Galois closures
for monogenic degree-4 extensions of rings

Riccardo Ferrario
riccardoferrario@gmail.com

Advised by Dr. Owen Biesel

Universiteit Leiden

Università degli Studi di Padova

ALGANT Master's Thesis - 9 July 2014

Acknowledgements

I would like to sincerely thank Owen Biesel, my Master's thesis advisor, who has been extremely kind and helpful with me. He generously and clearly explained to me his research interests, and he was always very patient and encouraging while assisting me with my thesis. I would also like to thank Alberto Facchini, Silvana Bazzoni, Bart de Smit, Hendrik Lenstra, David Holmes and Bas Edixhoven. It was a pleasure to attend their intriguing courses during those two years. May I express my warm thanks to all the staff of the Mathematisch Instituut in Leiden University, and to all the nice fellow students, who let me work in a professional and friendly environment during this year.

I would not be here without the caring support given to me by my wonderful parents and my big family; I am immensely grateful for their support in my major life choices. A huge thank you goes to Guido for having always heartened and helped me to find motivation in what I do. Finally, thanks to all the nice friends I met through my studies and my life path in Turin, Bordeaux, Padua, Leiden and The Hague. Special thanks to my amazing friend Tanja.

Ringraziamenti

Vorrei sentitamente ringraziare Owen Biesel, mio relatore di tesi, che è stato estremamente disponibile nei miei confronti e mi ha generosamente aiutato a comprendere i suoi interessi di ricerca. Gli sono molto grato per la pazienza avuta e per essere sempre stato incoraggiante. Desidero inoltre ringraziare Alberto Facchini, Silvana Bazzoni, Bart de Smit, Hendrik Lenstra, David Holmes e Bas Edixhoven, per gli entusiasmanti corsi da loro tenuti che ho avuto il piacere di seguire. Un ringraziamento di cuore va anche allo staff del Mathematisch Instituut dell'Università di Leida, e a coloro con cui ho qui condiviso quest'anno di lavoro in questo stimolante ambiente di formazione e ricerca.

Non sarei qui senza il premuroso appoggio datomi dai miei fantastici genitori e da tutta la mia estesa famiglia; sono immensamente grato per il loro sostegno nelle mie importanti scelte di vita. Un enorme ringraziamento va a Guido per avermi sempre spronato e aiutato a trovare motivazione in quello che faccio. Infine un ringraziamento a tutte le belle persone incontrate nel mio percorso di vita e di studio, tutte le amiche e tutti gli amici di Torino, Bordeaux, Padova, Leida e L'Aia. Un particolare ringraziamento alla mitica Tanja!

Introduction

In this thesis we will consider Galois closures for monogenic degree-4 ring extensions. We will start by giving the definition of a G-closure for a degree-n ring extension as in O. Biesel's PhD thesis [1], where $G \leq S_n$. This definition generalizes classical finite Galois Theory, with the property of having a G-closure corresponding to having the Galois group contained in G. We will also recall some properties of G-closures which will help us to give parametrizations in the case of a monogenic degree-4 extension of a ring R, that is, an R-algebra obtained by adjoining a variable x to R and quotienting by a degree-4 polynomial $f(x)$. To do this, we will consider 4-multivariate polynomial rings and try to describe their invariants under certain subgroups of S_4 as an algebra over the symmetric polynomials. Finally, a counterexample will point out that it is not possible to generalize the definition of Galois group (as the minimal subgroup $G \leq S_n$ for which a G-closure exists), giving a negative answer to the first of Questions 4.4.3 in [1].

First, we review the relevant facts from classical Galois Theory. Consider a finite separable field extension $K \to L$ of degree n and fix a separable closure $\bar{K}$ of K. Let N be the Galois closure of L/K, that is, the minimal subfield of $\bar{K}$ containing all the images of the field homomorphisms $L \to \bar{K}$ over K. We have n field homomorphisms $L \to N$ fixing K, that we can call $\pi_1, \dots, \pi_n$, choosing an order for them. Then the Galois group $G = \mathrm{Gal}(N/K)$ of the field extension $K \to L$ acts on the left on $\{\pi_1, \dots, \pi_n\}$ by composition. This is easily seen to be a faithful action, so that we can consider G as a subgroup of S_n via $\sigma\pi_i = \pi_{\sigma(i)}$.

This allows us to construct a K-algebra map

$$\begin{aligned} \Phi : \qquad L^{\otimes n} &\longrightarrow N \\ \ell_1 \otimes \ell_2 \otimes \cdots \otimes \ell_n &\longmapsto \prod_{i=1}^{n} \pi_i(\ell_i). \end{aligned}$$

Also, there is a left action of $G \leq S_n$ on the K-algebra $L^{\otimes n}$, defined by

$$\sigma(\ell_1 \otimes \cdots \otimes \ell_n) = \ell_{\sigma^{-1}(1)} \otimes \cdots \otimes \ell_{\sigma^{-1}(n)}$$

which makes Φ a G-map of K-algebras. Hence Φ restricts to a K-algebra map $\varphi : (L^{\otimes n})^G \to N^G = K$, giving the following commutative diagram:

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

One can prove that this is a tensor product diagram, i.e. $L^{\otimes n} \otimes_{(L^{\otimes n})^G} K \cong N$ via the induced map (this is a consequence, for example, of Theorem 1 from [1]).

To generalize this, we first point out some properties of the K-algebra homomorphism φ. For $\ell \in L$ we denote

$$\ell^{(j)} = 1 \otimes \cdots \otimes 1 \otimes \ell \otimes 1 \otimes \cdots \otimes 1, \; j \in \{1, \dots, n\},$$

where the only ℓ in the simple tensor lies in the j-th position. We define $e_k(\ell) := e_k(\ell^{(1)}, \dots, \ell^{(n)})$, the k-th elementary symmetric polynomial computed in $\ell^{(1)}, \ldots, \ell^{(n)}$. This element clearly lies in $(L^{\otimes n})^{S_n} \subseteq (L^{\otimes n})^G$, and it is sent by φ to $s_k(\ell)$, the k-th symmetric polynomial in the n conjugates $\pi_1(\ell), \ldots, \pi_n(\ell)$. This happens to be the k-th *signed coefficient* of the characteristic polynomial of ℓ. That is, using ℓ to indicate a matrix of $\ell\cdot : L \to L$,

$$\det(\lambda \cdot \mathrm{id}_L - \ell) = \prod_{j=1}^{n} (\lambda - \pi_j(\ell)) = \lambda^n - s_1(\ell)\lambda^{n-1} + \ldots + (-1)^n s_n(\ell).$$

For example, $\varphi(e_1(\ell)) = s_1(\ell) = \sum_{j=1}^{n} \pi_j(\ell)$, the *trace* of ℓ over K, and $\varphi(e_n(\ell)) = s_n(\ell) = \prod_{j=1}^{n} \pi_j(\ell)$, the *norm* of ℓ over K.

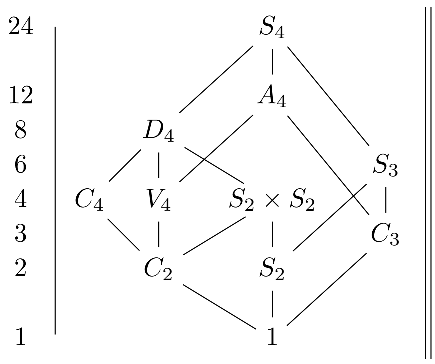
Moving to the case of rings, we define a degree-n extension of R, an associative commutative unital ring, to be a commutative R-algebra A which is locally free of rank n, that is, $A_{r_i} \cong R_{r_i}^n$ as R_{r_i}-modules, for some set $\{r_1, ..., r_m\} \subseteq R$ generating the unit ideal. For $a \in A$, the definition of $e_k(a) \in A^{\otimes n}$ is exactly the same, and also the coefficient $s_k(a) \in R$ can be defined, since the characteristic polynomials on the free localizations can be glued together.

Instead of defining the Galois group for ring extensions, we adopt the following approach: we fix a subgroup $G \leq S_n$, and define G-closures for the extension $R \to A$ as tensor product diagrams like the one we obtain in the case of a degree-n separable field extension. More precisely, a G-closure is a map $\varphi : (A^{\otimes n})^G \to R$ sending $e_k(a) \mapsto s_k(a)$, for $k = 1, \ldots, n$, together with an R-algebra B realizing a tensor product diagram

$$\begin{array}{ccc} (A^{\otimes n})^G & \xrightarrow{\varphi} & R \\ \downarrow & & \downarrow \\ A^{\otimes n} & \longrightarrow & B \end{array} \quad \text{i.e. } B \cong A^{\otimes n} \otimes_{(A^{\otimes n})^G} R.$$

An R-algebra map sending $e_k(a) \mapsto s_k(a)$ like φ is called a *normative* map. One can define morphisms of G-closure in the following way: there is a morphism only if the normative maps are the same, and for each pair of G-closures (B, φ), (B', φ) a morphism consists of an $A^{\otimes n}$-algebra map $B \to B'$. Then it is easily seen that all such morphisms are actually isomorphisms, and that isomorphism classes of G-closures are parametrized by normative maps $(A^{\otimes n})^G \to R$. We denote the set of such maps with $\mathrm{Norm}_R((A^{\otimes n})^G, R)$. For $G = S_n$ there exists a unique normative map $\varphi_0 : (A^{\otimes n})^{S_n} \to R$, called the *Ferrand* map. This is proven in [1], Chapter 2. Hence we can view R as an $(A^{\otimes n})^{S_n}$-algebra via φ_0, so that, for $G \leq S_n$, normative maps $(A^{\otimes n})^G \to R$ are just $(A^{\otimes n})^{S_n}$-algebra maps. For a finite separable field extension, it can be proven that the Galois group of the extension is (up to conjugation) the minimal $G \leq S_n$ for which a G-closure for the field extension exists. In Section 1.1 we will give more detailed definitions and results of Galois closures for finite ring extensions.

For $n \leq 3$ and $G \leq S_n$, parametrizations of G-closures for monogenic degree-n extensions of rings, i.e. R-algebras of the form $R \to R[x]/(f(x))$ (where f is a monic degree-n polynomial, can be easily obtained using the results in [1]. This is why in our thesis the aim is to consider monogenic degree-4 extensions of rings $R \to R[x]/(f(x))$, with $f(x) = x^4 - s_1x^3 + s_2x^2 - s_3x + s_4$, and to give criteria for when G-closures exist, for each subgroup $G \leq S_4$. Up to conjugation, the subgroups of S_4 are laid out all together in Figure 1. In order to do this, we will use some results for monogenic extensions from [1].



$$
\begin{aligned}
A_4 &= \langle V_4, C_3 \rangle\\
D_4 &= \langle \sigma, (1\ 3) \rangle\\
S_3 &= \langle (1\ 2\ 3), (1\ 3) \rangle\\
V_4 &= \{1, \sigma^2, (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}\\
C_4 &= \langle \sigma \rangle\\
S_2 \times S_2 &= \langle (1\ 3), (2\ 4) \rangle\\
C_3 &= \langle (1\ 2\ 3) \rangle\\
S_2 &= \langle (1\ 3) \rangle\\
C_2 &= \langle \sigma^2 \rangle
\end{aligned}
$$

Figure 1: A diagram representing (up to conjugation) all the subgroups of S_4, where σ stands for the 4-cycle (1 2 3 4) and the numbers on the left are the orders of the subgroups lying on that line.

In Section 1.2 we will give a proof of Theorem 1.2.1. This theorem states that if $G = S_{d_1} \times \cdots \times S_{d_k} \leq S_n$, with $d_1 + \cdots + d_k = n$, then isomorphism classes of G-closures are in one-to-one correspondence with factorizations of the polynomial defining the monogenic extension into monic polynomials of degrees $d_1, \ldots, d_k$. This allows us to describe the G-closure for a monogenic degree-4 extensions when $G \in \{1, S_2, S_3, S_2 \times S_2, S_4\}$ in terms of factorizations of f.

In Section 1.3 we will give an easier description of G-closures for monogenic extensions in terms of invariant polynomials. Specifically, one can give to R an $R[x_1, \ldots, x_n]^{S_n}$-algebra structure via the R-algebra map $R[x_1, \ldots, x_n]^{S_n} \to R$ sending the k-th elementary symmetric polynomial, which we will denote by e_k, to the k-th signed coefficient of the polynomial defining the monogenic extension. Recall that indeed we have $R[x_1, \ldots, x_n]^{S_n} = R[e_1, \ldots, e_n]$ by the fundamental theorem of symmetric polynomials. Whenever the order of G is not a zero-divisor in R, then G-closures are in one-to-one correspondence with $R[x_1, \ldots, x_n]^{S_n}$-algebra maps $R[x_1, \ldots, x_n]^G \to R$. We will explain how an $R[x_1, \ldots, x_n]^{S_n}$-algebra description of $R[x_1, \ldots, x_n]^G$ can be given.

In [1], this is done to describe A_n-closures for monogenic extensions. There the following isomorphism of $R[x_1, \ldots, x_n]^{S_n}$-algebras is proven:

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

where Γ is the sum over the A_n-orbit of the monomial $x_1^0 x_2^1 \cdots x_n^{n-1}$ and Γ' is the sum of the monomials on the complementary orbit (that is, the polynomial Γ acted on by any odd permutation of the variables x_i). Then by Theorem 1.3.3, A_n-closures for a monogenic degree-n extension of rings $R \to A = R[x]/(f(x))$ are in one-to-one correspondence with maps of $R[x_1, \ldots, x_n]^{S_n}$-algebra $R[x_1, \ldots, x_n]^{A_n} \to R$, hence with roots in R of the polynomial $x^2 - \varphi_0(\Gamma + \Gamma')x + \varphi_0(\Gamma\Gamma')$, which are the possible images of Γ. Here φ_0 denotes the map $R[x_1, \ldots, x_n]^{S_n} \to R$ sending the k-th elementary symmetric polynomial e_k to the k-th signed coefficient of f. This allows us to immediately parametrize A_4-closures for monogenic degree-4 ring extensions, while in order to parametrize C_3-closures one has to be a bit more careful.

In Chapter 2 we will give explicit parametrizations of G-closures for monogenic degree-4 extensions $R \to A = R[x]/(f(x))$, focusing on the subgroups for which there was no previous immediate or explicit description, that is, $G \in \{V_4, C_4, C_2, C_3\}$. To make things simpler, we will suppose that $2 \in R$ is not a zero-divisor. While D_4-closures (as stated in [1]) are in one-to-one correspondence with roots of f's resolvent cubic $g(x) = x^3 - s_2x^2 + (s_1s_3 - 4s_4)x - (s_3^2 - 4s_2s_4 + s_1^2s_4)$, we will see that V_4-closures are in one-to-one correspondence with g's splittings into monic linear factors, agreeing with classical Galois theory (see Chapter 4 in [4]). Next, we will find explicit polynomial equations parametrizing C_4-closures when $2 \in R^\times$, after giving a free basis for the $\mathbb{Z}\left[\frac{1}{2}\right][x_1, x_2, x_3, x_4]^{S_4}$-module $\mathbb{Z}\left[\frac{1}{2}\right][x_1, x_2, x_3, x_4]^{C_4}$. After that, we will deal with C_2-closures, which can be easily parametrized by presenting $\mathbb{Z}[x_1, x_2, x_3, x_4]^{C_2}$ as an $\mathbb{Z}[x_1, x_2, x_3, x_4]^{S_2\times S_2}$-algebra.

Finally, in Section 2.5 we will apply the criteria for G-closures on some particular monogenic degree-4 ring extensions, and we will also lay out a counterexample which gives a negative answer to the first of Questions 4.4.3 in [1]. Specifically, this counterexample establishes that it is not possible to define the Galois group of a ring extension as the minimal subgroup up to conjugation $G \le S_n$ such that a G-closure exists, since there are such minimal subgroups which are not conjugate.

Notation & Conventions

- $0 \in \mathbb{N}$.
- All rings considered are commutative, associative and with an identity.
- For $n \in \mathbb{N}$ we denote $[n] = \{1, \ldots, n\}$.
- When working with a degree-n extension of rings, we denote $R[\mathbf{x}] := R[x_1, \ldots, x_n]$. Moreover, each time we are working with a polynomial ring $R[x_1, \ldots, x_n]$, we denote by e_r the r-th elementary symmetric polynomial in the n variables $x_1, \ldots, x_n$.
- If G is a group, we write $H \le G$ to mean that H is a subgroup of G, and $H \trianglelefteq G$ to mean that H is a normal subgroup of G. For any group G acting on a set I we denote $I^G := \{t \in I : \forall \sigma \in G, \sigma t = t\}$.
- For any R-algebra A and finite set D we denote $A^{\otimes_R D}$ the tensor product over R of copies of the R-algebra A indexed by D. We denote it shortly as $A^{\otimes D}$ if it is clear for the context that A is regarded as an R-algebra. For $n \in \mathbb{N}$, we consider $A^{\otimes n} := A^{\otimes [n]}$. (For $n = 0$, $A^{\otimes 0} = R$, the initial object in the category of R-algebras.) For $j \in D$ and $a \in A$, we denote by $a^{(j)} \in A^{\otimes D}$ the simple tensor with a in the position indexed by j and 1 everywhere else.
- For any set I, we denote by S_I the symmetric group $\mathrm{Bij}(I, I)$ of I. For $n \in \mathbb{N}$, we write $S_n := S_{[n]}$. Given $s \in \mathbb{Z}_{>0}$ distinct elements $k_1, \ldots, k_s \in I$, we use the cycle notation $(k_1\ k_2\ \cdots\ k_s)$ for the permutation in S_I sending $k_i \mapsto k_{i+1}$ for $i \in [s-1]$, $k_s \mapsto k_1$, and fixing all the rest of I. For $a, b \in I$, we denote by $\tau_{ab} := (a\ b)$ the permutation in S_I interchanging $a \leftrightarrow b$ and fixing all the rest of I. Since permutations are functions, for $\sigma_1, \sigma_2 \in S_I$,

we denote by $\sigma_1\sigma_2$ the composition of the two permutations, where σ_1 is applied *after* σ_2.

Contents

Chapter 1

G-closures for monogenic extensions

1.1 Galois closures for finite ring extensions

In this section we will define finite ring extensions and their Galois closures. We will also state some important facts about them before moving to the case of monogenic ring extensions.

Definition 1.1.1. Let R be a ring and $n \in \mathbb{N}$. An R-module M is said to be *locally free of rank n* if there exist elements $r_1, \dots, r_m \in R$ such that $\langle r_1, \dots, r_m \rangle_R = R$ and $M_{r_i} \cong R^n_{r_i}$ as R_{r_i}-modules for all $i \in \{1, \dots, m\}$.

Definition 1.1.2. Let R be a ring and $n \in \mathbb{N}$. A *degree-n ring extension* of R is an R-algebra A such that A is locally free of rank n as an R-module.

To define normative maps, we need to prove that it makes sense to define the characteristic polynomial of an element $a \in A$, for $R \to A$ a degree-n extension. This is done in the following lemma. Recall that for any R-algebra A which is finite free as an R-module we can define the characteristic polynomial of each element $a \in A$, that is, $f_a(\lambda) = \det(\lambda \cdot \mathrm{id}_A - a)$, where a also denotes any matrix associated to the R-linear map $a\cdot : A \to A$. It is well defined, in the sense that it does not depend on the R-basis of A used to define the matrix a.

