

See Appendix A.1 for more information on multisets.

Rings and modules:

- All rings are commutative with unity.
- A module M of a ring R is *locally free (of rank n)* if there exist elements $\{r_1, \ldots, r_k\}$ such that the ideal $(r_1, \ldots, r_k)$ is all of R, and such that $R_{r_i} \otimes M$ is a free R_{r_i}-module (of rank n) for each i in $\{1, \ldots, k\}$. A locally free module of finite rank is automatically projective and finitely presented.
- Let R be a ring and M an R-module. Let d be a natural number, and let $\alpha \subseteq M^d$ be a finite set of tuples of elements of M. Then the element $e(\alpha)$ of $A^{\otimes d}$ is the sum
$$e(\alpha) = \sum_{(m_1,\ldots,m_d)\in\alpha} m_1 \otimes \ldots \otimes m_d.$$
- Let R be a ring and M an R-module. Let d be a natural number. Then there are d canonical R-linear functions $M \to M^{\otimes d}$, denoted $m \mapsto m^{(i)}$ for each $i \in [d]$.
- Let R be a ring. A *ring extension of degree n* is an R-algebra A which is locally free of rank n as an R-module.
- Let R be a ring and A be an R-algebra. Let d be a natural number and let $k \in [d]$. For each $a \in A$, denote by $e_k(a)$ the elementary symmetric polynomial in the d elements $a^{(1)}, \ldots, a^{(d)}$ of $A^{\otimes d}$.
- If A is a degree-n extension of a ring R, and $a \in A$ and $k \in [n]$, then $s_k(a)$ is the kth signed coefficient of the characteristic polynomial of the R-linear map $\times a : A \to A$.
- If A is a degree-n extension of a ring R, and f is an R-algebra homomorphism whose domain is a subalgebra of $A^{\otimes n}$, we call f *normative* if $f(e_k(a))$ is defined and equals $s_k(a)$ for each $a \in A$ and $k \in [n]$.

- A degree-n ring extension $R \to A$ is *monogenic* if there exists an R-algebra isomorphism $A \cong R[x]/(m(x))$, where m is a monic, degree-n polynomial with coefficients in R.

- If R is a ring and S is a set, then R^S is the product ring $\prod_{s \in S} R$.

- If R is a ring and A, B are two R-algebras, the set of R-algebra homomorphisms $A \to B$ is denoted $\mathrm{Hom}_R(A, B)$, and the group of R-algebra automorphisms of A is denoted $\mathrm{Aut}_R(A)$.

- If R is a ring and M, N are two R-modules, the set of R-module homomorphisms $M \to N$ is denoted $\mathrm{Hom}(M, N)$.

- An element p of a ring R is called *primoid* if, whenever a and b are elements of R and p^2 divides ab, then a or b is a multiple of p.

Polynomial laws:

- If M and N are R-modules, a *polynomial law* $p : M \to N$ is a family of functions $p_S : S \otimes M \to S \otimes N$ for each R-algebra S, such that for every map $S \to S'$ of R-algebras, the following square commutes:

$$\begin{array}{ccc} S \otimes M & \xrightarrow{p_S} & S \otimes N \\ \downarrow & & \downarrow \\ S' \otimes M & \xrightarrow{p_{S'}} & S' \otimes N \end{array}$$

- If M and N are R-modules, a polynomial law $p : M \to N$ is called *homogeneous of degree* d if $p_S(sm) = s^d p_S(m)$ for each R-algebra S and elements $s \in S$, $m \in S \otimes M$.

- The set of polynomial laws $M \to N$ is denoted $\mathrm{Poly}(M, N)$, and, the set of homogeneous degree-d polynomial laws $M \to N$ is denoted $\mathrm{Poly}_d(M, N)$.

- If $p : M \to N$ is a polynomial law, and $\alpha \sqsubseteq I$ is a multiset, then $p^{(\alpha)} : M^I \to N$ is the polynomial law sending $(m_i)_{i \in I}$ to the coefficient of λ^α in $p(\sum_{i \in \alpha} \lambda_i m_i)$.

- Let M be a locally free R-module, and let d be a natural number. Then $\Delta : M \to (M^{\otimes d})^{S_d}$ is the degree-d polynomial law such that $\Delta : m \mapsto m \otimes m \otimes \ldots \otimes m$.

- Let M be an R-module, and let d be a natural number. For each multiset $\alpha \in M^d/S_d$, we denote by $e(\alpha)$ the element of $M^{\otimes d}$ that is the coefficient of λ^α in $\Delta(\sum_{a \in \alpha} \lambda_a a)$.

- Let A be a degree-n extension of a ring R. Then $\det : A \to R$ is the degree-n polynomial law sending an element $a \in S \otimes A$ to the determinant of the S-linear map given by multiplication by a.

- Let A be a degree-n extension of a ring R. For each multiset $\alpha \in A^d/S_d$, we denote by $s(\alpha)$ the element of R that is the coefficient of λ^α in $\det(\sum_{a \in \alpha} \lambda_a a)$.

- Let R be a ring, with R-algebras A and B. A polynomial law $p : A \to B$ is *multiplicative* if $p_S(aa') = p_S(a)p_S(a')$ in $S \otimes B$ for each R-algebra S and pair of elements $a, a' \in S \otimes A$.

See Appendices A.2 and following for more information on polynomial laws.

Chapter 2

Existence and uniqueness of S_n-closures

This section is concerned with proving Theorem 6, that every degree-n extension A of a ring R has a unique S_n-closure. We will proceed in the following way: First, we prove Theorem 5, which implies that isomorphism classes of S_n-closures of A over R correspond to normative R-algebra homomorphisms $(A^{\otimes n})^{S_n} \to R$. Then, we show that such a homomorphism is unique if it exists, because $(A^{\otimes n})^{S_n}$ is generated as an R-algebra by the set of elements of the form $e_k(a)$ with $a \in A$ and $k \in [n] = \{1, \ldots, n\}$. Finally, we demonstrate existence by factoring the function $\det : A \to R : a \mapsto \det(\times a)$ as

$$\det = \varphi_0 \circ \Delta : A \to (A^{\otimes n})^{S_n} \to R,$$

where $\Delta : A \to (A^{\otimes n})^{S_n}$ sends a to $a \otimes \ldots \otimes a$, and $\varphi_0 : (A^{\otimes n})^{S_n}$ is the desired normative R-algebra homomorphism, called *the Ferrand map*. The unique S_n-closure of A is then given, up to unique isomorphism, as the $A^{\otimes n}$-algebra $A^{\otimes n} \bigotimes_{(A^{\otimes n})^{S_n}} R$, where the tensor product is defined using the inclusion $(A^{\otimes n})^{S_n} \hookrightarrow A^{\otimes n}$ and the Ferrand map $\varphi_0 : (A^{\otimes n})^{S_n} \to R$.

Along the way, we will show that this homomorphism φ_0 is not merely normative, but satisfies the more general condition $\varphi_0 : e(\alpha) \mapsto s(\alpha)$ for each multiset $\alpha \sqsubseteq A$ of size n, where $e(\alpha)$ and $s(\alpha)$ will be suitably defined as the coefficients of λ^α in $\Delta(\sum_{a\in\alpha} \lambda_a a)$ and $\det(\sum_{a\in\alpha} \lambda_a a)$, respectively. Therefore, if $\Psi \subseteq A^n/S_n$ is a set of multisets such that $\{e(\alpha) : \alpha \in \Psi\}$ generates $(A^{\otimes n})^{S_n}$ as an R-algebra, the Ferrand map is the unique R-algebra homomorphism $(A^{\otimes n})^{S_n} \to R$ sending $e(\alpha) \mapsto s(\alpha)$ for each $\alpha \in \Psi$.

Note that for each such choice of $\Psi \subseteq A^d/S_d$, we can write the S_n-closure of A over R more concretely as the quotient $A^{\otimes n} \bigotimes_{(A^{\otimes n})^{S_n}} R \cong A^{\otimes n}/I(A,R)$, where $I(A,R)$ is the ideal of $A^{\otimes n}$ generated by elements of the form $e(\alpha) - s(\alpha)$ with $\alpha \in \Psi$. (This ideal is independent of Ψ, so long as $\{e(\alpha) : \alpha \in \Psi\}$ does generate $(A^{\otimes n})^{S_n}$ as an R-algebra.) In particular, $I(A,R)$ is the ideal generated by elements of the form $e_k(a) - s_k(a)$ with $a \in A$ and $k \in [n]$. In [2], the quotient of $A^{\otimes n}$ by this ideal is the definition of S_n-closure, so our definition of S_n-closure reduces to the one given there.

2.1 G-closures and normative homomorphisms

Our first task is to prove Theorems 4 and 5, which can together be summarized as the following statement:

Theorem 2.1.1. *Let R be a ring with a degree-n extension A, and let G be a subgroup of S_n. Let $\mathcal{C}$ be the set of normative R-algebra homomorphisms $(A^{\otimes n})^G \to R$, viewed as a discrete category. Then the functor F from $\mathcal{C}$ to the category of G-closures of A over R, given by*

$$F : \quad \big(\varphi : (A^{\otimes n})^G \to R\big) \quad \longmapsto \quad \left(A^{\otimes n} \bigotimes_{(A^{\otimes n})^G} R \ , \ \varphi \right),$$

is an equivalence of categories. In other words, every G-closure arises in this way

up to isomorphism, and for each pair B_1, B_2 of G-closures of A, there is a unique isomorphism $B_1 \xrightarrow{\sim} B_2$ if any G-closure morphism $B_1 \to B_2$ exists at all.

Proof. For the first part, let (B, φ) be a G-closure of A over R. Then by Definition 2, we know that there is an $A^{\otimes n}$-algebra isomorphism $A^{\otimes n} \bigotimes_{(A^{\otimes n})^G} R \xrightarrow{\sim} B$, which is therefore an isomorphism of G-closures

$$\left(A^{\otimes n} \bigotimes_{(A^{\otimes n})^G} R \ , \ \varphi \right) \xrightarrow{\sim} (B, \varphi).$$

Next we show that for each pair of G-closures of A over R, there is at most one G-closure morphism between them. This is because G-closure morphisms are $A^{\otimes n}$-algebra homomorphisms, and each canonical $A^{\otimes n}$-algebra homomorphism from $A^{\otimes n}$ to $A^{\otimes n} \bigotimes_{(A^{\otimes n})^G} R$ is a surjection. Therefore, any two G-closure morphisms $B_1 \to B_2$ agree on the image of $A^{\otimes n}$ in B_1, which is all of B_1. In other words, the category of G-closures of A over R is a subcategory of the category of quotient objects of $A^{\otimes n}$, and hence a preorder.

Now suppose that there is a G-closure morphism $(B_1, \varphi_1) \to (B_2, \varphi_2)$. By definition, this means that $\varphi_1 = \varphi_2$, and so B_1 and B_2 are each isomorphic as $A^{\otimes n}$-algebras to the same tensor product

$$B_1 \cong A^{\otimes n} \bigotimes_{(A^{\otimes n})^G} R \cong B_2.$$

So we have a G-closure morphism $f : B_1 \to B_2$ and a G-closure isomorphism $B_1 \cong B_2$; by the above, these two morphisms must be equal, so f is an isomorphism. $\square$

2.2 Generators for $(A^{\otimes d})^{S_d}$ when A is locally free

In this section, we establish various generating sets for $(A^{\otimes d})^{S_d}$, where A is an R-algebra that is locally free as an R-module. The generators we use will all be of the form $e(\alpha)$, where $\alpha \in A^d/S_d$ is a multiset from A of size d, defined as

$$\begin{aligned} e(\alpha) = &\text{ the coefficient of } \lambda^\alpha \text{ in } \Delta\left(\sum_{a\in\alpha} \lambda_a a\right) \\ &= \sum_{(a_1,\ldots,a_d)\in\alpha} a_1 \otimes \ldots \otimes a_d. \end{aligned}$$

(See Definition A.2.12 and Lemma A.2.13 for a more general definition of $e(\alpha)$ and a proof of this equivalence.) First, we show that $\{e(\alpha) : \alpha \in A^d/S_d\}$ generate $(A^{\otimes d})^{S_d}$ as an R-module. Then we establish that each element of the form $e(\alpha)$ may be written as a polynomial in elements of the form $e_k(a)$; thus $\{e_k(a) : a \in A \text{ and } k \in [d]\}$ generates $(A^{\otimes d})^{S_d}$ as an R-algebra. We follow up by proving that if $\Omega \subseteq A$ is a set of elements of A whose powers generate A as an R-module, then $\{e_k(\omega) : \omega \in \Omega \text{ and } k \in [d]\}$ is an even smaller generating set for $(A^{\otimes d})^{S_d}$, which is useful when A is monogenic.

Lemma 2.2.1. *Let R be a ring, and let A be an R-algebra that is locally free as an R-module. Let d be a natural number. Then $\{e(\alpha) : \alpha \in A^d/S_d\}$ generates $(A^{\otimes d})^{S_d}$ as an R-module.*

Proof. This is Corollary A.3.6 in the case that $G = S_d$ and $M = A$. The proof proceeds by first establishing the result in the case that A is free as an R-module, and then arguing locally in case A is merely locally free. Details may be found in Section A.3. □

Lemma 2.2.2. *Let R be a ring, and let A be an R-algebra generated as an R-module by $\Theta \subseteq A$. Let $\alpha \in A^d/S_d$ be a multiset from A of size d. If $m = d - \alpha(1)$ is the number of elements of α other than 1, then the element $e(\alpha)$ of $A^{\otimes d}$ is in the subalgebra of $(A^{\otimes d})^{S_d}$ generated by $\{e_k(\theta) : \theta \in \Theta \text{ and } k \leq m\}$.*

Proof. We use induction on m. If $m = 0$, then every element of α is 1, and $e(\alpha) = 1 \otimes \ldots \otimes 1 = 1$, which is in every subalgebra of $(A^{\otimes d})^{S_d}$.

For the induction step, suppose that whenever $d - \beta(1) < m$, the element $e(\beta)$ is in the subalgebra generated by $\{e_k(\theta) : k < m \text{ and } \theta \in \Theta\}$. Now let $\alpha = [(a_1, \ldots, a_m, 1, \ldots, 1)]$ be a multiset such that $d - \alpha(1) = m$. Expanding out each a_j for $j \in [m]$ as an R-linear combination of the generators Θ, and writing $e(\alpha)$ as the resulting R-linear combination of pure tensors, we may tackle each term in turn and assume that $\alpha = [(\theta_1, \ldots, \theta_m, 1, \ldots, 1)]$ with $\theta_j \in \Theta$ for each $j \in [m]$. If any of the θ_j is equal to 1, we are done by the induction hypothesis. Otherwise, each θ_j differs from 1, so consider the product

$$P = \prod_{\theta \in \{\theta_1, \ldots, \theta_m\}} e_{\alpha(\theta)}(\theta).$$

Since $\alpha(\theta_j) \leq m$ for each $j \in [m]$, this product P belongs to the subalgebra of $(A^{\otimes d})$ generated by $\{e_k(\theta) : \theta \in \Theta \text{ and } k \leq m\}$. On the other hand, each pure tensor in the expansion of P corresponds to an assignment of each θ_j to some tensor factor, so we may write

$$P = \sum_{f:[m]\to[d]} \left(\prod_{j=1}^{m} \theta_j^{(f(j))} \right).$$

On the other hand, $e(\alpha)$ has a similar expansion

$$e(\alpha) = \sum_{\substack{f:[m]\to[d] \\ \text{injective}}} \left(\prod_{j=1}^{m} \theta_j^{(f(j))} \right).$$

Therefore, the difference is

$$P - e(\alpha) = \sum_{\substack{f:[m]\to[d] \\ \text{not injective}}} \left(\prod_{j=1}^{m} \theta_j^{(f(j))} \right).$$

The terms on the right-hand side of this equation may be collected into S_d-orbits $e(\beta)$, and each such β must have $\beta(1) > \alpha(1) = d - m$; this is because the m non-1 elements of α are not assigned to distinct tensor factors in any term of $e(\beta)$. Each such $e(\beta)$ therefore has $d - \beta(1) < m$, and by the induction hypothesis belongs to the subalgebra of $(A^{\otimes d})$ generated by $\{e_k(\theta) : \theta \in \Theta \text{ and } k \leq m\}$. Since P is in this subalgebra, and so is $P - e(\alpha)$, the subalgebra must contain $e(\alpha)$ as well. □

Corollary 2.2.3. *Let R be a ring, and let A be an R-algebra that is locally free and generated as an R-module by $\Theta \subseteq A$. Then*

$$\{e_k(\theta) : \theta \in \Theta \text{ and } k \in [d]\}$$

generates $(A^{\otimes d})^{S_d}$ as an R-algebra.

Proof. By Lemma 2.2.1, the set $\{e(\alpha) : \alpha \in A^d/S_d\}$ generates $(A^{\otimes d})^{S_d}$ as an R-module. Each such $e(\alpha)$ is in the subalgebra generated by $\{e_k(\theta) : \theta \in \Theta \text{ and } k \in [d]\}$ by Lemma 2.2.2, so the latter subalgebra is all of $(A^{\otimes d})^{S_d}$. □

Example 2.2.4. The proof of Lemma 2.2.2 provides an algorithm for expressing an element $e(\alpha)$ of $(A^{\otimes d})^{S_d}$ as a polynomial in elements of the form $e_k(\theta)$. In particular, the element $e_k(x + y)$ should be expressible as a polynomial in $\{e_\ell(m) : \ell \leq k \text{ and } m \text{ is a monomial in } x \text{ and } y\}$. For $k = 1$, we have

$$\begin{aligned} e_1(x+y) &= ((x+y) \otimes 1 \otimes 1 \otimes \ldots) + (1 \otimes (x+y) \otimes 1 \otimes \ldots) + \ldots \\ &= (x \otimes 1 \otimes \ldots) + (y \otimes 1 \otimes \ldots) + (1 \otimes x \otimes \ldots) + (1 \otimes y \otimes \ldots) + \ldots \\ &= e_1(x) + e_1(y). \end{aligned}$$

For $k = 2$, we may expand

$$\begin{aligned} e_2(x+y) &= ((x+y) \otimes (x+y) \otimes 1 \otimes \ldots) + ((x+y) \otimes 1 \otimes (x+y) \otimes \ldots) \\ &= e_2(x) + e_2(y) + e_1(x)e_1(y) \\ &\quad - [(xy \otimes 1 \otimes 1 \otimes \ldots) + (1 \otimes xy \otimes 1 \otimes \ldots) + (1 \otimes 1 \otimes xy \otimes \ldots) + \ldots] \\ &= e_2(x) + (e_1(x)e_1(y) - e_1(xy)) + e_2(y). \end{aligned}$$

The case $k = 3$ gives us the similar identity

$$\begin{aligned} e_3(x+y) = e_3(x) &+ (e_2(x)e_1(y) - e_1(x)e_1(xy) + e_1(x^2y)) \\ &+ (e_1(x)e_2(y) - e_1(xy)e_1(y) + e_1(xy^2)) + e_3(y). \end{aligned}$$

See [2, Rmk. 14] for proofs of the corresponding identities with each e_k replaced by s_k; the fact that every identity in the e_k corresponds to an equation in the s_k is a natural corollary of Theorem 6. A general formula for $e_k(x+y)$ in terms of the e_i of monomials in x and y is due to C. Reutenauer and M.-P. Schützenberger and may be found in [11].

The following lemma is a mild but useful strengthening of Corollary 2.2.3. In the case that A is a polynomial ring $R[x_1, \ldots, x_m]$ and $\Omega \subseteq A$ is the set of primitive monomials, this lemma appears as Theorem 4.13 in [15].

Lemma 2.2.5. *Let R be a ring, and let A be an R-algebra that is locally free as an R-module, and let $\Omega \subseteq A$ be a set of elements of A whose powers generate A as an R-module. Then $\{e_k(\omega) : k \in [d] \text{ and } \omega \in \Omega\}$ generates $(A^{\otimes d})^{S_d}$ as an R-algebra.*

Proof. Let A' be the subalgebra generated by the $e_k(\omega)$ as ω ranges over Ω. By the fundamental theorem of symmetric polynomials, each element $e_k(\omega^n)$ belongs to A'. Since $\{\omega^n : \omega \in \Omega \text{ and } n \in \mathbb{N}\}$ generates A as an R-module by assumption,

Corollary 2.2.3 tells us that $\{e_k(\omega^n) : k \in [d],\ \omega \in \Omega,\ \text{and } n \in \mathbb{N}\}$ generates A as an R-algebra. Therefore $A' = A$. □

In particular, if a one-element set $\{\omega\}$ generates A as an R-algebra, we have a simple generating set for $(A^{\otimes d})^{S_d}$:

Corollary 2.2.6. *Let R be a ring, and let A be an R-algebra which is locally free as an R-module. Suppose a single element $\omega \in A$ generates A as an R-algebra. Then for each natural number d, the d-element set $\{e_k(\omega) : k \in [d]\}$ generates $(A^{\otimes d})^{S_d}$ as an R-algebra.*

Proof. Lemma 2.2.5 applies in the case that $\Omega = \{\omega\}$, since powers of ω generate A as an R-module. Therefore $\{e_k(\omega) : k \in [d]\}$ generates $(A^{\otimes d})^{S_d}$ as an R-algebra. □

2.3 The determinant as a polynomial law

If A is an R-algebra that is free as an R-module, we can define the *determinant* of an element a of A as the determinant of the R-linear map $\times a : A \to A$, calculated with respect to any R-basis for A. We can also define this map $\det : A \to R$ when A is merely locally free: On each localization A_r that is free as an R_r-module, the determinant defines a function $A_r \to R_r$, and for each $a \in A$ the images of a in the R_r are compatible, and correspond to a well-defined element of R. We can therefore define a determinant function $\det : A \to R$, but what sort of function is it? It is multiplicative—$\det(aa') = \det(a)\det(a')$ for each pair $a, a' \in A$—but det is not a ring homomorphism because it is not R-linear. For our purposes, the kind of morphism we want $\det : A \to R$ to be is a *polynomial law*:

Lemma 2.3.1. *Let R be a ring, and let A be an R-algebra that is locally free of rank n as an R-module. Then the family of functions $\{\det_S : S \otimes A \to S : S \text{ is an } R\text{-algebra}\}$, where $\det_S$ sends an element of $S \otimes A$ to its determinant in S, defines a homogeneous degree-d multiplicative polynomial law $\det : A \to R$.*

Proof. In order for det to qualify as a polynomial law, the above family of functions must satisfy a compatibility requirement: for each R-algebra morphism $S \to S'$, the square diagram

$$\begin{array}{ccc} S \otimes A & \xrightarrow{\det_S} & S \\ \downarrow & & \downarrow \\ S' \otimes A & \xrightarrow{\det_{S'}} & S' \end{array}$$

must commute (see Appendix A.2 for a definition and discussion of polynomial laws). For each $r \in R$ such that A_r is a free R_r-module, the square

$$\begin{array}{ccc} S_r \otimes_{R_r} A_r & \xrightarrow{\det_{S_r}} & S_r \\ \downarrow & & \downarrow \\ S'_r \otimes_{R_r} A_r & \xrightarrow{\det_{S'_r}} & S'_r \end{array}$$

commutes, because the image of the determinant of a matrix is equal to the determinant of the image of a matrix. Then since the two composite paths in the original square are equal on each $S_r \otimes_{R_r} A_r$, they must in fact be equal.

We have already observed that det is multiplicative: if S is an R-algebra and $a, a' \in S \otimes A$, then $\det_S(aa') = \det_S(a)\det_S(a')$; this equation holds on each free localization of $S \otimes A$, and hence on $S \otimes A$ as well.

