Theory of Equations, Lagrange and Galois Theory

Annick Valibouze

Theory of Equations
Lagrange and Galois Theory

Lesson in DEA ALGO (UPMC, France, 1995,...), in Pisa (Italie, 1997), in Marrakech (Maroc, 1996),...

Annick VALIBOUZE

LIP6, UPMC, 4 place Jussieu, F-75252 Paris Cedex 05
E-mail address: annick.valibouze@lip6.fr

supported by Galois Project of GDR de Calcul Formel MEDICIS and by Dipartemento
Projet Galois :
http://medicis.polytechnique.fr/medicis/projetGalois
http://groups.google.fr/group/evariste-galoisdi Matematica di la Università di Pisa
.

Contents

Avertissement au lecteur : complément 2008

Ce document rédigé tout d'abord en français (1995) puis en anglais (à Pise, en 1997) servit de support de cours dispensé dans différents endroits. Depuis, de nombreux résultats s'y trouvant ont été publiés et souvent améliorés. Malgré la mauvaise qualité de rédaction, je me suis décidée à le rendre public car des questions me parvenant y trouvent leur réponse. Certains résultats ne sont toujours pas publiés (souvent refusés pour cause de la mauvaise qualité de la langue anglaise ...). J'espère que mis en libre service les anglo-saxons qui en auront besoin sauront décoder cet anglais approximatif.

Changements de terminologie

Désormais les idéaux de Galois sont dénommés des idéaux galoisiens, le stabilisateur d'un idéal galoisien est appelé un injecteur.On peut se référencer à cet article pour en savoir plus :
A. Valibouze *Sur les relations entre les racines d'un polynôme.* Acta Arithmetica, 131, nř 1,1-27, 2008. [Version préliminaire : Prépublication du Laboratoire LSTA 3 Mai 2006]

Bases de données

Idéaux Galoisiens : http://docs.google.com/Doc?id=dd9dj4wn$_4$4*hgttks*3*d*
*Polynmesdedegr*12 : *http* : *//www*−*spiral.lip*6.*fr/ avb/Bibliographies/RapInt.htmldegre*12*inv*

Logiciels

La fonction SplittingField existe dans plusieurs logiciels mais n'est pas nécessairement performante.
Le calcul du groupe de Galois existe dans maple (implanté par Soicher ; jusqu'en degré 7) et pari (implanté par Eichenlaub) par les méthodes respectives de McKay-Soicher (calcul de résolvantes particulières) et de Jordan (inclusion des sous-groupes) avec la méthode numérique de Stauduhar pour calculer les résolvantes relatives.
De nombreuses résolvantes dont les algorithmes figurent dans ce document sont disponibles sous Maxima (module SYM) :
http://maxima.sourceforge.net/docs/manual/en/maxima_32.htmlSEC125

Introduction

Let f be a univariate polynomial with coefficients in a perfect field k. The motivation of the computational Galois theory is to compute in the splitting field of the polynomial f, denoted by D_f. In all this lecture the polynomial f will be represented by Ω (or Ω_f) an ordered set of its roots in an algebraic closure of k.

Let $x_1, \ldots, x_n$ be n indeterminated and $k[x_1, \ldots, x_n]$, the ring of polynomials of coefficients in k and in the variables $x_1, \ldots, x_n$.

The ideal I_Ω of Ω-*relations* is the ideal of polynomials in $k[x_1, \ldots, x_n]$ vanishing in the roots of the polynomial f:

$$I_\Omega = \{R \in k[x_1, \ldots, x_n] \mid \ R(\Omega) = 0\} \qquad .$$

The ideal of Ω-relations is a maximal ideal of $k[x_1, \ldots, x_n]$ which have been investigated by many authors (see **[61]**).

The splitting field of the polynomial f is k-isomorphic to the quotient ring

$$k[x_1, \ldots, x_n]/I_\Omega \ .$$

Thus, when the ideal I_Ω is computed it is possible to compute in D_f.

The *Galois group of* Ω *over* k is the subgroup G_Ω of $\mathfrak{S}_n$, the symmetric group of degree n, which leaves invariant the relations among the roots of f:

$$G_\Omega = \{\sigma \in \mathfrak{S}_n \mid \ (\forall R \in I_\Omega) \mid \sigma.R \in I_\Omega\} \ .$$

Let Θ be a polynomial in $k[x_1, \ldots, x_n]$ invariant only by the permutations of the Galois group G_Ω and not degenerated (Θ is called *separable*). A generating system of ideal I_Ω can be computed using Θ. Thus, when the Galois group G_Ω is computed it is possible to compute in the splitting field D_f.

This presentation studies the links between the fields, the ideals and the groups and gives several results about the computational Galois theory for computing the Galois group G_Ω and the ideal of Ω-relations I_Ω.