Lemma 1.1.3. *Let $R \to A$ be a degree-n extension of rings, with free localizations $A_{r_i} \cong R^n_{r_i}$ (as R_{r_i}-modules), where $(r_1, ..., r_m) = 1$, and take $a \in A$. Then there exist unique elements $s_k(a)$, for $k \in [n]$ such that $\lambda^n - s_1(a)\lambda^{n-1} + \cdots + (-1)^n s_n(a)$ is the characteristic polynomial of the R_{r_i}-linear map $a\cdot : A_{r_i} \to A_{r_i}$ for each $i \in [m]$. Moreover, this polynomial vanishes at $\lambda = a$.*

We call $\lambda^n - s_1(a)\lambda^{n-1} + \cdots + (-1)^n s_n(a)$ the *characteristic polynomial* of $a \in A$, and $s_k(a)$ its k-th *signed coefficient.*

Proof. For each $r \in R$ we have $R_r = \mathcal{O}_{\mathrm{Spec}(R)}(U_r)$, where $U_r = \{\mathfrak{p} \in \mathrm{Spec}(R) : r \notin \mathfrak{p}\}$. Then $U_r \cap U_s = U_{rs}$, so that $R_{rs} = \mathcal{O}_{\mathrm{Spec}(R)}(U_r \cap U_s)$, where the restriction map $R_r \to R_{rs}$ is the canonical one. Whenever r and s realize free localizations, we want to show that the coefficients of the characteristic polynomials of the R_r-linear map $A_r \to A_r$ and the R_s-linear map $A_s \to A_s$ sending $x \mapsto a \cdot x$ are the same on the intersection, that is, in R_{rs}. Then the coefficients glue and become elements of R, because $\mathcal{O}_{\mathrm{Spec}(R)}$ is a sheaf and the opens U_{r_i} cover $\mathrm{Spec}(R)$, as $(r_1, ..., r_m) = 1$. This can be done by showing that the characteristic polynomial of $a\cdot : A_r \to A_r$ is also the characteristic polynomial of $a\cdot : A_{rs} \to A_{rs}$, which is unique (the same holding for the localization over s). As passing from A_r to A_{rs} means just tensoring with R_{rs}, each free R_r-basis for A_r is also a free R_{rs}-basis for A_{rs}. Then any matrix with coefficients in R_r representing the R_r-linear map $A_r \to A_r$ represents also the map $A_{rs} \to A_{rs}$, so that the characteristic polynomial of $a\cdot : A_r \to A_r$ becomes the characteristic polynomial of $a\cdot : A_{rs} \to A_{rs}$ in R_{rs}.

Finally, a is a root of its characteristic polynomial on each free localization by the Cayley-Hamilton theorem, so that it is (globally) a root of the characteristic polynomial, again because $\mathcal{O}_{\mathrm{Spec}(R)}$ is a sheaf and $\{U_{r_i}\}$ an open cover. □

Then we can give the definitions:

Definition 1.1.4. Let $R \to A$ be a degree-n ring extension and $G \leq S_n$. For $a \in A$ and $k \in [n]$ we denote $e_k(a) := e_k(a^{(1)}, \dots, a^{(n)}) \in (A^{\otimes n})^{S_n}$, and with $s_k(a) \in R$ we denote the k-th signed coefficient of the characteristic polynomial of a. We say that an R-algebra map $(A^{\otimes n})^G \to R$ is *normative* if it maps $e_k(a) \mapsto s_k(a)$ for all $a \in A$ and $k \in [n]$.

Remark 1.1.5. Adjoining a variable y to the ring $(A^{\otimes n})^G$, for all $a \in A$ we have the identity $\prod_{i=1}^n (y-a)^{(i)} = \sum_{k=0}^n (-1)^k e_k(a) y^{n-k}$ (where $e_0(a) = 1$), so that an R-algebra map $(A^{\otimes n})^G \to R$ is normative if and only if the induced R-algebra map $(A^{\otimes n})^G[y] \to R[y]$ (mapping $y \mapsto y$) sends $\prod_{i=1}^n (y-a)^{(i)}$ to the characteristic polynomial of a in the variable y.

Definition 1.1.6. Let $R \to A$ be a degree-n ring extension and $G \leq S_n$. We call a *G-closure for the ring extension* $R \to A$ the data (φ, B), where $\varphi : (A^{\otimes n})^G \to R$ is a normative map and B is an $A^{\otimes n}$-algebra realizing a tensor product diagram

$$\begin{array}{ccc} (A^{\otimes n})^G & \xrightarrow{\varphi} & R \\ \downarrow & & \downarrow \\ A^{\otimes n} & \longrightarrow & B \end{array} \quad \text{i.e. } B \cong A^{\otimes n} \otimes_{(A^{\otimes n})^G} R.$$

We define a morphism of G-closures $(\varphi, B) \mapsto (\varphi', B')$ to be an equality of the normative maps together with a map of $A^{\otimes n}$-algebras $B \to B'$.

The tensor product diagram makes it clear that two G-closures with same normative map are isomorphic, so that we will mostly be interested in the set of normative maps $\mathrm{Norm}((A^{\otimes n})^G, R)$. Indeed, this set parametrizes isomorphism classes of G-closures. As said in the introduction, we have the following theorem:

Theorem 1.1.7. *Let R be a ring, and let A be a degree-n extension of R. Then there exists a unique isomorphism class of S_n-closures for $R \to A$, i.e., there exists exactly one normative map $\varphi_0 : (A^{\otimes n})^{S_n} \to R$. We call φ_0 the* Ferrand map *associated to the ring extension $R \to A$.* □

This is proven in [1], Chapter 2. The proof proceeds by constructing such a map φ_0 of R-modules, and then it is proven to be an R-algebra homomorphism.

Uniqueness is established by showing that $(A^{\otimes n})^{S_n}$ is generated as R-algebra by the set $\{e_k(a) : a \in A, k \in [n]\}$.

Now suppose $G \leq H \leq S_n$. Then the inclusion $(A^{\otimes n})^H \hookrightarrow (A^{\otimes n})^G$ induces a map:

$$\begin{aligned} \gamma_{H,G} : \mathrm{Norm}_R((A^{\otimes n})^G, R) &\to \mathrm{Norm}_R((A^{\otimes n})^H, R) \\ \varphi &\mapsto \varphi|_{(A^{\otimes n})^H} \end{aligned} \tag{1.1}$$

This allows, given a G-closure (φ, B) to induce canonically the isomorphism class of H-closures represented by $(\varphi|_{(A^{\otimes n})^H}, A^{\otimes n} \otimes_{(A^{\otimes n})^H} R)$. Hence a G-closure gives a canonical H-closure. We recall that considering this for $H = S_n$ allows us to consider normative maps just as $(A^{\otimes n})^{S_n}$-algebra maps $(A^{\otimes n})^G \to R$.

In the case of a separable degree-n field extension $K \to L$, Theorem 1 in [1] states that, for every $H \leq S_n$, an H-closure for $K \to L$ exists if and only if H contains the Galois group G of N over K for some identification of $[n]$ with the set $\mathrm{Hom}_K(L, N)$, where N is the Galois closure of the field extension in the classical sense. As we said in the introduction, by some basic Galois theory $\mathrm{Hom}_K(L, N)$ has n elements, and the left action of G on $\mathrm{Hom}_K(L, N)$ by composition is transitive, so that any bijection $\pi : [n] \to \mathrm{Hom}_K(L, N)$ allows us to see $G \leq S_n$ via $\sigma \mapsto \pi^{-1} \circ (\sigma\cdot) \circ \pi$, where $\sigma\cdot$ is the bijection $\mathrm{Hom}_K(L, N) \to \mathrm{Hom}_K(L, N)$ defined by σ. This theorem assures that the definition of G-closure given is a generalization of the classical Galois theory. Morally, this theorem suggests that the Galois group of a finite ring extension $R \to A$ should be regarded as the minimal subgroup $G \leq S_n$, up to conjugation, such that there exists a G-closure for the extension $R \to A$, if it exists (but we will see that this is not always the case). The fact that we can work up to conjugation can be explained with the following lemma:

Lemma 1.1.8. *Suppose that $R \to A$ is an algebra and $G_1, G_2 \leq S_n$ are conjugates subgroups. Then there exists a natural isomorphism of $(A^{\otimes n})^{S_n}$-algebras $(A^{\otimes n})^{G_1} \cong (A^{\otimes n})^{G_2}$*

Proof. Suppose that $G_2 = \sigma G_1 \sigma^{-1}$ for some $\sigma \in S_n$. Then we have the isomorphism of R-algebras $\chi : A^{\otimes n} \to A^{\otimes n}$ sending $a^{(i)} \mapsto a^{(\sigma(i))}$. The map χ turns out to be a G_1-map by defining, for $\tau \in G_1$, $\tau \cdot a^{(i)} = a^{(\tau(i))}$ in the domain and $\tau \cdot a^{(i)} = a^{(\sigma\tau\sigma^{-1}(i))}$ in the codomain. Hence the image of $(A^{\otimes n})^{G_1}$ is the subring of $A^{\otimes n}$ fixed by G_1 in the codomain via the "conjugated action", which is just $(A^{\otimes n})^{G_2}$. Hence $(A^{\otimes n})^{G_1} \cong (A^{\otimes n})^{G_2}$ via χ, which is an isomorphism of $(A^{\otimes n})^{S_n}$-algebras since the symmetric tensors are fixed by σ. □

Another important property of G-closures is that they are preserved via base change $R \to R'$. The following appears as Lemma 3.1.1 and Theorem 3.1.3 in [1]:

Theorem 1.1.9. *Let $R \to A$ be a degree-n ring extension of R, $R \to R'$ an R-algebra and define $A' = R' \otimes A$. Let $G \leq S_n$ and take a normative map $\varphi : (A^{\otimes n})^G \to R$. Then $R' \to A'$ is a degree-n extension and the map $\varphi' : (A'^{\otimes_{R'} n})^G \cong R' \otimes (A^{\otimes n})^G \xrightarrow{id_{R'} \otimes \varphi} R'$ is normative. The G-closure of the extension $R' \to A'$ corresponding to φ' is isomorphic to*

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

In the next two sections, we will consider the specific case of a monogenic extension of rings. Let us first define what monogenic algebras are, and then see what they are like in the case of a degree-n ring extension.

Definition 1.1.10. Let A be an R-algebra. We call it *monogenic* if it is generated by a single element $\alpha \in A$, that is, the R-algebra map $R[x] \to A$ sending $x \to \alpha$ is surjective.

We will now prove that all monogenic degree-n ring extensions are actually of the form $R \to R[x]/(f(x))$:

Lemma 1.1.11. *Let $R \to A$ be a degree-n extension of rings, with A a monogenic R-algebra. Then A is isomorphic to $R[x]/(f(x))$ as an R-algebra, for some monic degree-n polynomial f.*

Proof. Let α be a single generator of A as an R-algebra, and consider the surjective R-algebra map $\pi : R[x] \to A$ sending $x \mapsto \alpha$. By Lemma 1.1.3, which we can apply as $R \to A$ is a degree-n extension, α has a degree-n monic characteristic polynomial $f(x)$, and $f(\alpha) = 0$. In particular, $(f(x)) \subseteq \ker \pi$, so that π factors as

$$R[x] \twoheadrightarrow \frac{R[x]}{(f(x))} \overset{\bar{\pi}}{\twoheadrightarrow} A.$$

To conclude, we prove that $\bar{\pi}$ is an isomorphism of R-modules. It is enough to prove this on the free localizations. Notice that, for $A_r \cong R_r^n$, the map $\bar{\pi}_r : \left(\frac{R[x]}{(f(x))}\right)_r \to A_r$ is still surjective. Then, given an R_r-basis $\beta_0, \ldots, \beta_{n-1}$ of A_r we can consider the isomorphism of R_r-modules $\psi : A_r \to \left(\frac{R[x]}{(f(x))}\right)_r$ sending $\beta_j \mapsto x^j$, and $\bar{\pi}_r$ is an isomorphism if and only if the onto map $\bar{\pi}_r \circ \psi : A_r \to A_r$ is an isomorphism, which is the case by Theorem 1 in [5]. $\square$

Hence, given a ring R, a monogenic degree-n extension of R is just an R-algebra of the form $A = R[x]/(f(x))$, for $f(x) \in R[x]$ a monic polynomial of degree n. It is a free R-module with free basis $\{1, x, \ldots, x^{n-1}\}$, and since x has to satisfy its characteristic polynomial, this turns out to be equal to $f(x)$. We will set $s_0 = 1$ and write down $f(x) = \sum_{k=0}^{n}(-1)^k s_k x^{n-k} = x^n - s_1 x^{n-1} + s_2 x^{n-2} - ... + (-1)^n s_n$, so that $s_k = s_k(x)$.

The following lemma tells us how it is possible to generate $(A^{\otimes n})^{S_n}$ as an R-algebra starting by a few symmetric tensor powers. It will be useful to give a proof of next session's main theorem.

Lemma 1.1.12. *Let R be a ring, and consider a monogenic degree-n extension $R \to A = R[x]/(f(x))$. Then $(A^{\otimes n})^{S_n}$ is generated as an R-algebra by $\{e_k(x) : k \in [n]\}$.* $\square$

Proof. Lemma 2.2.5 in [1] states that $\{e_k(\omega) : k \in [n], \omega \in \Omega\}$ generates $(A^{\otimes n})^{S_n}$ as an R-algebra whenever the powers of elements of Ω generate A as an R-module. As $\{1, x, \ldots, x^{n-1}\}$ generates A as an R-module, we can apply that lemma with $\Omega = \{x\}$. $\square$

1.2 $\prod_j S_{d_j}$-closures for monogenic extensions

In this section, we will prove that given a monogenic degree-n ring extension $R \to A = R[x]/f(x)$ and $G = S_{d_1} \times \cdots \times S_{d_m} \leq S_n$, normative maps $(A^{\otimes n})^G \to R$ are in one-to-one correspondence with decompositions of f into monic polynomials of degrees $d_1, \dots, d_m$. As the subgroups of S_n can be considered up to conjugation, it is not important to distinguish how the embedding $S_{d_1} \times \cdots \times S_{d_m} \leq S_n$ is realized. Hence, without loss of generality, we can assume that S_{d_j} acts on $D_j := \{d_1 + \cdots + d_{j-1} + 1, \dots, d_1 + \cdots + d_{j-1} + d_j\} \subseteq [n]$.

Theorem 1.2.1. *Let $R \to A = R[x]/(f(x))$ be a monogenic degree-n extension of rings. Take a partition of n into m positive integers $d_1, \dots, d_m$, and view $\prod_j S_{d_j}$ as a subgroup of S_n. Then the following are in one-to-one correspondence:*

- *isomorphism classes of $\prod_j S_{d_j}$-closures for $R \to R[x]/(f(x))$;*
- *factorizations into monic polynomials $f(x) = \prod_j f_j(x)$, with $\deg f_j = d_j$.*

The $\prod_j S_{d_j}$-closure corresponding to the factorization $f(x) = \prod_j f_j(x)$ is isomorphic to the tensor product of the S_{d_j}-closures for the ring extensions $R \to A_j := R[x]/(f_j(x))$.

Proof. For $a \in A$, let us denote by $E_{j,k}(a) \in A^{\otimes n}$ the k-th elementary symmetric polynomial on the d_j elements $a^{(l)} \in A^{\otimes n}$, with $l \in D_j$. Dealing with any ring map θ, we will denote with abuse of notation still by θ the map between the two rings with an adjoined variable. As in the statement, we will not write everywhere explicitly that j ranges over $[m]$. We want to define a correspondence

$$\left\{ (f_j)_j \;\middle|\; \begin{array}{l} \deg f_j = d_j \\ f_j \text{ monic, } f = \prod_j f_j \end{array} \right\} \underset{\mathcal{D}}{\overset{\mathcal{C}}{\rightleftarrows}} \mathrm{Norm}_R((A^{\otimes n})^{\prod_j S_{d_j}}, R).$$

For each factorization $f = \prod_j f_j$ we consider the monogenic ring extensions $R \to A_j = R[x]/(f_j(x))$ and denote by $\varphi_j : (A_j^{\otimes d_j})^{S_{d_j}} \to R$ their Ferrand map. We then define $\mathcal{C}((f_j)_j) = \varphi$ as the following composite, where π is the tensoring of canonical projections $A \to A_j$:

$$\varphi : (A^{\otimes n})^{\prod_j S_{d_j}} \cong \bigotimes_{j \in [m]} (A^{\otimes d_j})^{S_{d_j}} \xrightarrow{\pi} \bigotimes_{j \in [m]} (A_j^{\otimes d_j})^{S_{d_j}} \xrightarrow{\otimes_j \varphi_j} R \qquad (1.2)$$

The isomorphism is the one from Remark A.2.6. For each $j \in [m]$ and $k \in [d_j]$, we have that $E_{j,k}(x) \in A^{\otimes n}$ corresponds via the isomorphism to $e_k(x)^{(j)}$, which is mapped to $s_{j,k}$ via $\otimes_j \varphi_j \circ \pi$, so that the resulting φ is normative. Indeed, the polynomial $\sum_{k=0}^n (-1)^k e_k(x) y^{n-k} \in A^{\otimes n}[y]$ is equal to $\prod_{i=1}^n (y - x^{(i)})$, which can be factorized as the product over $j \in [m]$ of the polynomials $\prod_{i \in D_j} (y - x^{(i)})$. Since those are mapped via φ_j to $f_j(y)$, we get that φ maps $\sum_{k=0}^n (-1)^k e_k(x) y^{n-k}$ to $f(y)$.

Conversely, suppose we have a normative map $\varphi : (A^{\otimes n})^{\prod_j S_{d_j}} \to R$. Since $E_{j,k}(x) \in (A^{\otimes n})^{\prod_j S_{d_j}}$, for all j we can define

$$f_j(y) = \sum_{k=0}^{d_j} (-1)^k \varphi(E_{j,k}(x)) y^{d_j - k} = \varphi\Big(\prod_{i \in D_j} (y - x^{(i)}) \Big).$$

Then $\prod_j f_j(y) = \varphi\left(\prod_{i=1}^n (y - x^{(i)})\right) = f(x)$ and we can define

$$\mathcal{D}(\varphi) = (\sum_{k=0}^{d_j} (-1)^k \varphi(E_{j,k}(x)) x^{d_j - k})_j.$$

We now prove that the two associations $\mathcal{C}$ and $\mathcal{D}$ are each others' inverses. For $\varphi \in \mathrm{Norm}_R((A^{\otimes})^{\prod_j S_{d_j}}, R)$, we define the maps

$$(A_j^{\otimes d_j})^{S_{d_j}} \ni e_k(x) \overset{\varphi_j}{\mapsto} s_{j,k} := \varphi(E_{j,k}(x)) \in R.$$

Then $(\mathcal{C} \circ \mathcal{D})(\varphi)$ is precisely the composition of $(\otimes_j \varphi_j) \circ \pi$ after the isomorphism $(A^{\otimes n})^{\prod_j S_{d_j}} \cong \bigotimes_{j \in [m]} (A^{\otimes d_j})^{S_{d_j}}$.