Lastly, suppose A is locally free of rank n, and let S be an R-algebra. For each element $s \in S$ and element $a \in S \otimes A$, we have $\det_S(sa) = s^n(a)$; again, this equation is true because it holds on each free localization of A. This qualifies the polynomial law $\det : A \to R$ as homogeneous of degree n. □

Recall that for a multiset $\alpha \in A^n/S_n$, or for a pair of elements $a \in A$ and $k \in [n]$, we have distinguished elements of $(A^{\otimes n})^{S_n}$ given by

$$e(\alpha) = \text{ the coefficient of } \lambda^\alpha \text{ in } \Delta\left(\sum_{a\in\alpha} \lambda_a a\right)$$

$$e_k(a) = \text{ the coefficient of } \lambda^k\mu^{n-k} \text{ in } \Delta\left(\lambda a + \mu\right),$$

where $\Delta : A \to (A^{\otimes n})^{S_n}$ is the polynomial law sending $a \mapsto a \otimes \ldots \otimes a$, as in Lemma A.3.7. (In particular, so long as $a \neq 1$, the definition of $e_k(a)$ is a special case of that of $e(\alpha)$, when $\alpha \in A^d/S_d$ is given by $\alpha(a) = k$ and $\alpha(1) = n - k$.) We use the polynomial law $\det : A \to R$ to define similar elements of R:

Definition 2.3.2. Let R be a ring, and let A be an R-algebra that is locally free of rank n as an R-module. For each multiset $\alpha \in A^n/S_n$, define the element $s(\alpha) \in R$ by

$$s(\alpha) = \text{ the coefficient of } \lambda^\alpha \text{ in } \det\left(\sum_{a\in\alpha} \lambda_a a\right),$$

and for each pair of elements $a \in A$ and $k \in [n]$, define $s_k(a) \in R$ by

$$s_k(a) = \text{ the coefficient of } \lambda^k\mu^{n-k} \text{ in } \det\left(\lambda a + \mu\right).$$

(Again, if $a \neq 1$ then the definition of $s_k(a)$ is a special case of that of $s(\alpha)$, when $\alpha(a) = k$ and $\alpha(1) = n - k$.) We could just as easily have stated the definition of $s_k(a)$ as $s_k(a) = (-1)^k \cdot (\text{the coefficient of } \lambda^{n-k} \text{ in } \det(\lambda - a))$, which establishes that $s_k(a)$ is the kth signed coefficient of the characteristic polynomial of a.

Lemma 2.3.3. *Let A be an R-algebra that is locally free of rank n as an R-module. Then there is a unique R-module homomorphism $\varphi_0 : (A^{\otimes n})^{S_n} \to R$ such that $\varphi_0 : e(\alpha) \mapsto s(\alpha)$ for every multiset $\alpha \in A^n/S_n$. This homomorphism φ_0 is called* the Ferrand map.

Proof. Uniqueness holds, since, by Corollary A.3.6, the set $\{e(\alpha) : \alpha \in A^d/S_d\}$ generates $(A^{\otimes d})^{S_d}$ as an R-module. Existence comes from the factorization provided by Theorem A.3.8: there is a unique R-linear function $\varphi_0 : (A^{\otimes n})^{S_n} \to R$ such that the homogeneous degree-n polynomial law $\det : A \to R$ factors as

$$\det = \varphi_0 \circ \Delta : A \to (A^{\otimes n})^{S_n} \to R.$$

Now we must show that $\varphi_0 : e(\alpha) \to s(\alpha)$ for each multiset $\alpha \in A^n/S_n$. Since $\det = \varphi_0 \circ \Delta$ is a factorization of polynomial laws, we have a factorization

$$\det_S = (S \otimes \varphi_0) \circ \Delta_S$$

for each R-algebra S. For each finite subset $F \subseteq A$, consider the polynomial ring $S = R[\lambda_a : a \in \alpha]$, for which we have

$$\det_S \left(\sum_{a \in F} \lambda_a a \right) = \sum_{\alpha \in F^n/S_n} \lambda^\alpha s(\alpha)$$

by Lemma A.2.8. On the other hand, from the factorization $\det_S = (S \otimes \varphi_0) \circ \Delta_S$,

$$\begin{aligned} \det_S \left(\sum_{a \in F} \lambda_a a \right) &= (S \otimes \varphi_0) \circ \Delta_S \left(\sum_{a \in F} \lambda_a a \right) \\ &= (S \otimes \varphi_0) \left(\sum_{\alpha \in F^n/S_n} \lambda^\alpha e(\alpha) \right) \\ &= \sum_{\alpha \in F^n/S_n} \lambda^\alpha \varphi_0(e(\alpha)). \end{aligned}$$

Since this is an equality in the polynomial ring $R[\lambda_a : a \in F]$, we may compare the coefficients of λ^α to deduce that $\varphi_0(e(\alpha)) = s(\alpha)$ for each $\alpha \sqsubseteq F$. Since every multiset from A of size n is a multiset from some finite $F \subseteq A$, we conclude that φ_0 sends each $e(\alpha)$ to $s(\alpha)$, as desired. □

While $\det : A \to R$ fails to be a ring homomorphism because it is not R-linear, the Ferrand map $\varphi_0 : (A^{\otimes n})^{S_n} \to R$ succeeds on both counts:

Lemma 2.3.4. *Let R be a ring, and let A be an R-algebra that is locally free of rank n as an R-module. Let $\varphi_0 : (A^{\otimes n})^{S_n} \to R$ be the Ferrand map, the unique R-module homomorphism sending $e(\alpha)$ to $s(\alpha)$ for each $\alpha \in A^n/S_n$, as in Lemma 2.3.3. Then φ_0 is an R-algebra homomorphism.*

Proof. All we must show is that that φ_0 preserves 1 and binary products. We know that φ_0 sends $e([(1, \ldots, 1)]) = 1$ to the determinant of the $n \times n$ identity matrix, which is also 1, so $\varphi_0(1) = 1$.

As for binary products, it suffices to check only that φ_0 preserves products of elements that generate $(A^{\otimes n})^{S_n}$ as an R-module, and then extend by linearity. The principal tool is Lemma A.4.2, applied with the two multiplicative laws $p = \Delta$ and $p = \det$. For the setup, let $\{x_i : i \in I\}$ and $\{y_j : j \in J\}$ be two families of elements of A, and let $\alpha \sqsubseteq I$ and $\beta \sqsubseteq J$ be multisets of size n. Then we have

$$e(x_\alpha)e(y_\beta) = \sum_{\gamma \in \Gamma_{\alpha\beta}} e((xy)_\gamma)$$

in the notation of Lemma A.4.2, using the facts that $\Delta : A \to (A^{\otimes d})^{S_d}$ is multiplicative and the $e(x_\alpha)$ are its coefficients. So

$$\begin{aligned} \varphi_0\left(e(x_\alpha)e(y_\beta)\right) &= \varphi_0\left(\sum_{\gamma \in \Gamma_{\alpha\beta}} e((xy)_\gamma)\right) \\ &= \sum_{\gamma \in \Gamma_{\alpha\beta}} \varphi_0(e((xy)_\gamma)) \end{aligned}$$

since φ_0 is R-linear, and so by construction of φ_0 we have

$$\begin{aligned}\varphi_0\left(e(x_\alpha)e(y_\beta)\right) &= \sum_{\gamma\in\Gamma_{\alpha\beta}} s((xy)_\gamma)\\ &= s(x_\alpha)s(y_\beta)\end{aligned}$$

using Lemma A.4.2 again and the facts that $\det : A \to R$ is multiplicative and the $s(x_\alpha)$ are its coefficients. Therefore $\varphi_0\left(e(x_\alpha)e(y_\beta)\right) = \varphi_0(e(x_\alpha))\varphi_0(e(y_\beta))$. Finally, since elements of the form $e(x_\alpha)$ generate $(A^{\otimes d})^{S_d}$ as an R-module, this shows that $\varphi_0 : (A^{\otimes d})^{S_d} \to R$ is multiplicative, and therefore an R-algebra homomorphism. □

The proof of Theorem 6 is now an easy corollary:

Theorem 2.3.5. *Let R be a ring, and let A be an R-algebra that is locally free of rank n as an R-module. There exists a unique R-algebra homomorphism $\varphi_0 : (A^{\otimes n})^{S_n} \to R$ such that $\varphi_0 : e_k(a) \mapsto s_k(a)$ for each $a \in A$ and $k \in [n]$. Furthermore, this R-algebra homomorphism φ_0 sends $e(\alpha) \mapsto s(\alpha)$ for each multiset $\alpha \in A^n/S_n$.*

Proof. As for existence, the Ferrand map $\varphi_0 : (A^{\otimes n})^{S_n} \to R$ of Lemma 2.3.4 satisfies all the conditions of the theorem. And uniqueness holds, since by Corollary 2.2.3 the set $\{e_k(a) : a \in A \text{ and } k \in [n]\}$ generates $(A^{\otimes n})^{S_n}$ as an R-algebra. □

In the language of the introduction, Theorem 2.3.5 may be reworded as follows: Let R be a ring, and let A be a degree-n extension of R. There exists a unique normative R-algebra homomorphism $\varphi_0 : (A^{\otimes n})^{S_n} \to R$. Furthermore, this R-algebra homomorphism maps $\varphi_0 : e(\alpha) \mapsto s(\alpha)$ for each multiset $\alpha \in A^n/S_n$.

Theorem 2.1.1 tells us that normative homomorphisms $(A^{\otimes n})^{S_n} \to R$ correspond to isomorphism classes of S_n-closures of A over R, and that isomorphisms between G-closures are always unique when they exist. Therefore each degree-n extension A of R has an S_n-closure, which is unique up to unique isomorphism. This S_n-closure

may be constructed from $\varphi_0 : (A^{\otimes n})^{S_n} \to R$ as the tensor product $A^{\otimes n} \bigotimes_{(A^{\otimes n})^{S_n}} R$, or alternatively, as the quotient $A^{\otimes n}/I(A,R)$, where $I(A,R)$ is the ideal of $A^{\otimes n}$ generated by $\{v - \varphi_0(v) : v \in (A^{\otimes n})^{S_n}\}$. The generation theorems of Section 2.2 provide us with alternate descriptions of $I(A,R)$:

Corollary 2.3.6. *Let R be a ring with a degree-n extension A, and let $I(A,R) \subseteq A^{\otimes n}$ be the kernel of the unique S_n closure $A^{\otimes n} \to B$ of A over R. Then each of the following is a complete description of $I(A,R)$:*

1. *The ideal $I(A,R)$ of $A^{\otimes n}$ is generated by $\{e(\alpha) - s(\alpha) : \alpha \in A^d/S_d\}$.*
2. *Let $\Omega \subseteq A$ be a subset of elements whose powers generate A as an R-module. Then the ideal $I(A,R)$ of $A^{\otimes n}$ is generated by $\{e_k(\omega) - s_k(\omega) : k \in [d], \omega \in \Omega\}$.*

Proof. Each purported generating set for $I(A,R)$ is of the form $\{e(\alpha) - s(\alpha) : \alpha \in \Psi\}$, where Ψ is such that $\{e(\alpha) : \alpha \in \Psi\}$ generates $(A^{\otimes n})^{S_n}$ as an R-algebra. (See Lemmas 2.2.1 and 2.2.5.) Denote the ideal generated by $\{e(\alpha) - s(\alpha) : \alpha \in \Psi\}$ by J; it is straightforward that $J \subseteq I(A,R)$; we will show that $I(A,R) \subseteq J$.

Let v be an arbitrary element of $(A^{\otimes n})^{S_n}$; we will show that $v - \varphi_0(v)$ belongs to J. Since $\{e(\alpha) : \alpha \in \Psi\}$ generates $(A^{\otimes n})^{S_n}$, there exists some multivariate polynomial p such that $v = p(e(\alpha_1), e(\alpha_2), \ldots)$, where each α_i belongs to Ψ. Then

$$\begin{aligned} v - \varphi_0(v) &= p(e(\alpha_1), e(\alpha_2), \ldots) - \varphi_0(p(e(\alpha_1), e(\alpha_2), \ldots)) \\ &= p(e(\alpha_1), e(\alpha_2), \ldots) - p(\varphi_0(e(\alpha_1)), \varphi_0(e(\alpha_2)), \ldots)) \\ &= p(e(\alpha_1), e(\alpha_2), \ldots) - p(s(\alpha_1), s(\alpha_2), \ldots). \end{aligned}$$

In the quotient $A^{\otimes n}/J$, the right-hand side of this equation vanishes, and hence the left-hand side must too. Therefore $v - \varphi_0(v)$ must belong to J. Since $I(A,R)$ is generated by $\{v - \varphi_0(v) : v \in (A^{\otimes n})^{S_n}\}$, we therefore have $I(A,R) \subseteq J$, as desired. $\square$

Remark 2.3.7. Note that the work of this section may be adapted to show that if A and B are R-algebras with A locally free, then each multiplicative homogeneous degree-d polynomial law $A \to B$ corresponds to a ring homomorphism $(A^{\otimes d})^{S_d} \to B$; indeed, this is the main result of [13]. For example, one could use the determinant of any linear representation: given a ring homomorphism $p : A \to M_n(B)$, where $M_n(R)$ is the (noncommutative) ring of $n \times n$ matrices over B, we obtain a degree-n polynomial law $\det(p) : A \to B$. In fact, all examples of multiplicative homogeneous polynomial laws come from ones of this type: in [16], F. Vaccarino shows that for each ring R with algebras A, B and a multiplicative polynomial law $p : A \to B$ that is homogeneous of degree n, there exist R-algebras A' and B' with R-algebra homomorphisms $\alpha : A' \twoheadrightarrow A$, $p' : A' \to M_n(B')$, and $\beta : B' \to B$ such that $p \circ \alpha = \beta \circ \det(p') : A' \to B$.

Chapter 3

The interactions of G-closures

In this section we explore the interactions between G-closures of algebras A over rings R, as the groups G and the rings R vary. In particular, we will first show that G-closures are *preserved by base change*, that is, if $R \to A$ has a G-closure B, then $R' \to R' \otimes A$ has a G-closure $R' \otimes B$, and in particular, existence of the former implies existence of the latter. Next, we discuss the way in which a G-closure of A over R induces an H-closure of A over R for each subgroup H containing G. Finally, for each pair of subgroups $G \subseteq H$ of S_n, we discuss the universal algebra over which a G-closure exists that induces a given H-closure of A over R.

3.1 Base extension of G-closures

Our first task is to show that base change $R \to R'$ preserves G-closures of extensions of R. The remainder of this section may be considered an alternate, and more general, proof of [2, Thm. 1].

Lemma 3.1.1. *Let R be a ring, and let A be a degree-n extension of R. Let G be a subgroup of S_n, and let $\varphi : (A^{\otimes n})^G \to R$ be normative. Let R' be an R-algebra, and let $A' = R' \otimes A$. Then A' is a degree-n extension of R', and the homomorphism*

$$\varphi' : (A'^{\otimes_{R'} n})^G \cong R' \otimes (A^{\otimes n})^G \xrightarrow{R' \otimes \varphi} R'$$

is also normative.

Proof. First, note that φ' is well-defined, since the canonical R'-algebra homomorphism $R' \otimes (A^{\otimes n})^G \to (A'^{\otimes_{R'} n})^G$ is an isomorphism by Lemma A.3.5.

We must show that $\varphi' : (A'^{\otimes_{R'} n})^G \to R'$ is normative. Since φ is normative, it sends $e_k(a)$ to $s_k(a)$ for each $a \in A$ and $k \in [n]$; therefore φ' sends $e_k(1 \otimes a)$ to $s_k(1 \otimes a)$ for each $a \in A$. The set $\{1 \otimes a : a \in A\}$ generates A' as an R-module, so by Theorem 2.3.5 and Corollary 2.2.3, the restriction of φ' to the subalgebra $(A'^{\otimes_{R'} n})^{S_n}$ is the Ferrand map for A' over R'. □

Lemma 3.1.2. *Let R be a ring, and let A be a degree-n extension of R. Let $H \subseteq G$ be subgroups of S_n, and let $\varphi : (A^{\otimes n})^G \to R$ be a normative R-algebra homomorphism. Let R' be a ring, and let A' and φ' be as in Lemma 3.1.1. Then the canonical homomorphism*

$$R' \otimes (A^{\otimes n})^H \bigotimes_{(A^{\otimes n})^G} R \to (A'^{\otimes_{R'} n})^H \bigotimes_{(A'^{\otimes_{R'} n})^G} R'$$

is an isomorphism, where the structure maps for the tensor product on the right are inclusion and φ'.

Proof. Extension of scalars $R \to R'$ is a left adjoint, so it preserves tensor product diagrams (which are categorical colimits). And by Lemma A.3.5, we have isomorphisms $R' \otimes (A^{\otimes n})^G \xrightarrow{\sim} (A'^{\otimes_{R'} n})^G$ and $R' \otimes (A^{\otimes n})^H \xrightarrow{\sim} (A'^{\otimes_{R'} n})^H$. □

Theorem 3.1.3. *Let R be a ring, and let A be a degree-n extension of R. Let G be a subgroup of S_n, and let (B, φ) be a G-closure of A over R. Let R' be an arbitrary R-algebra; then $A' := R' \otimes A$ is a degree-n extension of R', and $B' := R' \otimes B$ is an $A'^{\otimes_{R'} n}$-algebra. Let $\varphi' : (A'^{\otimes_{R'} n})^G \to R'$ be as in Lemma 3.1.1. Then (B', φ') is a G-closure of A' over R'.*

Proof. By Lemma 3.1.1, the homomorphism φ' is normative. All that remains to show, then, is that there is an isomorphism of $A'^{\otimes_{R'}n}$-algebras

$$A'^{\otimes_{R'}n} \bigotimes_{(A'^{\otimes_{R'}n})^G} R' \to B'.$$

Because (B, φ) is a G-closure of A over R, we have an isomorphism of $A^{\otimes n}$-algebras $A^{\otimes n} \bigotimes_{(A^{\otimes n})^G} R \xrightarrow{\sim} B$. Tensoring with R', we obtain an isomorphism $R' \otimes A^{\otimes n} \bigotimes_{(A^{\otimes n})^G} R \xrightarrow{\sim} B'$. By Lemma 3.1.2 with $H = 1$, we therefore have an isomorphism

$$A'^{\otimes_{R'}n} \bigotimes_{(A'^{\otimes_{R'}n})^G} R' \xrightarrow{\sim} B'. \qquad \square$$

3.2 Induction of G-closures

We briefly note the following elementary, but important fact:

Theorem 3.2.1. *Let R be a ring, and let A be a degree-n extension of R. Let $G \subseteq H$ be subgroups of S_n, and let (B, φ) be a G-closure of A over R. This G-closure canonically induces an H-closure of A over R, namely*

$$\left(A^{\otimes n} \bigotimes_{(A^{\otimes n})^H} R \ , \ \varphi\,\big|_{(A^{\otimes n})^H} \right).$$

Proof. Indeed, $\varphi\,\big|_{(A^{\otimes n})^H} : (A^{\otimes n})^H \to R$ is normative because φ is, and the above is the resulting H-closure. $\square$

In particular, every G-closure induces the canonical S_n-closure. In contrast, a 1-closure rarely exists—there must be a normative R-algebra homomorphism $A^{\otimes n} \to R$, whereas typically there is no homomorphism at all—but if an R-algebra A does have a 1-closure, then A also has a G-closure for every subgroup $G \subseteq S_n$.

From Theorem 1, one might expect that the underlying R-algebra of the H-closure may be recovered as a power of the underlying R-algebra of the G-closure. However, this is not the case; see Counterexample 4.4.4.

3.3 Universal algebras for G-closures

We begin by recalling from Theorem 2.1.1 that G-closures of a degree-n extension $R \to A$ are parametrized by normative R-algebra homomorphisms $(A^{\otimes n})^G \to R$, or in other words, by homomorphisms $(A^{\otimes n})^G \to R$ whose composite with the inclusion $(A^{\otimes n})^{S_n} \to (A^{\otimes n})^G$ is the Ferrand map $(A^{\otimes n})^{S_n} \to R$. These correspond in turn to R-algebra homomorphisms $(A^{\otimes n})^G \bigotimes_{(A^{\otimes n})^{S_n}} R \to R$.

Or put another way, for each degree-n extension $R \to A$, the Ferrand map $\varphi_0 : (A^{\otimes n})^{S_n} \to R$ gives the ring R an $(A^{\otimes n})^{S_n}$-algebra structure. We may then say that G-closures of A over R are parametrized by $(A^{\otimes n})^{S_n}$-algebra homomorphisms $(A^{\otimes n})^G \to R$. Using the adjunction between extension and restriction of scalars along $(A^{\otimes n})^{S_n} \to R$, such $(A^{\otimes n})^{S_n}$-algebra homomorphisms correspond to R-algebra homomorphisms $(A^{\otimes n})^G \bigotimes_{(A^{\otimes n})^{S_n}} R \to R$.

This alternative parametrization will be very useful in Chapter 6, when we explicitly compute this tensor product to check for homomorphisms to R. But for now, we will prove a generalization pointed out by L. Taelman:

Theorem 3.3.1. *Let R be a ring, and let A be a degree-n extension of R. Let G be a subgroup of S_n. For each R-algebra R', there is a canonical correspondence between isomorphism classes of G-closures of $R' \otimes A$ over R' and R-algebra homomorphisms $(A^{\otimes n})^G \bigotimes_{(A^{\otimes n})^{S_n}} R \to R'$.*

In other words, the functor F from R-algebras to sets, where F sends R' to the set of isomorphism classes of G-closures of $R' \otimes A$ over R', is represented by $(A^{\otimes n})^G \bigotimes_{(A^{\otimes n})^{S_n}} R$.

Proof. Let $F(R')$ be the set of isomorphism classes of G-closures of $A' := R' \otimes A$ over R'. We use the parametrization of $F(R')$ preceding the theorem, as well as Theorem 3.1.1 and the adjunction between extension and restriction of scalars:

$$\begin{aligned} F(R') &\cong \mathrm{Hom}_{R'}\left((A'^{\otimes_{R'} n})^G \bigotimes_{(A'^{\otimes_{R'} n})^{S_n}} R', R' \right) \\ &\cong \mathrm{Hom}_{R'}\left(R' \otimes (A^{\otimes n})^G \bigotimes_{(A^{\otimes n})^{S_n}} R, R' \right) \\ &\cong \mathrm{Hom}_{R}\left((A^{\otimes n})^G \bigotimes_{(A^{\otimes n})^{S_n}} R, R' \right). \end{aligned}$$

□

In particular, the R-algebra $R_G = (A^{\otimes n})^G \bigotimes_{(A^{\otimes n})^{S_n}} R$ admits the identity homomorphism to itself; thus there exists a canonical G-closure of $R_G \otimes A$ over R_G. Then R_G may be viewed as *the universal algebra over which A admits a G-closure*, in the sense that every G-closure of a base change of $R \to A$ is the result of base changing the canonical G-closure of $R_G \otimes A$ over R_G.

As an example, the S_n-closure $A^{\otimes n} \bigotimes_{(A^{\otimes n})^{S_n}} R$ is a tensor product of this form. We may therefore interpret the S_n-closure of A over R as the universal algebra over which A admits a 1-closure. Hence 1-closures of A correspond to homomorphisms to R from its S_n-closure.

In Chapter 6, we will show that the tensor product $(A^{\otimes n})^{A_n} \bigotimes_{(A^{\otimes n})^{S_n}} R$ is locally free of rank 2; therefore we can say A_n-closures of A over R correspond to 1-closures of $(A^{\otimes n})^{A_n} \bigotimes_{(A^{\otimes n})^{S_n}} R$ over R by Theorem 5.1.1.