Hence for all $j \in [m]$ and $k \in [d_j]$ we get $(\mathcal{C} \circ \mathcal{D})(\varphi)(E_{j,k}(x)) = \varphi(E_{j,k}(x))$. And since the elements $E_{j,k}$ correspond to $e_k^{(j)}$ via the isomorphism $(A^{\otimes n})^{\prod_j S_{d_j}} \cong \bigotimes_{j \in [m]} (A^{\otimes d_j})^{S_{d_j}}$, they generate the whole $(A^{\otimes n})^{\prod_j S_{d_j}}$ — because $\{e_k(x) : k \in [d_j]\}$ generates $(A^{\otimes d_j})^{S_{d_j}}$ as an R-algebra for all $j \in [m]$ by Lemma 1.1.12. This gives $(\mathcal{C} \circ \mathcal{D})(\varphi) = \varphi$. Conversely, for any decomposition $f = \prod_j f_j$ we consider $A_j = A/(f_j)$, take the Ferrand maps $\varphi_j : (A_j^{\otimes d_j})^{S_{d_j}} \to R$ which send $e_k(x) \mapsto s_{j,k}$, and define φ as in (1.2). This gives

$$(\mathcal{D} \circ \mathcal{C})((f_j)_j) = \left(\sum_{k=0}^{d_j} (-1)^k \varphi(E_{j,k}(x)) x^{d_j - k} \right)_j = (f_j)_j.$$

Hence we have a one-to-one correspondence. Given a factorization into monic polynomials $f = \prod_j f_j$, the $\prod_j S_{d_j}$-closure given by the corresponding normative map $\varphi = \mathcal{C}((f_j)_j)$ is

$$\begin{aligned} B_{(f_j)_j} = A^{\otimes n} \bigotimes_{(A^{\otimes n})^{\prod_j S_{d_j}}} R &\cong A^{\otimes n} / (E_{j,k}(x) - s_{j,k} : j \in [m], k \in [d_j]) \\ &\cong \bigotimes_j A^{\otimes d_j} / (e_k(x) - s_{j,k} : k \in [d_j]). \end{aligned}$$

Since over $A^{\otimes d_j}/(e_k(x) - s_{j,k} : k \in [d_j])$ we have $f_j(x) = \prod_{k \in [d_j]} (x - x^{(k)})$, one has $f_j(x^{(k)}) = 0$, so that

$$\begin{aligned} B_{(f_j)_j} &\cong \bigotimes_j A^{\otimes d_j} / (f_j(x^{(k)}), e_k(x) - s_{j,k} : k \in [d_j]) \\ &\cong \bigotimes_j A_j^{\otimes d_j} / (e_k(x) - s_{j,k} : k \in [d_j]) \cong \bigotimes_j \big(A^{\otimes d_j} \bigotimes_{(A_j^{\otimes d_j})^{S_{d_j}}} R \big). \end{aligned}$$

and the corresponding $\prod_j S_{d_j}$-closure is isomorphic to the tensor product of the S_{d_j}-closures for the extensions $R \to R[x]/(f_j(x))$. $\square$

An easy particular case is the following corollary for $G = S_{n-1} \times S_1$.

Corollary 1.2.2. *Let $R \to A = R[x]/(f(x))$ be a monogenic degree-n extension of rings. Then isomorphism classes of $S_{n-1} \times S_1$-closures for $R \to A$ are in one-to-one correspondence with roots of f in R. For $r \in R$ a root of f, the corresponding $S_{n-1} \times S_1$-closure of $R \to A$ is isomorphic to the unique S_{n-1}-closure of the monogenic extension $R \to R[x]/(\frac{f(x)}{x-r})$.*

Proof. It is an immediate application of Theorem 1.2.1, together with the following well-known lemma, which allows us to define $f(x)/(x-r)$, for r a root of f. $\square$

Lemma 1.2.3 (Factorization lemma)**.** *Let R be a ring and $p \in R[x]$ be a non-constant polynomial such that $p(r) = 0$. Then there exists a unique polynomial $p_r \in R[x]$ such that $p = (x-r)p_r$.*

Proof. Let $n = \deg p > 0$ and write $p = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n$. Then such a factorization can only occur if p_r has degree $n-1$, because the leading coefficient of $p = (x-r)p_r$ is equal to the leading coefficient of p_r, hence it must be the coefficient of the monomial of degree $n-1$. Then we write down $p_r = b_1x^{n-1} + ... + b_{n-1}x + b_n$, and $p = (x-r)p_r$ is equivalent to the system of equations (defining $b_0 = 0$)

$$\begin{cases} b_j - rb_{j-1} = a_{j-1},\ 1 \leq j \leq n \\ a_n = -b_nr \end{cases} \iff \begin{cases} b_j = a_{j-1} + rb_{j-1},\ 1 \leq j \leq n \\ 0 = -(a_n + a_{n-1}r + ... + a_0r^n) \end{cases}$$

where the first row uniquely defines $b_1, \dots, b_n$, and the second row is true by hypothesis (since it states that $-p(r) = 0$). This implies that there exist uniquely determined coefficients $b_1, \dots, b_n$ for p_r, hence the existence and uniqueness of p_r such that $p = (x-r)p_r$. $\square$

1.3 G-closures for monogenic extensions via polynomials

In [1], O. Biesel uses invariants of multivariate polynomials to give a description of G-closures for monogenic extensions. We will now explain how this can be done. For $R \to A = R[x]/(f(x))$ a monogenic degree-n ring extension, tensoring the canonical surjection $R[x] \to A$ with itself we get a map $R[x]^{\otimes n} \to A^{\otimes n}$. Notice that $R[x]^{\otimes n} \cong R[\mathbf{x}] := R[x_1, \dots, x_n]$ via $x^{(j)} \mapsto x_j$. The left action of S_n on the tensor factors of $R[x]^{\otimes n}$ induces the left action of S_n on the R-algebra $R[\mathbf{x}]$ defined by $\sigma \cdot x_j = x_{\sigma(j)}$ (since $\sigma \cdot x^{(j)} = x^{(\sigma(j))}$), or more explicitly via $(\sigma \cdot p)(x_1, ..., x_n) = p(x_{\sigma(1)}, \dots, x_{\sigma(n)})$.

Example 1.3.1. The S_n-action on $R[\mathbf{x}]$ can be surprisingly confusing, so here is an example. Suppose $n = 4$, and consider $\pi, \sigma \in S_4$ with $\pi = (1\ 3)$ and $\sigma = (1\ 2\ 4)$. Then $\pi\sigma = (1\ 3)(1\ 2\ 4) = (1\ 2\ 4\ 3)$. For a polynomial $p \in R[x_1, x_2, x_3, x_4]$, we have $(\pi(\sigma p))(x_1, x_2, x_3, x_4) = (\sigma p)(x_3, x_2, x_1, x_4)$. Since $(\sigma p)(y_1, \dots, y_4) = p(y_2, y_4, y_3, y_1)$, we can let $(y_1, y_2, y_3, y_4) = (x_3, x_2, x_1, x_4)$ and get

$$(\pi(\sigma p))(x_1, \dots, x_4) = p(y_2, y_4, y_3, y_1) = p(x_2, x_4, x_1, x_3) = ((\pi\sigma)p)(x_1, \dots, x_4)).$$

which is what we expect from a left action. The action of S_n on $R[\mathbf{x}]$ should not be regarded as the permutation of the arguments of a polynomial p, which is actually a right action. In fact, if we permute the arguments according to σ and then according to π, we get $p(x_1, x_2, x_3, x_4) \mapsto p(x_2, x_4, x_3, x_1) \mapsto p(x_3, x_4, x_2, x_1)$, which is exactly what we get by permuting the argument of p according to $\sigma\pi = (1\ 3\ 2\ 4)$.

We recall that $e_r \in R[\mathbf{x}]^{S_n}$ is the r-th elementary symmetric polynomial in the n variables $x_1, \ldots, x_n$.

Remark 1.3.2. Given a G-closure $\varphi : (A^{\otimes n})^G \to R$ of the monogenic degree n extension $R \to A$, we can compose it with $(R[\mathbf{x}])^G \to (A^{\otimes n})^G$ to get an R-algebra map $(R[\mathbf{x}])^G \to R$ sending $e_k \mapsto s_k$. Under reasonable conditions on R, one can prove that each such map $(R[\mathbf{x}])^G \to R$ comes from a unique normative map, as stated in the following Theorem from [1]:

Theorem 1.3.3. *Let $R \to A = R[x]/(f(x))$ be the monogenic degree-n extension of rings given by $f(x) = \sum_{k=0}^{n}(-1)^k s_k x^{n-k}$, where $s_0 = 1$. Let $G \leq S_n$ and suppose that $|G|$ is not a zero-divisor in R. Then isomorphism classes of G-closures for $R \to A$ are in one-to-one correspondence with R-algebra maps $\chi : R[\mathbf{x}]^G \to R$ sending $e_k \mapsto s_k$. Given such a map χ, the corresponding normative map $\varphi_\chi : (A^{\otimes n})^G \to R$ is the composition of χ after the R-algebra maps $(A^{\otimes n})^G \to R[\mathbf{x}]^G$ sending $x^{(j)} \mapsto x_j$.* □

To apply this theorem, one can try to find free $R[\mathbf{x}]^{S_n}$-module generators for $R[\mathbf{x}]^G$ (if possible) and, finding out algebraic relations among them, present $R[\mathbf{x}]^G$ as an $R[\mathbf{x}]^{S_n}$-algebra. For this reason, we will point out some useful facts about polynomial invariants. Over the complex numbers, we have this result, appearing as part of Theorem 2.7.6 in [6]:

Theorem 1.3.4. *Let $G \leq S_n$. Then $\mathbb{C}[\mathbf{x}]^G$ is a free $\mathbb{C}[\mathbf{x}]^{S_n}$-module of rank $n!/|G|$, and it has a free basis consisting of homogeneous polynomials. The degrees of such homogeneous generators do not depend on the choice of basis.*

Using this theorem we can prove the following slight generalization:

Lemma 1.3.5. *Let $G \leq H \leq S_n$. If $\mathbb{Z}[\mathbf{x}]^G$ is a finite free $\mathbb{Z}[\mathbf{x}]^H$-module generated by homogeneous polynomials, then it has rank $|H : G|$ over $\mathbb{Z}[\mathbf{x}]^H$. The degrees of such homogeneous generators don't depend on choice of basis.*

Proof. Suppose that $\mathcal{B}$ is a free $\mathbb{Z}[\mathbf{x}]^H$-basis for $\mathbb{Z}[\mathbf{x}]^G$ consisting of non-zero homogeneous polynomials. Then tensoring with $\mathbb{C}$ we get $\mathbb{C}[\mathbf{x}]^G \cong \bigoplus_{b\in\mathcal{B}} \mathbb{C}[\mathbf{x}]^H b$, and applying Theorem 1.3.4 we get

$$(\mathbb{C}[\mathbf{x}]^{S_n})^{|S_n:G|} \cong \bigoplus_{b\in\mathcal{B}} (\mathbb{C}[\mathbf{x}]^{S_n})^{|S_n:H|} b.$$

This implies that $|\mathcal{B}| < \infty$, and more precisely $|\mathcal{B}| = |S_n : G||S_n : H|^{-1} = |H : G|$. Moreover, the degrees of the homogeneous polynomial in $\mathcal{B}$ are uniquely determined by the degrees of any homogeneous $\mathbb{C}[\mathbf{x}]^{S_n}$-bases $\mathcal{G}$ for $\mathbb{C}[\mathbf{x}]^G$ and $\mathcal{H}$ for $\mathbb{C}[\mathbf{x}]^H$. Indeed, for a finite set of homogeneous polynomials $\mathcal{S} \subseteq \mathbb{C}[\mathbf{x}]$ one can define $D_{\mathcal{S}}(t) = \sum_{s\in\mathcal{S}} t^{\deg s} \in \mathbb{Z}[t]$. It is easily seen, as $\mathbb{C}[\mathbf{x}]$ is a domain, that $D_{\mathcal{S}\cdot\mathcal{S}'} = D_{\mathcal{S}} D_{\mathcal{S}'}$, denoting $\mathcal{S}\cdot\mathcal{S}' = \{s\cdot s' : s \in \mathcal{S}, s' \in \mathcal{S}'\}$. Then, since $\mathcal{G}$ and $\mathcal{B}\cdot\mathcal{H}$ are both free $\mathbb{C}[\mathbf{x}]^{S_n}$-bases for $\mathbb{C}[\mathbf{x}]^G$, Theorem 1.3.4 gives $D_{\mathcal{G}} = D_{\mathcal{B}\cdot\mathcal{H}} = D_{\mathcal{B}} D_{\mathcal{H}}$ which, $\mathbb{Z}[t]$ being a UFD, uniquely determines $D_{\mathcal{B}}$, and hence the degrees of the polynomials in $\mathcal{B}$. □

We now explain a way to recover the degrees of homogeneous free generators. We denote $N_{G,d} := \dim_{\mathbb{C}}(\mathbb{C}[\mathbf{x}]_d^G)$, where $\mathbb{C}[\mathbf{x}]_d^G$ denotes the submodule of $\mathbb{C}[\mathbf{x}]^G$ consisting of homogeneous polynomials of degree d. This allows us to define the *Molien formal series*:

$$\mathcal{M}_G(t) = \sum_{d\in\mathbb{Z}} N_{G,d} t^d \in \mathbb{C}[[t]]$$

Then, given a free $\mathbb{Z}[\mathbf{x}]^H$-basis $\mathcal{B} = \{g_1, ..., g_r\}$ for $\mathbb{Z}[\mathbf{x}]^G$, and $d_i = \deg g_i$, we get

$$\mathbb{C}[\mathbf{x}]^G = \bigoplus_{i=1}^r g_i \mathbb{C}[\mathbf{x}]^H = \bigoplus_{i=1}^r g_i \bigoplus_{d\in\mathbb{Z}} \mathbb{C}[\mathbf{x}]^H_{d-d_i} = \bigoplus_{d\in\mathbb{Z}} \bigoplus_{i=1}^r g_i \mathbb{C}[\mathbf{x}]^H_{d-d_i},$$

which means $N_{G,d} = \sum_{i=1}^r N_{H,d-d_i}$. Then we can expand out the Molien series

$$\mathcal{M}_G(t) = \sum_{d\in\mathbb{Z}} \sum_{i=1}^r N_{H,d-d_i} t^d = \sum_{i=1}^r t^{d_i} \sum_{d\in\mathbb{Z}} N_{H,d} t^d = \mathcal{M}_H(t) \sum_{i=1}^r t^{d_i}.$$

Hence what we need to do to recover the d_i is just to divide $\mathcal{M}_G(t)$ by $\mathcal{M}_H(t)$. To compute a Molien series we can use Molien's theorem (see [6], theorem 2.2.1), which gives

$$\mathcal{M}_G(t) = \frac{1}{|G|} \sum_{\sigma\in G} \frac{1}{\det(\mathrm{id} - t\sigma)}.$$

where we interpret $\sigma \in G \leq S_n$ as an element of $GL(\mathbb{C}, n)$. The polynomial $\det(I - t\sigma)$ is constant over the conjugacy class of σ in S_n, so that we just need to consider the sizes $l_1 + ... + l_s = n$ of the disjoint cycles into which σ decomposes. After reordering the basis, $I - t\sigma$ can be written as a matrix which is block diagonal, whose diagonal blocks are of the form

$$\begin{pmatrix} 1 & -t & & \\ & \ddots & \ddots & \\ & & 1 & -t \\ -t & & & 1 \end{pmatrix}$$

and whose determinant is given by $\prod_{j=1}^s (1 - t^{l_j})$.

The Molien series is an useful tool for finding a homogeneous $\mathbb{Z}[\mathbf{x}]^H$-basis for $\mathbb{Z}[\mathbf{x}]^G$, if it exists. They allow us to easily decide if $\mathbb{C}[\mathbf{x}]^G$ is a free $\mathbb{C}[\mathbf{x}]^H$-module, which is not always the case (for example, $\mathbb{Z}[x_1, x_2, x_3, x_4]^{C_4}$ is not a free $\mathbb{Z}[x_1, x_2, x_3, x_4]^{D_4}$-module, see Example 2.0.3), but this does not immediately imply that a graded $\mathbb{Z}[\mathbf{x}]^H$-basis for $\mathbb{Z}[\mathbf{x}]^G$ exists (see Proposition 2.2.1).

Chapter 2

Criteria for monogenic degree-4 extensions

In this chapter we will parametrize isomorphism classes of G-closures for monogenic degree-4 extensions $R \to A = R[x]/(f(x))$, for $G \leq S_4$, using the results we recalled in Chapter 1. We will start by pointing out for which subgroups of S_4 this is already done in [1] or follows immediately from the previous chapter. Then we will work the remaining subgroups in separate sections.

First, notice that for $G \in \{1, S_2, S_3, S_2 \times S_2, S_4\}$ we can apply Theorem 1.2.1 to put in one-to-one correspondence isomorphism classes of G-closures with particular factorizations of f. More precisely, we have the following correspondences:

- there exists precisely one isomorphism class of S_4-closures for $R \to A$;
- isomorphism classes of S_3-closures for $R \to A$ are in one-to-one correspondence with roots $r \in R$ of the monic polynomial f by Corollary 1.2.2;
- isomorphism classes of $(S_2 \times S_2)$-closures for $R \to A$ are in one-to-one correspondence with factorizations of f into two monic polynomials of degree 2 in $R[x]$, that is, quadruples $(u_1, u_2, v_1, v_2) \in R^4$ such that $f(x) = (x^2 - u_1 x + u_2)(x^2 - v_1 x + v_2)$;
- isomorphism classes of S_2-closures for $R \to A$ are in one-to-one correspondence with factorizations of f into a monic polynomial of degree 2 and two monic linear factors in $R[x]$, that is, quadruples $(u_1, u_2, r_1, r_2) \in R^4$ such that $f(x) = (x^2 - u_1 x + u_2)(x - r_1)(x - r_2)$
- isomorphism classes of 1-closures for $R \to A$ are in one-to-one correspondence with splittings of f into monic linear factors in $R[x]$, that is, quadruples $(r_1, r_2, r_3, r_4) \in R^4$ such that $f(x) = (x - r_1)(x - r_2)(x - r_3)(x - r_4)$.

Moreover, as said in the introduction, the parametrization of A_n-closures given in [1] allows us to give an explicit parametrization of A_4-closures for monogenic extensions, which the reader can find in Appendix B.1. Similarly, but paying a bit more attention, one can use the parametrization of A_n-closures to give a parametrization of C_3-closures when 6 is not a zero-divisor. This is done in Section 2.4.

Considering Figure 1 from the introduction, it is clear the only remaining subgroups to consider are D_4, V_4, C_4 and C_2. The case $G = D_4$ is treated in [1]. There is proven the following:

Lemma 2.0.1. *Let R be a ring and $\lambda = x_1x_3 + x_2x_4$. Then $\{1, \lambda, \lambda^2\}$ is a free basis for $R[\mathbf{x}]^{D_4}$ as an $R[\mathbf{x}]^{S_4}$-module.*

The proof is given for $R = \mathbb{Z}$, the result for any other R following by tensoring everything with R (over $\mathbb{Z}$). It is a constructive proof, since it allows us to explicitly write down any $p \in \mathbb{Z}[\mathbf{x}]^{D_4}$ as $p = a_p + b_p\lambda + c_p\lambda^2$. We here write down the explicit equations from [1] for obtaining a_p, b_p, c_p (with a different notation), which will be useful when dealing with C_4-invariant polynomials, in Appendix B.2. We define

$$\omega_p = \frac{\tau_{14}p - \tau_{12}p}{(x_1 - x_3)(x_2 - x_4)} \quad \text{and} \quad \chi_p = \frac{\tau_{14}\omega_p - \tau_{12}\omega_p}{(x_1 - x_3)(x_2 - x_4)}.$$

Then we get the symmetric coefficients:

$$\begin{aligned} c_p &= -\chi_p \\ b_p &= \omega_p - c_p(x_1 + x_3)(x_2 + x_4) = \omega_p + \chi_p(e_2 - \lambda) \\ a_p &= p - b\lambda - c\lambda^2 = p - \omega_p\lambda + \chi_p\lambda^2 - \chi_p(e_2 - \lambda)\lambda \end{aligned}$$

As λ is a root of $r_1(\Lambda) = (\Lambda-\lambda)(\Lambda-\tau_{14}\lambda)(\Lambda-\tau_{12}\lambda) = \Lambda^3 - e_2\Lambda^2 + (e_1e_3 - 4e_4)\Lambda - (e_3^2 - 4e_2e_4 + e_1^2e_4) \in \mathbb{Z}[\mathbf{x}]^{S_4}$, we get an isomorphism $R[\mathbf{x}]^{D_4} \cong R[\mathbf{x}]^{S_4}[\Lambda]/(r_1(\Lambda))$, so that finding a map $R[\mathbf{x}]^{D_4} \to R$ sending $e_k \mapsto s_k$ is equivalent to find a root $l \in R$ for the polynomial $g(x) = x^3 - s_2x^2 + (s_1s_3 - 4s_4)x - (s_3^2 - 4s_2s_4 + s_1^2s_4)$. This polynomial is called the *resolvent cubic* of the polynomial f. Hence the following parametrization from [1]:

Theorem 2.0.2. *Let R be a ring such that $2 \in R$ is not a zero-divisor. Consider the monogenic degree-4 extension $R \to A = R[x]/(f(x))$, where $f(x) = x^4 - s_1x^3 + s_2x^2 - s_3x + s_4$. Then isomorphism classes of D_4-closures for $R \to A$ are in one-to-one correspondence with roots $\ell \in R$ of the resolvent cubic $g(x) = x^3 - s_2x^2 + (s_1s_3 - 4s_4)x - (s_3^2 - 4s_2s_4 + s_1^2s_4)$.*

In the the following three sections, we will present the polynomial invariants $R[\mathbf{x}]^G$ as an $R[\mathbf{x}]^{S_4}$-algebra, for $G \in \{C_2, C_4, V_4\}$. This will allow us to give parametrizations of G-closures via Theorem 1.3.3. In order to do this, we will use Molien series, as defined in previous chapter, to get information about the possible degrees of polynomials generating $R[\mathbf{x}]^G$ as a free $R[\mathbf{x}]^{S_4}$-module. We compute them in this example:

Example 2.0.3. In this table we write down $\det(\mathrm{id} - t\sigma)$ in relation to the conjugation class of $\sigma \in S_4$, that is, its cycle type. We also write how many elements of each conjugation class there are in certain subgroups of S_4:

cycle type	S_4	D_4	C_4	V_4	$\det(\mathrm{id} - t\sigma)$
$1+1+1+1$	1	1	1	1	$(1-t)^4$
$2+1+1$	6	2	0	0	$(1-t^2)(1-t)^2 = (1-t)^3(1+t)$
$2+2$	3	3	1	3	$(1-t^2)^2 = (1-t)^2(1+t)^2$
$3+1$	8	0	0	0	$(1-t^3)(1-t) = (1-t)^2(1+t+t^2)$
4	6	2	2	0	$1-t^4 = (1-t)(1+t)(1+t^2)$

This allows us to compute the Molien series for those four subgroups of S_4:

$$\begin{aligned}
\mathcal{M}_{S_4}(t) =& \frac{1}{24}\left(\frac{1}{(1-t)^4} + \frac{6}{(1-t)^3(1+t)} + \frac{3}{(1-t^2)^2} + \frac{8}{(1-t)^2(1+t+t^2)} + \frac{6}{1-t^4}\right) \\
=& \frac{1}{(1-t)^4(1+t)^2(1+t+t^2)(1+t^2)} \\
\mathcal{M}_{D_4}(t) =& \frac{1}{8}\left(\frac{1}{(1-t)^4} + \frac{2}{(1-t)^3(1+t)} + \frac{3}{(1-t^2)^2} + \frac{2}{1-t^4}\right) \\
=& \frac{1-t+t^2}{(1-t)^4(1+t)^2(1+t^2)} \\
\mathcal{M}_{V_4}(t) =& \frac{1}{4}\left(\frac{1}{(1-t)^4} + \frac{3}{(1-t^2)^2}\right) = \frac{1-t+t^2}{(1-t)^4(1+t)^2} \\
\mathcal{M}_{C_4}(t) =& \frac{1}{4}\left(\frac{1}{(1-t)^4} + \frac{1}{(1-t^2)^2} + \frac{2}{1-t^4}\right) = \frac{t^3+t^2-t+1}{(1-t)^4(1+t)^2(1+t^2)}
\end{aligned}$$

Then one gets for example that $\frac{\mathcal{M}_{D_4}(t)}{\mathcal{M}_{S_4}(t)} = (1-t+t^2)(1+t+t^2) = 1+t^2+t^4$, which means that possible homogeneous generators for $\mathbb{Z}[\mathbf{x}]^{D_4}$ as $\mathbb{Z}[\mathbf{x}]^{S_4}$-modules have to be of degrees 0, 2 and 4, in agreement with Lemma 2.0.1. Moreover, $\frac{\mathcal{M}_{C_4}(t)}{\mathcal{M}_{D_4}(t)} = (t^3+t^2-t+1)(1-t+t^2)^{-1} \notin \mathbb{Z}[t]$, which shows that $\mathbb{C}[\mathbf{x}]^{C_4}$ is not a free $\mathbb{C}[\mathbf{x}]^{D_4}$-module (and of course this cannot be true with polynomials over $\mathbb{Z}$).

2.1 V_4-closures for monogenic degree-4 extensions

In this section, we will consider $V_4 = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ and parametrize V_4-closures for monogenic degree-4 ring extensions, assuming that $2 \in R$ is not a zero-divisor. In this case, Theorem 2.1.4 states that V_4-closures for the monogenic degree-4 extension $R \to R[x]/(f(x))$ are in one-to-one correspondence with splittings of the resolvent cubic of the polynomial $f(x)$.

To prove this, we want to describe $R[\mathbf{x}]^{V_4}$ as an $R[\mathbf{x}]^{D_4}$-algebra. From the Molien series computed in Example 2.0.3, we get $\frac{\mathcal{M}_{V_4}(t)}{\mathcal{M}_{D_4}(t)} = 1+t^2$, suggesting that $R[\mathbf{x}]^{V_4}$ may be a free $R[\mathbf{x}]^{D_4}$-module generated by two polynomials of degree 0 and 2. This is actually true:

Lemma 2.1.1. *Let R be any ring, $\lambda = x_1x_3 + x_2x_4 \in R[\mathbf{x}]$ and $\mu = \tau_{14}\lambda = x_1x_2 + x_3x_4$. Then*

$$R[\mathbf{x}]^{V_4} = R[\mathbf{x}]^{D_4} \oplus R[\mathbf{x}]^{D_4}\mu$$

Proof. This can be proved for $R = \mathbb{Z}$, the result for any other ring following just by tensoring with it over $\mathbb{Z}$. For $p \in \mathbb{Z}[\mathbf{x}]^{V_4}$, we have that $p - \tau_{13}p$ changes sign under τ_{13} and under τ_{24}. Then such a difference is mapped to zero via both the quotient maps $\mathbb{Z}[\mathbf{x}] \to \mathbb{Z}[\mathbf{x}]/(x_1 - x_3)$ and $\mathbb{Z}[\mathbf{x}] \to \mathbb{Z}[\mathbf{x}]/(x_2 - x_4)$, because there it coincides with its opposite, and 2 is not a zero-divisor in $\mathbb{Z}$. Now, as $\mathbb{Z}[\mathbf{x}]$ is a UFD, we can define

$$\rho_p = \frac{p - \tau_{13}p}{(x_1 - x_3)(x_2 - x_4)}.$$

We immediately see that $\rho_\mu = 1$. Notice that the numerator and the denominator of ρ_p do both change sign under τ_{13} and are both V_4-invariant, so that ρ_p is invariant under $\langle V_4, \tau_{13}\rangle = D_4$.

Suppose that $0 = \alpha + \beta\mu$, with $\alpha, \beta \in \mathbb{Z}[\mathbf{x}]^{D_4}$. Then by computing $\rho_0 = 0$ we obtain $\beta = 0$, hence $\alpha = 0$. This proves linear independence of 1 and μ over $\mathbb{Z}[\mathbf{x}]^{D_4}$.

On the other hand, for $p \in \mathbb{Z}[\mathbf{x}]^{V_4}$ we can define $\beta = \rho_p$ and $\alpha = p - \beta\mu$. Then $\beta \in \mathbb{Z}[\mathbf{x}]^{D_4}$ as already noticed, $p = \alpha + \beta\mu$ by definition of α, and $\alpha \in \mathbb{Z}[\mathbf{x}]^{D_4}$: it is in $\mathbb{Z}[\mathbf{x}]^{V_4}$ by definition, and $\alpha - \tau_{13}\alpha = (p - \tau_{13}p) - (x_1x_2 + x_3x_4 - x_1x_4 - x_2x_3)\beta = (x_1 - x_3)(x_2 - x_4)\rho_p - (x_1 - x_3)(x_2 - x_4)\beta = 0$. This proves that $1, \mu$ are generators for $\mathbb{Z}[\mathbf{x}]^{V_4}$ as an $\mathbb{Z}[\mathbf{x}]^{D_4}$-module. □

Lemma 2.1.2. *Let R be any ring, $\lambda = x_1x_3 + x_2x_4 \in R[\mathbf{x}]$ and $\mu = \tau_{14}\lambda = x_1x_2 + x_3x_4$. Then $\{1, \lambda, \lambda^2, \mu, \lambda\mu, \lambda^2\mu\}$ is a free basis for $R[\mathbf{x}]^{V_4}$ as an $R[\mathbf{x}]^{S_4}$-module.*

Proof. This is just a combination of Lemma 2.0.1 and Lemma 2.1.1. □

Now we let $\nu = \tau_{12}\lambda = x_1x_4 + x_2x_3$. Then λ is a root of the polynomial

$$r_1(\Lambda) = (\Lambda - \lambda)(\Lambda - \mu)(\Lambda - \nu) = \Lambda^3 - e_2\Lambda^2 + (e_1e_3 - 4e_4)\Lambda - (e_3^2 - 4e_2e_4 + e_1^2e_4),$$

which has coefficients in $\mathbb{Z}[\mathbf{x}]^{S_4}$, and factors in $\mathbb{Z}[\mathbf{x}]^{D_4}[\Lambda]$ as

$$r_1(\Lambda) = (\Lambda - \lambda)(\Lambda^2 - (e_2 - \lambda)\Lambda + \lambda^2 - e_2\lambda + e_1e_3 - 4e_4).$$

Denoting $H(\Lambda, M) := M^2 - (e_2 - \Lambda)M + \Lambda^2 - e_2\Lambda + e_1e_3 - 4e_4$, we have

Lemma 2.1.3. *For any ring R, consider the polynomials $r_1(\Lambda)$ and $H(\Lambda, M)$ as above. Then we have an isomorphism of $R[\mathbf{x}]^{S_4}$-algebras*

$$\frac{R[\mathbf{x}]^{S_4}[\Lambda, M]}{(r_1(\Lambda), H(\Lambda, M))} \xrightarrow{\sim} R[\mathbf{x}]^{V_4}$$

sending $\Lambda \mapsto \lambda$ and $M \mapsto \mu$.

Proof. To define such a morphism we just need to say where to send Λ and M, in such a way that $r_1(\Lambda)$ and $H(\Lambda, M)$ are mapped to zero. But this is actually the case, since $r_1(\Lambda) \mapsto r_1(\lambda) = 0$, and $H(\Lambda, M) \mapsto H(\lambda, \mu) = 0$. With an easy induction one can prove that $\{1, \Lambda, \Lambda^2, M, M\Lambda, M\Lambda^2\}$ is a set of $R[\mathbf{x}]^{S_4}$-generators of the domain, and since they are mapped to the $R[\mathbf{x}]^{S_4}$-basis $\{1, \lambda, \lambda^2, \mu, \mu\lambda, \mu\lambda^2\}$, the map is bijective. Indeed any linear combination is sent to a linear combination of the basis, which is zero if and only if the coefficients are all zero (proving injectivity), and the image of map is generated by $\{1, \lambda, \lambda^2, \mu, \mu\lambda, \mu\lambda^2\}$ (proving surjectivity). □

Theorem 2.1.4. *Let R be a ring such that $2 \in R$ is not a zero-divisor. Consider the monogenic degree-4 extension $R \to A = R[x]/(f(x))$, where $f(x) = x^4 - s_1x^3 + s_2x^2 - s_3x + s_4$. Then isomorphism classes of V_4-closures for A over R are in one-to-one correspondence with triples $(\ell_1, \ell_2, \ell_3) \in R^3$ of roots of the resolvent cubic $g(x) = x^3 - s_2x^2 + (s_1s_3 - 4s_4)x - (s_3^2 - 4s_2s_4 + s_1^2s_4)$ realizing $g(x) = (x - \ell_1)(x - \ell_2)(x - \ell_3)$.*

Proof. Since $|V_4| = 4$ is not a zero-divisor (as 2 is not), we can apply Theorem 1.3.3, so that isomorphism classes of V_4-closures for $R \to A$ are in one-to-one correspondence with R-algebra maps $R[\mathbf{x}]^{V_4} \to R$ mapping $e_k \mapsto s_k$. By Lemma 2.1.3, determining such a map is equivalent to choosing $(\ell, m) \in R^2$ such that $g(\ell) = 0$ (since the coefficients of g are the image of the coefficients of r_1) and m is a root of the polynomial $g(x)/(x-\ell)$. This division makes sense thanks to Lemma 1.2.3, and the same lemma allows us to conclude that isomorphism classes of V_4-closures for $R \to A$ are in one-to-one correspondence with triples $(\ell_1, \ell_2, \ell_3) \in R^3$ such that $g(t) = (t-\ell_1)(t-\ell_2)(t-\ell_3)$. □

2.2 C_4-closures for monogenic degree-4 extensions

In this section, we will consider $C_4 = \{1, \sigma, \sigma^2, \sigma^3\}$, with $\sigma = (1\ 2\ 3\ 4)$, and parametrize C_4-closures for monogenic degree-4 ring extensions, assuming that 2 is a unit. We prove that under this condition $R[\mathbf{x}]^{C_4}$ is a free $R[\mathbf{x}]^{S_4}$-module with free basis $\{1, \lambda, \lambda^2, \eta, \theta, \lambda\eta\}$, where

$$\begin{aligned}
\lambda &= x_1x_3 + x_2x_4, \\
\eta &= (x_1 - x_3)(x_2 - x_4)(x_1 - x_2 + x_3 - x_4), \text{ and} \\
\theta &= (x_1 - x_3)(x_2 - x_4)(x_1x_3 - x_2x_4).
\end{aligned}$$

Hence λ, η and θ generate $R[\mathbf{x}]^{C_4}$ as an $R[\mathbf{x}]^{S_4}$-algebra, and we present it as a quotient of $R[\Lambda, H, \Theta]$ by six equations.

Since 2 is a unit, one can assume, by changing variables to $x' = x - s_1/4$, that the polynomial $f(x)$ is of the form $x^4 + s_2x^2 - s_3x + s_4$, and get that isomorphism classes of C_4-closures for the extension are in one-to-one correspondence with triples $(\ell, h, t) \in R^3$ satisfying the following equalities, where $g(x) = x^3 - s_2x^2 + (s_1s_3 - 4s_4)x - (s_3^2 - 4s_2s_4 + s_1^2s_4)$ is the resolvent cubic of f:

$$\begin{cases}
g(\ell) = 0 \\
h^2 = 8s_2\ell^2 + (-4s_2^2 + 16s_4)\ell + (-4s_2^3 - 12s_3^2 - 16s_2s_4) \\
t^2 = 16s_4\ell^2 - 3s_3^2\ell - s_2s_3^2 - 64s_4^2 \\
ht = 6s_3\ell^2 - 4s_2s_3\ell - 2s_2^2s_3 - 32s_3s_4 \\
2t(\ell - s_2) + s_3h = 0 \\
h\ell^2 + 2s_3t - 4s_4h = 0
\end{cases}$$

First, we point out that it is not possible to have free homogeneous generators for $\mathbb{Z}[\mathbf{x}]^{C_4}$ as an $\mathbb{Z}[\mathbf{x}]^{S_4}$-module, explicitly using the fact that 2 is not invertible in $\mathbb{Z}$:

Proposition 2.2.1. *$\mathbb{Z}[\mathbf{x}]^{C_4}$ is not a graded free $\mathbb{Z}[\mathbf{x}]^{S_4}$-module of any rank.*

Proof. Suppose it were. Then we could apply Lemma 1.3.5, and considering the Molien series for C_4 and S_4 computed in Example 2.0.3 we would have

$$\frac{\mathcal{M}_{C_4}(t)}{\mathcal{M}_{S_4}(t)} = (1 + t + t^2)(t^3 + t^2 - t + 1) = 1 + t^2 + t^3 + 2t^4 + t^5.$$

implying the existence of six homogeneous free $\mathbb{Z}[\mathbf{x}]^{S_4}$-module generators $p_1, \ldots, p_6$ for $\mathbb{Z}[\mathbf{x}]^{C_4}$ of degree $0, 2, 3, 4, 4, 5$. Then $\mathbb{Z}[\mathbf{x}]^{C_4}$ would coincide with its $\mathbb{Z}[\mathbf{x}]^{S_4}$-submodule $\langle \bigcup_{d=0}^{5} \mathbb{Z}[\mathbf{x}]_d^{C_4} \rangle$. As the $\mathbb{Z}[\mathbf{x}]^{S_4}$-span of the six polynomials $g_1 = 1$, $g_2 = x_1x_3 + x_2x_4$, $g_3 = x_1^2x_2 + x_2^2x_3 + x_3^2x_4 + x_4^2x_1$, $g_4 = (x_1x_3 + x_2x_4)^2$, $g_5 = x_1^3x_2 + x_2^3x_3 + x_3^3x_4 + x_4^3x_1$, $g_6 = x_1^3x_2^2 + x_2^3x_3^2 + x_3^3x_4^2 + x_4^3x_1^2$ contains all $\bigcup_{d=0}^{5} \mathbb{Z}[\mathbf{x}]_d^{C_4}$, they would have to generate all of $\mathbb{Z}[\mathbf{x}]^{C_4}$, hence be a free basis (since the $\mathbb{Z}[\mathbf{x}]^{S_4}$-module endomorphism of $\mathbb{Z}[\mathbf{x}]^{C_4}$ sending $g_i \mapsto p_i$ would need to be bijective, by the same arguments given in the proof of Lemma 2.1.3). But this is not true, since the polynomial $p_0 = x_1^3x_2x_3^2 + x_2^3x_3x_4^2 + x_3^3x_4x_1^2 + x_4^3x_1x_2^2$ is not in their $\mathbb{Z}[\mathbf{x}]^{S_4}$-span. Indeed,

$$\begin{aligned} 2p_0 =& (e_1^2e_2^2 - 2e_2^3 - 2e_1^3e_3 + 3e_1e_2e_3 - 2e_3^2 + 2e_1^2e_4 + 2e_2e_4)g_1 \\ &+ (e_2^2 + e_1e_3 - 2e_4)g_2 + (-e_1^3 + 3e_1e_2 - e_3)g_3 + (-e_1^2 + e_2)g_4 \\ &+ (e_1^2 - 2e_2)g_5 - e_1g_6, \end{aligned}$$

which by linear independence implies that all the symmetric coefficient should be divisible by 2, while $e_1 = x_1 + x_2 + x_3 + x_4$ is not. Thus no free basis can exist. □

The previous proof's final part suggests that $R[\mathbf{x}]^{C_4}$ can be a graded free $R[\mathbf{x}]^{S_4}$-module if we require 2 to be a unit in R. We will now show that this is actually the case:

Proposition 2.2.2. *Let R be a ring such that $2 \in R^\times$. Consider the following C_4-invariant polynomials:*

$$\begin{aligned} \lambda &= x_1x_3 + x_2x_4 \\ \eta &= (x_1 - x_3)(x_2 - x_4)(x_1 - x_2 + x_3 - x_4) \\ \theta &= (x_1 - x_3)(x_2 - x_4)(x_1x_3 - x_2x_4) \end{aligned}$$

Then $\{1, \lambda, \lambda^2, \eta, \theta, \lambda\eta\}$ is a free basis for $R[\mathbf{x}]^{C_4}$ as an $R[\mathbf{x}]^{S_4}$-module.