More generally, we can also argue in the style of Theorem 3.3.1 that, given a pair of subgroups $G \subseteq H$ of S_n and a G-closure (B, φ) of A, the tensor product $(A^{\otimes n})^H \bigotimes_{(A^{\otimes n})^G} R$ is the universal algebra over which A admits an H-closure inducing (B, φ) in the sense of Theorem 3.2.1.

Chapter 4

G-closures of étale extensions

This section is concerned with developing the theory of G-closures of *étale extensions*, algebras which are locally free as modules and which locally have invertible discriminants. In the end, we will prove Theorem 1, which classifies G-closures of finite separable field extensions, and which grounds the theory of G-closures in classical Galois theory.

We begin by analyzing the situation for *trivial étale algebras*, algebras of the form $R \to R^n$. We then use the fact that étale extensions are precisely those which become trivial after changing the base to an étale cover, to show that each G-closure of an étale extension is étale. Next, we employ an antiequivalence between the category of étale extensions and the category of finite sets equipped with a continuous action by a certain profinite group, in order to clasify G-closures of étale extensions. Finally, we will connect this result with our knowledge of Galois theory to prove Theorem 1.

4.1 G-closures of trivial étale algebras

Definition 4.1.1. Let R be a ring, and let S be an n-element set. By R^S we denote the rank-n R-algebra $\prod_{s\in S} R$. The natural R-basis for R^S is denoted $\{e_s : s \in S\}$, so that $e_s e_{s'} = \delta_{ss'} e_s$ and $1 = \sum_{s\in S} e_s$.

Note that if R is a ring, and S is an n-element set, then $(R^S)^{\otimes n} \cong R^{\mathrm{Hom}([n],S)}$, where e_π on the right corresponds to $e_{\pi_1} \otimes \ldots \otimes e_{\pi_n} = \prod_{i=1}^n e_{\pi_i}^{(i)}$ on the left, for each $\pi : [n] \to S$. We can extend this observation to a description of the S_n-closure of R^S:

Lemma 4.1.2. *Let R be a ring, and let S be an n-element set. Then the Ferrand map $\varphi_0 : ((R^S)^{\otimes n})^{S_n} \to R$ sends*

$$\varphi_0 : e([(e_{\pi_1}, \ldots, e_{\pi_n})]) \mapsto \begin{cases} 1 & \text{if } \pi : [n] \to S \text{ is a bijection} \\ 0 & \text{otherwise.} \end{cases}$$

The unique S_n-closure of R^S is

$$(R^S)^{\otimes n} \bigotimes_{((R^S)^{\otimes n})^{S_n}} R \cong R^{\mathrm{Bij}([n],S)},$$

where e_π on the right corresponds to $e_{\pi_1} \otimes \ldots \otimes e_{\pi_n} = \prod_{i=1}^n e_{\pi_i}^{(i)}$ on the left, for each bijection $\pi : [n] \to S$.

Proof. By Theorem 2.3.5, the normative homomorphism $\varphi_0 : ((R^S)^{\otimes n})^{S_n} \to R$ sends

$$e([(e_{\pi_1}, \ldots, e_{\pi_n})]) \mapsto s([(e_{\pi_1}, \ldots, e_{\pi_n})]).$$

Letting $\alpha = [(\pi_1, \ldots, \pi_n)]$, we know that $s([(e_{\pi_1}, \ldots, e_{\pi_n})])$ is the coefficient of λ^α in $\det(\sum_{s \in S} \lambda_s e_s)$, by definition. But in the natural basis for R^S, $\sum_{s \in S} \lambda_s e_s$ acts diagonally, sending $e_{s'}$ to $\delta_{ss'} \lambda_s e_s$, so its determinant is $\prod_{s \in S} \lambda_s$. Thus $s(\alpha) = 1$ if $\lambda^\alpha = \prod_{s \in S} \lambda_s$ and $s(\alpha) = 0$ otherwise, i.e. $s(\alpha) = 1$ if π is a bijection and $s(\alpha) = 0$ otherwise.

By Corollary 2.3.6, the S_n-closure of R^S is the quotient of $(R^S)^{\otimes n} \cong R^{\mathrm{Hom}([n],S)}$ by the ideal I generated by

$$\left\{ e([(e_{\pi_1}, \ldots, e_{\pi_n})]) - s([(e_{\pi_1}, \ldots, e_{\pi_n})]) : \pi \in \mathrm{Hom}([n], S) \right\}.$$

With $s([(e_{\pi_1}, \ldots, e_{\pi_n})])$ evaluated according to the first part of the lemma, and employing the isomorphism $(R^S)^{\otimes n} \cong R^{\mathrm{Hom}([n],S)}$, we can write this generating set as

$$\left\{ \left(\sum_{\pi \in \mathrm{Bij}([n],S)} e_\pi \right) - 1 \right\} \cup \left\{ \left(\sum_{\pi \in \mathcal{O}} e_\pi \right) : \mathcal{O} \in \mathrm{Hom}([n],S)/S_n, \mathcal{O} \neq \mathrm{Bij}([n],S) \right\}.$$

We show that this ideal is equal to $J := (e_\pi : \pi \notin \mathrm{Bij}([n],S))$. To show that $e_\pi \in I$ whenever π is not a bijection, note that

$$1 - \sum_{\pi' \in \mathrm{Bij}([n],S)} e_{\pi'} \in I, \text{ so}$$

$$e_\pi - \left(\sum_{\pi' \in \mathrm{Bij}([n],S)} e_{\pi'} \right) e_\pi \in I,$$

but the second term vanishes because $e_{\pi'} e_\pi = 0$ whenever $\pi' \neq \pi$, which here is always the case since π' is a bijection while π is not. Thus $J \subseteq I$.

Conversely, we know that

$$\sum_{\pi \in \mathrm{Hom}([n],S)} e_\pi = 1 \text{ in } R^{\mathrm{Hom}([n],S)}.$$

Therefore

$$\left(\sum_{\pi \in \mathrm{Hom}([n],S)} e_\pi \right) - 1 = 0 \in J.$$

But e_π itself is in J whenever π is not a bijection, so the sum of the remaining terms must also belong to J:

$$\left(\sum_{\pi \in \mathrm{Bij}([n],S)} e_\pi \right) - 1 \in J.$$

And if $\mathcal{O}$ is an S_n-equivalence class of non-bijective $\pi : [n] \to S$, then $\sum_{\pi \in \mathcal{O}} e_\pi \in J$ because each $e_\pi \in J$. Therefore $I \subseteq J$.

Hence the isomorphism $(R^S)^{\otimes n} \cong R^{\mathrm{Hom}([n],S)}$ descends to an isomorphism

$$\begin{aligned}(R^S)^{\otimes n} \bigotimes_{((R^S)^{\otimes n})^{S_n}} R &\cong R^{\mathrm{Hom}([n],S)}/I \\ &= R^{\mathrm{Hom}([n],S)}/(e_\pi : \pi \notin \mathrm{Bij}([n],S)) \\ &= R^{\mathrm{Bij}([n],S)}. \end{aligned}$$

□

Recall that a *connected* ring is a ring with exactly two idempotents, 0 and 1 (the *trivial* idempotents), such as a domain or a field. If R is a connected ring, then we can generalize Lemma 4.1.2 to subgroups G of S_n:

Lemma 4.1.3. *Let R be a connected ring, and let S be an n-element set. Let G be a subgroup of S_n. Then the G-closures of R^S correspond naturally to the G-orbits of* $\mathrm{Bij}([n], S)$*, where the G-action is by pre-composition. The G-closure corresponding to such an orbit $\mathcal{O} \subseteq \mathrm{Bij}([n], S)$ is*

$$(R^S)^{\otimes n} \bigotimes_{((R^S)^{\otimes n})^G} R \cong R^{\mathcal{O}},$$

where e_π on the right corresponds to $\prod_{i=1}^n e_{\pi_i}^{(i)}$ on the left.

Proof. First note that for the unique normative homomorphism $\varphi_0 : ((R^S)^{\otimes n})^{S_n} \to R$, we have

$$\varphi_0 \left(\sum_{\pi \in \mathrm{Bij}([n],S)} e_\pi \right) = 1$$

by Lemma 4.1.2. For each extension of φ_0 to a normative homomorphism $\varphi : ((R^S)^{\otimes n})^G \to R$, we can break up this sum into G-orbits:

$$\sum_{\mathcal{O} \in \mathrm{Bij}([n],S)/G} \varphi \left(\sum_{\pi \in \mathcal{O}} e_\pi \right) = 1.$$

Each term in parentheses is an idempotent in $((R^S)^{\otimes n})^G$, so if R is connected, exactly

one such term is sent to 1 and the rest to 0. The G-closures of R^S over R thus correspond to the orbits $\mathcal{O} \in \mathrm{Bij}([n], S)/G$.

Fixing such an orbit $\mathcal{O}$, the corresponding G-closure is a quotient of the S_n-closure $R^{\mathrm{Bij}([n],S)}$ given by

$$(R^S)^{\otimes n} \bigotimes_{((R^S)^{\otimes n})^G} R \cong R^{\mathrm{Bij}([n],S)} / \left(\sum_{\pi \in \mathcal{O}'} e_\pi - \delta_{\mathcal{O}\mathcal{O}'} : \mathcal{O}' \in \mathrm{Bij}([n], S)/G \right)$$

For each $\pi \notin \mathcal{O}$, multiplying the relation $1 = \sum_{\pi' \in \mathcal{O}} e_{\pi'}$ by e_π tells us that $e_\pi = 0$, and conversely, if $e_\pi = 0$ for each $\pi \notin \mathcal{O}$, then $1 = \sum_{\pi \in \mathrm{Bij}([n],S)} e_\pi = \sum_{\pi \in \mathcal{O}} e_\pi$. Therefore the above quotient may be written as

$$(R^S)^{\otimes n} \bigotimes_{((R^S)^{\otimes n})^G} R \cong R^{\mathrm{Bij}([n],S)} / \left(e_\pi : \pi \notin \mathcal{O} \right) \cong R^{\mathcal{O}}. \qquad \square$$

To treat the case that R is not necessarily connected, we will use the following terminology:

Definition 4.1.4. Let R be a ring, and let I be a finite set. A *complete set of orthogonal idempotents of R indexed by I* is a family of elements $I \to R : i \mapsto p_i$ such that

1. each p_i is idempotent: $p_i^2 = p_i$ for each $i \in I$;
2. the family is pairwise *orthogonal*: $p_i p_j = 0$ for each $i, j \in I$ with $i \neq j$; and
3. the family of elements is *complete*: $\sum_{i \in I} p_i = 1$.

Complete sets of orthogonal idempotents of R indexed by I correspond to R-algebra homomorphisms $R^I \to R$, as the images of the generators $e_i \in R^I$.

Lemma 4.1.5. *Let R be a ring, and let S be an n-element set. Let G be a subgroup of S_n. Let $I = \mathrm{Bij}([n], S)/G$ be the set of G-orbits of $\mathrm{Bij}([n], S)$, where the G-action is by*

pre-composition. Then G-closures of R^S over R correspond naturally to complete sets of orthogonal idempotents of R indexed by I, and each such G-closure is isomorphic to $R^{|G|}$ as an R-algebra.

Proof. As in the proof of Lemma 4.1.3, we wish to parametrize normative homomorphisms $\varphi : ((R^S)^{\otimes n})^G \to R$. Such homomorphisms correspond to homomorphisms

$$U := ((R^S)^{\otimes n})^G \bigotimes_{((R^S)^{\otimes n})^{S_n}} R \to R.$$

The tensor product U is generated as an R-algebra by G-orbit sums $\sum_{\pi\in\mathcal{O}} e_\pi$ for each orbit $\mathcal{O} \in \mathrm{Hom}([n], S_n)/G$, but because of the relation $\sum_{\pi\in\mathrm{Bij}([n],S_n)} e_\pi = 1$, we may use only the orbits $\mathcal{O} \in I$, those consisting of bijections. Since the G-orbit sums are idempotent and pairwise orthogonal, we may therefore present U abstractly as an R-algebra:

$$\begin{aligned} U &= ((R^S)^{\otimes n})^G \bigotimes_{((R^S)^{\otimes n})^{S_n}} R \\ &\cong R[x_\mathcal{O} : \mathcal{O} \in I] \Big/ \left(1 - \sum_{\mathcal{O}\in I} x_\mathcal{O}\ ,\ x_\mathcal{O} x_{\mathcal{O}'} - \delta_{O O'} x_\mathcal{O} : \mathcal{O}, \mathcal{O}' \in I\right) \\ &\cong R^I, \end{aligned}$$

where the isomorphism sends $x_\mathcal{O}$ to $\sum_{\pi\in\mathcal{O}} e_\pi$. Homomorphisms from U to R, then, correspond to complete sets of orthogonal idempotents of R indexed by I, namely, the images of the $x_\mathcal{O}$.

Now fix such a complete set of idempotents $I \to R : \mathcal{O} \mapsto p_\mathcal{O}$, and define a normative homomorphism $\varphi : ((R^S)^{\otimes n})^G \to R$ by

$$\varphi : \sum_{\pi\in\mathcal{O}} e_\pi \mapsto \begin{cases} p_\mathcal{O} & \text{if } \mathcal{O} \subseteq \mathrm{Bij}([n], S), \\ 0 & \text{otherwise.} \end{cases}$$

Then the R-algebra B underlying the corresponding G-closure may be written

$$\begin{aligned} B &\cong ((R^S)^{\otimes n}) \bigotimes_{((R^S)^{\otimes n})^G} R \\ &\cong R^{\mathrm{Bij}([n],S)} / \left(p_{\mathcal{O}} - \sum_{\pi \in \mathcal{O}} e_\pi : \mathcal{O} \in I \right) \\ &\cong R^{\mathrm{Bij}([n],S)} / \left(p_{\mathcal{O}} e_\pi - e_\pi : \pi \in \mathcal{O} \in I \right). \end{aligned}$$

We claim that this last R-algebra is isomorphic to $R^{|G|}$ (though not canonically). First, choose an ordering of each orbit $\mathcal{O}$, which has $|G|$ elements, and write $\{e_\pi : \pi \in \mathcal{O}\} = \{x_{\mathcal{O},1} \ldots, x_{\mathcal{O},|G|}\}$. Replacing the dummy index $\mathcal{O} \in I$ by $i \in I$, then, we have

$$B \cong R^{\{x_{i,j} : i \in I, j \in [|G|]\}} / (p_i x_{i,j} - x_{i,j} : i \in I, j \in [|G|]).$$

We argue that $B \cong R^{\{y_j : j \in [|G|]\}}$; the relevant isomorphisms are

$$\begin{aligned} R^{\{y_j : j \in [|G|]\}} &\leftrightarrow R^{\{x_{i,j} : i \in I, j \in [|G|]\}} / (p_i x_{i,j} - x_{i,j} : i \in I, j \in [|G|]) \\ &: y_j \mapsto \sum_{i \in I} x_{i,j} \text{ for each } j \in [|G|] \\ &: p_i y_j \leftarrow\!\shortmid x_{i,j} \text{ for each } i \in I, j \in [|G|]; \end{aligned}$$

These are inverses: each $y_j \mapsto \sum_{i \in I} x_{i,j} \mapsto \sum_{i \in I} p_i y_j = y_j$, because $\sum_{i \in I} p_i = 1$; and each $x_{i,j} \mapsto p_i y_j \mapsto p_i \sum_{i' \in I} x_{i',j} = p_i \sum_{i' \in I} p_{i'} x_{i',j} = p_i x_{i,j} = x_{i,j}$, because $p_i p_{i'} = 0$ unless $i = i'$. Therefore $B \cong R^{\{y_j : j \in [|G|]\}} \cong R^{|G|}$, as desired. □

4.2 G-closures of étale extensions are étale

In this section, we prove that if A is a degree-n extension of R which is étale as an R-algebra, then each G-closure of A over R is an étale degree-$|G|$ extension of R. We

use the following lemma, whose present formulation is that of [2, Lem. 15], but which also appears in slightly different language as Theorem 5.10 in [7]:

Lemma 4.2.1. *Let R be a ring, and let B be an R-algebra that is finitely generated as an R-module. Then B is an étale degree-n extension of R if and only if there exists an étale R-algebra C such that the morphism of schemes $\mathrm{Spec}(C) \to \mathrm{Spec}(R)$ is surjective and the R-algebras $C \otimes B$ and C^n are isomorphic.*

Then it is an easy consequence of the previous section that G-closures of étale extensions are étale:

Theorem 4.2.2. *Let R be a ring, and let A be a degree-n extension of R that is étale as an R-algebra. Let G be a subgroup of S_n, and let (B, φ) be a G-closure of A over R. Then B is an étale degree-$|G|$ extension of R.*

Proof. Because A is finitely generated as an R-module, we may use Lemma 4.2.1 to obtain an R-algebra C such that $\mathrm{Spec}(C) \to \mathrm{Spec}(R)$ is surjective and $C \otimes A \cong C^n$ as R-algebras.

Applying Theorem 3.1.3, we find that $C \otimes B$ naturally has the structure of being a G-closure of $C \otimes A$ over C. But $C \otimes A \cong C^n$, so by Lemma 4.1.5 and Theorem 3.1.3, we must have $C \otimes B \cong C^{|G|}$. Therefore B is an étale degree-$|G|$ extension of R, again by Lemma 4.2.1. □

An immediate consequence of this theorem is that if A is an étale extension of R and (B, φ) is G-closure of A over R, then B is locally free of positive rank as an R-module, and in particular the homomorphism $R \to B$ is injective. Therefore the G-closure structure map $\varphi : (A^{\otimes n})^G \to R$ may be recovered from the underlying $A^{\otimes n}$-algebra B as the restriction of the defining homomorphism $A^{\otimes n} \to B$ to $(A^{\otimes n})^G$.

4.3 G-closures and fundamental groups

The content of the following theorem is found in [7, Thms. 1.11, 2.9], and it allows us to more fully describe the situation of G-closures of étale extensions:

Theorem 4.3.1. *Let R be a connected ring, and let Ω be an R-algebra which is an algebraically closed field. Let F_Ω be the contravariant functor from finite étale extensions of R to finite sets sending $A \mapsto \mathrm{Hom}_R(A, \Omega)$. Then the natural automorphisms of this functor form a profinite group G_R, making F_Ω an antiequivalence between finite étale extensions of R and finite sets equipped with a continuous G_R-action. For a field K with separable closure $\bar{K}$, the fundamental group G_K is isomorphic to the the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$, and the antiequivalence may be taken to be the functor $L \mapsto \mathrm{Hom}_K(L, \bar{K})$ for each separable K-algebra L.*

Note that if A is an étale degree-n extension of R, then $\Omega \otimes A$ is an étale degree-n extension of Ω, namely Ω^n up to isomorphism. Therefore $F_\Omega(A) = \mathrm{Hom}_R(A, \Omega) \cong \mathrm{Hom}_\Omega(\Omega \otimes A, \Omega) \cong \mathrm{Hom}_\Omega(\Omega^n, \Omega)$ is an n-element set. We list a few more consequences of Theorem 4.3.1 below:

Lemma 4.3.2. *Let R be a connected ring, and G_R its fundamental group. Under the antiequivalence of Theorem 4.3.1, the zero algebra (resp. R, a product of R-algebras, a tensor product diagram of R-algebras) corresponds to the empty set (resp. a singleton $\{*\}$, a disjoint union of G_R-sets, a fibered product diagram of G_R-sets). If A is an étale R-algebra, corresponding to the G_R-set S, and G is a group acting on A such that the G-invariant subalgebra A^G is étale, then A^G corresponds to the G_R-set S/G of G-orbits of S.*

Proof. These are all incarnations of the fact that categorical limits and colimits are interchanged under an antiequivalence of categories (together with the fact that products and tensor products of étale algebras are étale). □

Lemma 4.3.3. *Let A be an étale degree-n extension of R, and let $\varphi_0 : (A^{\otimes n})^{S_n} \to R$ be the Ferrand map. Under the antiequivalence of Theorem 4.3.1, let A correspond to a finite G_R-set S. Then φ_0 corresponds to the map of G_R-sets*

$$\mathrm{Bij} : \{*\} \to \mathrm{Hom}([n], S)/S_n$$

sending the single element $*$ to the class of bijections $\mathrm{Bij}([n], S)$.

Proof. By Lemma 4.3.2, the R-algebras $A^{\otimes n}$ and R correspond to $S^n \cong \mathrm{Hom}([n], S)$ and a singleton $\{*\}$, respectively. Therefore the Ferrand map $\varphi_0 : (A^{\otimes n})^{S_n} \to R$ corresponds to a map of G_R-sets

$$\{*\} \to \mathrm{Hom}([n], S)/S_n$$

sending $*$ to an S_n-orbit of $\mathrm{Hom}([n], S)$). We can find out which orbit by changing base to an R-algebra over which A becomes a trivial algebra, such as an algebraically (or separably) closed field. In that case, by Lemma 4.1.2, the S_n-closure fits into a tensor product diagram

$$\begin{array}{ccc} (R^{\mathrm{Hom}([n],S)})^{S_n} & \xrightarrow{\varphi_0} & R \\ \downarrow & & \downarrow \\ R^{\mathrm{Hom}([n],S)} & \longrightarrow & R^{\mathrm{Bij}([n],S)}, \end{array}$$

so the étale set corresponding to the S_n-closure fits into a fibered product diagram by Lemma 4.3.2:

$$\begin{array}{ccc} \mathrm{Hom}([n], S)/S_n & \xleftarrow{\mathrm{Bij}} & \{*\} \\ \uparrow & & \uparrow \\ \mathrm{Hom}([n], S) & \longleftarrow & \mathrm{Bij}([n], S). \end{array}$$

Thus the orbit of $\mathrm{Hom}([n], S)/S_n$ picked out by the Ferrand map is $\mathrm{Bij}([n], S)$. □

We can now describe the G-closures of an étale extension $R \to A$ in terms of its G_R-set:

Theorem 4.3.4. *Let R be a connected ring, and let A be an étale degree-n extension of R corresponding to an n-element G_R-set S. Let G' be the resulting image of G_R in* $\mathrm{Bij}(S, S)$*, and let G be a subgroup of S_n. Then isomorphism classes of G-closures of A over R correspond to G_R-invariant G-orbits of* $\mathrm{Bij}([n], S)$*. Furthermore, if B is the étale R-algebra corresponding to the G_R-set G' (with the action given by post-composition), then every G-closure of A over R is isomorphic to $B^{|G|/|G'|}$ as an R-algebra.*

Remark 4.3.5. Note that, given a G-closure of A over R and its corresponding G_R-invariant G-orbit of $\mathrm{Bij}([n], S)$, we may choose an element $\pi : [n] \xrightarrow{\sim} S$ of that orbit and obtain an identification of $[n]$ with S under which G contains G'. Conversely, such an identification gives rise to a G_R-invariant G-orbit in $\mathrm{Bij}([n], S)$, hence to a G-closure of A over R.