It is enough to prove this for $R = \mathbb{Z}\left[\frac{1}{2}\right]$. Indeed, the result for R any other ring with $2 \in R^\times$ can be obtained by tensoring over $\mathbb{Z}$ with R itself, since $\mathbb{Z}\left[\frac{1}{2}\right] \otimes_{\mathbb{Z}} R \cong R$. To do this, we will use the two following lemmas:

Lemma 2.2.3. *Take x_i, x_j, x_k indeterminates in $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]$ with $x_i \neq x_j$, and let $f \in \mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]$ be fixed by τ_{ij}. Then the polynomial $g_{i,j,k;f} := \tau_{jk}f - \tau_{ik}f$ is divisible by $(x_j - x_i)$ and $g_{i,j,k;f}/(x_j - x_i)$ is fixed by τ_{ij}.*

Proof. We have $\tau_{ij}(g_{i,j,k;f}) = \tau_{ij}\tau_{jk}f - \tau_{ij}\tau_{ik}f = \tau_{ik}\tau_{ij}f - \tau_{jk}\tau_{ij}f = \tau_{ik}f - \tau_{jk}f = -g_{i,j,k;f}$. Then in the quotient $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]/(x_j - x_i)$ one has $g_{i,j,k;f} = \tau_{ij}g_{i,j,k;f} = -g_{i,j,k;f}$, so that $g_{i,j,k;f} = 0$ since 2 is not a zero-divisor in R, and so neither in $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]/(x_j - x_i)$. Since $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]$ is a UFD, $g_{i,j,k;f}$ is divisible by $x_j - x_i$. Their ratio is fixed by τ_{ij} as it changes both their signs. □

For any polynomial $p \in R[\mathbf{x}]$ we will denote $\tilde{p} := \tau_{13}p$. Moreover, we will denote $\sigma = (1\ 2\ 3\ 4)$.

Lemma 2.2.4. *For R a ring, denote*

$$\begin{aligned} R[\mathbf{x}]^{C_4}_{+,D_4} &= \{f \in R[\mathbf{x}]^{C_4} : \tilde{f} = f\} = R[\mathbf{x}]^{D_4}, \\ R[\mathbf{x}]^{C_4}_{-,D_4} &= \{f \in R[\mathbf{x}]^{C_4} : \tilde{f} = -f\}, \text{ and} \\ R[\mathbf{x}]^{S_2 \times S_2}_{-,D_4} &= \{f \in R[\mathbf{x}] : \tilde{f} = f, \sigma f = -f\}. \end{aligned}$$

1. *If $2 \in R^\times$, then $R[\mathbf{x}]^{C_4} = R[\mathbf{x}]^{C_4}_{+,D_4} \oplus R[\mathbf{x}]^{C_4}_{-,D_4}$ as $R[\mathbf{x}]^{S_4}$-submodules of $R[\mathbf{x}]^{C_4}$.*

2. The following is an isomorphism of $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{S_4}$*-modules:*

$$\begin{aligned} \mathbb{Z}\left[\tfrac{1}{2}\right][\mathbf{x}]^{S_2\times S_2}_{-,D_4} &\to \mathbb{Z}\left[\tfrac{1}{2}\right][\mathbf{x}]^{C_4}_{-,D_4} \\ f &\mapsto (x_1-x_3)(x_2-x_4)f \end{aligned}$$

Proof. First, note that $R[\mathbf{x}]^{C_4}_{+,D_4}$, $R[\mathbf{x}]^{C_4}_{-,D_4}$ and $R[\mathbf{x}]^{S_2\times S_2}_{-,D_4}$ are clearly $R[\mathbf{x}]^{S_4}$-submodules of $R[\mathbf{x}]^{C_4}$ as they are closed under sum and multiplication by symmetric polynomials. For all $p \in R[\mathbf{x}]^{C_4}$, one has $p = \frac{p+\tilde{p}}{2} + \frac{p-\tilde{p}}{2}$, which makes sense as $2 \in R^\times$. Clearly $\frac{p+\tilde{p}}{2} \in R[\mathbf{x}]^{C_4}_{+,D_4}$ and $\frac{p-\tilde{p}}{2} \in R[\mathbf{x}]^{C_4}_{-,D_4}$. Hence $R[\mathbf{x}]^{C_4} = R[\mathbf{x}]^{C_4}_{+,D_4} + R[\mathbf{x}]^{C_4}_{-,D_4}$. Moreover, if $p \in R[\mathbf{x}]^{C_4}_{+,D_4} \cap R[\mathbf{x}]^{C_4}_{-,D_4}$ then $p = \tilde{p} = -p$, so that $2p = 0$ and $p = 0$. Hence the decomposition $R[\mathbf{x}]^{C_4} = R[\mathbf{x}]^{C_4}_{+,D_4} \oplus R[\mathbf{x}]^{C_4}_{-,D_4}$.

The map $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{S_2\times S_2}_{-,D_4} \to \mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{C_4}_{-,D_4}$ sending $f \mapsto (x_1-x_3)(x_2-x_4)f$ is well-defined, since for f in the domain we have

$$\sigma((x_1-x_3)(x_2-x_4)f) = (x_2-x_4)(x_3-x_1)(-f) = (x_1-x_3)(x_2-x_4)f$$

and

$$\tau_{13}((x_1-x_3)(x_2-x_4)f) = (x_3-x_1)(x_2-x_4)f = -(x_1-x_3)(x_2-x_4)f.$$

It clearly respects the $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{S_4}$-module structure, and it is injective since $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]$ is an integral domain. Moreover, for any polynomial $g \in R[\mathbf{x}]^{C_4}$ such that $\tau_{13}g = -g$, we also have $\tau_{24}g = \tau_{24}\sigma^2 g = \tau_{13}g = -g$, so that g coincides with its opposite when mapped to each of the quotient rings $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]/(x_3-x_1)$ and $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]/(x_4-x_2)$, implying that g vanishes there. As $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]$ is a UFD, one gets $(x_1-x_3)(x_2-x_4)|g$, and this allows us to conclude that the map above is also surjective. $\square$

Proof of Proposition 2.2.2. As already said, we can reduce to $R = \mathbb{Z}\left[\frac{1}{2}\right]$. By point 1 in Lemma 2.2.4, we have $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{C_4} = \mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{C_4}_{+,D_4} \oplus \mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{C_4}_{-,D_4}$, where $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{C_4}_{+,D_4} = \mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{S_4} \oplus \mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{S_4}\lambda \oplus \mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{S_4}\lambda^2$ by Lemma 2.0.1. It only remains to prove that $\{\eta, \theta, \lambda\eta\}$ is a free $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{S_4}$-basis for $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{C_4}_{-,D_4}$.

By Lemma 2.2.4, point 2, we just need to prove that $\{\rho_\eta, \rho_\theta, \rho_{\lambda\eta}\}$ is a free $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{S_4}$-basis for $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{S_2\times S_2}_{-,D_4}$, where we denote, for $\Omega \in \mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{C_4}_{-,D_4}$,

$$\rho_\Omega := \frac{\Omega}{(x_1-x_3)(x_2-x_4)} \in \mathbb{Z}\left[\tfrac{1}{2}\right][\mathbf{x}]^{S_2\times S_2}_{-,D_4}.$$

Hence, for $p \in \mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{S_2\times S_2}_{-,D_4}$, we are interested in decompositions of the form

$$p = \alpha\rho_\eta + \beta\rho_\theta + \gamma\rho_{\lambda\eta}, \text{ with } \alpha, \beta, \gamma \in \mathbb{Z}\left[\tfrac{1}{2}\right][\mathbf{x}]^{S_4}. \tag{2.1}$$

As $p \in \mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{S_2\times S_2}_{-,D_4}$ is fixed by τ_{24}, we can apply Lemma 2.2.3 twice, with $(i,j,k) = (2,4,1)$, and define

$$p' := \frac{\tau_{14}p - \tau_{12}p}{x_4 - x_2}, \quad p'' := \frac{\tau_{14}p' - \tau_{12}p'}{x_4 - x_2}.$$

Now $p'' - \tau_{13}p''$ vanishes in the quotient $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]/(x_3 - x_1)$, and we can define

$$\delta_p := \frac{p'' - \tau_{13}p''}{x_3 - x_1}.$$

With some easy computation we obtain:

Ω	ρ_Ω	ρ'_Ω	ρ''_Ω	δ_{ρ_Ω}
η	$x_1 - x_2 + x_3 - x_4$	2	0	0
θ	$x_1x_3 - x_2x_4$	$x_1 + x_3$	1	0
$\lambda\eta$	$\lambda\rho_\eta$	$(x_1 - x_3)^2 + (x_1 + x_3)(x_2 + x_4)$	$e_1 - 4x_3$	-4

Then the equality (2.1) implies the conditions

$$\begin{cases} p' = 2\alpha + \beta(x_1 + x_3) + \gamma((x_1 - x_3)^2 + (x_1 + x_3)(x_2 + x_4)) \\ p'' = \beta + \gamma(e_1 - 4x_3) \\ \delta_p = -4\gamma \end{cases} \tag{2.2}$$

Notice that if we suppose (2.1) holds with $p = 0$, then p', p'', δ_p do all vanish, so that third equation gives $\gamma = 0$, then the second gives $\beta = 0$ and the first $\alpha = 0$. Hence we have linear independence of ρ_η, ρ_θ and $\rho_{\lambda\eta}$.

For any $p \in \mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{S_2 \times S_2}_{-,D_4}$, by solving equations (2.2) we get uniquely defined values of α, β and γ. We want to prove that they are symmetric polynomials satisfying (2.1). Equations (2.2) give

$$\gamma = -\frac{1}{4}\delta_p, \quad \beta = p'' + \frac{1}{4}(e_1 - 4x_3)\delta_p, \quad \alpha = \frac{1}{2}p' - \frac{1}{2}(x_1 + x_3)p'' + \frac{1}{2}x_3^2\delta_p.$$

To prove that α, β, γ are symmetric, we start by noticing some symmetries of the polynomials p, p', p'' and δ_p. First, observe that p, p', p'' are invariant under τ_{24} by Lemma 2.0.1, and so is δ_p by definition. We also know that p is invariant under τ_{13} and changes sign under $\sigma = (1\,2\,3\,4)$. Moreover, $\tau_{34}\sigma = (1\,2\,4) = \tau_{12}\tau_{24}$ and $\tau_{23}\sigma = (1\;3\;4) = \tau_{14}\tau_{13}$, implying

$$\tau_{34}p = -\tau_{34}\sigma p = -\tau_{12}p \quad \text{and} \quad \tau_{23}p = -\tau_{23}\sigma p = -\tau_{14}p.$$

Then p' is also invariant under τ_{13}:

$$\tau_{13}p' = \frac{\tau_{34}\tau_{13}p - \tau_{23}\tau_{13}p}{x_4 - x_2} = \frac{\tau_{34}p - \tau_{23}p}{x_4 - x_2} = \frac{\tau_{14}p - \tau_{12}p}{x_4 - x_2} = p'$$

Now p'' is invariant under τ_{14}, since

$$\begin{aligned} \tau_{14}p'' - p'' &= \tau_{14}\frac{\tau_{14}p' - \tau_{12}p'}{x_4 - x_2} - \frac{\tau_{14}p' - \tau_{12}p'}{x_4 - x_2} = \frac{p' - \tau_{12}p'}{x_1 - x_2} - \frac{\tau_{14}p' - \tau_{12}p'}{x_4 - x_2} \\ &= \frac{\frac{\tau_{14}p - \tau_{12}p}{x_4 - x_2} - \frac{\tau_{14}p - p}{x_4 - x_1}}{x_1 - x_2} - \frac{\frac{p - \tau_{12}p}{x_1 - x_2} - \frac{\tau_{14}p - p}{x_4 - x_1}}{x_4 - x_2} \\ &= \frac{(x_4 - x_1) + (x_2 - x_4) + (x_1 - x_2)}{(x_4 - x_2)(x_1 - x_2)(x_4 - x_1)}(\tau_{14}p - p) = 0, \end{aligned}$$

meaning that p'' is symmetric in the variables x_1, x_2, x_4.

From this we can see that δ_p is symmetric, since it is not only invariant under τ_{13} and τ_{24}, but also under τ_{14}:

$$\begin{aligned}\tau_{14}\delta_p - \delta_p &= \frac{\tau_{14}p'' - \tau_{14}\tau_{13}p''}{x_3 - x_4} - \frac{p'' - \tau_{13}p''}{x_3 - x_1} \\ &= \frac{(x_4 - x_1)p'' - (x_3 - x_1)\tau_{14}\tau_{13}p'' + (x_3 - x_4)\tau_{13}p''}{(x_3 - x_4)(x_3 - x_1)} \\ &= \frac{\tau_{12}((x_4 - x_2)p'') + \tau_{14}\tau_{13}\tau_{12}((x_4 - x_2)p'') - \tau_{13}\tau_{12}((x_4 - x_2)p'')}{(x_3 - x_4)(x_3 - x_1)} \\ &= \frac{\tau_{12}(\tau_{14}p' - \tau_{12}p') + \tau_{14}\tau_{13}\tau_{12}(\tau_{14}p' - \tau_{12}p') - \tau_{13}\tau_{12}(\tau_{14}p' - \tau_{12}p')}{(x_3 - x_4)(x_3 - x_1)} \\ &= \frac{\tau_{14}p' - p' + \tau_{34}p' - \tau_{14}p' - \tau_{34}p' + p'}{(x_3 - x_4)(x_3 - x_1)} = 0\end{aligned}$$

Hence γ is symmetric. Now, the second equation of (2.2) makes it clear that β is symmetric in the variables x_1, x_2, x_4. Then β is symmetric since it is also invariant under τ_{13}:

$$\begin{aligned}\tau_{13}\beta - \beta &= \frac{1}{4}\delta_p(e_1 - 4x_1) + \tau_{13}p'' - \frac{1}{4}\delta_p(e_1 - 4x_3) - p'' \\ &= (x_3 - x_1)\delta_p - (p'' - \tau_{13}p'') = 0\end{aligned}$$

Finally, from the first equation of (2.2) we clearly see that α is invariant under τ_{24} and τ_{13}. Then α is symmetric since it is also invariant under τ_{14}:

$$\begin{aligned}\tau_{14}\alpha - \alpha &= \frac{\tau_{14}p' - p'}{2} - \frac{x_4 - x_1}{2}p'' \\ &= \frac{1}{2}\tau_{12}(\tau_{12}\tau_{14}p' - \tau_{12}p' - (x_4 - x_2)p'') \\ &= \frac{1}{2}(\tau_{14}p' - \tau_{12}p' - (\tau_{14}p' - \tau_{12}p')) = 0\end{aligned}$$

To conclude the proof, we prove that (2.1) holds. To do so, we prove that $\psi := p - (\alpha\rho_\eta + \beta\rho_\theta + \gamma\rho_{\lambda\eta}) \in \mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{S_2\times S_2}_{-,D_4}$ is zero, using the fact that $\psi' = 0$, which is guaranteed by the first equation of (2.2). Then $\tau_{14}\psi = \tau_{12}\psi$, and $\psi = \tau_{12}\tau_{12}\psi = \tau_{12}\tau_{14}\psi = \tau_{14}\tau_{24}\psi = \tau_{14}\psi$. Since ψ is already fixed by τ_{13} and τ_{24}, it is a symmetric polynomial, so that $\psi = \sigma\psi = -\psi$, implying $\psi = 0$. Hence $\{\rho_\eta, \rho_\theta, \rho_{\lambda\eta}\}$ is a free $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{S_4}$-basis for $\mathbb{Z}\left[\frac{1}{2}\right][\mathbf{x}]^{S_2\times S_2}_{-,D_4}$, and this was the only thing left to prove. $\square$

Now we look for polynomial relations satisfied by the generators. We already know that λ is a root of

$$\begin{aligned}r_1(\Lambda) &= (\Lambda - \lambda)(\Lambda - \tau_{14}\lambda)(\Lambda - \tau_{12}\lambda) \\ &= \Lambda^3 - e_2\Lambda^2 + (e_1e_3 - 4e_4)\Lambda - (e_3^2 - 4e_2e_4 + e_1^2e_4).\end{aligned}$$

As both η, θ change sign under τ_{13}, their squares and their product are stable under τ_{13}, so that they are all D_4-invariant. Hence $\eta^2, \theta^2, \eta\theta \in \langle 1, \lambda, \lambda^2\rangle_{R[\mathbf{x}]^{S_4}}$ and we can compute their coefficients using the formulas we wrote after Lemma 2.0.1. This gives three polynomials

$$r_2(\Lambda, H, \Theta) = H^2 - (a_{\eta^2} + b_{\eta^2}\Lambda + c_{\eta^2}\Lambda^2)$$

$$r_3(\Lambda, H, \Theta) = \Theta^2 - (a_{\theta^2} + b_{\theta^2}\Lambda + c_{\theta^2}\Lambda^2)$$
$$r_4(\Lambda, H, \Theta) = H\Theta - (a_{\eta\theta} + b_{\eta\theta}\Lambda + c_{\eta\theta}\Lambda^2)$$

that vanish under $\Lambda \mapsto \lambda$, $H \mapsto \eta$, $\Theta \mapsto \theta$. On the other hand, $\widetilde{\eta\lambda^2} = \tilde{\eta}\lambda^2 = -\eta\lambda^2$, and $\widetilde{\theta\lambda} = \tilde{\theta}\lambda = -\theta\lambda$, so that $\eta\lambda^2$ and $\theta\lambda$ can be written as linear combinations of η, θ and $\eta\lambda$ by computing, as in the proof of Proposition 2.2.2, the correspondent polynomials ρ, ρ', ρ'', δ_ρ, which allows us to obtain the symmetric coefficients α, β and γ. This gives two polynomials

$$r_5(\Lambda, H, \Theta) = H\Lambda^2 - (\alpha_{\eta\lambda^2}H + \beta_{\eta\lambda^2}\Theta + \gamma_{\eta\lambda^2}H\Lambda)$$
$$r_6(\Lambda, H, \Theta) = \Theta\Lambda - (\alpha_{\theta\lambda}H + \beta_{\theta\lambda}\Theta + \gamma_{\theta\lambda}H\Lambda)$$

that again vanish under $\Lambda \mapsto \lambda$, $H \mapsto \eta$, $\Theta \mapsto \theta$. These six polynomials are computed explicitly in terms of the e_k in Appendix B.2.

Lemma 2.2.5. *For R a ring with $2 \in R^\times$, we have an isomorphism of $R[\mathbf{x}]^{S_4}$-algebras*

$$R[\mathbf{x}]^{S_4}[\Lambda, H, \Theta]/I \xrightarrow{\sim} R[\mathbf{x}]^{C_4}$$

sending $\Lambda \mapsto \lambda$, $H \mapsto \eta$ and $\Theta \mapsto \theta$, where I is the ideal generated by the six polynomials $r_i(\Lambda, H, \Theta)$ in the list above.

Proof. As the six polynomials generating I are zero on λ, η and θ, the map in the statement is well-defined. To prove it is a bijection, it is enough to prove that the set $\{1, \Lambda, \Lambda^2, H, \Theta, \Lambda H\}$ generates the domain of the map as an $R[\mathbf{x}]^{S_4}$-module, because it is mapped to $\{1, \lambda, \lambda^2, \eta, \theta, \lambda\eta\}$, which is an $R[\mathbf{x}]^{S_4}$-basis for $R[\mathbf{x}]^{C_4}$ by Proposition 2.2.2.

The ring $R[\mathbf{x}]^{S_4}[\Lambda, H, \Theta]/I$ is $R[\mathbf{x}]^{S_4}$-generated by the set of monomials $\{\Lambda^{n_1}H^{n_2}\Theta^{n_3} : n_1, n_2, n_3 \in \mathbb{N}\}$. As we quotient by r_1, each of those monomial is an $R[\mathbf{x}]^{S_4}$-linear combination of monomials with unchanged exponents n_2 and n_3, and a strictly lower exponent for Λ, whenever $n_1 \geq 3$. Then the set $\{\Lambda^{n_1}H^{n_2}\Theta^{n_3} : n_1, n_2, n_3 \in \mathbb{N}, n_1 \leq 2\}$ still generates $R[\mathbf{x}]^{S_4}[\Lambda, H, \Theta]/I$ as an $R[\mathbf{x}]^{S_4}$-module, by an easy induction. Similarly, as we quotient by r_2, r_3 and r_4, we can reduce this set of generators to $\{\Lambda^{n_1}H^{n_2}\Theta^{n_3} : n_1, n_2, n_3 \in \mathbb{N}, n_1 \leq 2, n_2 + n_3 \leq 1\} = \{1, \Lambda, \Lambda^2, H, \Lambda H, \Lambda^2 H, \Theta, \Lambda\Theta, \Lambda^2\Theta\}$. Finally, quotienting by r_5 and r_6 we can express $\Lambda^2\Theta$ as an $R[\mathbf{x}]^{S_4}$-linear combination of ΛH, $\Lambda\Theta$ and $\Lambda^2 H$, and we can express both $\Lambda\Theta$ and $\Lambda^2 H$ as an $R[\mathbf{x}]^{S_4}$-linear combination of H, Θ and ΛH. Hence $\{1, \Lambda, \Lambda^2, H, \Theta, \Lambda H\}$ generates $R[\mathbf{x}]^{S_4}[\Lambda, H, \Theta]/I$ as an $R[\mathbf{x}]^{S_4}$-module. $\square$

If we fix a monogenic extension $R \to R[x]/(f(x))$, with $f(x) = x^4 - s_1x^3 + s_2x^2 - s_3x + s_4$, we can map via $\varphi_0 : e_k \mapsto s_k$ the symmetric coefficients of the polynomials $r_1, ..., r_6$, and obtain 6 polynomials in $R[\Lambda, H, \Theta]$. The set of triples $(\ell, h, t) \in R^3$ satisfying the six polynomials parametrizes the classes of C_4-closures for $R \to R[x]/(f(x))$:

Theorem 2.2.6. *Let R be a ring such that $2 \in R^\times$. Consider the monogenic degree-4 extension $R \to A = R[x]/(f(x))$, where $f(x) = x^4 - s_1x^3 + s_2x^2 - s_3x + s_4$. Let $g(x) = x^3 - s_2x^2 + (s_1s_3 - 4s_4)x - (s_3^2 - 4s_2s_4 + s_1^2s_4)$ be the resolvent cubic of f. Then isomorphism classes of C_4-closures for A over R are in one-to-one correspondence with triples $(\ell, h, t) \in R^3$ satisfying conditions (B.1) in Appendix B.2.*

Proof. $|C_4| = 4$ is not a zero-divisor since $2 \in R^\times$ is not, so that we can apply Theorem 1.3.3. Then isomorphism classes of C_4-closures for $R \to A$ are in one-to-one correspondence with R-algebra maps $R[\mathbf{x}]^{C_4} \to R$ mapping $e_k(t) \mapsto s_k$. By Lemma 2.2.5, which we can apply since $2 \in R^\times$, determining such a map is equivalent to choosing $(\ell, h, t) \in R^3$ images of λ, η, θ in R, and the conditions (B.1) in Appendix B.2 are precisely the ones needed to make (ℓ, h, t) satisfy the necessary relations. $\square$

Remark 2.2.7. Since $2 \in R^\times$, each monogenic degree-4 ring extension of rings is isomorphic to a monogenic degree-4 ring extension with coefficient $s_1 = 0$. Indeed, if $f(x) = x^4 - s_1x^3 + s_2x^2 - s_3x + s_4$, then for $r_0 \in R$ we have $\hat{f}(x) := f(x+r_0) = x^4 - (s_1 - 4r_0)x^3 + (s_2 - 3r_0s_1 + 6r_0^2)x^2 - (s_3 - 2r_0s_2 + 3r_0^2s_1 - 4r_0^3)x + f(r_0)$, and the isomorphism of R-algebra $R[x]/(f(x)) \to R[x]/(\hat{f}(x))$ sending $x \mapsto x - r_0$. In particular, the coefficient of x^3 is zero in $\hat{f}(x)$ for $r_0 = s_1/4$. Then the equations (B.1) in Appendix B.2 simplify to

$$\begin{cases} \ell^3 - s_2\ell^2 - 4s_4\ell - (s_3^2 - 4s_2s_4) = 0 \\ h^2 = 4\big(2s_2\ell^2 + (4s_4 - s_2^2)\ell - (s_2^3 + 3s_3^2 + 4s_2s_4)\big) \\ t^2 = 16s_4\ell^2 - 3s_3^2\ell - s_2s_3^2 - 64s_4^2 \\ ht = 2(3s_3\ell^2 - 2s_2s_3\ell - s_2^2s_3 - 16s_3s_4) \\ 2t(\ell - s_2) + s_3h = 0 \\ h\ell^2 + 2s_3t - 4s_4h = 0 \end{cases}$$

2.3 C_2-closures for monogenic degree-4 extensions

In this section, we will consider $C_2 := \langle \tau_{13}\tau_{24} \rangle \le S_4$ and parametrize C_2-closures for monogenic degree-4 ring extensions, assuming that $2 \in R$ is not a zero-divisor. We will prove that they are in one-to-one correspondence with the data of a factorization of f into two degree-2 polynomials together with a root of a certain degree-2 polynomial depending on the factorization. This can be done quite easily by considering the $R[\mathbf{x}]^{S_2\times S_2}$-algebra structure of $R[\mathbf{x}]^{C_2}$.

First, we note that $R[\mathbf{x}]^{C_2}$ is a free $R[\mathbf{x}]^{S_2\times S_2}$-module:

Lemma 2.3.1. *Let R be any ring, $\lambda = x_1x_3 + x_2x_4 \in R[\mathbf{x}]$ and $\mu = \tau_{14}\lambda = x_1x_2 + x_3x_4$. Then*

$$R[\mathbf{x}]^{C_2} = R[\mathbf{x}]^{S_2\times S_2} \oplus R[\mathbf{x}]^{S_2\times S_2}\mu.$$

The proof of this lemma follows verbatim the one we gave for Lemma 2.1.1. Consider the monic polynomial

$$H(\lambda, M) = M^2 - (e_2 - \lambda)M + \lambda^2 - e_2\lambda + e_1e_3 - 4e_4 \in R[\mathbf{x}]^{S_2\times S_2}[M],$$

where $H(\Lambda, M)$ is the polynomial from Lemma 2.1.3. Since μ is a root of $H(\lambda, M)$, we immediately get the following isomorphism:

Lemma 2.3.2. *For any ring R, consider the polynomial $H(\lambda, M)$ as above. Then we have an isomorphism of $R[\mathbf{x}]^{S_2\times S_2}$-algebras sending $M \mapsto \mu$:*

$$\frac{R[\mathbf{x}]^{S_2\times S_2}[M]}{(H(\lambda, M))} \xrightarrow{\sim} R[\mathbf{x}]^{C_2}$$

We denote in the following way these two-variable symmetric polynomials:

$$U_1 = x_1 + x_3, \quad U_2 = x_1x_3, \quad V_1 = x_2 + x_4, \quad V_2 = x_2x_4.$$

Then we can prove the following parametrization for C_2-closures:

Theorem 2.3.3. *Let R be a ring such that $2 \in R$ is not a zero-divisor. Consider the monogenic degree-4 extension $R \to A = R[x]/(f(x))$, where $f(x) = x^4 - s_1x^3 + s_2x^2 - s_3x + s_4$. Consider $g(x) = x^3 - s_2x^2 + (s_1s_3 - 4s_4)x - (s_3^2 - 4s_2s_4 + s_1^2s_4)$, the resolvent cubic of f. Then the following are in one-to-one correspondence:*

- *isomorphism classes of C_2-closures of $R \to A$;*
- *quintuples $(u_1, u_2, v_1, v_2, m) \in R^5$ such that $f(x) = (x^2 - u_1x + u_2)(x^2 - v_1x + v_2)$ and m is a root of $g(x)/(x - u_2 - v_2)$;*
- *septuples $(u_1, u_2, v_1, v_2, \ell_1, \ell_2, \ell_3) \in R^7$ such that $\ell_1 = u_2 + v_2$, $f(x) = (x^2 - u_1x + u_2)(x^2 - v_1x + v_2)$ and $g(x) = (x - \ell_1)(x - \ell_2)(x - \ell_3)$.*

Proof. As $2 \in R$ is not a zero-divisor, we can apply Theorem 1.3.3 for $G = C_2$. Then isomorphism classes of C_2-closures for the monogenic extension $R \to A$ are in one-to-one correspondence with maps of $R[\mathbf{x}]^{S_4}$-algebras $R[\mathbf{x}]^{C_2} \to R$. Then, by the isomorphism (of $R[\mathbf{x}]^{S_4}$-algebras) in Lemma 2.3.2, those are given by a map of $R[\mathbf{x}]^{S_4}$-algebras $\phi : R[\mathbf{x}]^{S_2 \times S_2} \to R$ together with a root of the polynomial $\phi(H(\lambda, M))$. Giving such a map ϕ is equivalent, by Theorems 1.2.1 and 1.3.3 combined together (the latter being applicable since $4 \in R$ is not a zero-divisor), to give a factorization into monic polynomial of the form $f(x) = (x^2 - u_1x + u_2)(x^2 - v_1x + v_2)$, precisely via $\phi(U_j) = u_j$ and $\phi(V_j) = v_j$. Notice that $\lambda = U_2 + V_2$ is mapped to a root of the resolvent cubic g, say $\ell = u_2 + v_2$, and that $(M - \ell)\phi(H(\lambda, M)) = \phi((M - \lambda)H(\lambda, M)) = g(M)$. This gives exactly the parametrization in terms of quintuples for which we were looking, since the image of M has to be a root of $g(x) = (x - u_2 - v_2)$. The parametrization in terms of septuples is equivalent to the previous one via Lemma 1.2.3. $\square$

2.4 C_3-closures for monogenic degree-4 extensions

In this section, we will consider $C_3 = \{1, (1\,2\,3), (1\,3\,2)\} \leq S_4$ and parametrize C_3-closures for monogenic degree-4 ring extensions, assuming that 6 is not a zero-divisor.

We define $\gamma = x_2x_3^2 + x_1^2x_3 + x_1x_2^2$, and denote by e'_j the j-th elementary symmetric polynomial in the variables x_1, x_2, x_3. Then, applying Example 5.4.4 in [1], one has: $\gamma + \tau_{12}\gamma = e'_1e'_2 - 3e'_3$ and $\gamma \cdot (\tau_{12}\gamma) = e'^3_2 - 6e'_1e'_2e'_3 + e'^3_1e'_3 + 9e'^2_3$. This gives the following description of the polynomial invariants:

$$\begin{aligned} R[\mathbf{x}]^{C_3} &= (R[x_1, x_2, x_3])^{C_3}[x_4] = (R[x_1, x_2, x_3])^{S_3}[\gamma][x_4] = R[\mathbf{x}]^{S_3}[\gamma] \\ &\cong \frac{R[\mathbf{x}]^{S_3}[y]}{(y^2 - (e'_1e'_2 - 3e'_3)y + (e'^3_2 - 6e'_1e'_2e'_3 + e'^3_1e'_3 + 9e'^2_3))} \end{aligned}$$

We assume that 6 is not a zero-divisor, i.e., 2 and 3 are not zero-divisors. Then by Theorem 1.3.3 we have that C_3-closure are in one-to-one correspondence with maps $R[\mathbf{x}]^{C_3} \to R$ sending $e_k \mapsto s_k$. By the description of $R[\mathbf{x}]^{C_3}$ that we gave, such maps are uniquely determined by a map $\varphi : R[\mathbf{x}]^{S_3} \to R$ sending $e_k \mapsto s_k$together with a root in R of the polynomial to which $x_3^2-(e_1'e_2'-3e_3')x_3+(e_2'^3-6e_1'e_2'e_3'+e_1'^3e_3'+9e_3'^2)$ is sent via ϕ. Using that 6 is not a zero-divisor and applying Theorem 1.3.3 together with Corollary 1.2.2, we have that maps $R[\mathbf{x}]^{S_3} \to R$ sending $e_k \mapsto s_k$ are uniquely determined by a root of f, i.e., by a decomposition $f(x) = (x-r)(x^3-s_1'x^2+s_2'x-s_3')$, where the map corresponding to such a decomposition is the one sending $e_j' \mapsto s_j'$. This proves the following:

Theorem 2.4.1. *Let R be a ring such that $6 \in R$ is not a zero-divisor. Consider the monogenic degree-4 extension $R \to A = R[x]/(f(x))$, where $f(x) = x^4 - s_1x^3 + s_2x^2 - s_3x + s_4$. Then the following are in one-to-one correspondence:*

- *isomorphism classes of C_3-closures of $R \to A$;*
- *quintuples $(r, s_1', s_2', s_3', c) \in R^5$ such that $f(x) = (x-r)(x^3-s_1'x^2+s_2'x-s_3')$ and $c^2 = (s_1's_2' - 3s_3')c - (s_2'^3 - 6s_1's_2's_3' + s_1'^3s_3' + 9s_3'^2)$.*

2.5 Examples and Classical Galois Theory

For separable degree-4 field extensions, a good reference about computing the Galois group is the Section **Quartic polynomials** from Chapter 4 in [4]. The parametrizations of D_4-closures and V_4-closures we pointed out in this chapter are a natural generalization of the ones from classical Galois theory which are expressed in terms of the resolvent cubic g of the polynomial f defining the extension (respectively, the Galois group G is contained in D_4 if and only if g has root in the base field, and G is contained in V_4 if and only if g splits in the base field).

We will now apply the criteria we gave on some specific monogenic degree-4 extensions. The last of those is the most important, as it makes it clear that it is not possible to have a unique minimal subgroup G of S_n (up to conjugation) for which a G-closure exists. Such a subgroup G would generalise the definition of Galois group in the case of a ring extension. This answers negatively the first of Questions 4.4.3 in [1]. The ring R we consider in that counterexample is a domain, but it is not integrally closed. It remains unknown if the answer to the question is positive supposing that R is an integrally closed domain, or at least supposing that R is a UFD.

Example 2.5.1. Consider the field extension $\mathbb{F}_3 \to \mathbb{F}_{81} = \mathbb{F}_3[x]/(x^4+x^2+x+1)$. By basic Galois theory (as a reference, see Section **Finite Fields** from Chapter 4 in [4]), this extension has cyclic Galois group C_4 (generated by the Frobenius automorphism $\alpha \mapsto \alpha^3$). Hence we have a C_4-closure for the extension. This is indeed consistent with Theorem 2.2.6, which we can apply since 2 is a unit: the resolvent cubic is $g(x) = x^3 - x^2 - 4x = x(x^2 - x - 1)$ and it has the unique root $\ell = 0$. Then the other equations from Remark 2.2.7 are:

$$\begin{cases} h^2 = 1 \\ t^2 = 1 \\ ht = 1 \\ t - h = 0 \\ t - h = 0 \end{cases}$$

giving $h = t = \pm 1$. Hence we have two distinct classes of C_4-closures for our ring extension.

Example 2.5.2. Consider the ring extension $R \to A = R[x]/(x^4 + x^2 + x + 1)$, with $R = \mathbb{Z}/9\mathbb{Z}$. It is easy to check that $x^4 + x^2 + x + 1$ is irreducible in $\mathbb{Z}/9\mathbb{Z}[x]$, so that by Theorem 1.2.1 there exists no G-closure for intransitive G. Since 2 is a unit, we can apply Theorems 2.0.2, 2.1.4 and 2.2.6: the resolvent cubic is $g(x) = x^3 - x^2 - 4x + 3 = (x - 3)(x^2 + 2x + 2)$ and it has the unique root $\ell = 3$. This means that there exists exactly one class of D_4-closures, and no V_4-closure. For C_4-closures, we have 5 other equations from Remark 2.2.7:

$$\begin{cases} h^2 = 4 \\ t^2 = 7 \\ ht = 1 \\ 4t - h = 0 \\ -2t - 4h = 0 \end{cases}$$

but there are no solutions, meaning that there is no C_4-closure for our extension. Moreover, there is no A_4-closure: if it existed, we would have a map $R[\mathbf{x}]^{A_4} \to R$ sending $e_k \mapsto s_k$, while finding such a map requires, as seen in Appendix B.1, there to be a root in R for the quadratic polynomial $x^2 - x + 4 = (x + 4)^2 - 3$, which does not exist as 3 is not a square in R.

Example 2.5.3. Here we want to study the extension $R \to R[x]/(x^4 - 4x^2 + 2)$ for $R = \mathbb{Z}$. If a G-closure for this extension in the case $R = \mathbb{Z}$ exists, then by Theorem 1.1.9 also a G-closure in the case $R = \mathbb{Q}$ has to exist. For $R = \mathbb{Q}$, $f(x) = x^4 + 4x^2 + 2$ is irreducible, so that we cannot have a G-closure for $G \leq S_4$ an intransitive subgroup. Moreover, $g(x) = x^3 - 4x^2 - 8x + 32 = (x - 4)(x^2 - 8)$, so that there exists a unique isomorphism class of D_4-closures (even for $R = \mathbb{Z}$). If $R = \mathbb{Q}$ we have the 5 other equations for C_4-closures from Remark 2.2.7:

$$\begin{cases} h^2 = 0 \\ t^2 = 16^2 \\ ht = 0 \\ 0 = 0 \\ 16h - 8h = 0 \end{cases}$$

which give two classes of C_4-closures for our extension when $R = \mathbb{Q}$. In this case the Galois group of the field extension is C_4, and we have a G-closure if and only if $G \in \{C_4, D_4, S_4\}$. If $R = \mathbb{Z}$, the criterium for C_4-closures cannot be applied, and it is not immediate to decide if a C_4-closure does exist or not.