Proof of Theorem 4.3.4. Isomorphism classes of G-closures of A over R correspond to R-algebra homomorphisms $(A^{\otimes n})^G \to R$ restricting to the Ferrand map; see Theorem 2.1.1. By Lemmas 4.2.1, A.3.4, and A.3.5, the R-algebra $(A^{\otimes n})^G$ is étale, so such homomorphisms correspond to G_R-set maps $\{*\} \to \mathrm{Hom}([n], S)/G$ projecting to the class of bijections $\{*\} \to \mathrm{Hom}([n], S)/S_n$. Each such map is entirely defined by the image of $*$, which must therefore be a G_R-invariant G-orbit $\mathcal{O}$ of $\mathrm{Bij}([n], S)$. Furthermore, such an orbit $\mathcal{O}$ fits into a fibered product diagram

$$\begin{array}{ccc} \mathrm{Hom}([n], S)/G & \xleftarrow{\mathcal{O}} & \{*\} \\ \uparrow & & \uparrow \\ \mathrm{Hom}([n], S) & \longleftarrow & \mathcal{O}, \end{array}$$

so $\mathcal{O}$ is the G_R-set corresponding to that G-closure of A over R. This G_R-set is

isomorphic to the disjoint union of $|G|/|G'|$ copies of G', so each G-closure of A over R is isomorphic to $B^{|G|/|G'|}$ as an R-algebra. □

4.4 G-closures of field extensions

In the case of finite separable field extensions, we can make Theorem 4.3.4 even more explicit. We will use the following facts from elementary Galois theory:

Lemma 4.4.1. *Let K be a field with separable closure $\bar{K}$ and absolute Galois group $G_K = \mathrm{Gal}(\bar{K}/K)$ as in Theorem 4.3.1. Let $K \to L$ be a degree-n separable field extension, with corresponding G_K-set $S = \mathrm{Hom}_K(L, \bar{K})$. Let $N = \sum_{s \in S} \mathrm{im}(s) \subseteq \bar{K}$ be the normal closure of L in $\bar{K}$, with Galois group $G' = \mathrm{Gal}(N/K)$.*

1. *Since each $s \in S$ restricts to a homomorphism $L \to N$, the group G' has a natural action on S. This action is faithful, so G' may be regarded as a subgroup of $\mathrm{Bij}(S, S)$.*

2. *The image of G_K in $\mathrm{Bij}(S, S)$ is this subgroup G'. The resulting action of G_K on G' by post-composition is continuous with respect to the profinite topology on G_K, making G' a finite G_K-set.*

3. *The finite G_K-set corresponding to the separable K-algebra N is the G_K-set G'.*

Proof. 1. Let $g \in G'$ and suppose that $g \circ s = s$ for all $s \in \mathrm{Hom}_K(L, N)$. Then for each element $\alpha \in N$, writing α as a sum $\alpha = \sum_s s(\ell_s)$ with $\ell_s \in L$ for each $s \in \mathrm{Hom}_K(L, N)$, we have $g(\alpha) = \sum_s g(s(\ell_s)) = \sum_s s(\ell_s) = \alpha$. Therefore g is the identity element of G', so the action of G' on S is faithful.

2. Every automorphism of $\bar{K}$ over K restricts to an automorphism of N over K, so the map $G_K \to \mathrm{Bij}(S, S)$ factors through G'. Note that the kernel of the homomorphism $G_K \to \mathrm{Bij}(S, S)$ is the set of automorphisms of $\bar{K}$ that restrict

to the identity on N, namely G_N, so we have a group homomorphism $G_K/G_N \to G'$; the fundamental theorem of Galois theory for infinite extensions (see, for example, [7, Thm. 2.3]) tells us that G_N is an open finite-index subgroup of G_K and that $G_K/G_N \to G'$ is an isomorphism, giving G' a continuous G_K-action.

3. Note that N is its own normal closure; composition with $N \hookrightarrow \bar{K}$ is a bijection $G' = \mathrm{Aut}_K(N) \xrightarrow{\sim} \mathrm{Hom}_K(N, \bar{K})$. The action of G_K by post-composition is the same on both sides, so this is an isomorphism of finite G_K-sets. □

We are now in a position to prove Theorem 1.

Theorem 4.4.2. *Let K be a field with separable closure $\bar{K}$ and absolute Galois group $G_K = \mathrm{Gal}(\bar{K}/K)$. Let $K \to L$ be a degree-n separable field extension, with corresponding G_K-set $S = \mathrm{Hom}_K(L, \bar{K})$. Let N be the normal closure of L in $\bar{K}$, with Galois group $G' = \mathrm{Gal}(N/K)$, regarded as a subgroup of $\mathrm{Bij}(S, S)$ and as a finite G_K-set as in Lemma 4.4.1. Let G be a subgroup of S_n. Then the following are equivalent:*

1. *There exists a bijection $\pi : [n] \xrightarrow{\sim} S$ such that G contains $\pi^{-1}G'\pi$.*

2. *There exists a G-closure of L over K.*

Furthermore, every G-closure of L over K is isomorphic to $N^{|G|/|G'|}$ as a K-algebra.

Proof. By Lemma 4.4.1, the subgroup $G' \subseteq \mathrm{Bij}(S, S)$ is the image of G_K, so according to Remark 4.3.5, isomorphism classes of G-closures of L over K correspond to equivalence classes of bijections $\pi : [n] \xrightarrow{\sim} S$ for which $\pi^{-1}G'\pi \subseteq G$; this proves the desired equivalence. In fact, given such a bijection $\pi : i \mapsto \pi_i$, we may form the K-algebra homomorphism $L^{\otimes n} \to N : \ell^{(i)} \mapsto \pi_i(\ell)$. Because $G \supseteq \pi^{-1}G'\pi$, each element of $L^{\otimes n}$ that is invariant under the action of G permuting the tensor factors is sent to a G'-invariant element of N, i.e. an element of $K \subseteq N$. We therefore obtain the desired homomorphism $\varphi : (L^{\otimes n})^G \to K$, and it is straightforward to show, by changing the base to $\bar{K}$ and computing characteristic polynomials there, that this homomorphism

φ is normative. Lastly, because the G_K-set corresponding to N is G', Theorem 4.3.4 tells us that each G-closure of L over K is isomorphic to $N^{|G|/|G'|}$. $\square$

Thus for finite separable field extensions, and more generally for étale extensions, the minimal groups G for which a G-closure exists are all conjugate as subgroups of S_n, and in the case of fields they are the subgroups conjugate to the Galois group of the normal closure of the extension. Furthermore, every G-closure is isomorphic to a power of the minimal closure as an algebra over the base ring. One might hope, then, that this situation generalizes:

Questions 4.4.3. Let R be a ring, and let A be a degree-n extension of R.

1. The set of subgroups $G \subseteq S_n$ for which G-closures of A over R exist is upward-closed by Theorem 3.2.1—are its minimal elements necessarily conjugate to each other, as in the étale case?

2. Let $G \subseteq H$ be subgroups of S_n, and let (B, φ) be a G-closure of A over R. We may restrict $\varphi : (A^{\otimes n})^G \to R$ to $(A^{\otimes n})^H$ to obtain an H-closure of A over R—is this H-closure necessarily isomorphic to $B^{|H|/|G|}$ as an R-algebra, as in the étale case?

The answer to the first question is not yet known; it may be that there is an extension with G_1- and G_2-closures for which G_1 and G_2 are minimal but not conjugate as subgroups of S_n. However, the answer to the second question is No:

Counterexample 4.4.4. Consider a degree-2 extension of the form $\mathbb{Z} \to A := \mathbb{Z}[x]/(x^2 - c^2)$, where $c \in \mathbb{Z}$. It has a 1-closure given by $(\mathbb{Z}, \varphi)$, where $\varphi : A^{\otimes 2} \to \mathbb{Z}$ sends $x \otimes 1 \mapsto c$ and $1 \otimes x \mapsto -c$. However, its S_2-closure is isomorphic to A, and $A \ncong \mathbb{Z}^2$. There is a natural map $A \to \mathbb{Z}^2$ sending $x \mapsto (c, -c)$, which is indeed essentially the only candidate for an isomorphism, but it is bijective if and only if $2c$ is a unit, but this is never the case in $\mathbb{Z}$. Changing the base to one in which $2c$ is invertible would also make the extension étale, as its discriminant is $4c^2$.

Chapter 5

G-closures of monogenic extensions

Recall that a *monogenic extension* of a ring R is an R-algebra of the form $R[x]/(m(x))$ for some monic polynomial $m(x)$; such an algebra is always free of rank $\deg m$ as an R-module. In this chapter, we will always write the polynomial $m(x)$ as

$$m(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \ldots + (-1)^n s_n,$$

so that in $R[x]/(m(x))$ we have $s_k = s_k(x)$ for each $k \in [n]$. and we will investigate G-closures of monogenic extensions for various groups G. First, we will discuss G-closures of extensions with degree 0, 1, or 2, which are all (locally) monogenic. Then we tackle the case of intransitive G-closures, and show that $S_{k_1} \times \ldots \times S_{k_m}$-closures correspond to factorizations of m into factors of degree $k_1, \ldots, k_m$. Finally, we will show, assuming $|G|$ is a non-zerodivisor in R, that G-closures of $R[x]/(m(x))$ over R correspond to R-algebra homomorphisms $(R[x]^{\otimes n})^G \to R$ sending $e_k(x)$ to s_k. By giving generators and relations for $(R[x]^{\otimes n})^G$, then, we can give exact criteria for the existence of G-closures. We do so first for the family $A_n \subseteq S_n$, and then for the single permutation group $D_4 \subseteq S_4$.

5.1 G-closures of extensions with degree ≤ 2

In this section, we analyze extensions of degree at most two and their G-closures. First, note that the only degree-0 extension is the zero algebra $R \to 0$, because the R-module R^0 is the zero module. Its S_0-closure is R, however, because $0^{\otimes 0} \cong R$. In general, letting 1 be the trivial subgroup of S_n, every 1-closure of an extension $R \to A$ is isomorphic to R, because $A^{\otimes n} \bigotimes_{A^{\otimes n}} R \cong R$.

Every degree-1 extension $R \to A$ is isomorphic to R as an algebra of itself. Indeed, for a free extension $A \cong R^1$ with R-basis $\{\theta\}$, its algebra structure is given by $1 = e\theta$ and $\theta^2 = m\theta$ for some $e, m \in R$ satisfying $em = 1$; therefore e is invertible and we can let 1 be a basis element for A, so that the R-algebra homomorphism $R \to A$ is an isomorphism. Then for an arbitrary degree-1 extensions $R \to A$, this map is locally an isomorphism and hence itself an isomorphism. And again, S_1 is the trivial group, so the S_1-closure of $R \to A$ is R.

For degree-2 extensions, the situation becomes more interesting, because $S_2 \ncong 1$ and so having a 1-closure is not automatic.

Theorem 5.1.1. *Let R be a ring, and let A be a degree-2 extension of R. The S_2-closure of A over R is isomorphic to A, and isomorphism classes of 1-closures of A over R correspond to R-algebra homomorphisms $A \to R$.*

Proof. We begin by proving that A is locally monogenic. Indeed, A is locally free, so we will show that a free rank-2 algebra is monogenic. If $\{\theta_1, \theta_2\}$ is a free R-basis for A over R, then the ring structure on A gives us identities $\theta_1^2 = a\theta_1 + b\theta_2$, $\theta_1\theta_2 = c\theta_1 + d\theta_2$, and $1 = i\theta_1 + j\theta_2$ for some $a, b, c, d, i, j \in R$. Then we can deduce that $\theta_1 = (1)\theta_1 = (i\theta_1 + j\theta_2)\theta_1 = i(a\theta_1 + b\theta_2) + j(c\theta_1 + d\theta_2) = (ia + jc)\theta_1 + (ib + jd)\theta_2$, so $ia + jc = 1$ and $ib + jd = 0$. In particular, the two-by-two matrix $\begin{pmatrix} i & j \\ -c & a \end{pmatrix}$ has unit determinant and is therefore invertible over R. Therefore an alternate R-basis

for A is

$$\begin{pmatrix} i & j \\ -c & a \end{pmatrix} \begin{pmatrix} \theta_1 \\ \theta_2 \end{pmatrix} = \begin{pmatrix} i\theta_1 + j\theta_2 \\ -c\theta_1 + a\theta_2 \end{pmatrix} = \begin{pmatrix} 1 \\ \theta \end{pmatrix}$$

where $\theta = -c\theta_1 + a\theta_2$. Hence $\{1, \theta\}$ is an R-basis for A.

Now letting $s, t \in R$ be such that $\theta^2 = s\theta - t$, we have an R-algebra homomorphism $R[x]/(x^2 - sx + t) \to A$ which sends the R-basis $\{1, x\}$ to the R-basis $\{1, \theta\}$, and is thus an isomorphism.

For each monogenic ring $A = R[x]/(x^2 - sx + t)$, there is a canonical R-algebra automorphism $A \to A$ given by $x \mapsto s - x$. Then the S_2-closure of A over R is given by the $A^{\otimes 2} \bigotimes_{(A^{\otimes 2})^{S_2}} R \cong R[x, y]/(x^2 - sx + t, y^2 - sy + t, x + y - s, xy - t)$, which is isomorphic to $R[x]/(x^2 - sx + t) = A$ via $x \mapsto x$ and $y \mapsto s - x$.

This R-algebra automorphism of A may be described in a coordinate-free way as $\sigma : A \to A : a \mapsto s_1(a) - a$, and is therefore independent of choice of generator. Letting A be an arbitrary degree-2 extension of R, there is then a canonical R-algebra involution $\sigma : A \to A$ sending $a \mapsto s_1(a) - a$, since this map is an R-algebra isomorphism on each free localization of A. Note that $a + \sigma(a) = s_1(a)$ and $a\sigma(a) = s_2(a)$. Therefore the homomorphism $A \otimes A \to A$ sending $a \otimes 1 \mapsto a$ and $1 \otimes a \mapsto \sigma(a)$ is normative, giving us a homomorphism from the S_2-closure of A to A, which is locally an isomorphism by the above.

Given that the S_2-closure of A over R is again A, it is automatic that 1-closures of A over R correspond to R-algebra homomorphisms $A \to R$; see Theorem 3.3.1 and the following discussion. □

Note that in the proof of Theorem 5.1.1, we showed that free extensions of degree up to 2 are monogenic, and in particular can be chosen to have 1 as a basis element. This is not necessarily true beginning in degree 3: Let R be a ring with a module P which is not free, but which satisfies $R \oplus P \cong R^3$. (See [3] for an example of such a module.) Giving $A := R \oplus P$ the structure of an R-algebra with trivial multiplication

on $P \otimes P$, we have a free degree-3 extension of R such that the R-module $A/R \cong P$ is not free. Therefore A does not have an R-basis containing 1, and *a fortiori* is not monogenic.

However, we can still give exact criteria for the existence of G-closures for monogenic degree-3 extensions using the results in this and the next chapter. There are four subgroups of S_3 up to conjugation, so four potential Galois groups for rank-3 extensions: S_3 itself, $C_3 = A_3$, $S_2 \times S_1$, and $S_1 \times S_1 \times S_1 = 1$. There is always a unique S_3-closure B of A over R by Theorem 6. If A is a monogenic R-algebra $A = R[x]/(x^3 - sx^2 + tx - u)$, then in Example 6.2.2, we show that C_3-closures of A are in one-to-one correspondence with elements $\gamma \in R$ satisfying the quadratic equation

$$\gamma^2 - (st - 3u)\gamma + (t^3 - 6stu + s^3u + 9u^2) = 0.$$

(Similar equations exist whose solutions parametrize A_n-closures of monogenic rank-n extensions, and are described in Chapter 6.) The subgroups $S_2 \times S_1$ and $S_1 \times S_1 \times S_1$ of S_3 are intransitive and will be covered in the next section.

5.2 G-closures for intransitive G

In this section we show that $S_{k_1} \times \ldots S_{k_\ell}$-closures of $R[x]/(m(x))$ over R correspond to factorizations of $m(x)$ into factors of degrees $k_1, \ldots, k_\ell$. We begin by giving a precise description of $S_{n-1} \times S_1$-closures for $A = R[x]/(m(x))$.

Lemma 5.2.1. *Let $A = R[x]/(m(x))$ be a monogenic degree-n extension of R. Roots of $m(x)$ in R are in one-to-one correspondence with $(S_{n-1} \times S_1)$-closures of A over R. If $\gamma \in R$ is such a root of $m(x)$, then the corresponding $(S_{n-1} \times S_1)$-closure of A is the S_{n-1}-closure of the degree-$(n-1)$ monogenic extension $A' = R[x]/(m(x)/(x-\gamma))$ of R.*

Proof. We argue that roots of $m(x)$ are in one-to-one correspondence with normative R-algebra homomorphisms $(A^{\otimes n})^{S_{n-1}\times S_1} \to R$. First note that if γ is a root of $m(x)$, there exists a unique degree-$(n-1)$ monic polynomial

$$m'(x) = x^{n-1} - s'_1 x^{n-2} + s'_2 x^{n-3} - \ldots + (-1)^{n-1} s'_{n-1}$$

such that $m(x) = m'(x)(x-\alpha)$. This equivalence is due to the fact that such an $m'(x)$ satisfies $s_k = s'_k + \gamma s'_{k-1}$ for each $k \in [n]$, where we set $s_0 = s'_0 = 1$ and $s'_n = 0$. Each s'_k is uniquely determined given s'_{k-1}, so starting from $s'_0 = 1$ we may inductively define s'_k as $s_k - \gamma s'_{k-1}$, and in the end we obtain $s'_n = s_n - s_{n-1}\gamma + s_{n-2}\gamma^2 - \ldots \pm \gamma^n = \pm m(\gamma) = 0$.

If $\varphi : (A^{\otimes n})^{S_{n-1}\times S_1} \to R$ is any R-algebra homomorphism, then let $\gamma = \varphi(x^{(n)}) \in R$, so that $m(\gamma) = m(\varphi(x^{(n)})) = \varphi(m(x^{(n)})) = \varphi(0) = 0$. Then we obtain the factorization $m(x) = m'(x)(x-\alpha)$ described above. For each $k \in [n-1]$, let $e'_k \in A^{\otimes n-1}$ be the kth elementary symmetric polynomial in $x^{(1)}, \ldots, x^{(n-1)}$. We will show that the only normative R-algebra homomorphism $\varphi : (A^{\otimes n})^{S_{n-1}\times S_1} \to R$ that sends $x^{(n)}$ to γ is given by

$$\begin{aligned} \varphi : (A^{\otimes n})^{S_{n-1}\times S_1} \cong (A^{\otimes n-1})^{S_{n-1}} \otimes A &\to R \\ : \quad 1 \otimes x &\mapsto \gamma \\ : \quad e'_k(x) \otimes 1 &\mapsto s'_k \end{aligned}$$

for each $k \in [n-1]$. First, we show that this map is indeed normative. Consider the element $e_k(x) \in A^{\otimes n}$, which corresponds to $e'_{k-1}(x) \otimes x + e'_k(x) \otimes 1$ in $A^{\otimes n-1} \otimes A$. Its image in R is $\gamma s'_{k-1} + s'_k = s_k$, so by Corollary 2.2.6 the map φ is normative.

Conversely, suppose $\varphi : (A^{\otimes n})^{S_{n-1}\times S_1} \to R$ is normative and sends $x^{(n)} \mapsto \gamma$. Then for each $k \in [n]$,

$$s_k = \varphi(e_k(x)) = \varphi(e'_{k-1}(x) \otimes x + e'_k(x) \otimes 1) = \varphi(e'_{k-1}(x) \otimes 1)\gamma + \varphi(e'_k(x) \otimes 1),$$

so by induction on k we have $\varphi(e'_k(x)) = s'_k$. (The edge cases $e'_0(x) = 1$ and $e'_n(x) = 0$ are true by definition.)

Hence this map $\varphi : (A^{\otimes n})^{S_{n-1} \times S_1} \to R$ is the unique normative homomorphism sending $x^{(n)} \mapsto \gamma$, so the $(S_{n-1} \times S_1)$-closures of A over R correspond to roots of $m(x)$ in R.

The corresponding $(S_{n-1} \times S_1)$-closure B_γ of A over R may be described as the quotient

$$\begin{aligned} B_\gamma &\cong A^{\otimes n}/(x^{(n)} - \gamma, e'_k(x) \otimes 1 - s'_k : k \in [n-1]) \\ &\cong A^{\otimes n-1}/(e'_k(x) - s'_k : k \in [n-1]). \end{aligned}$$

Over B, the polynomial $m'(x)$ factors as $\prod_{i \in [n-1]}(x - x^{(i)})$, so $m'(x^{(i)}) = 0$ for each $i \in [n-1]$. Thus this quotient is

$$\begin{aligned} B_\gamma &\cong A^{\otimes n-1}/(m'(x^{(i)}), e'_k(x) - s'_k : i, k \in [n-1]) \\ &\cong A'^{\otimes n-1}/(e'_k(x) - s'_k : k \in [n-1]), \end{aligned}$$

which is the S_{n-1}-closure of A' over R, as desired. □

Similarly, if $n = \sum_j k_j$ is a partition of n, we find a correspondence between $(\prod_j S_{k_j})$-closures of A and factorizations $m(x) = \prod_j m_j(x)$, where each $m_j(x)$ has degree k_j.

Theorem 5.2.2. *Let $A = R[x]/(m(x))$ be a monogenic degree-n extension of R, and let $n = \sum_j k_j$ be a partition of n. Factorizations $m(x) = \prod_j m_j(x)$, where each $m_j(x) \in R[x]$ has degree k_j, are in one-to-one correspondence with $(\prod_j S_{k_j})$-closures of A over R. Given such a factorization, the corresponding $(\prod_j S_{k_j})$-closure of A is the tensor product of the S_{k_j}-closures of each $A_j = R[x]/(m_j(x))$ over R.*

Proof. Suppose $\varphi : (A^{\otimes n})^{\prod_j S_{k_j}} \to R$ is normative; then in the corresponding $(\prod_j S_{k_j})$-closure, the polynomial $m(x)$ factorizes as

$$m(x) = \prod_{i \in [n]} (x - x^{(i)}).$$

Breaking this product up into $\prod_j S_{k_j}$-orbits, we obtain a factorization of $m(x)$ as $\prod_j m_j(x)$ with $\deg m_j(x) = k_j$; the coefficients of each $m_j(x)$ belong to R because they belong to $(A^{\otimes n})^{\prod_j S_{k_j}}$. Conversely, φ is determined by the images of these coefficients, and it is the map given by

$$(A^{\otimes n})^{\prod_j S_{k_j}} \cong \bigotimes_j (A^{\otimes k_j})^{S_{k_j}} \to \bigotimes_j (A_j^{\otimes k_j})^{S_{k_j}} \to R.$$

Thus the $(\prod_j S_{k_j})$-closures of A correspond to factorizations $m(x) = \prod_j m_j(x)$ with $\deg m_j(x) = k_j$ for each j. □

Corollary 5.2.3. *Let $A = R[x]/(m(x))$ be a monogenic degree-n extension of R. If $m(x)$ is irreducible over R, then A has G-closures only for transitive $G \subseteq S_n$. Conversely, if $m(x)$ is reducible over R, then there exists an intransitive $G \subseteq S_n$ such that A has a G-closure.*

Proof. If $m(x)$ is reducible over R, then by Theorem 5.2.2, there exists an $S_k \times S_{n-k}$-closure for some $k \in [n-1]$. Meanwhile, every intransitive subgroup $G \subseteq S_n$ is contained in $S_k \times S_{n-k}$ up to conjugation, for some $k \in [n-1]$, and the existence of a G-closure implies the existence of an $(S_k \times S_{n-k})$-closure, and hence a factorization of $m(x)$. □

5.3 An alternative description of G-closures

In this section, we provide a parametrization of G-closures for monogenic extensions that is similar to Theorem 5, but that is more helpful in establishing the existence of G-closures.

The first step is to simplify our description of G-closures when they exist:

Lemma 5.3.1. *Let $A = R[x]/(m(x))$ be a monogenic degree-n extension of R, and let $\varphi : A^{\otimes n} \to B$ be a G-closure of A over R. Then*

$$B \cong R[x_1, \ldots, x_n] \bigotimes_{R[x_1,\ldots,x_n]^G} R,$$

where the map $R[x_1, \ldots, x_n]^G \to R$ is the restriction of the composite $R[x_1, \ldots, x_n] \to A^{\otimes n} \to B$.

Proof. First, recall that

$$B \cong A^{\otimes n} \bigotimes_{(A^{\otimes n})^G} R$$

by definition. Second, note that since $R[x] \to A$ is a surjection, by Lemma A.3.9 so is $R[x_1, \ldots, x_n]^G \cong (R[x]^{\otimes n})^G \to (A^{\otimes n})^G$. Therefore we may write

$$B \cong A^{\otimes n} \bigotimes_{R[x_1,\ldots,x_n]^G} R\,,$$

since a tensor product is unchanged if its base is extended by an epimorphism. Third, consider the tensor product

$$R[x_1, \ldots, x_n] \bigotimes_{R[x_1,\ldots,x_n]^G} R\,.$$

Since $m(x)$ factors over this ring as

$$m(x) = \prod_{i \in [n]} (x - x_i),$$

we have $m(x_i) = 0$ for each $i \in [n]$. Therefore

$$R[x_1, \ldots, x_n] \bigotimes_{R[x_1,\ldots,x_n]^G} R = R[x_1, \ldots, x_n] \bigotimes_{R[x_1,\ldots,x_n]^G} R \Big/ (m(x_i) : i \in [n]) \cong A^{\otimes n} \bigotimes_{R[x_1,\ldots,x_n]^G} R \cong B.$$

□

Under reasonably mild conditions, every such tensor product is also a G-closure:

Lemma 5.3.2. *Let $A = R[x]/(m(x))$ be a monogenic degree-n extension of R, and let G be a subgroup of S_n. Let $R[x_1, \ldots, x_n]^G \to R$ be an R-algebra homomorphism sending $e_k(x) \mapsto s_k$ for each $k \in [n]$. Define an R-algebra B by*

$$B = R[x_1, \ldots, x_n] \bigotimes_{R[x_1,\ldots,x_n]^G} R\ .$$

Then B is naturally an $A^{\otimes n}$-algebra, and if the R-algebra homomorphism $R \to B$ is injective, then $A^{\otimes n} \to B$ is a G-closure of A over R.

Proof. Over B, the polynomial $m(x)$ factors as $m(x) = \prod_{i \in [n]} (x - x_i)$, so $m(x_i) = 0$ in B for each $i \in [n]$. Thus

$$B = R[x_1, \ldots, x_n] \bigotimes_{R[x_1,\ldots,x_n]^G} R \cong A^{\otimes n} \bigotimes_{R[x_1,\ldots,x_n]^G} R$$

is an $A^{\otimes n}$-algebra, as desired. Now suppose the canonial homomorphism $R \to B$ is

injective. Consider the image factorization of the composite

$$\begin{aligned} & R[x_1, \ldots, x_n]^G \twoheadrightarrow (A^{\otimes n})^G \to A^{\otimes n} \to B \\ = {} & R[x_1, \ldots, x_n]^G \to R[x_1, \ldots, x_n] \to A^{\otimes n} \to B \\ = {} & R[x_1, \ldots, x_n]^G \to R[x_1, \ldots, x_n] \to B \\ = {} & R[x_1, \ldots, x_n]^G \twoheadrightarrow R \hookrightarrow B. \end{aligned}$$

The image of $(A^{\otimes n})^G$ in B is thus contained in R, and we obtain a factorization of $R[x_1, \ldots, x_n]^G \to R$ as

$$R[x_1, \ldots, x_n]^G \to (A^{\otimes n})^G \to R.$$

Then the R-algebra homomorphism $(A^{\otimes n})^G \to R$ sends $e_k(x)$ to s_k for each $k \in [n]$, so it is normative, and by Lemma 5.3.1, the corresponding G-closure of A is B. $\square$

In order to use Lemma 5.3.2, we need criteria for proving that

$$R \to R[x_1, \ldots, x_n] \bigotimes_{R[x_1, \ldots, x_n]^G} R$$

is injective. The following lemma provides a quick-and-dirty, but nonetheless useful, guarantee:

Lemma 5.3.3. *Let R be a ring, let n be a natural number, and let G be a finite group acting on an R-algebra A. Let $A^G \to R$ be an R-algebra homomorphism, and construct the R-algebra homomorphism $R \to A \bigotimes_{A^G} R$. If $|G|$ is a non-zerodivisor in R, then this homomorphism is injective.*

Proof. Consider the A^G-module homomorphism $A \to A^G$ given by $p \mapsto \sum_{\sigma \in G} \sigma.p$. The composite $A^G \to A \to A^G$ is then just multiplication by $|G|$. Changing the base along $A^G \to R$, the composite R-linear map $R \to A \bigotimes_{A^G} R \to R$ is still just

multiplication by $|G|$. Since $|G|$ is a non-zerodivisor in R, this R-linear map $R \to R$ is injective, and therefore the map $R \to A \bigotimes_{A^G} R$ must be injective as well. $\square$

Corollary 5.3.4. *Let $A = R[x]/(m(x))$ be a monogenic degree-n extension of R, and let $G \subseteq S_n$ with $|G|$ a non-zerodivisor in R. Then isomorphism classes of G-closures of A over R correspond to R-algebra homomorphisms $R[x_1, \ldots, x_n]^G \to R$ sending $e_k(x) \mapsto s_k$.*

Proof. By Lemmas 5.3.1 and 5.3.2, isomorphism classes of G-closures of A over R correspond to R-algebra homomorphisms $R[x_1, \ldots, x_n]^G \to R$ such that $e_k(x) \mapsto s_k$ and

$$R \to R[x_1, \ldots, x_n] \bigotimes_{R[x_1, \ldots, x_n]^G} R$$

is injective. By Lemma 5.3.3, since $|G|$ is a non-zerodivisor the latter condition is guaranteed to hold. $\square$

5.4 A_n-closures

In this section we give generators and relations for $R[x_1, \ldots, x_n]^{A_n}$ as an $R[x_1, \ldots, x_n]^{S_n}$-algebra, and combine this presentation with our earlier results to parametrize A_n-closures of monogenic extensions.

Lemma 5.4.1. *Let n be a natural number. Then $\mathbb{Z}[x_1, \ldots, x_n]^{A_n}$ is a $\mathbb{Z}[x_1, \ldots, x_n]^{S_n}$-module with free basis $\{1, \Gamma\}$, where Γ is the A_n-orbit sum of $\prod_{i=1}^{n} x_i^{i-1}$.*

Proof. First, for each $p \in \mathbb{Z}[x_1, \ldots, x_n]^{A_n}$, denote the action of any odd permutation on p by $\tilde{p}$. Then it is easily calculated that

$$\Gamma - \widetilde{\Gamma} = \prod_{i>j} (x_i - x_j).$$

Now let $p \in \mathbb{Z}[x_1, \ldots, x_n]^{A_n}$. We know that $p - \tilde{p} \mapsto 0$ in $\mathbb{Z}[x_1, \ldots, x_n]/(x_i - x_j)$ for each pair $i > j$. Therefore $p - \tilde{p}$ contains a factor of $(x_i - x_j)$ whenever $i > j$, so $p - \tilde{p}$ is a multiple of $\Gamma - \widetilde{\Gamma}$. Write

$$(p - \tilde{p}) = q(\Gamma - \widetilde{\Gamma});$$

every permutation either fixes both sides or changes the sign of both sides, so it must be the case that $q \in \mathbb{Z}[x_1, \ldots, x_n]^{S_n}$. Now define r as $p - q\Gamma$. Then $r - \tilde{r} = (p - \tilde{p}) - q(\Gamma - \widetilde{\Gamma}) = 0$, so $r \in \mathbb{Z}[x_1, \ldots, x_n]^{S_n}$ as well. Thus we have written

$$p = q\Gamma + r$$

with q and $r \in \mathbb{Z}[x_1, \ldots, x_n]^{S_n}$, so 1 and Γ generate $\mathbb{Z}[x_1, \ldots, x_n]^{A_n}$ as a $\mathbb{Z}[x_1, \ldots, x_n]^{S_n}$-module. To show they are a free basis, suppose that $q\Gamma + r = 0$ with q and r in $\mathbb{Z}[x_1, \ldots, x_n]^{S_n}$. Then we also have $0 = q\widetilde{\Gamma} + r$, so

$$0 = q(\Gamma - \widetilde{\Gamma}).$$

Since $\mathbb{Z}[x_1, \ldots, x_n]$ is a domain and $\Gamma - \widetilde{\Gamma} \neq 0$, we must have $q = 0$, and therefore $r = 0$ as well. □

Corollary 5.4.2. *Let R be a ring and let n be a natural number. Then*

$$R[x_1, \ldots, x_n]^{S_n}[x]/((x - \Gamma)(x - \widetilde{\Gamma})) \cong R[x_1, \ldots, x_n]^{A_n}$$

as $R[x_1, \ldots, x_n]^{S_n}$-algebras.

Proof. The isomorphism is given by $x \mapsto \Gamma$. This homomorphism is bijective since it maps the $R[x_1, \ldots, x_n]^{S_n}$-module basis $\{1, x\}$ to the $R[x_1, \ldots, x_n]^{S_n}$-module basis $\{1, \Gamma\}$. □

Theorem 5.4.3. *Let R be a ring, and let n be a natural number such that $|A_n| = n!/2$ is a non-zerodivisor in R. Let $A = R[x]/(m(x))$ be a monogenic degree-n extension of R, and let $\varphi_0 : R[x_1, \ldots, x_n]^{S_n} \to R$ be the R-algebra homomorphism sending $e_k(x) \mapsto s_k$ for each $k \in [n]$. Then isomorphism classes of A_n-closures of A over R correspond to roots in R of the quadratic polynomial*

$$x^2 - \varphi_0(\Gamma + \widetilde{\Gamma})x + \varphi_0(\Gamma\widetilde{\Gamma}).$$

Proof. By Corollary 5.3.4, isomorphism classes of A_n-closures of A over R correspond to R-algebra homomorphisms $R[x_1, \ldots, x_n]^{A_n} \to R$ sending $e_k(x) \mapsto s_k$. And by Lemma 5.4.2, such homomorphisms correspond to $R[x_1, \ldots, x_n]^{S_n}$-algebra homomorphisms

$$R[x_1, \ldots, x_n]^{S_n}[x]/(x^2 - (\Gamma + \widetilde{\Gamma})x + \Gamma\widetilde{\Gamma}) \to R,$$

where R is an $R[x_1, \ldots, x_n]^{S_n}$-algebra via the map φ_0. Such a homomorphism is completely determined by the image of x in R, which must then be a solution to

$$x^2 - \varphi_0(\Gamma + \widetilde{\Gamma})x + \varphi_0(\Gamma\widetilde{\Gamma}) = 0$$

as desired. □

Example 5.4.4. Let $A = R[x]/(x^3 - sx^2 + tx - u)$, and suppose $|A_3| = 3$ is a non-zerodivisor in R. Then $\Gamma \in R[x, y, z] = x^2y + y^2z + xz^2$ and $\widetilde{\Gamma} = x^2z + xy^2 + yz^2$.

Then

$$\begin{aligned}
\Gamma + \widetilde{\Gamma} &= x^2y + y^2z + xz^2 + x^2z + xy^2 + yz^2 \\
&= (xy + xz + yz)(x + y + z) - 3(xyz) \\
&= e_2(x)e_1(x) - 3e_3(x), \text{ so} \\
\varphi_0(\Gamma + \widetilde{\Gamma}) &= s_2(x)s_1(x) - 3s_3(x) \\
&= st - 3u.
\end{aligned}$$

Similarly,

$$\begin{aligned}
\Gamma\widetilde{\Gamma} &= (x^2y + y^2z + xz^2)(x^2z + xy^2 + yz^2) \\
&= (xy + xz + yz)^3 - 6(x + y + z)(xy + xz + yz)(xyz) \\
&\quad + (x + y + z)^3(xyz) + 9(xyz)^2 \\
&= e_2(x)^3 - 6e_1(x)e_2(x)e_3(x) + e_1(x)^3e_3(x) + 9e_3(x)^2, \text{ so} \\
\varphi_0(\Gamma\widetilde{\Gamma}) &= s_2(x)^3 - 6s_1(x)s_2(x)s_3(x) + s_1(x)^3s_3(x) + 9s_3(x)^2 \\
&= t^3 - 6stu + s^3u + 9u^2.
\end{aligned}$$

Therefore isomorphism classes of A_3-closures of A over R correspond to roots in R of

$$x^2 - (st - 3u)x + (t^3 - 6stu + s^3u + 9u^2).$$

5.5 D_4-closures

In this section we give generators and relations for $R[x_1, x_2, x_3, x_4]^{D_4}$ as an algebra over $R[x_1, x_2, x_3, x_4]^{S_4}$, and use this presentation to show that if 2 is a non-zerodivizor in R, then D_4-closures of $R[x]/(m(x))$ correspond to roots in R of the resolvent cubic of $m(x)$, where $D_4 \subseteq S_4$ is the subgroup generated by the permutations (13) and

(1234).

Lemma 5.5.1. *The ring* $\mathbb{Z}[x_1, x_2, x_3, x_4]^{D_4}$ *is a free* $\mathbb{Z}[x_1, x_2, x_3, x_4]^{S_4}$*-module with basis* $\{1, \Lambda, \Lambda^2\}$*, where* $\Lambda = x_1x_3 + x_2x_4$*.*

Proof. First, we fix some helpful notation. If $p \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{D_4}$, 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 $\{p, p', p''\}$:

$$(23) \text{ and } (14) \text{ interchange } p \leftrightarrow p' \text{ and fix } p''$$

$$(12) \text{ and } (34) \text{ interchange } p \leftrightarrow p'' \text{ and fix } p'$$

$$(13) \text{ and } (24) \text{ interchange } p' \leftrightarrow p'' \text{ and fix } p.$$

If $p \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{D_4}$ and any two of $\{p, p', p''\}$ are equal, then $p \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{S_4}$. In particular, Λ, Λ', and Λ'' are all distinct:

$$\Lambda - \Lambda' = (x_1 - x_4)(x_3 - x_2)$$

$$\Lambda - \Lambda'' = (x_1 - x_2)(x_3 - x_4)$$

$$\Lambda' - \Lambda'' = (x_1 - x_3)(x_2 - x_4).$$

Now note that if $p \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{D_4}$, then $p - p' \mapsto 0$ in $\mathbb{Z}[x_1, x_2, x_3, x_4]/(x_1 - x_4)$ or $\mathbb{Z}[x_1, x_2, x_3, x_4]/(x_2 - x_3)$, so $p - p'$ must contain factors of both $(x_1 - x_4)$ and $(x_2 - x_3)$. 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 $\Lambda - \Lambda'$. By acting with (12), it follows that $p' - p''$ is a multiple of $\Lambda' - \Lambda''$, and in fact, the ratio $\rho = \frac{p' - p''}{\Lambda' - \Lambda''}$ belongs to $\mathbb{Z}[x_1, x_2, x_3, x_4]^{D_4}$:

$$(13).\rho = (13).\left(\frac{p' - p''}{\Lambda' - \Lambda''}\right) = \frac{p'' - p'}{\Lambda'' - \Lambda'} = \rho,$$

and

$$\begin{aligned}(1234).\rho &= (12)(23)(34).\rho \\ &= (12)(23)(34).\left(\frac{p'-p''}{\Lambda'-\Lambda''}\right) \\ &= (12)(23).\left(\frac{p'-p}{\Lambda'-\Lambda}\right) \\ &= (12).\left(\frac{p-p'}{\Lambda-\Lambda'}\right) \\ &= \frac{p''-p'}{\Lambda''-\Lambda'} = \rho.\end{aligned}$$

Now we will show that 1, Λ, and Λ^2 are linearly independent over $\mathbb{Z}[x_1,x_2,x_3,x_4]^{S_4}$. Suppose $q\Lambda^2+r\Lambda+s=0$, with $q,r,s\in\mathbb{Z}[x_1,x_2,x_3,x_4]^{S_4}$. 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 $s=0$.

Finally, we show that each $p\in\mathbb{Z}[x_1,x_2,x_3,x_4]^{D_4}$ may be written as a linear combination of 1, Λ, and Λ^2 with coefficients in $\mathbb{Z}[x_1,x_2,x_3,x_4]^{S_4}$. Let $\rho=\frac{p'-p''}{\Lambda'-\Lambda''}$; then $\rho\in\mathbb{Z}[x_1,x_2,x_3,x_4]^{D_4}$ as before. Now set

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

We claim that $q \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{S_4}$. 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

$$r = \rho - q(\Lambda' + \Lambda'') \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{D_4}.$$

Again, we claim that $r \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{S_4}$, 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

$$s = p - q\Lambda^2 - r\Lambda \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{D_4}.$$

Again, we claim that $s \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{S_4}$:

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

Once again, the numerator and denominator each change sign under the action of any transposition, so s is fixed by $\mathbb{Z}[x_1, x_2, x_3, x_4]^{S_4}$. Thus we have written $p = q\Lambda^2 + r\Lambda + s$ with $q, r, s \in \mathbb{Z}[x_1, x_2, x_3, x_4]^{S_4}$, as desired. □

Corollary 5.5.2. *Let R be a ring. Then*

$$R[x_1, x_2, x_3, x_4]^{S_4}[x]/((x-\Lambda)(x-\Lambda')(x-\Lambda'')) \cong R[x_1, x_2, x_3, x_4]^{D_4}$$

as $R[x_1, x_2, x_3, x_4]^{S_4}$-algebras.

Proof. The isomorphism is given by $x \mapsto \Lambda$. This homomorphism is bijective since it maps the $R[x_1, x_2, x_3, x_4]^{S_4}$-module basis $\{1, x, x^2\}$ to the $R[x_1, x_2, x_3, x_4]^{S_4}$-module basis $\{1, \Lambda, \Lambda^2\}$. □

Theorem 5.5.3. *Let R be a ring such that 2 is a non-zerodivisor in R. Let $A = R[x]/(m(x))$ be a monogenic degree-4 extension of R, and let $\varphi_0 : R[x_1, x_2, x_3, x_4]^{S_4} \to R$ be the R-algebra homomorphism sending $e_k(x) \mapsto s_k$ for each $k \in [n]$. Then isomorphism classes of D_4-closures of A over R correspond to roots in R of the cubic polynomial*

$$x^3 - \varphi_0(\Lambda + \Lambda' + \Lambda'')x^2 + \varphi_0(\Lambda\Lambda' + \Lambda\Lambda'' + \Lambda'\Lambda'')x - \varphi_0(\Lambda\Lambda'\Lambda''),$$

called the resolvent cubic *of $m(x)$.*

Proof. Since 2 is a non-zerodivisor in R, so is $|D_4| = 8$, so by Corollary 5.3.4, isomorphism classes of D_4-closures of A over R correspond to R-algebra homomorphisms $R[x_1, x_2, x_3, x_4]^{D_4} \to R$ sending $e_k(x) \mapsto s_k$. And by Lemma 5.5.2, such homomorphisms correspond to $R[x_1, x_2, x_3, x_4]^{S_4}$-algebra homomorphisms

$$R[x_1, x_2, x_3, x_4]^{S_4}[x]/(x^3 - (\Lambda + \Lambda' + \Lambda'')x^2 + (\Lambda\Lambda' + \Lambda\Lambda'' + \Lambda'\Lambda'')x - (\Lambda\Lambda'\Lambda'')) \to R,$$

where R is an $R[x_1, \ldots, x_n]^{S_n}$-algebra via the map φ_0. Such a homomorphism is completely determined by the image of x in R, which must then be a solution to

$$x^3 - \varphi_0(\Lambda + \Lambda' + \Lambda'')x^2 + \varphi_0(\Lambda\Lambda' + \Lambda\Lambda'' + \Lambda'\Lambda'')x - \varphi_0(\Lambda\Lambda'\Lambda''),$$

as desired. □

Chapter 6

A_n-closures revisited

In Chapter 4, we showed that the G-closures of a field extension exists exactly when G contains the Galois group of that field extension. For example, if R is a field in which 2 is a unit, and A is a rank-n R-algebra, then A has an A_n-closure if and only if the discriminant of A over R is a square in R. In this section, we show that the previous sentence holds if we replace "field" with "ring." Then we return to the quadratic polynomial of Theorem 5.4.3, and show that its roots in R parametrize A_n-closures of A without any assumptions on the ring R. Finally, we relax the condition that 2 be a unit for A_n-closures to correspond to square roots of the discriminant.

Throughout this section, we will no longer be assuming that A is monogenic, but we will assume that A is free of rank n as an R-module. This allows us to define the discriminant of A over R as

$$D(\theta_1, \ldots, \theta_n) = \det \begin{pmatrix} s_1(\theta_1\theta_1) & \cdots & s_1(\theta_1\theta_n) \\ \vdots & \ddots & \vdots \\ s_1(\theta_n\theta_1) & \cdots & s_1(\theta_n\theta_n) \end{pmatrix} = \det \Big(s_1(\theta_i\theta_j) \Big)_{ij}$$

for each R-basis $\{\theta_1, \ldots, \theta_n\}$; the discriminant is only well-defined up to multiplication by square units in R.

6.1 A_n-closures and discriminants

We know that if Θ is a free R-basis for A, then a free R-basis for $(A^{\otimes n})^{S_n}$ is given by $\{e(\alpha) : \alpha \in \Theta^n/S_n\}$. It will be helpful to know similar bases for $(A^{\otimes n})^{A_n}$. To that end, we define two distinguished elements of $(A^{\otimes n})^{A_n}$ that do not belong to $(A^{\otimes n})^{S_n}$.

Definition 6.1.1. Let A be an R-algebra with free R-basis $\Theta = \{\theta_1, \ldots, \theta_n\}$. Define $\Gamma \in A^{\otimes n}$ as the A_n-orbit sum of $\theta_1 \otimes \theta_2 \otimes \ldots \otimes \theta_n$, that is,

$$\Gamma = \sum_{\sigma \in A_n} \prod_{i=1}^{n} \theta_i^{(\sigma(i))}.$$

Let $\widetilde{\Gamma}$ be the unique other element of $A^{\otimes n}$ in the S_n-orbit of Γ, so that

$$\Gamma + \widetilde{\Gamma} = e([(\theta_1, \ldots, \theta_n)]).$$

Note that both Γ and $\widetilde{\Gamma}$ are fixed by the action of A_n on $A^{\otimes n}$, and hence belong to $(A^{\otimes n})^{A_n}$.

Lemma 6.1.2. *Let A be an R-algebra with free R-basis $\Theta = \{\theta_1, \ldots, \theta_n\}$. Either of the following is a free R-basis for $(A^{\otimes n})^{A_n}$:*

$$\{e(\alpha) : \alpha \in \Theta^n/S_n \text{ and } \alpha \neq [(\theta_1, \ldots, \theta_n)]\} \cup \{\Gamma, \widetilde{\Gamma}\}, \quad \{e(\alpha) : \alpha \in \Theta^n/S_n\} \cup \{\Gamma\}.$$

In particular, $(A^{\otimes n})^{A_n}$ is the direct sum of its submodules $(A^{\otimes n})^{S_n}$ and $R\Gamma$.

Proof. The former basis is the more natural; it consists precisely of A_n-orbit sums of pure tensors $\theta_{i_1} \otimes \ldots \otimes \theta_{i_n}$. The reason is that if $\alpha = [(\theta_{i_1}, \ldots, \theta_{i_n})]$ contains any element of multiplicity at least 2, there is some transposition in S_n that fixes $\theta_{i_1} \otimes \ldots \otimes \theta_{i_n}$, and so the A_n-orbit of $\theta_{i_1} \otimes \ldots \otimes \theta_{i_n}$ is the full S_n-orbit. The only other possibility is that $(\theta_{i_1}, \ldots, \theta_{i_n})$ contains each element of Θ exactly once, in which case the A_n-orbit sum of $\theta_{i_1} \otimes \ldots \otimes \theta_{i_n}$ is either Γ or $\widetilde{\Gamma}$. And since an element of $A^{\otimes n}$ is

fixed by A_n if and only if the coefficients of its basis pure tensors are constant along A_n-orbit sums, this set forms a free R-basis for $(A^{\otimes n})^{A_n}$.