Example 2.5.4 (Counterexample to existence of Galois group for ring extensions)**.** Consider the monogenic degree-4 extension $R \to A = R[x]/(x^4 + s)$, supposing that $s \in R \setminus \{0\}$, with R a domain where 2 is a unit and 3 is not a zero-divisor. The resolvent cubic is then equal to $g(x) = x^3 - 4sx = x(x^2 - 4s)$. Then by Theorem 2.0.2 there necessarily exists a D_4-closure, as $g(0) = 0$. By the parametrization in Appendix B.1, isomorphism classes of A_4-closures are in one-to-one correspondence with roots of $x^2 - 64s^3$. This implies that an A_4-closure exists if and only if $64s^3$ is a square in R, which is equivalent to s^3 being a square in R. The resolvent cubic $g(x)$ splits into monic linear factors over R if and only if there exists roots $\ell_1, \ell_2, \ell_3 \in R$ of g realizing the split. In particular, this requires the product $\ell_1\ell_2\ell_3$ to be equal to zero, so that, R being a domain, one of the ℓ_i should be 0, and by Lemma 1.2.3 we need the other two to be roots of $g(x)/x = x^2 - 4s$. Hence, by Theorem 2.1.4, a V_4-closure exists if and only if $4s$ is a square in R, which is equivalent to s being a square in R.

Now take $R = \mathbb{Q}[y^2, y^3]$ and $s = y^2$. Then R is a domain (being a subring of the polynomial ring $\mathbb{Q}[y]$) and $s^3 = y^6 = (y^3)^2$ is a square, while s is not (since its only two square roots in the fraction field $\mathbb{Q}(y)$ are $\pm y \notin R$). Hence there exist a D_4-closure and an A_4-closure, but no V_4-closure for this ring extension. Notice that the third of the conditions on a triple $(\ell, h, t) \in R^3$ parametrizing C_4-closures from Remark 2.2.7 is $t^2 = -64y^4$, which is not realizable with $t \in R$ (not even with $t \in \mathbb{Q}(y)$). Hence there is no C_4-closure for this ring extension. It can also be easily checked that $f(x)$ is irreducible over R, so that no $(S_2 \times S_2)$-closures, no S_3-closures and no C_3-closures exist. In conclusion, D_4 and A_4 are two minimal subgroups in $\{G \leq S_4 : \text{a } G\text{-closure of } R \to A \text{ exists}\}$, but they are not conjugates. This means that first of Questions 4.4.3 in [1] has a negative answer.

Appendices

Appendix A

Invariant algebras and tensor powers

In this appendix, for $R \to A$ a degree-n ring extension, we will prove the isomorphism of tensor powers

$$(A^{\otimes n})^{\prod_j S_{d_j}} \cong \bigotimes_{j \in [m]} (A^{\otimes d_j})^{S_{d_j}}$$

that we use to give a proof of Theorem 1.2.1, parametrizing $\prod_j S_{d_j}$-closures for a monogenic extension $R \to R[x]/(f(x))$ in terms of splittings of f into monic factors f_j of degrees d_j.

A.1 Localization and invariants

We are now going to prove that in any R-algebra localization commutes with taking invariants under an action of a finite group G. Actually, this is not only true for localization, but for any flat base change, as said in Proposition A7.1.3 from [2]. We here rephrase part of statement and proof of this proposition:

Lemma A.1.1. *Let A and R' be R-algebras, and G be a finite group with an action on the R-algebra A. Then the action of G induces an action on the R'-algebra $R' \otimes_R A$ via $\sigma \cdot (r' \otimes a) = r' \otimes (\sigma \cdot a)$. If R' is a flat R-algebra, then the following is an isomorphism of R'-algebras:*

$$\begin{aligned} \psi : R' \otimes_R A^G &\xrightarrow{\sim} (R' \otimes_R A)^G \\ r' \otimes a &\longmapsto r' \otimes a \end{aligned}$$

Proof. For all $\sigma \in G$, the expression $\sigma \cdot (r' \otimes a) = r' \otimes (\sigma \cdot a)$ defines the R-algebra endomorphism $\mathrm{id}_{R'} \otimes \sigma$ of $R' \otimes_R A$. Since it is easily checked to be also an R'-linear map, this is actually an endomorphism of $R' \otimes_R A$ as an R'-algebra. It is clear by the definition that compositions work fine, so that this is an action of G on the R'-algebra $R' \otimes_R A$.

Sending $r' \otimes a \mapsto r' \otimes a$ we define an R'-algebra map $R' \otimes_R A^G \to (R' \otimes_R A)^G$ (the image of each simple tensor is clearly G-invariant). To prove that when R'

is flat the map is an isomorphism, we can just regard it as a map of R'-modules. Writing down $G = \{\sigma_1, \dots, \sigma_{|G|}\}$, we notice that A^G is the kernel of the R-linear map $A \to A^{|G|}$ sending $a \mapsto (a - \sigma_j \cdot a)_j$, and that $(R' \otimes_R A)^G$ is the kernel of the R-linear map $R' \otimes_R A \to (R' \otimes_R A)^{|G|} \cong R' \otimes_R A^{|G|}$ with analogue definition. Being R' flat, the kernel are preserved after tensoring with $\mathrm{id}_{R'}$, so that $R' \otimes_R A^G$ and $(R' \otimes_R A)^G$ coincide in $R' \otimes_R A$, i.e., φ is an isomorphism of R'-modules. $\square$

In particular, we can consider a multiplicative subset $S \subseteq R$, and take $R' = S^{-1}R$. Since localization is flat, we immediately get the following result:

Corollary A.1.2. *Let G be a finite group acting on an R-algebra A, and $S \subseteq R$ a multiplicative subset. Then the action of G induces an action on the $S^{-1}R$-algebra $S^{-1}A$ via $\sigma \cdot \frac{a}{s} = \frac{\sigma a}{s}$, and the following is an isomorphism of $S^{-1}R$-algebras:*

$$\begin{aligned} \psi : S^{-1}A^G &\longrightarrow (S^{-1}A)^G \\ \frac{a}{s} &\longmapsto \frac{a}{s} \end{aligned}$$

A.2 Invariant tensor powers

We are now going to prove some lemmas which will allow us to prove the isomorphism

$$(A^{\otimes n})^{\prod_j S_{d_j}} \cong \bigotimes_{j \in [m]} (A^{\otimes d_j})^{S_{d_j}}.$$

For a fixed ring R, we associate every finite set C to the power R-algebra R^C, and for any map of sets $\alpha : C \to D$ we call *the R-algebra map $R^D \to R^C$ induced by α* the one that sends $e_d \mapsto \sum_{\alpha(c)=d} e_c$, for any $d \in D$. Here we denote by e_c the c-th standard basis element of R^C, for every $c \in C$ (we will keep this notation in the rest of the appendix, even if it has nothing to do with the one used in the main thesis). It is easily seen that the R-algebra map induced by a composition of set maps is the composition of the R-algebra maps induced by the set maps (i.e., we have defined a contravariant functor from finite sets to R-algebras) so that bijections induce isomorphisms of R-algebras.

Lemma A.2.1. *Let R be a ring and $m, k \in \mathbb{N}$, $I = [m]$ and $J = [k]$. Consider:*

$$\begin{aligned} S_m \times R^{Map(I,J)} &\longrightarrow R^{Map(I,J)} \\ (\sigma, e_\pi) &\longmapsto e_{\pi\sigma^{-1}} \end{aligned}$$

This defines a left group action of S_m on the R-algebra $R^{Map(I,J)}$, i.e., we have the group homomorphism $S_m \to Aut_{R-\mathbf{Alg}}(R^{Map(I,J)})$ which sends $\sigma \mapsto (p \mapsto \sigma p)$. Moreover, endowing $(R^J)^{\otimes I}$ with the S_m-action defined by $\sigma \cdot a^{(i)} = a^{(\sigma(i))}$ for all $a \in R^J$, the following defines an S_m-isomorphism of R-algebra:

$$\begin{aligned} Q : R^{Map(I,J)} &\longrightarrow (R^J)^{\otimes I} \\ e_\pi &\longmapsto e_{\pi(1)} \otimes \cdots \otimes e_{\pi(m)} = \prod_{i \in I} e^{(i)}_{\pi(i)} \end{aligned}$$

Proof. First, we have that Q is an isomorphism of R-algebras. It is well-defined because it sends the e_π to a complete set of orthogonal idempotents (it can immediately checked that $\sum_\pi Q(e_\pi) = 1$ and $Q(e_\pi)Q(e_\gamma) = \delta_{\pi,\gamma}Q(e_\pi)$, where $\delta_{\pi,\gamma}$ is Kronecker's delta). Since the $Q(e_\pi)$ form an R-module basis for $(R^J)^{\otimes I}$, the map is actually an isomorphism. It can be easily seen that the inverse map is $Q^{-1}(e_j^{(i)}) = \sum_{\pi:\pi(i)=j} e_\pi$.

To conclude the proof it is sufficient to notice that the G-action induced on $R^{\mathrm{Map}(I,J)}$ via Q is exactly the one considered in the lemma:

$$\sigma \cdot Q(e_\pi) = \sigma \cdot \left(\prod_{i \in I} e^{(i)}_{\pi(i)} \right) = \prod_{i \in I} e^{(\sigma(i))}_{\pi(i)} = \prod_{i \in I} e^{(i)}_{\pi(\sigma^{-1}(i))} = Q(e_{\pi\sigma^{-1}})$$

so that the action is well defined and makes Q a G-map. □

Lemma A.2.2. *Let R be a ring, $n \in \mathbb{N}$ and G a group acting on $[n]$. Consider*

$$\begin{aligned} G \times R^n &\longrightarrow R^n \\ (\sigma, e_j) &\longmapsto e_{\sigma(j)}. \end{aligned}$$

This defines a left group action of G on the R-algebra R^n. Moreover, the R-algebra map $R^{[n]/G} \to R^n$ induced by the canonical projection $[n] \to [n]/G$ factors through an isomorphism $R^{[n]/G} \xrightarrow{\sim} (R^n)^G$.

Proof. As G permutes the elements of the R-basis respecting compositions on the left, the above defines an action of G on the R-module R^n. Also multiplication is preserved, making it an action of R-algebras.

For $\mathfrak{o} \in [n]/G$, the map $R^{[n]/G} \to R^n$ sends $e_\mathfrak{o} \mapsto \sum_{j \in \mathfrak{o}} e_j$, which is G-invariant since G acts on $\mathfrak{o}$, hence the map factors through $R^{[n]/G} \to (R^n)^G$. To prove that this is an isomorphism, it is enough to show that the elements $\sum_{j \in \mathfrak{o}} e_j$, with $\mathfrak{o} \in [n]/G$, form an R-basis for $(R^n)^G$.

For every $r \in (R^n)^G$ we have $r = \sum_{j \in [n]} r_j e_j$, and

$$\sum_{j \in [n]} r_j e_j = \sigma \Bigg(\sum_{j \in [n]} r_j e_j \Bigg) = \sum_{j \in [n]} r_j e_{\sigma(j)} = \sum_{j \in [n]} r_{\sigma^{-1}(j)} e_j$$

so that $r_j = r_{\sigma_{-1} j}$ for all $\sigma \in G$, and denoting $\mathfrak{o}_j = G \cdot j \in [n]/G$ we can define $r_{\mathfrak{o}_j} = r_j$, obtaining $\sum_{j \in [n]} r_j e_j = \sum_{\mathfrak{o} \in [n]/G} r_\mathfrak{o} \Big(\sum_{j \in \mathfrak{o}} e_j \Big)$. Hence the elements $\sum_{j \in \mathfrak{o}} e_j$ are R-generators for $(R^n)^G$.

As concerns linear independence, notice that if we have some elements $r_\mathfrak{o} \in R$ such that $\sum_{\mathfrak{o} \in [n]/G} r_\mathfrak{o} \sum_{j \in \mathfrak{o}} e_j = 0$, then we get $\sum_{\mathfrak{o} \in [n]/G} \sum_{j \in \mathfrak{o}} r_\mathfrak{o} e_j = 0$, implying that all the $r_\mathfrak{o}$ are zero since the e_i, $i \in [n]$, are linearly independent in R^n. □

From this lemma follows immediately the following result:

Corollary A.2.3. *Let R be a ring and $m, k \in \mathbb{N}$, $I = [m]$ and $J = [k]$. Let S_m act on the R-algebra $R^{Map(I,J)}$ as in Lemma A.2.1, and on the set $Map(I,J)$ via $\sigma \cdot \pi = \pi \circ \sigma^{-1}$. Let $G \leq S_m$. Then the R-algebra map $R^{Map(I,J)/G} \to R^n$ induced by the canonical projection $Map(I,J) \to Map(I,J)/G$ factors through an isomorphism $R^{Map(I,J)/G} \xrightarrow{\sim} (R^{Map(I,J)})^G$.*

Now we can prove the following isomorphism of invariant subalgebras of tensor powers:

Lemma A.2.4. *Let M be a locally free R-module of rank n, and $h, k \in \mathbb{N}$. Let $H \leq S_h$, $K \leq S_k$, and view $H \times K \leq S_h \times S_k \leq S_{h+k}$. Then the isomorphism of R-algebras $M^{\otimes h} \otimes M^{\otimes k} \cong M^{\otimes h+k}$ restricts to an isomorphism $(M^{\otimes h})^H \otimes (M^{\otimes k})^K \cong (M^{\otimes h+k})^{H\times K}$. More precisely, there exists an isomorphism γ making the following diagram commute:*

$$\begin{tikzcd}
(M^{\otimes h})^H \otimes (M^{\otimes k})^K \arrow[r, "\gamma"] \arrow[d] & (M^{\otimes h+k})^{H\times K} \arrow[d] \\
M^{\otimes h} \otimes M^{\otimes k} \arrow[r, "\sim"] & M^{\otimes h+k}
\end{tikzcd}$$

where the vertical arrows are the canonical inclusions.

Proof. First, notice that existence of γ is equivalent to the image of the composite map $(M^{\otimes h})^H \otimes (M^{\otimes k})^K \to M^{\otimes h} \otimes M^{\otimes k} \to M^{\otimes h+k}$ being $H \times K$-invariant, which is immediately checked on the R-module generators of the domain $\xi \otimes \zeta$, with $\xi \in (M^{\otimes h})^H$ and $\zeta \in (M^{\otimes k})^K$.

The fact that γ is an isomorphism of R-modules can be proved locally on the free localizations $M_r \cong R_r^n$. As localization commutes with both tensor products and taking invariants under group actions (Corollary A.1.2), it is enough to prove that γ is an isomorphism when $M = R^n$.

We will actually show that γ is an isomorphism of R-algebras, endowing R^n with the product ring structure. Using the canonical isomorphism of R-algebras from Lemma A.2.1, and denoting $\mathrm{Map}(a,b) := \mathrm{Map}([a],[b])$ for $a, b \in \mathbb{N}$, we have the following commutative diagram:

$$\begin{tikzcd}
(R^n)^{\otimes h} \otimes (R^n)^{\otimes k} \arrow[r] & (R^n)^{\otimes h+k} \\
R^{\mathrm{Map}(h,n)\times \mathrm{Map}(k,n)} \arrow[r] \arrow[u, "\wr"'] & R^{\mathrm{Map}(h+k,n)} \arrow[u, "\wr"']
\end{tikzcd}$$

It is easy to see that the lower arrow has to send $e_{(f_1,f_2)} \mapsto e_{f_1 \sqcup f_2}$, where $f_1 \sqcup f_2 : [h+k] \to [n]$ maps $i \mapsto f_1(i)$ and $j + h \mapsto f_2(j)$, for $i \in [h]$ and $j \in [k]$. Hence this arrow is exactly the R-algebra map induced by the bijection $\beta : \mathrm{Map}(h+k,n) \to \mathrm{Map}(h,n) \times \mathrm{Map}(k,n)$ sending a map f to its compositions with the inclusions of $[h]$ in the first h integers and $[k]$ in the last k integers in $[h+k]$. We call $\bar{\beta}$ the induced bijection $\mathrm{Map}(h+k,n)/(H\times K) \to \mathrm{Map}(h,n)/H \times \mathrm{Map}(k,n)/K$, where H and K act on the maps by pre-composition.

Then, we taking invariants and consider the map θ obtained by making the following diagram commute, where the vertical arrows are obtained using the isomorphism from Corollary A.2.3:

$$\begin{tikzcd}
((R^n)^{\otimes h})^H \otimes ((R^n)^{\otimes k})^K \arrow[r, "\gamma"] & ((R^n)^{\otimes h+k})^{H\times K} \\
R^{\mathrm{Map}(h,n)/H\times \mathrm{Map}(k,n)/K} \arrow[r, "\theta"] \arrow[u, "\wr"'] & R^{\mathrm{Map}(h+k,n)/(H\times K)} \arrow[u, "\wr"']
\end{tikzcd}$$

We claim that θ is induced by the bijection $\bar{\beta}$, which is enough to prove that θ is an isomorphism, and so is γ.

To prove this claim, it is sufficient to consider the following diagram, which is obtained from the one in the statement, again through the isomorphism in Lemma A.2.1:

$$\begin{tikzcd} R^{\mathrm{Map}(h,n)/H\times \mathrm{Map}(k,n)/K} \arrow[r, "\theta"] \arrow[d] & R^{\mathrm{Map}(h+k,n)/(H\times K)} \arrow[d] \\ R^{\mathrm{Map}(h,n)\times \mathrm{Map}(k,n)} \arrow[r] & R^{\mathrm{Map}(h+k,n)} \end{tikzcd}$$

Generators of the upper-left R-module are of the form $e_{f_1\circ H, f_2\circ K}$, and we can denote $f = f_1 \sqcup f_2$. They are mapped via the vertical arrow to the elements $\sum_{\substack{\eta\in H\\ \mu\in K}} e_{f_1\circ\eta, f_2\circ\mu}$, which must be mapped to $\sum_{\nu\in H\times K} e_{f\circ\nu}$. Since these elements come from $e_{f\circ(H\times K)}$ via the vertical map on the right, which is injective, we have that θ has to send $e_{f_1\circ H, f_2\circ K} \mapsto e_{f\circ(H\times K)}$, and the claim is proved. □

The previous lemma generalizes to the case with more than two summands by an easy induction, giving the following:

Corollary A.2.5. *Let M be a locally free R-module of rank n, take $h_1, ..., h_s \in \mathbb{N}$ and call $\ell = \sum_j h_j$. Let $H_j \le S_{h_j}$ and view $\prod_j H_{d_j} \le \prod_j S_{h_j} \le S_\ell$. Then the isomorphism $\bigotimes_j M^{\otimes h_j} \cong M^{\otimes \ell}$ restricts to an isomorphism $\bigotimes_j (M^{\otimes h_j})^{H_j} \cong (M^{\otimes \ell})^{\prod_j H_j}$. More precisely, there exists an isomorphism γ making the following diagram commute:*

$$\begin{tikzcd} \bigotimes_j (M^{\otimes h_j})^{H_j} \arrow[r, "\gamma"] \arrow[d] & (M^{\otimes m})^{\prod_j H_j} \arrow[d] \\ \bigotimes_j M^{\otimes h_j} \arrow[r, "\sim"] & M^{\otimes m} \end{tikzcd}$$

where the vertical arrows are the canonical inclusions. □

Remark A.2.6. If $R \to A$ is a degree-n extension of R, then the isomorphism $\gamma : \bigotimes_j (M^{\otimes h_j})^{H_j} \to (M^{\otimes m})^{\prod_j H_j}$ from the previous corollary is also an isomorphism of R-algebras. Indeed, all the other arrows in the diagram are R-algebra maps, so that composing the right vertical arrow (which is an injective map) after γ we get an R-algebra map, and γ itself must therefore respect multiplication.