That the second set is also a free R-basis is demonstrated by the invertibility of (the nontrivial block of) the change-of-basis matrix:

$$\begin{pmatrix} \Gamma \\ \widetilde{\Gamma} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \Gamma \\ \Gamma + \widetilde{\Gamma} \end{pmatrix}. \qquad \square$$

Remark 6.1.3. Note that while $\Gamma + \widetilde{\Gamma} = e([(\theta_1, \ldots, \theta_n)])$ is an S_n-invariant, the difference $\Gamma - \widetilde{\Gamma}$ changes sign under the action of odd permutations, and may be written as a determinant:

$$\begin{aligned} \Gamma - \widetilde{\Gamma} &= \sum_{\sigma \in A_n} \prod_{i=1}^{n} \theta_i^{(\sigma(i))} - \sum_{\sigma \in S_n \setminus A_n} \prod_{i=1}^{n} \theta_i^{(\sigma(i))} \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} \theta_i^{(\sigma(i))} \\ &= \det \left(\theta_i^{(j)} \right)_{ij}. \end{aligned}$$

Lemma 6.1.4. *Let A be an R-algebra with free R-basis $\Theta = \{\theta_1, \ldots, \theta_n\}$. Under any normative homomorphism $(A^{\otimes n})^{A_n} \to R$, the image of $\Gamma - \widetilde{\Gamma}$ in R is a square root of the discriminant $D(\theta_1, \ldots, \theta_n)$ of A over R, with respect to the basis Θ.*

Proof. From Remark 6.1.3 we know that $\Gamma - \widetilde{\Gamma} = \det \left(\theta_i^{(j)} \right)_{ij} = \det \left(\theta_k^{(j)} \right)_{jk}$. Multiplying these two expressions, we obtain

$$\begin{aligned} (\Gamma - \widetilde{\Gamma})^2 &= \det \left(\theta_i^{(j)} \right)_{ij} \det \left(\theta_k^{(j)} \right)_{jk} = \det \left(\left(\theta_i^{(j)} \right)_{ij} \left(\theta_k^{(j)} \right)_{jk} \right) \\ &= \det \left(\sum_j \theta_i^{(j)} \theta_k^{(j)} \right)_{ik} = \det \left(e_1(\theta_i \theta_k) \right)_{ik} \\ &\mapsto \det \left(s_1(\theta_i \theta_k) \right)_{ik} = D(\theta_1, \ldots, \theta_n). \end{aligned}$$

Therefore the image of $(\Gamma - \widetilde{\Gamma})$ must be an element of R whose square is the discriminant $D(\theta_1, \ldots, \theta_n)$ of A over R. $\square$

Because of the significance of the quantity $(\Gamma - \widetilde{\Gamma})$, we would rather use it than Γ as a basis element of $(A^{\otimes n})^{A_n}$. However, this is only convenient when 2 is a unit:

Lemma 6.1.5. *Suppose R is a ring in which 2 is a unit, and let A be an R-algebra with free R-basis $\Theta = \{\theta_1, \ldots, \theta_n\}$. Then the following is a free R-basis for $(A^{\otimes n})^{A_n}$:*

$$\{e(\alpha) : \alpha \in \Theta^n/S_n\} \cup \{\Gamma - \widetilde{\Gamma}\}.$$

In particular, $(A^{\otimes n})^{A_n}$ is the direct sum of its submodules $(A^{\otimes n})^{S_n}$ and $R(\Gamma - \widetilde{\Gamma})$.

Proof. Starting from the free basis $\{e(\alpha) : \alpha \in \Theta^n/S_n\} \cup \{\Gamma\}$ for $(A^{\otimes n})^{A_n}$ as in Lemma 6.1.2, the nontrivial block of the change-of-basis matrix is

$$\begin{pmatrix} \Gamma + \widetilde{\Gamma} \\ \Gamma - \widetilde{\Gamma} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} \Gamma + \widetilde{\Gamma} \\ \Gamma \end{pmatrix}.$$

Since the determinant is 2, a unit in R, we may replace Γ by $\Gamma - \widetilde{\Gamma}$ in the R-basis for $(A^{\otimes n})^{A_n}$. $\square$

Remark 6.1.6. Notice that in the decomposition

$$(A^{\otimes n})^{A_n} \cong (A^{\otimes n})^{S_n} \oplus R(\Gamma - \widetilde{\Gamma}),$$

the R-multiples of $\Gamma - \widetilde{\Gamma}$ are the only ones that change sign under the action of odd permutations on the tensor factors. Therefore each product of the form $e(\alpha)(\Gamma - \widetilde{\Gamma})$, which also changes sign under odd permuations, must itself be an R-multiple of $(\Gamma - \widetilde{\Gamma})$ (and not just an $A^{\otimes n}$-multiple). So if we have any hope of a ring homomorphism extension of $f : (A^{\otimes n})^{S_n} \to R$ to all of $(A^{\otimes n})^{A_n}$, that R-multiple had better be $s(\alpha)(\Gamma - \widetilde{\Gamma})$.

In fact, the equation $e(\alpha)(\Gamma - \widetilde{\Gamma}) = s(\alpha)(\Gamma - \widetilde{\Gamma})$ does in fact hold in $A^{\otimes n}$ for each multiset $\alpha \in A^n/S_n$. We will prove this fact first in the special case that $\alpha = [(a, \ldots, a)]$ for some $a \in A$, and then deduce the general case.

Lemma 6.1.7. *Let A be an R-algebra with free R-basis $\Theta = \{\theta_1, \ldots, \theta_n\}$. Then for each element $a \in A$, the following identity holds in the ring $A^{\otimes n}$:*

$$\Delta(a)(\Gamma - \widetilde{\Gamma}) = \det(a)(\Gamma - \widetilde{\Gamma}),$$

where $\Delta(a)$ is the pure tensor $a \otimes \ldots \otimes a$ and $\det(a)$ is the determinant of the $n \times n$ matrix given by the R-linear action of multiplication by a on the R-basis Θ.

Proof. Using Remark 6.1.3, and the fact that $\Delta(a) = \prod_{j=1}^{n} a^{(j)}$, we have:

$$\begin{aligned}\Delta(a)(\Gamma - \widetilde{\Gamma}) &= \left(\prod_{j=1}^{n} a^{(j)}\right) \det\left(\theta_i^{(j)}\right)_{ij} \\ &= \det\left(a^{(j)}\theta_i^{(j)}\right)_{ij}.\end{aligned}$$

Now if we write each $a\theta_i$ as an R-linear combination $a\theta_i = \sum_{k=1}^{n} a_{ik}\theta_k$, where the a_{ik} are appropriate elements of R, we may continue:

$$\begin{aligned}\Delta(a)(\Gamma - \widetilde{\Gamma}) &= \det\left(\sum_k a_{ik}\theta_k^{(j)}\right)_{ij} \\ &= \det\left(\left(a_{ik}\right)_{ik}\left(\theta_k^{(j)}\right)_{kj}\right) \\ &= \det\left(a_{ik}\right)_{ik} \det\left(\theta_k^{(j)}\right)_{kj} \\ &= \det(a)(\Gamma - \widetilde{\Gamma}),\end{aligned}$$

since the matrix on the left is just the transpose of the matrix corresponding to multiplication by a in the R-basis Θ. □

Corollary 6.1.8. *Let A be an R-algebra with free R-basis Θ. For each multiset $\alpha \in A^n/S_n$, the following identity holds in the ring $A^{\otimes n}$:*

$$e(\alpha)(\Gamma - \widetilde{\Gamma}) = s(\alpha)(\Gamma - \widetilde{\Gamma}).$$

Proof. Letting I be any finite subset of A, apply Lemma 6.1.7 to the ring $R' = R[\lambda_a : a \in I]$ and R'-algebra $A' = A[\lambda_a : a \in I]$. (Since $A' = A \otimes_R R'$, Θ is still a free R'-basis for A'.) We have

$$\Delta\left(\sum_{a\in I} \lambda_a a\right)(\Gamma - \widetilde{\Gamma}) = \det\left(\sum_{a\in I} \lambda_a a\right)(\Gamma - \widetilde{\Gamma}),$$

which we can rewrite as

$$\sum_{\alpha\in I^n/S_n} \lambda^\alpha e(\alpha)(\Gamma - \widetilde{\Gamma}) = \sum_{\alpha\in I^n/S_n} \lambda^\alpha s(\alpha)(\Gamma - \widetilde{\Gamma}).$$

Comparing the coefficients of λ^α, we find that $e(\alpha)(\Gamma - \widetilde{\Gamma}) = s(\alpha)(\Gamma - \widetilde{\Gamma})$. □

We are now ready to prove the main theorem of this section.

Theorem 6.1.9. *Let R be a ring in which 2 is a unit, and let A be a free degree-n extension of R. If D is the discriminant of A over R computed with respect to any basis, then there is a one-to-one correspondence between square roots of D in R and isomorphism classes of A_n-closures of A over R. In particular, an A_n-closure exists if and only if the discriminant is a square in R.*

Proof. Let $\Theta = \{\theta_1, \ldots, \theta_n\}$ be a free R-basis for A. Note that by Lemma 6.1.5, each R-linear extension of f to $(A^{\otimes n})^{A_n}$ is uniquely determined by the image of $\Gamma - \widetilde{\Gamma}$, and by Lemma 6.1.4, if this extension is to be a ring homomorphism we must have $\Gamma - \widetilde{\Gamma}$ map to a square root of $D(\theta_1, \ldots, \theta_n)$ in R.

Conversely, we show that for each square root d of $D(\theta_1, \ldots, \theta_n)$ in R, the assignment $\Gamma - \widetilde{\Gamma} \mapsto d$ does extend f to a ring homomorphism $(A^{\otimes n})^{A_n} \to R$. We need only check multiplicativity of the extension on basis elements $\{e(\alpha) : \alpha \in \Theta^n/S_n\} \cup \{\Gamma - \widetilde{\Gamma}\}$. We already have $e(\alpha)e(\beta) \mapsto s(\alpha)s(\beta)$ since f is a ring homomorphism. And we have $(\Gamma - \widetilde{\Gamma})^2 \mapsto d^2 = D(\theta_1, \ldots, \theta_n)$ as required, by assumption. So all that remains to check is multiplicativity on the product $e(\alpha)(\Gamma - \widetilde{\Gamma})$. But by Corollary 6.1.8, we have

$$e(\alpha)(\Gamma - \widetilde{\Gamma}) = s(\alpha)(\Gamma - \widetilde{\Gamma}) \mapsto s(\alpha)d$$

as required. Therefore each choice of square root d for the image of $(\Gamma - \widetilde{\Gamma})$ uniquely determines a ring homomorphism extension of f to all of $(A^{\otimes n})^{A_n}$. □

6.2 A_n-closures and the quadratic criterion

There is a more general condition guaranteeing the existence of A_n-closures. There is a quadratic polynomial over R whose roots correspond to isomorphism classes of A_n-closures:

Theorem 6.2.1. *Let R be a ring, and let A be a degree-n extension of R with free R-basis Θ. Then the universal algebra over which A has an A_n-closure is*

$$(A^{\otimes n})^{A_n} \bigotimes_{(A^{\otimes n})^{S_n}} R \cong R[x]/(x^2 - \varphi_0(\Gamma + \widetilde{\Gamma})x + \varphi_0(\Gamma\widetilde{\Gamma})).$$

Therefore, solutions γ in R to the quadratic equation $\gamma^2 - \varphi_0(\Gamma + \widetilde{\Gamma})\gamma + \varphi_0(\Gamma\widetilde{\Gamma}) = 0$ correspond to normative R-algebra homomorphisms $(A^{\otimes n})^{A_n} \to R$, and hence to isomorphim classes of A_n-closures of A over R.

Proof. We show that $R' = (A^{\otimes n})^{A_n} \bigotimes_{(A^{\otimes n})^{S_n}} R$ has a free R-basis given by 1 and the image of Γ. Consider that R' may be presented as an R-module in the following way, where

angle brackets denote the R-linear span:

$$\begin{aligned} R' &\cong (A^{\otimes n})^{A_n}/(e(\alpha) - s(\alpha) : \alpha \in \Theta^n/S_n) \\ &= (A^{\otimes n})^{A_n}/(\langle e(\beta)(e(\alpha) - s(\alpha)) : \alpha, \beta \in \Theta^n/S_n\rangle + \langle \Gamma(e(\alpha) - s(\alpha)) : \alpha \in \Theta^n/S_n\rangle). \end{aligned}$$

Note that each $\Gamma(e(\alpha) - s(\alpha))$ is S_n-invariant; its image under any transposition is $\widetilde{\Gamma}(e(\alpha) - s(\alpha))$, but these are equal by Lemma 6.1.8.

Now note that $R + (e(\alpha) - s(\alpha) : \alpha \in \Theta^n/S_n)$ contains each $e(\alpha)$ and in turn consists only of S_n-invariant elements, so $R + (e(\alpha) - s(\alpha) : \alpha \in \Theta^n/S_n) = (A^{\otimes n})^{S_n}$. Therefore the quotient of R' by the image of R is isomorphic to

$$\begin{aligned} R'/R &\cong (A^{\otimes n})^{A_n}/(R + (e(\alpha) - s(\alpha) : \alpha \in \Theta^n/S_n)) \\ &\cong (A^{\otimes n})^{A_n}/(A^{\otimes n})^{S_n} \\ &= (\langle e(\alpha) : \alpha \in \Theta^n/S_n\rangle \oplus \langle \Gamma\rangle)/\langle e(\alpha) : \alpha \in \Theta^n/S_n\rangle \cong \langle \Gamma\rangle, \end{aligned}$$

a free R-module with R-basis $\{\Gamma\}$. It follows that the homomorphism $R \to R'$ is injective, or else some nontrivial R-multiples of Γ would vanish. Therefore R' has free R-basis $\{1, \Gamma\}$. Since $\Gamma^2 = (\Gamma + \widetilde{\Gamma})\Gamma - (\Gamma\widetilde{\Gamma}) = \varphi_0(\Gamma + \widetilde{\Gamma})\Gamma - \varphi_0(\Gamma\widetilde{\Gamma})$ in R', we thus have a bijective homomorphism

$$R[x]/(x^2 - \varphi_0(\Gamma + \widetilde{\Gamma})x + \varphi_0(\Gamma\widetilde{\Gamma})) \xrightarrow{\sim} R',$$

as desired. □

Example 6.2.2. Recall the monogenic degree-3 extension $A = R[x]/(x^3 - sx^2 + tx - u)$. Using the R-basis $(1, x, x^2)$, we may write

$$\Gamma = 1 \otimes x \otimes x^2 + x \otimes x^2 \otimes 1 + x^2 \otimes 1 \otimes x.$$

The calculation in Example 5.4.4 shows that $\varphi_0(\Gamma + \widetilde{\Gamma}) = st - 3u$ and that $\varphi_0(\Gamma\widetilde{\Gamma}) =$

$t^3-6stu+s^3u+9u^2$. Then an A_3-closure of A over R exists if and only if the quadratic equation

$$\gamma^2 - (st - 3u)\gamma + (t^3 - 6stu + s^3u + 9u^2) = 0$$

has a solution for γ in R.

Recall that an element p of a ring R is called *primoid* if, whenever a and b are elements of R with ab divisible by p^2, then a or b is divisible by p. The importance of this property is found primarily in the following lemma:

Lemma 6.2.3. *Let R be a ring, and let $m(x) = x^2 + bx + c$ be a monic quadratic polynomial with $s, t \in R$. Suppose that 2 is a primoid non-zerodivisor of R. Then roots of m in R correspond to square roots in R of the discriminant $D = b^2 - 4c$.*

Proof. Suppose m has a root $r \in R$, and let $r' = -b - r$. Then $r + r' = -b$ and $rr' = -br - r^2 = c$, so $(r - r')^2 = r^2 - 2rr' + r'^2 = (r + r')^2 - 4(rr') = b^2 - 4c = D$, so $(r - r') = 2r + b$ is a square root of D in R.

Conversely, suppose d is a square root of D in R. Then $b^2 - 4c = d^2$, so $(-b + d)(-b - d) = b^2 - d^2 = 4c$ is a multiple of 4. Since 2 is primoid in R, either $-b + d$ or $-b - d$ is a multiple of 2, and hence both are, since they differ by $2d$. Since 2 is a non-zerodivisor in R, division by 2 is well-defined whenever possible, so $\frac{-b\pm d}{2}$ are well-defined elements of R. We have

$$\frac{-b+d}{2} + \frac{-b-d}{2} = \frac{-2b}{2} = -b \text{ and}$$

$$\frac{-b+d}{2}\frac{-b-d}{2} = \frac{b^2-d^2}{4} = \frac{4c}{4} = c,$$

because 2 is a non-zerodivisor in R. Therefore $r = \frac{-b+d}{2}$ is a root of m in R. Lastly, the operations $r \mapsto 2r + b$ and $d \mapsto (-b + d)/2$ are inverses to each other, so the correspondence is one-to-one. □

We can combine Theorem 6.2.1 with Lemma 6.2.3 to weaken the hypotheses of Theorem 6.1.9:

Corollary 6.2.4. *Let R be a ring in which 2 is a primoid non-zerodivisor, and let A be an R-algebra with free R-basis $\Theta = \{\theta_1, \ldots, \theta_n\}$. If $D(\theta_1, \ldots, \theta_n)$ is the discriminant of A over R with respect to the basis Θ, then there is a one-to-one correspondence between square roots of $D(\theta_1, \ldots, \theta_n)$ in R and isomorphism classes of A_n-closures of A over R.*

Proof. The only fact to check is that the discriminant of the quadratic polynomial

$$x^2 - \varphi_0(\Gamma + \widetilde{\Gamma})x + \varphi_0(\Gamma\widetilde{\Gamma})$$

is equal to $D(\theta_1, \ldots, \theta_n)$. But the discriminant of the quadratic is

$$(\varphi_0(\Gamma + \widetilde{\Gamma}))^2 - 4\varphi_0(\Gamma\widetilde{\Gamma}) = \varphi_0((\Gamma - \widetilde{\Gamma})^2),$$

which is $D(\theta_1, \ldots, \theta_n)$ by Lemma 6.1.4. □

The condition in this lemma that 2 be primoid is necessary. The following is an example of a degree-2 extension in which 2 is a non-zerodivisor and for which the discriminant is square, but the extension has no A_2-closure:

Example 6.2.5. Let R be the ring $\mathbb{Z}[\sqrt{5}]$, and let A be the monogenic R-algebra $R[x]/(x^2-x-1)$. The discriminant of this extension is $D(1, x) = 5$, a square in R, but there is no R-algebra homomorphism $A^{\otimes 2} \to R$, hence no A_2-closure of A, because the golden ratio $\Phi = \frac{1+\sqrt{5}}{2}$ is not an element of R. Indeed, the number 2 is not a primoid element of R, since $(1 + \sqrt{5})(1 - \sqrt{5}) = -4$ is a multiple of 4, while neither of $1 \pm \sqrt{5}$ is a multiple of 2 in R. And we should not desire there to be an A_2-closure: if one existed, then employing base extension along the ring homomorphism $\mathbb{Z}[\sqrt{5}] \to \mathbb{F}_2$,

we would also obtain an A_2-closure for the field extension $\mathbb{F}_2 \subseteq \mathbb{F}_2[x]/(x^2-x-1) \cong \mathbb{F}_4$. But the latter is an S_2-extension, so it should not have an A_2-closure.

It is not hard to invent similar examples of degree-3 ring extensions whose discriminants are square, but which do not have an A_3-closure for precisely the same reason.

Appendix A

Appendix

A.1 Multisets

In the following, we will make heavy use of the notion of *multisets*, which like sets are unordered collections of elements, but which allow duplicates. Specifically, we define multisets as follows:

Definition A.1.1. Let X be a set, and $d \in \mathbb{N}$ a natural number. Define an S_d-action on X^d by $\sigma : (x_1, \ldots, x_d) \mapsto (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(d)})$ for each $\sigma \in S_d$. For each subgroup G of S_d, define X^d/G to be the set of orbits of X^d under the action of G. Write the G-orbit of an element $(x_1, \ldots, x_d)$ of X^d as $[(x_1, \ldots, x_d)]_G$, or as $[(x_1, \ldots, x_d)]$ if $G = S_d$. A *multiset from X of size d* is an element of X^d/S_d. We write $\xi \sqsubseteq X$ to mean that ξ is a multiset from X of unspecified finite size. For each multiset α we denote its size by $|\alpha|$.

Remark A.1.2. We may alternatively define a multiset by noting that the only information retained in passing from $(x_1, \ldots, x_d)$ to $[(x_1, \ldots, x_d)] = \xi$ is how often each $x \in X$ appears in $(x_1, \ldots, x_d)$, called its *multiplicity* $\xi(x)$. Then we may alternatively let a multiset of size d be a function $\xi : X \to \mathbb{N}$ such that $\sum_{x \in X} \xi(x) = d$ (and in particular, $\xi(x)$ is nonzero for only finitely many $x \in X$). We will use both of these

notations, and write $x \in \xi$ to mean that $x = x_j$ for some j whenever $\alpha = [(x_1, \ldots, x_d)]$, or equivalently, that $\alpha(x) > 0$. On occasion, we will also use the nuts-and-bolts definition of a multiset as an equivalence class and write $(x_1, \ldots, x_d) \in \xi$ to mean that $[(x_1, \ldots, x_d)] = \xi$, but whether this or the previous meaning of "$\in \xi$" is meant should be clear from context.

Definition A.1.3. Let X and Y be sets, and let $f : X \to Y$ be a function. Let d be a natural number and G a subgroup of S_d. We define the *pushforward* $f_* : X^d/G \to Y^d/G$ by

$$f_* : [(x_1, \ldots, x_d)]_G \mapsto [(f(x_1), \ldots, f(x_d))]_G.$$

In particular, if $\{y_i : i \in I\}$ is an indexed family of elements of Y, and α is a multiset from I, we can form the pushforward multiset $y_\alpha \sqsubseteq Y$ in the same manner.

Definition A.1.4. Multisets are closely connected to monomials: if multiplication in a set Y makes sense, and if we have an indexed set $\{\theta_i : i \in I\}$ of elements of Y (or equivalently, if we have a function $\theta : I \to Y$), and if α is a multiset of elements of I, then we define θ^α to be the monomial

$$\theta^\alpha = \prod_{i \in \alpha} \theta_i^{\alpha(i)}.$$

Example A.1.5. If we are working in $Y = R[x_1, x_2, \ldots, x_n]$ for some ring R, then we may view the indeterminate variables as a function $x : \{1, 2, \ldots, n\} \to Y$ and write, for each multiset of indices α,

$$x^\alpha = x_1^{\alpha(1)} x_2^{\alpha(2)} \cdots x_n^{\alpha(n)},$$

as is often conventional to do. In particular, an R-basis for the d-graded component of $R[x_1, x_2, \ldots, x_n]$ is given by $\{x^\alpha : \alpha \in [n]^d/S_d\}$.

Example A.1.6. Similarly, if $\Theta = \{\theta_i : i \in I\}$ is a free R-basis for a module M, then the symmetric power $\mathrm{Sym}^n(M) = M^{\otimes n}/S_n$ has a natural R-basis given by the set of monomials $\{\theta^\alpha : \alpha \in I^n/S_n\}$, which is in a one-to-one correspondence with the set Θ^n/S_n of multisets from Θ of size n.

A.2 Polynomial laws

The definitive text on polynomial laws is N. Roby's, [12]. In this section we cover the main definitions and examples we will be using, to save the effort of translating (literally and figuratively) between there and here.

Definition A.2.1. Let R be a ring. Then if M and N are two R-modules, a *polynomial law* $p : M \to N$ is a family of functions $p_S : S \otimes M \to S \otimes N$ for each R-algebra S, such that the family is compatible in the sense that, for each R-algebra homomorphism $S \to T$, the following square commutes:

$$\begin{array}{ccc} S \otimes M & \to & S \otimes N \\ \downarrow & & \downarrow \\ T \otimes M & \to & T \otimes N \end{array}$$

If furthermore for all R-algebras S and for all $a \in S, m \in S \otimes M$, we have

$$p_S(a \cdot m) = a^d \cdot p_S(m),$$

then we say that $p : M \to N$ is *homogeneous of degree d*.

We will denote the set of polynomial laws $M \to N$ by $\mathrm{Poly}(M, N)$, and the set of those which are homogeneous of degree d by $\mathrm{Poly}_d(M, N)$. Both naturally are equipped with the structure of an R-module, making $\mathrm{Poly}_d(M, N)$ a submodule of $\mathrm{Poly}(M, N)$.

Remark A.2.2. We can understand Definition A.2.1 categorically as follows: If M is an R-module, define the functor $U_M : R\text{-}\mathbf{Alg} \to \mathbf{Set}$ by mapping each R-algebra S to the underlying set of $S \otimes M$, and each R-algebra homomorphism $S \to T$ to the induced function $S \otimes M \to T \otimes M$. Then a polynomial law $M \to N$ is just a natural transformation $U_M \to U_N$.

Remark A.2.3. Each polynomial law $p : M \to N$ gives, in particular, a function $p_R : M \to N$. However, the mapping $p \mapsto p_R$ is not injective: let $R = \mathbb{F}_q$ and define a polynomial law $p : R \to R$ by $p_S : S \to S : s \mapsto s^q - s$. This is not the zero law (since, for example, $p_{R[x]}(x) \neq 0$), but p_R is identically 0.

Example A.2.4. Two basic constructions for polynomial laws follow:

1. Each R-linear map $f : M \to N$ induces a homogeneous degree-1 polynomial law $p : M \to N$ given by $p_S = \mathrm{id}_S \otimes f : S \otimes M \to S \otimes N$. More generally, each multilinear map $M_1 \times \cdots \times M_k \to N$ induces in the same way a polynomial law which is homogeneous of degree k.

2. If $M \to N$ and $N \to P$ are polynomial laws, then for each R-algebra S we may form the composite function $S \otimes M \to S \otimes N \to S \otimes P$, which together form a polynomial law $M \to P$. If $M \to N$ and $N \to P$ are homogeneous of degrees d and e, then $M \to P$ is homogeneous of degree de.

Putting these two constructions together, we immediately obtain our first non-trivial example of a polynomial law:

Lemma A.2.5. *If M is an R-module and d is a natural number, then the family of diagonal maps*

$$\Delta_S : (S \otimes M) \to S \otimes (M^{\otimes d}) \cong (S \otimes M)^{\otimes_S d}$$
$$: m \mapsto m \otimes \ldots \otimes m \text{ for all } m \in S \otimes M$$

defines a homogeneous polynomial law $\Delta : M \to M^{\otimes d}$ of degree d.

Proof. One can either verify this directly, or form the composite polynomial law

$$M \to M^d \to M^{\otimes d},$$

where the first law comes from the linear diagonal embedding $m \mapsto (m, \ldots, m)$ and the second from the canonical multilinear map defining $M^{\otimes d}$. □

Lemma A.2.6. *If M is an R-module and p, q are polynomial laws $M \to R$, then the product polynomial law $pq : M \to R$ defined by*

$$(pq)_S = p_S q_S$$

is well-defined. Furthermore, if p and q are homogeneous of degrees d and e, then pq is homogeneous of degree $d + e$.

Proof. As suggested, for each R-algebra S define $(pq)_S$ to be the product function

$$\begin{aligned} p_S q_S : S \otimes M &\to S \\ : \sum_i s_i \otimes m_i &\mapsto p_S \left(\sum_i s_i \otimes m_i \right) q_S \left(\sum_i s_i \otimes m_i \right) \end{aligned}$$

This forms a compatible family: for each R-algebra homomorphism $f : S \to T$, we have the composite $f \circ (pq)_S : S \otimes M \to S \to T$ sending

$$\begin{aligned} \sum_i s_i \otimes m_i &\mapsto p_S \left(\sum_i s_i \otimes m_i \right) q_S \left(\sum_i s_i \otimes m_i \right) \\ &\mapsto f \left(p_S \left(\sum_i s_i \otimes m_i \right) q_S \left(\sum_i s_i \otimes m_i \right) \right) \\ &= f \left(p_S \left(\sum_i s_i \otimes m_i \right) \right) f \left(q_S \left(\sum_i s_i \otimes m_i \right) \right) \end{aligned}$$

since f is multiplicative. Therefore

$$\sum_i s_i \otimes m_i = p_T\left(\sum_i f(s_i) \otimes m_i\right) q_T\left(\sum_i f(s_i) \otimes m_i\right)$$

since p and q are both compatible with f. But this is the composite

$$(pq)_T \circ (f \otimes M) : S \otimes M \to T \otimes M \to T,$$

so pq is a well-defined polynomial law.

Furthermore, if p and q are homogeneous of degrees d and e, respectively, then for each S with $s \in S$ and $m \in S \otimes M$, we have

$$(pq)_S(s \cdot m) = p_S(s \cdot m)q_S(s \cdot m) = s^d \cdot p_S(m) \cdot s^e \cdot q_S(m) = s^{d+e} \cdot (pq)_S(m),$$

so pq is homogeneous of degree $d + e$. □

Lemma A.2.7. *If M and N are R-modules, and $M^* = \mathrm{Hom}(M, R)$ is the dual module to M, then there is a canonical map of R-modules*

$$\mathrm{Sym}^d(M^*) \otimes N \to \mathrm{Poly}_d(M, N)$$

sending an element of the form $(f_1 f_2 \cdots f_d) \otimes n_0$ to the law $p : M \to N$ defined by

$$\begin{aligned} p_S &: S \otimes M \to S \otimes N \\ &: s \otimes m \mapsto s^d(f_1(m)f_2(m)\cdots f_d(m)) \otimes n_0. \end{aligned}$$

Proof. First consider that each element of $M^* = \mathrm{Hom}(M, R)$ induces a polynomial law of degree 1 from M to R, so by Lemma A.2.6 there is a function

$$(M^*)^d \to \mathrm{Poly}_d(M, R)$$

sending a d-tuple $(f_1, f_2, \ldots, f_d)$ to the product law $f_1 f_2 \cdots f_d$. Since this function is multilinear and symmetric, it corresponds to a single linear map

$$\mathrm{Sym}^d(M^*) \to \mathrm{Poly}_d(M, R).$$

Tensoring this linear map with $N = \mathrm{Hom}(R, N) \to \mathrm{Poly}_1(R, N)$, we have

$$\mathrm{Sym}^d(M^*) \otimes N \to \mathrm{Poly}_d(M, R) \otimes \mathrm{Poly}_1(R, N) \to \mathrm{Poly}_d(M, N). \qquad \square$$

Lemma A.2.8. *Let M and N be R-modules, and $p : M \to N$ a polynomial law. Then for each finite set I there is a unique collection of polynomial laws*

$$p^{(\alpha)} : M^I \to N$$

for each α a multiset from I, such that $p^{(\alpha)}$ is separately homogeneous of degree $\alpha(i)$ in the i-th argument for all $i \in I$, and such that for each R-algebra S and elements $s = (s_i)_{i \in I} \in S^I$ and $m = (m_i)_{i \in I} \in (S \otimes M)^I$, we have

$$p_S\left(\sum_{i \in I} s_i m_i\right) = \sum_{\alpha \sqsubseteq I} p_S^{(\alpha)}(sm) = \sum_{\alpha \sqsubseteq I} s^\alpha p_S^{(\alpha)}(m).$$

We call $p^{(\alpha)}((m_i)_{i \in I})$ the coefficient of λ^α in $p\left(\sum_{i \in I} \lambda_i m_i\right)$.

Proof. Indeed, consider the ring $T = R[\lambda_i : i \in I]$, and for each $m = (m_i)_{i \in I} \in (S \otimes M)^I$ let $p_S^{(\alpha)}(m)$ be the coefficient of λ^α in

$$p_{S \otimes T}\left(\sum_{i \in I} \lambda_i m_i\right) \in (S \otimes T) \otimes N \cong (S \otimes N)[\lambda_i : i \in I].$$

Then compatibility of the p_S requires that the $p_S^{(\alpha)} : (S \otimes M)^I \to S \otimes N$ be compatible, be homogeneous of degree $\alpha(i)$ in each m_i, and sum to p_S in the manner required. $\square$

In particular, we may decompose polynomial laws by homogeneous degree; c.f. [12, Prop. I.4]:

Corollary A.2.9. *Every polynomial law can be written uniquely as a sum of homogeneous polynomial laws.*

Proof. Apply Lemma A.2.8 in the case $I = \{1\}$; a multiset α from $\{1\}$ is entirely determined by the multiplicity $d = \alpha(1)$, so a decomposition of $p : M \to N$ into the $p^{(\alpha)} : M \to N$ is precisely the same as a decomposition of p into a sum of homogeneous components. □

Remark A.2.10. The sums in Lemma A.2.8 and Corollary A.2.9 may not be finite; it may be that infinitely many of the $p^{(\alpha)}$ are nonzero for a fixed p. However, each sum will by construction have only finitely many nonzero terms for each choice of arguments, and so the sum makes sense elementwise. Consider, for example, the polynomial law $\mathbb{Z}^{\oplus\infty} \to \mathbb{Z}$ defined, for each ring S, by sending each sequence of elements $(s_1, s_2, s_3, \ldots)$ in $S \otimes (\mathbb{Z}^{\oplus\infty}) \cong S^{\oplus\infty}$ to the sum of all its finite products $1 + s_1 + s_2 + s_3 + \ldots + s_1s_2 + s_1s_3 + \ldots + s_2s_3 + \ldots + s_1s_2s_3 + \ldots$. Since every sequence in $S^{\oplus\infty}$ has only finitely many nonzero elements, this sum eventually terminates, but because the degrees of its terms can be unboundedly large, this law is not any finite sum of homogeneous polynomial laws.

Corollary A.2.11. *Every homogeneous degree-*1 *polynomial law is linear, and every homogeneous degree-*0 *polynomial law is constant; see [12, Props. 1.5-6].*

Proof. Let M and N be R-modules, and $p : M \to N$ be a homogeneous degree-1 polynomial law; we wish to show that there exists a linear map $f : M \to N$ such that $p_S = \mathrm{id}_S \otimes f : S \otimes M \to S \otimes N$. Since p is homogeneous of degree 1, we find from Lemma A.2.8 with $|I| = 2$ that there exist polynomial laws $q, q' : M^2 \to N$, each

homogeneous of degree 1, such that, for each $s, s' \in S$ and $m, m' \in S \otimes M$,

$$p_S(sm + s'm') = sq_S(m, m') + s'q'_S(m, m').$$

Setting $s = 1$ and $s' = 0$, this equation tells us that $p_S(m) = q_S(m, m')$. Similarly, we find that $p_S(m') = q'_S(m, m')$. Therefore we may write

$$p_S(sm + s'm') = sp_S(m) + s'p_S(m').$$

Thus each p_S is a linear function, and using linearity and compatibility of the p_S, we find that $p_S = \mathrm{id}_S \otimes p_R$ as desired.

Now suppose instead that $p : M \to N$ is homogeneous of degree 0, and again apply Lemma A.2.8 with $|I| = 2$. Since there is only one multiset of size 0, we find that there exists a polynomial law $q : M^2 \to N$, homogeneous of degree 0, such that, for each $s, s' \in S$ and $m, m' \in S \otimes M$, we have

$$p_S(sm + s'm') = q_S(m, m').$$

Setting $s = 1$ and $s' = 0$, we find that $p_S(m) = q_S(m, m')$, so the latter is independent of m'. Similarly, we find that $q_S(m, m')$ is independent of m. Therefore $p_S(m) = q_S(m, m')$ so $p_S(m) = 1 \otimes m_0$ for some $m_0 \in M$ independent of S by compatibility. $\square$

Definition A.2.12. Let R be a ring, and let M be an R-module. Let d be a natural number and let α be a finite subset of M^d. We define $e(\alpha) \in M^{\otimes d}$ as the sum

$$e(\alpha) = \sum_{(m_1,\ldots,m_d)\in\alpha} m_1 \otimes \ldots \otimes m_d.$$

In particular, if G is a subgroup of S_d, then $e([(m_1, m_2, \ldots, m_d)]_G) \in (M^{\otimes d})^G$ is the orbit sum of $m_1 \otimes \ldots \otimes m_d$ under the action of G permuting the tensor factors.

Lemma A.2.13. *Let M be an R-module, and $\Delta : M \to M^{\otimes d}$ the homogeneous degree-d polynomial law of Lemma A.2.5. Let $\alpha \in M^d/S_d$ be a multiset of d elements of M. Then $e(\alpha) \in M^{\otimes d}$ is is the coefficient of λ^α in $\Delta\left(\sum_{m\in\alpha} \lambda_m m\right)$, so that*

$$\Delta_S : \sum_{m\in M} s_m \otimes m \mapsto \sum_{\alpha\in M^d/S_d} s^\alpha \cdot e(\alpha)$$

for each R-algebra S and choice of $\sum_{m\in M} s_m \otimes m$ in $S \otimes M$.

Proof. Let I be the set of elements of α to avoid confusion, and consider the image of $\sum_{m\in I} \lambda_m m$ under Δ:

$$\begin{aligned}\Delta\left(\sum_{m\in I} \lambda_m m\right) &= \left(\sum_{m_1\in I} \lambda_{m_1} m_1\right) \otimes \ldots \otimes \left(\sum_{m_d\in I} \lambda_{m_d} m_d\right) \\ &= \sum_{(m_1,\ldots,m_d)\in I^d} \left(\prod_{j=1}^{d} \lambda_{m_j}\right) m_1 \otimes \ldots \otimes m_d\end{aligned}$$

The only terms whose coefficient is $\lambda^\alpha = \prod_{m\in\alpha} \lambda_m$ are those for which $(m_1, \ldots, m_d)$ are exactly the elements of α in some order, that is, for which $(m_1, \ldots, m_d)$ is an element of the equivalence class defining α. Thus the coefficient of λ^α is

$$e(\alpha) = \sum_{(m_1,\ldots,m_d)\in\alpha} m_1 \otimes \ldots \otimes m_d,$$

as desired. □

A.3 Polynomial laws for locally free modules

In this section, we are largely concerned with finding natural operations on R-modules $M \mapsto M'$ such that homogeneous degree-d polynomial laws $M \to N$ are in canonical correspondence with linear maps $M' \to N$. In general, such operations are given by divided powers algebras $M' = \Gamma_d(M)$; see [12, Thm. 4.1]. We are more interested

in parametrizing degree-d polynomial laws out of M by linear homomorphisms of $(M^{\otimes d})^{S_d}$; the latter is isomorphic to $\Gamma_d(M)$ whenever $n!$ is a unit in R (see [12, Cor. to Thm. III.3]) or M is flat (see [4, 5.5.2.5]), but in general they are different (see [9]). Here, we will show directly that $\mathrm{Poly}_d(M, N)$ is naturally isomorphic to $\mathrm{Hom}((M^{\otimes d})^{S_n}, N)$ when M is locally free.

If we know M to be free, the following result offers a useful and complete description of polynomial laws out of M; see [12, Thm. I.1] for the case that M is also finitely generated.

Lemma A.3.1. *Suppose M and N are modules over a ring R, and suppose further that M has a free R-basis Θ. Then every polynomial law $p : M \to N$ is of the form*

$$p_S\left(\sum_{\theta\in\Theta} s_\theta \otimes \theta\right) = \sum_{\alpha\sqsubseteq\Theta} s^\alpha \otimes n_\alpha$$

where $\sum_{\theta\in\Theta}(s_\theta \otimes \theta)$ is an arbitrary element of $S \otimes M$, α ranges over all multisets from Θ, and the n_α are fixed elements of N such that, for each finite subset F of Θ, only finitely many n_α with $\alpha \sqsubseteq F$ are nonzero.

Proof. Consider the ring $T = R[\lambda_\theta : \theta \in \Theta]$. The formal sum $\sum_{\theta\in\Theta} \lambda_\theta \otimes \theta$ does not correspond to any element of $T \otimes M$ if Θ is infinite, but we may form the sum

$$\Sigma_F = \sum_{\theta\in F} \lambda_\theta \otimes \theta \in T \otimes M$$

for each finite subset $F \subseteq \Theta$. For each such sum Σ_F, apply the component p_T of p to obtain an element $\sum_{\alpha\sqsubseteq\Theta} \lambda^\alpha \otimes n_{F,\alpha} \in T \otimes N$, where only finitely many of the $n_{F,\alpha}$ are nonzero. And in fact, using the fact that p_T must be compatible with the map $f_F : T \to T$ sending $\lambda_\theta \mapsto \lambda_\theta$ if $\theta \in F$ and $\lambda_\theta \mapsto 0$ otherwise, we find that $n_{F,\alpha} = 0$ unless $\alpha \sqsubseteq F$, so we have

$$p_T(\Sigma_F) = \sum_{\alpha\sqsubseteq F} \lambda^\alpha \otimes n_{F,\alpha}.$$

Furthermore, if F is contained in a larger finite subset $G \subseteq \Theta$, we may consider the image of $p_T(\Sigma_G)$ under $f_F \otimes N$. On the one hand, by compatibility we must obtain $p_T(\Sigma_F)$ since $f_F \otimes M : \Sigma_G \mapsto \Sigma_F$. On the other hand, we have

$$p_T(\Sigma_G) = \sum_{\alpha \sqsubseteq G} \lambda^\alpha \otimes n_{G,\alpha} \mapsto \sum_{\alpha \sqsubseteq F} \lambda^\alpha \otimes n_{G,\alpha}$$

since $f_F : \lambda^\alpha \mapsto 0$ unless $\alpha \sqsubseteq F$. Comparing the coefficients of λ^α in the two expressions, we must have $n_{G,\alpha} = n_{F,\alpha}$ whenever $F \subseteq G$, or indeed, whenever F and G both contain α. Therefore, setting $n_\alpha = n_{F,\alpha}$ whenever $\alpha \sqsubseteq F$, we have

$$p_T(\Sigma_F) = \sum_{\alpha \sqsubseteq F} \lambda^\alpha \otimes n_\alpha.$$

Now for each R-algebra S, and each element $\sum_{\theta \in \Theta} s_\theta \otimes \theta$ of $S \otimes M$, let $F = \{\theta \in \Theta : s_\theta \neq 0\}$, which is finite. Defining $f : T \to S : \lambda_\theta \mapsto s_\theta$, we have $(f \otimes M) : \Sigma_F \mapsto \sum_{\theta \in \Theta} s_\theta \otimes \theta$, so therefore

$$\begin{aligned}(f \otimes N) : p_T(\Sigma_F) &\mapsto p_S\left(\sum_{\theta \in \Theta} s_\theta \otimes \theta\right) \\ &: \sum_{\alpha \sqsubseteq F} \lambda^\alpha \otimes n_\alpha \mapsto \sum_{\alpha \sqsubseteq F} s^\alpha \otimes n_\alpha.\end{aligned}$$

And therefore

$$p_S\left(\sum_{\theta \in \Theta} s_\theta \otimes \theta\right) = \sum_{\alpha \sqsubseteq F} s^\alpha \otimes n_\alpha = \sum_{\alpha \sqsubseteq \Theta} s^\alpha \otimes n_\alpha$$

since $s^\alpha = 0$ if $\alpha \not\sqsubseteq F$, as desired.

Conversely, suppose $\{n_\alpha\}$ is a family of elements of N for each multiset α from Θ, such that for each finite subset $F \subseteq \Theta$, only finitely many n_α with $\alpha \sqsubseteq F$ are nonzero. Then we may define a polynomial law $p : M \to N$ whose components are

given by

$$p_S\left(\sum_{\theta\in\Theta} s_\theta \otimes \theta\right) = \sum_{\alpha\sqsubseteq\Theta} s^\alpha \otimes n_\alpha,$$

which by assumption is always a finite linear combination whenever all but finitely many of the s_θ vanish. □

Corollary A.3.2. *If M and N are R-modules, and M is free of finite rank, then there are canonical isomorphims:*

$$\mathrm{Sym}(M^*) \otimes N \cong \mathrm{Poly}(M, N), \text{ and}$$
$$\mathrm{Sym}^d(M^*) \otimes N \cong \mathrm{Poly}_d(M, N).$$

Proof. If M has a free R-basis $\{\theta_i : i \in I\}$ with I finite, then $\mathrm{Sym}(M^*)$ has a basis given by elements of the form $\tilde{\theta}^\alpha$, where α ranges over multisets from I, and which corresponds via the map of Lemma A.2.7 to the polynomial law with components

$$(\tilde{\theta}^\alpha)_S : \sum_{i\in I} s_i \otimes \theta_i \mapsto s^\alpha$$

for each R-algebra S. Therefore, elements of $\mathrm{Sym}(M^*) \otimes N$ correspond exactly to polynomial laws p of the form

$$p_S : \sum_{i\in I} s_i \otimes \theta_i \mapsto \sum_{\alpha\sqsubseteq I} s^\alpha \otimes n_\alpha$$

with only finitely many of the n_α nonzero. But since I is finite, this is exactly the form of all polynomial laws $p : M \to N$ by Lemma A.3.1.

And in the case of a fixed degree d, those polynomial laws of degree d are spanned by those coming from multisets α of size d, i.e. from the Sym^d component of $\mathrm{Sym}(M^*)$.

□

Remark A.3.3. While the isomorphisms in Corollary A.3.2 do not depend on the choice of free R-basis for M, they do depend on its existence. In general, M may not admit enough linear maps to R and $\mathrm{Sym}(M^*)$ will be too small: for example, let $R = \mathbb{Z}$ and $M = N = \mathbb{Z}/2$. Then the case $d = 1$ is not even true: $\mathrm{Hom}(M, R) \otimes N$ is trivial and does not even surject onto $\mathrm{Hom}(M, N)$.

Lemma A.3.4. *Let M be an R-module with free R-basis Θ. Let d be a natural number, and let G be a subgroup of S_d. Then the module $(M^{\otimes d})^G$ has a free R-basis given by $\{e(\alpha) : \alpha \in \Theta^d/G\}$.*

Proof. Since $M^{\otimes d}$ is free with basis

$$\{\theta_1 \otimes \ldots \otimes \theta_d : (\theta_1, \ldots, \theta_d) \in \Theta^d\}$$

and the action of G permutes the basis elements, an element m of $M^{\otimes d}$ is G-invariant if and only if its coefficients are constant on G-orbits, i.e. if and only if m is a linear combination of G-orbit sums. But the orbit sum of a basis element $\theta_1 \otimes \ldots \otimes \theta_d$ is exactly $e([(\theta_1, \ldots, \theta_d)])$ by definition. Therefore each element of $(M^{\otimes d})^G$ can be written uniquely as an R-linear combination of the $e(\alpha)$ with $\alpha \in \Theta^d/G$, as desired. □

Lemma A.3.5. *Let R be a ring with R-module M. Let R' be an R-algebra, and let M' be the R'-module $R' \otimes M$. Let d be a natural number, and let G be a subgroup of S_d. Then each of the following conditions is sufficient for the natural R'-module homomorphism $R' \otimes (M^{\otimes d})^G \to (M'^{\otimes_{R'} d})^G$ to be an isomorphism:*

1. *The R-module M is free.*
2. *There exists an element $r \in R$ such that $R' \cong R_r$.*
3. *The R-module M is locally free.*

Proof. We demonstrate the isomorphism for each case in turn; the third case builds on the previous two.