Appendix B

Explicit computations

In this appendix, we collect the computations carried out to present the A_4-invariant and the C_4-invariant polynomials as algebras over the symmetric polynomials. This allows us to give explicit parametrizations for A_4-closures and C_4-closures for a monogenic degree-4 ring extension of rings $R \to R[x]/(f(x))$.

To express any symmetric polynomial with elementary symmetric polynomials, one can use symmetric functions of Sage. For an introduction about symmetric functions, a good reference is Chapter 1 in [3]. We wrote down the following code in Sage:

```
sage: Z.<x1,x2,x3,x4> = PolynomialRing(QQ)
sage: Sym=SymmetricFunctions(QQ)
sage: e = Sym.elementary()
```

This makes it possible to work with four variables over $\mathbb{Q}$. Given a symmetric function, applying the command defined in the last line on it we will obtain the symmetric function expressed via elementary symmetric functions e_k, $k \in \mathbb{N}$. To obtain the symmetric function correspondent to a symmetric polynomial `p`, one can use the command:

```
sage: Sym.from_polynomial(p)
```

B.1 Conditions for A_4-closures

For $G = A_4$, we are in a very particular result in [1] describing A_n-closures for monogenic degree-n extensions of rings, as said in the introduction. We have the isomorphism of $R[\mathbf{x}]^{S_4}$-algebras

$$R[\mathbf{x}]^{A_n} \cong R[\mathbf{x}]^{S_n}[x]/(x - \Gamma)(x - \tau_{12}\Gamma)$$

where $\Gamma = \sum_{\pi \in A_4} \pi(x_2 x_3^2 x_4^3)$. An implementation of Sage allows us to compute $\Gamma + \tau_{12}\Gamma$ and $\Gamma \cdot \tau_{12}\Gamma$ in terms of symmetric polynomials:

```
sage: Gamma=x1^3*x2^2*x3+x1*x2^3*x3^2+x1^2*x2*x3^3+x1^2*x2^3*x4
        +x1^3*x3^2*x4+x2^2*x3^3*x4+x1^3*x2*x4^2+x2^3*x3*x4^2
        +x1*x3^3*x4^2+x1*x2^2*x4^3+x1^2*x3*x4^3+x2*x3^2*x4^3
sage: Sum=Gamma+Gamma(x2,x1,x3,x4)
sage: Prod=Gamma*Gamma(x2,x1,x3,x4)
```

```
sage: e(Sym.from_polynomial(Sum))
e[3, 2, 1] - 3*e[3, 3] - 3*e[4, 1, 1] + 4*e[4, 2] + 7*e[5, 1]
- 12*e[6]
sage: e(Sym.from_polynomial(Prod))
```

```
e[3, 3, 2, 2, 2] + e[3, 3, 3, 1, 1, 1] - 6*e[3, 3, 3, 2, 1]
+ 9*e[3, 3, 3, 3] + e[4, 2, 2, 2, 1, 1] - 4*e[4, 2, 2, 2, 2]
- 6*e[4, 3, 2, 1, 1, 1] + 22*e[4, 3, 2, 2, 1]
+ 6*e[4, 3, 3, 1, 1] - 42*e[4, 3, 3, 2]
+ 9*e[4, 4, 1, 1, 1, 1] - 42*e[4, 4, 2, 1, 1]
+ 36*e[4, 4, 2, 2] + 48*e[4, 4, 3, 1] - 64*e[4, 4, 4]
+ 2*e[5, 2, 2, 1, 1, 1] - 8*e[5, 2, 2, 2, 1]
- 7*e[5, 3, 1, 1, 1, 1] + 32*e[5, 3, 2, 1, 1]
+ 10*e[5, 3, 2, 2] - 58*e[5, 3, 3, 1] + 4*e[5, 4, 1, 1, 1]
- 44*e[5, 4, 2, 1] + 130*e[5, 4, 3] + 29*e[5, 5, 1, 1]
- 47*e[5, 5, 2] + 4*e[6, 2, 1, 1, 1, 1] - 9*e[6, 2, 2, 1, 1] -
12*e[6, 2, 2, 2] - 18*e[6, 3, 1, 1, 1] + 76*e[6, 3, 2, 1]
- 54*e[6, 3, 3] - 3*e[6, 4, 1, 1] + 16*e[6, 4, 2]
- 40*e[6, 5, 1] + 36*e[6, 6] - 9*e[7, 1, 1, 1, 1, 1]
+ 32*e[7, 2, 1, 1, 1] - 20*e[7, 2, 2, 1] - 18*e[7, 3, 1, 1]
- 8*e[7, 3, 2] + 30*e[7, 4, 1] - 8*e[7, 5]
+ 30*e[8, 1, 1, 1, 1] - 85*e[8, 2, 1, 1] + 48*e[8, 2, 2]
+ 32*e[8, 3, 1] - 32*e[8, 4] - 66*e[9, 1, 1, 1]
+ 98*e[9, 2, 1] - 18*e[9, 3] + 147*e[10, 1, 1] - 128*e[10, 2]
- 222*e[11, 1] + 288*e[12]
```

Notice that the meaning of $e[k_1,\ k_2,\ \ldots,\ k_s]$ in the output is just the elementary symmetric function $\prod_{i=1}^{s} e_{k_i}$. Rewriting this in our notation (and cancelling out e_k for $k > 4$), we have

$$\begin{aligned}\Gamma + \tau_{12}\Gamma &= e_3(e_1e_2 - 3e_3) + e_4(4e_2 - 3e_1^2), \text{ and}\\ \Gamma \cdot \tau_{12}\Gamma &= e_2^3e_3^2 + e_1^3e_3^3 - 6e_1e_2e_3^3 + 9e_3^4 + e_1^2e_2^3e_4 - 4e_2^4e_4 - 6e_1^3e_2e_3e_4 +\\ &\quad + 22e_1e_2^2e_3e_4 + 6e_1^2e_3^2e_4 - 42e_2e_3^2e_4 + 9e_1^4e_2^2 - 42e_1^2e_2e_4^2 +\\ &\quad + 36e_2^2e_4^2 + 48e_1e_3e_4^2 - 64e_4^3.\end{aligned}$$

so that A_4-closures for a monogenic degree-4 extension $R \to R[x]/(x^4 - s_1x^3 + s_2x^2 - s_3x + s_4)$ are in one-to-one correspondence with roots in R of the quadratic polynomial $x^2 - ax + b$, where

$$\begin{aligned}a &= s_3(s_1s_2 - 3s_3) + s_4(4s_2 - 3s_1^2), \text{ and}\\ b &= s_3^2(s_2^3 + s_1^3s_3 - 6s_1s_2s_3 + 9s_3^2 + 6s_1^2s_4 - 42s_2s_4) + 2s_1s_3s_4(11s_2^2 + 24s_4) +\\ &\quad + s_1^2(s_2^3s_4 - 6s_1s_2s_3s_4 + 9s_1^2s_2^2 - 42s_2s_4^2) + 4s_4(9s_2^2s_4 - s_2^4 - 16s_4^2).\end{aligned}$$

The hypothesis that 6 is not a zero-divisor can be dropped by Theorem 6.2.1 from [1].

B.2 Conditions for C_4-closures

We will here lay out explicitly the six polynomials $r_1, \ldots, r_6$ considered in Lemma 2.2.5 and deduce the equations whose solutions parametrize C_4-closures.

As already noticed, η^2, θ^2 and $\eta\theta$ are D_4-invariant polynomials. The following code uses the formulas from [1] that we have written after Lemma 2.0.1: given a polynomial D_4-invariant polynomial ψ, it computes symmetric coefficients a, b and c such that $\psi = a + b\lambda + c\lambda^2$, and express their correspondent symmetric function as a polynomial in the elementary symmetric functions:

```
sage: Lambda=x1*x3+x2*x4
sage: eta=(x1-x3)*(x2-x4)*(x1-x2+x3-x4)
sage: theta=(x1-x3)*(x2-x4)*(x1*x3-x2*x4)
sage: xi=Lambda*eta
sage: count=0
...   listpoly=['eta^2','theta^2','theta*eta']
...   for psi in [eta^2,theta^2,theta*eta]:
...       omega=(psi(x4,x2,x3,x1)-psi(x2,x1,x3,x4))/
                                    ((x1-x3)*(x2-x4))
...       chi=(omega(x4,x2,x3,x1)-omega(x2,x1,x3,x4))/
                                    ((x1-x3)*(x2-x4))
...       c=-chi
...       b=omega+chi*(x1+x3)*(x2+x4)
...       a=psi-b*Lambda-c*Lambda^2
...       print(listpoly[count])
...       count=count+1
...       print('a',a.denominator(),e(Sym.from_polynomial
                                    (a.numerator())))
...       print('b',b.denominator(),e(Sym.from_polynomial
                                    (b.numerator())))
...       print('c',c.denominator(),e(Sym.from_polynomial
                                    (c.numerator())))
```

```
eta^2
('a', 1, e[2, 2, 1, 1] - 4*e[2, 2, 2] - 4*e[3, 1, 1, 1]
+ 16*e[3, 2, 1] - 12*e[3, 3] + 4*e[4, 1, 1] - 16*e[4, 2]
+ 6*e[5, 1] + 24*e[6])
('b', 1, 2*e[2, 1, 1] - 4*e[2, 2] - 4*e[3, 1] + 16*e[4])
('c', 1, -3*e[1, 1] + 8*e[2])
theta^2
('a', 1, -e[3, 3, 2] - e[4, 2, 1, 1] + 16*e[4, 3, 1]
- 64*e[4, 4] + 4*e[5, 1, 1, 1] - 30*e[5, 2, 1] + 88*e[5, 3]
+ 11*e[6, 1, 1] - 8*e[6, 2] - 32*e[7, 1] + 32*e[8])
('b', 1, e[3, 2, 1] - 3*e[3, 3] - 3*e[4, 1, 1] + 23*e[5, 1]
- 48*e[6])
('c', 1, -e[3, 1] + 16*e[4])
theta*eta
('a', 1, -2*e[3, 2, 2] + 5*e[3, 3, 1] - 3*e[4, 1, 1, 1]
+ 12*e[4, 2, 1] - 32*e[4, 3] - 15*e[5, 1, 1] + 38*e[5, 2]
+ 10*e[6, 1] - 28*e[7])
('b', 1, e[2, 2, 1] - e[3, 1, 1] - 4*e[3, 2] + 4*e[4, 1]
+ 10*e[5])
('c', 1, -e[2, 1] + 6*e[3])
```

As can be seen in the code, the `1` in the output (in the second positions of each vector starting with `'a'`, `'b'` and `'c'`) are just a check that a, b and c are polynomials, since they are obtained by dividing polynomials. We write down the output in this table:

Ω	η^2	θ^2	$\eta\theta$
a_Ω	$e_1^2e_2^2 - 4e_2^3 - 4e_1^3e_3 +$ $+16e_1e_2e_3 - 12e_3^2 +$ $+4e_1^2e_4 - 16e_2e_4$	$-e_2e_3^2 - e_1^2e_2e_4 +$ $+16e_1e_3e_4 - 64e_4^2$	$-2e_2^2e_3 + 5e_1e_3^2 - 3e_1^3e_4 +$ $+12e_1e_2e_4 - 32e_3e_4$
b_Ω	$2e_1^2e_2 - 4e_2^2 +$ $-4e_1e_3 + 16e_4$	$e_1e_2e_3 - 3e_3^2 +$ $-3e_1^2e_4$	$e_1e_2^2 - e_1^2e_3 +$ $-4e_2e_3 + 4e_1e_4$
c_Ω	$-3e_1^2 + 8e_2$	$16e_4 - e_1e_3$	$-e_1e_2 + 6e_3$

Given a C_4-invariant polynomial ψ changing sign under τ_{13}, the following Sage code computes symmetric coefficients α, β and γ such that $\psi = \alpha\eta + \beta\theta + \gamma\lambda\eta$, and express their correspondent symmetric function as a polynomial in the elementary symmetric functions. This is done by using equations (2.2) from the proof of Proposition 2.2.2.

```
sage: count=0
...   listpoly=['theta*Lambda','eta*Lambda^2']
...   for psi in [theta*Lambda,eta*Lambda^2]:
...       rho= psi/((x2-x4)*(x1-x3))
...       rhoi=(rhopsi(x4,x2,x3,x1)-rhopsi(x2,x1,x3,x4))/(x4-x2)
...       rhoii=(rhoi(x4,x2,x3,x1)-rhoi(x2,x1,x3,x4))/(x4-x2)
...       delta=(rhoii-rhoii(x3,x2,x1,x4))/(x3-x1)
...       gamma=delta/(-4)
...       beta=(rhoii-gamma*(x1+x2-3*x3+x4))/1
...       alpha=(rhoi-beta*(x1+x3)-gamma*((x1-x3)^2
                                   +(x1+x3)*(x2+x4)))/2
...       print(listpoly[count])
...       count=count+1
...       print('alpha',alpha.denominator(),e(Sym.
                    from_polynomial(alpha.numerator())))
...       print('beta',beta.denominator(),e(Sym.
                     from_polynomial(beta.numerator())))
...       print('gamma',gamma.denominator(),e(Sym.
                    from_polynomial(gamma.numerator())))
```

```
theta*Lambda
('alpha', 1, -1/2*e[3])
('beta', 1, -1/4*e[1, 1] + e[2])
('gamma', 1, 1/4*e[1])
eta*Lambda^2
('alpha', 1, -1/2*e[3, 1] + 4*e[4])
('beta', 1, -1/4*e[1, 1, 1] + e[2, 1] - 2*e[3])
('gamma', 1, 1/4*e[1, 1])
```

We rewrite the output in this table:

Ω	$\theta\lambda$	$\eta\lambda^2$
α_Ω	$-e_3/2$	$-e_1e_3/2+4e_4$
β_Ω	$-e_1^2/4+e_2$	$-e_1^3/4+e_1e_2-2e_3$
γ_Ω	$e_1/4$	$e_1^2/4$

Hence the six polynomials satisfied by λ, η and θ in Section 2.2 are

$$\begin{aligned}
r_1(\Lambda,H,\Theta) =&(\Lambda-\lambda)(\Lambda-\tau_{14}\lambda)(\Lambda-\tau_{12}\lambda)\\
=&\Lambda^3-e_2\Lambda^2+(e_1e_3-4e_4)\Lambda-(e_1^2e_4+e_3^2-4e_2e_4)\\
r_2(\Lambda,H,\Theta) =&H^2-(-3e_1^2+8e_2)\Lambda^2-(2e_1^2e_2-4e_2^2-4e_1e_3+16e_4)\Lambda+\\
&-(e_1^2e_2^2-4e_2^3-4e_1^3e_3+16e_1e_2e_3-12e_3^2+4e_1^2e_4-16e_2e_4)\\
r_3(\Lambda,H,\Theta) =&\Theta^2-(16e_4-e_1e_3)\Lambda^2-(e_1e_2e_3-3e_3^2-3e_1^2e_4)\Lambda+\\
&-(-e_2e_3^2-e_1^2e_2e_4+16e_1e_3e_4-64e_4^2)\\
r_4(\Lambda,H,\Theta) =&H\Theta-(6e_3-e_1e_2)\Lambda^2-(e_1e_2^2-e_1^2e_3-4e_2e_3+4e_1e_4)\Lambda\\
&-(-2e_2^2e_3+5e_1e_3^2-3e_1^3e_4+12e_1e_2e_4-32e_3e_4)\\
r_5(\Lambda,H,\Theta) =&4\Theta\Lambda+2e_3H-(-e_1^2+4e_2)\Theta-e_1H\Lambda\\
r_6(\Lambda,H,\Theta) =&4H\Lambda^2-(-2e_1e_3+16e_4)H-(-e_1^3+4e_1e_2-8e_3)\Theta-e_1^2H\Lambda
\end{aligned}$$

We map the coefficients of those polynomials to R via $e_k \mapsto s_k$. If $2 \in R^\times$, then C_4-closures for the monogenic extension $R \to R[x]/(x^4-s_1x^3+s_2x^2-s_3x+s_4)$ are in one-to-one correspondence with triples $(\ell, h, t) \in R^3$ satisfying the following equation, where $g(x) = x^3-s_2x^2+(s_1s_3-4s_4)x-(s_3^2-4s_2s_4+s_1^2s_4)$

is the resolvent cubic of f:

$$\begin{cases} g(\ell) = 0 \\ h^2 = (-3s_1^2 + 8s_2)\ell^2 + (2s_1^2 s_2 - 4s_2^2 - 4s_1 s_3 + 16s_4)\ell + \\ \quad +(s_1^2 s_2^2 - 4s_2^3 - 4s_1^3 s_3 + 16s_1 s_2 s_3 - 12s_3^2 + 4s_1^2 s_4 - 16s_2 s_4) \\ t^2 = (16s_4 - s_1 s_3)\ell^2 + (s_3 s_2 s_1 - 3s_3^2 - 3s_1^2 s_4)\ell + \\ \quad +(-s_2 s_3^2 - s_1^2 s_2 s_4 + 16s_1 s_3 s_4 - 64s_4^2) \\ ht = (6s_3 - s_1 s_2)\ell^2 + (s_1 s_2^2 - s_1^2 s_3 - 4s_2 s_3 + 4s_1 s_4)\ell \\ \quad +(-2s_2^2 s_3 + 5s_1 s_3^2 - 3s_1^3 s_4 + 12s_1 s_2 s_4 - 32s_3 s_4) \\ 4t\ell - s_1 h\ell + 2s_3 h - (4s_2 - s_1^2)t = 0 \\ 4h\ell^2 - s_1^2 h\ell - (-s_1^3 + 4s_1 s_2 - 8s_3)t - (-2s_1 s_3 + 16s_4)h = 0 \end{cases} \tag{B.1}$$

If we suppose that $s_1 = 0$, then those equations simplify to

$$\begin{cases} \ell^3 - s_2\ell^2 - 4s_4\ell - (s_3^2 - 4s_2 s_4) = 0 \\ h^2 = 4\big(2s_2\ell^2 + (4s_4 - s_2^2)\ell - (s_2^3 + 3s_3^2 + 4s_2 s_4)\big) \\ t^2 = 16s_4\ell^2 - 3s_3^2\ell - s_2 s_3^2 - 64s_4^2 \\ ht = 2(3s_3\ell^2 - 2s_2 s_3\ell - s_2^2 s_3 - 16s_3 s_4) \\ 2t(\ell - s_2) + s_3 h = 0 \\ h\ell^2 + 2s_3 t - 4s_4 h = 0. \end{cases}$$

Bibliography

[1] Owen Biesel. Galois Closures for Rings. https://dl.dropboxusercontent.com/u/60592530/Galois_Closures_Owen_Biesel.pdf, 2013. [Online; accessed 22-June-2014].

[2] Nicholas M. Katz and Barry Mazur. *Arithmetic Moduli of Elliptic Curves*. Princeton University Press, 1985.

[3] Ian Macdonald. *Symmetric Functions and Orthogonal Polynomials, Second edition*. American Mathematical Society, 1998.

[4] James S. Milne. Fields and Galois theory. http://www.jmilne.org/math/CourseNotes/FT.pdf, 2014. [Online; accessed 22-June-2014].

[5] Morris Orzech. Onto endomorphisms are isomorphisms. *The American Mathematical Monthly*, 78(4):pp. 357–362, 1971.

[6] Bernd Sturmfels. *Algorithms in Invariant Theory, Second Edition*. Springer Wien New York, 2008.