1. We show that the image under f of a free R'-basis for $R' \otimes (M^{\otimes d})^G$ is a free R'-basis for $(M'^{\otimes_{R'} d})^G$.

   Let Θ be a free R-basis for M, and let $\Theta' = \{1 \otimes \theta : \theta \in \Theta\}$ be the corresponding free R'-basis for M'. Then $\{e(\alpha) : \alpha \in \Theta^d/G\}$ is a free R-basis for $(M^{\otimes d})^G$, by Lemma A.3.4, so $\{1 \otimes e(\alpha) : \alpha \in \Theta^d/G\}$ is a free R'-basis for $R' \otimes (M^{\otimes d})^G$. But the homomorphism f maps each $1 \otimes e(\alpha)$ to $e(\alpha')$, where $\alpha' \in \Theta'^d$ is the pushforward of α under the bijection $\Theta \to \Theta'$, and

   $$\{e(\alpha') : \alpha \in \Theta^d/S_d\} = \{e(\alpha) : \alpha \in \Theta'^d/S_d\}$$

   is a free R'-basis for $(M'^{\otimes_{R'} d})^G$. Therefore f is an isomorphism.

2. Suppose instead that R' is the localization R_r for some element r of R, and write M_r for $R_r \otimes M$. Since R_r is a flat R-algebra, we may regard $R_r \otimes (M^{\otimes d})^G$ as a submodule of $R_r \otimes (M^{\otimes d}$, so that f is a restriction of the isomorphism

   $$R_r \otimes M^{\otimes d} \to M_r^{\otimes_{R_r} d},$$

   and is therefore injective; it remains to show that f is surjective.

   To that end, let m/r^n be a G-fixed element of $M_r^{\otimes_{R_r} d}$, with $m \in M^{\otimes d}$. For each permutation $\sigma \in G$, we have $\sigma(m/r^n) = m/r^n$, so $(\sigma(m) - m)/r^n) = 0$. Therefore there exists a natural number ℓ such that $r^\ell(\sigma(m) - m) = 0$ in M; since G is finite we may choose ℓ large enough to be independent of σ. Then $\sigma(r^\ell m) = r^\ell m$ for all $\sigma \in G$, so $r^\ell m \in (M^{\otimes d})^G$, and $f : \frac{1}{r^{n+\ell}} \otimes r^\ell m \mapsto \frac{m}{r^n}$. (This argument is due to user QiL'8 of `math.stackexchange.com`; see [10].)

3. Now let M be a locally free R-module, so that there exists $B \subseteq R$ such that (B) is the unit ideal of R and M_r is free for each $r \in B$. Then for each $r \in B$, we have a chain of R'_r-module isomorphisms

$$\begin{aligned}
R'_r \otimes_{R'} R' \otimes (M^{\otimes d})^G &\cong R'_r \otimes (M^{\otimes d})^G \\
&\cong R'_r \otimes_{R_r} R_r \otimes (M^{\otimes d})^G \\
&\cong R'_r \otimes_{R_r} (M_r^{\otimes_{R_r} d})^G, \text{ by case (2)}, \\
&\cong ((R'_r \otimes_{R_r} M_r)^{\otimes_{R'_r} d})^G, \text{ by case (1)}, \\
&\cong ((R'_r \otimes_{R_r} R_r \otimes M)^{\otimes_{R'_r} d})^G \\
&\cong ((R'_r \otimes M)^{\otimes_{R'_r} d})^G \\
&\cong ((R'_r \otimes_{R'} R' \otimes M)^{\otimes_{R'_r} d})^G \\
&\cong ((R'_r \otimes_{R'} M')^{\otimes_{R'_r} d})^G \\
&\cong R'_r \otimes_{R'} (M'^{\otimes_{R'} d})^G, \text{ by case (2)},
\end{aligned}$$

and their composite is the localization $R'_r \otimes f$. Therefore f is locally an isomorphism, hence an isomorphism. □

Corollary A.3.6. *Let R be a ring, and let M be a locally free R-module. Let d be a natural number, and let G be a subgroup of S_d. Then the module $(M^{\otimes d})^G$ is generated as an R-module by $\{e(\alpha) : \alpha \in M^d/G\}$.*

Proof. Since M is locally free, we can choose a subset B of R such that B generates the unit ideal of R and M_r is free as an R_r-module for each $r \in B$. Let N be the submodule of $M^{\otimes d}$ generated by $\{e(\alpha) : \alpha \in M^d/G\}$. We will show that the inclusion $f : N \to (M^{\otimes d})^G$ is an isomorphism, by showing that its localization $R_r \otimes f$ is an isomorphism for each $r \in B$.

Let r be an element of B. Then M_r is a free R_r-module, so we may choose a free R_r-basis Θ for M_r. Without loss of generality, we may choose the basis to consist

of elements of M, since every element of M_r is a unit multiple of an element of M. Therefore N_r, being the submodule of $M_r^{\otimes d}$ generated by $\{e(\alpha) : \alpha \in M^d/G\}$, contains $\{e(\alpha) : \alpha \in \Theta^d/G\}$, a free R_r-module basis for $(M_r^{\otimes d})^G$. But the latter is isomorphic to $R_r \otimes (M^{\otimes d})^G$ by Lemma A.3.5(2), so N_r is isomorphic to $R_r \otimes (M^{\otimes d})^G$ as desired. □

Lemma A.3.7. *Let R be a ring and M a locally free R-module, and let d be a natural number. The polynomial law $\Delta : M \to M^{\otimes d} : m \mapsto m \otimes \ldots \otimes m$ restricts to a polynomial law*

$$\Delta : M \to (M^{\otimes d})^{S_d}.$$

Furthermore, $(M^{\otimes d})^{S_d}$ is the smallest submodule of $M^{\otimes d}$ for which this restriction is possible.

Proof. For each R-algebra S, the function $\Delta_S : S \otimes M \to S \otimes M^{\otimes d} \cong (S \otimes M)^{\otimes_S d}$ is given by

$$\Delta : m \mapsto m \otimes \ldots \otimes m \in ((S \otimes M)^{\otimes_S d})^{S_d}$$

for each $m \in S \otimes M$. This module $((S \otimes M)^{\otimes_S d})^{S_d}$ is isomorphic to $S \otimes (M^{\otimes d})^{S_d}$ by Lemma A.3.5(3), so we obtain a compatible family of functions

$$\Delta_S : S \otimes M \to S \otimes (M^{\otimes d})^{S_d}$$

as desired.

On the other hand, suppose Δ restricts to a polynomial law $\Delta : M \to N$ with $N \subseteq M^{\otimes d}$. For each finite subset F of M, we may consider the R-algebra $R' = R[\lambda_m : m \in F]$. We have

$$\begin{aligned} \Delta_{R'} : R' \otimes M &\to R' \otimes N \\ &\cong N[\lambda_m : m \in F] \\ : \sum_{m \in F} \lambda_m m &\mapsto \sum_{\alpha \in F^d/S_d} \lambda^\alpha e(\alpha). \end{aligned}$$

Therefore $e(\alpha)$ must belong to N for each multiset $\alpha \in M^d/S_d$. But the set $\{e(\alpha) : \alpha \in M^d/S_d\}$ generates $(M^{\otimes d})^{S_d}$ as an R-module by Lemma A.3.6, so N must contain $(M^{\otimes d})^{S_d}$. □

Theorem A.3.8. *Let M and N be R-modules, with M locally free. Then there is an isomorphism of R-modules*

$$\mathrm{Hom}((M^{\otimes d})^{S_d}, N) \xrightarrow{\sim} \mathrm{Poly}_d(M, N),$$

given by composition with the degree-d polynomial law $\Delta : M \to (M^{\otimes d})^{S_d}$, as in Lemma A.3.7. In other words, every degree-d polynomial law $p : M \to N$ factors uniquely as $p = \tilde{p} \circ \Delta : M \to (M^{\otimes d})^{S_d} \to N$ for some R-linear map $\tilde{p} : (M^{\otimes d})^{S_d} \to N$.

Proof. We will first show that this is an isomorphism if M is free, and then generalize to M locally free. Supposing that M is free, let $\tilde{p} : (M^{\otimes d})^{S_d} \to N$ be a linear map; we will show that requiring $\tilde{p} \circ \Delta$ to equal $p : M \to N$ specifies $\tilde{p}$ completely. So let Θ be an R-basis for M, and consider an arbitrary element $m = \sum_{\theta \in \Theta} s_\theta \otimes \theta \in S \otimes M$. We have

$$\begin{aligned} \Delta_S(m) &= \sum_{\alpha \in \Theta^d/S_d} s^\alpha \otimes e(\alpha), \quad \text{so} \\ (S \otimes \tilde{p}) \circ (\Delta_S)(m) &= (S \otimes \tilde{p}) \left(\sum_{\alpha \in \Theta^d/S_d} s^\alpha \otimes e(\alpha) \right) \\ &= \sum_{\alpha \in \Theta^d/S_d} s^\alpha \otimes \tilde{p}(e(\alpha)). \end{aligned}$$

On the other hand, by Lemma A.3.1, we know that there exist unique $n_\alpha \in N$ for each $\alpha \in \Theta^d/S_d$ such that the following holds identically:

$$p_S(m) = \sum_{\alpha \in \Theta^d/S_d} s^\alpha \otimes n_\alpha.$$

Therefore $\tilde{p} \circ \Delta = p$ if and only if $\tilde{p}(e(\alpha)) = n_\alpha$ for all $\alpha \in \Theta^d/S_d$. But the $e(\alpha)$ for $\alpha \in \Theta^d/S_d$ freely generate $(M^{\otimes d})^{S_d}$ as an R-module by Lemma A.3.4. Therefore $\tilde{p}$ exists and is unique: it sends $e(\alpha)$ to n_α and extends linearly to all of $(M^{\otimes d})^{S_d}$.

Now suppose that M is merely locally free. Choose elements $\{r_1, \ldots, r_k\} \subseteq R$ such that $(r_1, \ldots, r_k)$ is the unit ideal of R and such that M_{r_i} is free for each $i \in [k]$. Now let $p : M \to N$ be a polynomial law that is homogeneous of degree d. For each $i \in [k]$ we obtain a homogeneous degree-d polynomial law $p_{r_i} : M_{r_i} \to N_{r_i}$ given by $(p_{r_i})_S = p_S$ for each R_{r_i}-algebra S. Since each M_{r_i} is free, we know from the above argument that these laws correspond to R_{r_i}-linear maps

$$\tilde{p}_i : (M_{r_i}^{\otimes d})^{S_d} \to N_{r_i}$$

such that $\tilde{p}_i \circ \Delta = p_{r_i}$, and by Lemma A.3.5(1) these correspond to R_{r_i}-linear maps $R_{r_i} \otimes (M^{\otimes d})^{S_d} \to N_{r_i}$, and thus to R-linear maps $(M^{\otimes d})^{S_d} \to N_{r_i}$, for each $i \in [k]$. We may compile these k maps into a single R-module homomorphism

$$(M^{\otimes d})^{S_d} \to \prod_{i \in [k]} N_{r_i}.$$

This will factor through the canonical injection $N \hookrightarrow \prod_{i \in [k]} N_{r_i}$, giving us an R-module homomorphism $\tilde{p} : (M^{\otimes d})^{S_d} \to N$, if and only if the two composites

$$(M^{\otimes d})^{S_d} \to \prod_{i \in [k]} N_{r_i} \rightrightarrows \prod_{i,j \in [k]} N_{r_i r_j}$$

are equal, i.e. for each pair $i, j \in [k]$ and $v \in (M^{\otimes d})^{S_d}$ we have $\tilde{p}_i(v) = \tilde{p}_j(v)$ in $N_{r_i r_j}$. By Lemma A.3.6, it is enough to show that this equality holds for each v of the form $e(\alpha)$, with $\alpha \in M^d/S_d$.

For each finite subset F of M, consider the R-algebra $R' = R[\lambda_m : m \in F]$ and the image of $\sum_{m \in F} \lambda_m m$ under $p_{R'}$:

$$
\begin{aligned}
p_{R'}\left(\sum_{m\in F}\lambda_m m\right) &= (p_{r_i})_{R'}\left(\sum_{m\in F}\lambda_m m\right)\\
&= (R'\otimes\tilde{p}_i)\left(\Delta_{R'}\left(\sum_{m\in F}\lambda_m m\right)\right)\\
&= (R'\otimes\tilde{p}_i)\left(\sum_{\alpha\in F^d/S_d}\lambda^\alpha e(\alpha)\right)\\
&= \sum_{\alpha\in F^d/S_d}\lambda^\alpha\tilde{p}_i(e(\alpha)) \text{ in } N_{r_i}[\lambda_m : m\in F]
\end{aligned}
$$

This equation holds for each $i\in[k]$ and finite $F\subseteq M$, so we have

$$
\sum_{\alpha\in F^d/S_d}\lambda^\alpha\tilde{p}_i(e(\alpha)) = p_{R'}\left(\sum_{m\in F}\lambda_m m\right) = \sum_{\alpha\in F^d/S_d}\lambda^\alpha\tilde{p}_j(e(\alpha))
$$

in $N_{r_ir_j}[\lambda_m : m\in F]$, which implies that $\tilde{p}_i(e(\alpha)) = \tilde{p}_j(e(\alpha))$ in $N_{r_ir_j}$ for each multiset $\alpha\in M^d/S_d$ and pair $i,j\in[k]$. Thus the R-linear maps $(M^{\otimes d})^{S_d}\to N_{r_i}$ glue together into into a unique R-linear map

$$
\tilde{p} : (M^{\otimes d})^{S_d}\to N.
$$

All that remains is to check that the polynomial law $p : M\to N$ is equal to the composite $\tilde{p}\circ\Delta : M\to(M^{\otimes d})^{S_d}\to N$. Let S be an R-algebra, let F be a finite subset of M, and consider the sum $\sum_{m\in F}s_m\otimes m\in S\otimes M$ with $s_m\in S$ for each $m\in F$. We have

$$
\begin{aligned}
(S \otimes \tilde{p}) \circ \Delta_S \left(\sum_{m \in F} s_m \otimes m \right) &= (S \otimes \tilde{p}) \left(\sum_{\alpha \in F^d/S_d} s^\alpha e(\alpha) \right) \\
&= \sum_{\alpha \in F^d/S_d} s^\alpha \tilde{p}(e(\alpha)) \\
&= \sum_{\alpha \in F^d/S_d} s^\alpha \tilde{p}_i(e(\alpha)) \text{ in } (S \otimes N)_{r_i} \\
&= (S_{r_i} \otimes \tilde{p}_i) \left(\sum_{\alpha \in F^d/S_d} s^\alpha e(\alpha) \right) \\
&= (S_{r_i} \otimes \tilde{p}_i) \circ \Delta_{S_{r_i}} \left(\sum_{m \in F} s_m \otimes m \right) \\
&= (p_{r_i})_{S_{r_i}} \left(\sum_{m \in F} s_m \otimes m \right) \\
&= p_S \left(\sum_{m \in F} s_m \otimes m \right)
\end{aligned}
$$

Thus $(S \otimes \tilde{p}) \circ \Delta_S$ and p_S agree in N_{r_i} for each $i \in [k]$, so they agree in N. Therefore $\tilde{p} \circ \Delta = p$ as desired. □

Lemma A.3.9. *Suppose M and N are R-modules, and that N is locally free. Let $f : M \to N$ be an R-linear function. Let d be a natural number and let G be a subgroup of S_d. Then the induced linear map $f^{\otimes d} : (M^{\otimes d})^G \to (N^{\otimes d})^G$ is also surjective.*

Proof. This follows because each every surjection to a projective module splits and the $\bullet \mapsto (\bullet^{\otimes d})^G$ construction is functorial. More concretely, the R-module $(N^{\otimes d})^G$ is generated by $\{e(\alpha) : \alpha \in N^d/G\}$ by Lemma A.3.6. We claim that each such $e(\alpha)$ is in the image of f: The multiset α contains at most d elements of N, so choose a preimage in M for each and let $\beta \in M^d/G$ be the corresponding multiset with the same multiplicities. Then $f^{\otimes d} : e(\beta) \mapsto e(\alpha)$ and $e(\beta) \in (M^{\otimes d})^G$, so by linearity $f^{\otimes d} : (M^{\otimes d})^G \to (N^{\otimes d})^G$ is surjective. □

A.4 Algebras and multiplicative polynomial laws

The following definition and the statement of Lemma A.4.2 are also due to N. Roby, and may be found in [13]. The proof is elementary, so I have included it here for convenience.

Definition A.4.1. If R is a ring and A, B are two R-algebras, then a polynomial law $p : A \to B$ is called *multiplicative* if for each R-algebra S we have

$$p_S(1) = 1 \text{ and}$$
$$p_S(aa') = p_S(a)p_S(a')$$

for arbitrary elements $a, a' \in S \otimes A$.

Lemma A.4.2. *Let R be a ring and A, B two R-algebras with a multiplicative polynomial law $p : A \to B$. If $\alpha \sqsubseteq I$ and $\beta \sqsubseteq J$ are multisets, then let $p^{(\alpha)} : A^I \to B$ send $x = (x_i)_{i\in I}$ to the coefficient of λ^α in $p(\sum_{i\in I} \lambda_i x_i)$, and similarly $p^{(\beta)} : A^J \to B$ send $y = (y_j)_{j\in J}$ to the coefficient of μ^β in $p(\sum_{j\in J} \mu_j y_j)$, as in Lemma A.2.8. Then we may write*

$$p^{(\alpha)}(x)p^{(\beta)}(y) = \sum_{\gamma\in\Gamma_{\alpha\beta}} p^{(\gamma)}(xy),$$

where $\Gamma_{\alpha\beta}$ is the set of multisets γ from $I \times J$ such that $(\lambda\mu)^\gamma = \lambda^\alpha\mu^\beta$, i.e.

$$\sum_{j\in J} \gamma(i,j) = \alpha(i) \text{ for each } i \in I, \text{ and}$$
$$\sum_{i\in I} \gamma(i,j) = \beta(j) \text{ for each } j \in J.$$

(We are using the notation that, if $x = (x_i)_{i\in I}$ and $y = (y_j)_{j\in J}$ are two families of elements of a ring A, then $xy \in A^{I\times J}$ is the family with $(xy)_{(i,j)} = (x_i y_j)$. This is also applied to the "product" of $\lambda = (\lambda_i)_{i\in I}$ and $\mu = (\mu_j)_{j\in J}$.)

Proof. Working in the ring

$$S = R[\lambda_i : i \in I][\mu_j : j \in J]$$

and suppressing the S subscripts on p and its coefficients, consider the expansions:

$$p\left(\sum_{i\in I} \lambda_i x_i\right) = \sum_{\alpha \sqsubseteq I} \lambda^\alpha p^{(\alpha)}(x) \quad \text{and} \quad p\left(\sum_{j\in J} \mu_j y_j\right) = \sum_{\beta \sqsubseteq J} \mu^\beta p^{(\beta)}(y).$$

Their product is

$$\begin{aligned} p\left(\sum_{i\in I} \lambda_i x_i\right) p\left(\sum_{j\in J} \mu_j y_j\right) &= \sum_{\alpha \sqsubseteq I} \lambda^\alpha p^{(\alpha)}(x) \sum_{\beta \sqsubseteq J} \mu^\beta p^{(\beta)}(y) \\ &= \sum_{\alpha \sqsubseteq I, \beta \sqsubseteq J} \lambda^\alpha \mu^\beta (p^{(\alpha)}(x) p^{(\beta)}(y)). \end{aligned}$$

On the other hand, since p is multiplicative, we have

$$\begin{aligned} p\left(\sum_{i\in I} \lambda_i x_i\right) p\left(\sum_{j\in J} \mu_j y_j\right) &= p\left(\sum_{i\in I} \lambda_i x_i \sum_{j\in J} \mu_j y_j\right) \\ &= p\left(\sum_{i\in I, j\in J} \lambda_i \mu_j x_i y_j\right) \\ &= p\left(\sum_{(i,j)\in I\times J} (\lambda\mu)_{(i,j)} (xy)_{(i,j)}\right) \\ &= \sum_{\gamma \sqsubseteq I\times J} (\lambda\mu)^\gamma p^{(\gamma)}(xy) \\ &= \sum_{\alpha \sqsubseteq I, \beta \sqsubseteq J} \lambda^\alpha \mu^\beta \sum_{\gamma \in \Gamma_{\alpha\beta}} p^{(\gamma)}(xy). \end{aligned}$$

Comparing the $\lambda^\alpha \mu^\beta$ terms from both expressions for the product, we have

$$p^{(\alpha)}(x) p^{(\beta)}(y) = \sum_{\gamma \in \Gamma_{\alpha\beta}} p^{(\gamma)}(xy). \qquad \square$$

Bibliography

[1] M. Bhargava. Higher composition laws III: The parametrization of quartic rings. *The Annals of Mathematics*, 159(3):1329–1360, 2004.

[2] M. Bhargava and M. Satriano. On a notion of "Galois closure" for extensions of rings. *ArXiv e-prints*, August 2012, 1006.2562v3.

[3] K. Conrad. Stably free modules. Available at `http://www.math.uconn.edu/~kconrad/blurbs/linmultialg/stablyfree.pdf`. Accessed on 2012-02-28.

[4] P. Deligne. Cohomologie a supports propres. In *Théorie des topos et cohomologie étale des schémas*, volume 305 of *Lecture Notes in Mathematics*, pages 250–480. Springer, 1973.

[5] P. Deligne. Letter to Manjul Bhargava and Markus Rost, 2005.

[6] D. Ferrand. Un foncteur norme. *Bulletin de la Société Mathématique de France*, 126(1):1–50, 1998.

[7] H. Lenstra. Galois theory for schemes. Course notes, electronic 3rd edition. Available at `http://websites.math.leidenuniv.nl/algebra/GSchemes.pdf`, 2008.

[8] O. Loos. Discriminant algebras and adjoints of quadratic forms. *Beiträge zur Algebra und Geometrie*, 38(1):33–72, 1997.

[9] C. Lundkvist. Counterexamples regarding symmetric tensors and divided powers. *Journal of Pure and Applied Algebra*, 212(10):2236 – 2249, 2008.

[10] QiL'8. If m is locally free of finite rank, is the symmetric part of its tensor power? Mathematics Stack Exchange, `http://math.stackexchange.com/q/227054` (version: 2012-11-01).

[11] C. Reutenauer and M.-P. Schützenberger. A formula for the determinant of a sum of matrices. *Letters in Mathematical Physics*, 13(4):299–302, 1987.

[12] N. Roby. Lois polynomes et lois formelles en théorie des modules. *Annales Scientifiques de l'École Normale Supérieure. Troisième Série*, 80:213–348, 1963.

[13] N. Roby. Lois polynômes multiplicatives universelles. *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences. Séries A et B*, 290(19):A869–A871, 1980.

[14] M. Rost. The discriminant algebra of a cubic algebra. Available at `http://www.math.uni-bielefeld.de/~rost/data/cub-disc.pdf`, 2002.

[15] F. Vaccarino. Generalized symmetric functions and invariants of matrices. *Mathematische Zeitschrift*, 260(3):509–526, 2008.

[16] F. Vaccarino. Homogeneous multiplicative polynomial laws are determinants. *Journal of Pure and Applied Algebra*, 213(7):1283–1289, 2009.