We consider the *ideal* I^L *of* Ω*-relations which are invariant by a subset* L *of the symmetric group*:

$$I^L = \{R \in k[x_, \ldots, x_n] \mid \ (\forall \sigma \in L)\ \sigma.R \in I_\Omega\} \ .$$

The ideal I^L is a radical ideal. A useful tool in order to study the ideal I^L is its *stabilizer*, denoted by $\mathrm{Max}(I^L)$, which is the maximal subset M of the symmetric group which satisfies $I^L = I^M$. In particular, $G_\Omega = \mathrm{Max}(I_\Omega)$ is as well the *decomposition group* of the ideal of relations I_Ω.

Chapter 1 introduces the general informations (notations, definitions, ...).

Chapter 2 is devoted to recalls about characteristic and minimal polynomials of endomorphisms of a polynomial ring quotiented by a radical ideal.

One of tools of computational theory is the invariants associated with finite groups (see Chapter 3).

The particular cases of the *ideal of symmetric relations* and of the ideal of relations are studied in Chapter 4.

The classical Galois theory with the point of view of fields is described in Chapter 5 using the following simple fact. Let Θ be a multivariate polynomial, $\mathrm{M}_{\Theta,I_\Omega}$ be the minimal polynomial of the endomorphism induced by Θ in the quotient ring $k[x_1,\ldots,x_n]/I_\Omega$ and $\mathrm{Min}_{\theta,k}$ be the minimal polynomial over k of the evaluation θ of Θ at Ω. As the polynomials $\mathrm{Min}_{\theta,k}$ and $\mathrm{M}_{\Theta,I_\Omega}$ are equal and since k is perfect, the coefficients of $\mathrm{Min}_{\theta,k}$ belong to the field k.

Chapter 6 gives results about the ideals I^L. The definition of the *resolvent* associated with an ideal I^L is introduced and compared with the characteristic and the minimal polynomials.

One of the motivations of this lecture is to study the correspondence between the radical ideals I^L and its stabilizers. It is proved that the stabilizer of I^L is:

$$\star \qquad \mathrm{Max}(I^L) = G_\Omega L \qquad ,$$

Let L and H be two subgroups of the symmetric groups. The correspondence between stabilizers and ideals is the following:

$$\star\star \qquad I^L \subset I^H \qquad \text{if and only if} \qquad G_\Omega H \subset G_\Omega L \qquad .$$

If the group L contains the Galois group and a group H such that the decomposition group of the ideal I^H also contains the Galois group then a generating system of the ideal I^H is given by:

$$\star\star\star \qquad I^H = I^L + (R_{H,L}) \qquad ,$$

where $R_{H,L}$ is some polynomial which characterizes the ideal I^H relatively to I^L and is called an *L-primitive polynomial of I^H*.

Chapter 7 deals with the computational Galois theory. How to compute the ideal of Ω-relations I_Ω? The first idea is to compute a Gröbner basis of I_Ω, which is possible using factorizations of f in successive sub-extensions of D_f (see **[61]** and **[2]** or Chapter 4). However this computation is difficult. The second idea is to compute the Galois group of the polynomial f and deduce from it generators of the ideal I_Ω (see Chapter 4). This

method is always possible using *partitions* and *group matrices* as introduced in [**7**] and in [**65**]. The third idea is to simultaneously compute the Galois group G_Ω and the ideal of relations I_Ω using partition and group matrices: we find a group L containing the Galois group G_Ω and we compute a generating system of the ideal I^L. Computing modulo the ideal I^L, a new subgroup H is found that is included in the group L and contains the Galois group G_Ω. A generating system of the ideal I^H is given by the computation of an L-primitive polynomial of the ideal I^H (see $\star\star\star$). The situation is the following:

$$I_\Omega^{\mathfrak{S}_n} \subset I^L \subset I^H \subset I_\Omega \qquad .$$

Next the group L is replaced by the group H and the construction goes on until it reaches the ideal I_Ω of Ω-relations.

The fundamental tool of this algorithm is the resolvent associated with the ideal I^L. The irreducible factors over k of a resolvent are minimal polynomials over k of algebraic numbers of the decomposition field D_f. This minimal polynomials of elements of D_f are used for computing primitive polynomials of ideals. Chapter 10 gives an explicit example for this algorithm.

Chapter 8 is devoted to the particular case in which f is reducible.

Chapter 9 describes some methods for computing resolvents.

In Chapter 11 are given all useful sub-matrices of groups and partitions up to degree 7.

The point of view presented here is indebted to Tchebotarev's book (see [**61**]), K. Yokoyama, M. Noro and T. Takeshima (see [**67**]), the beginning of the thesis of F. Rouiller (see [**56**]), work with A. Machì about Tchebotarev's book and some conversations with C. Traverso and with J.M. Arnaudiès about endomorphisms associated with the ideal of symmetric relations (see [**6**]).

CHAPTER 1

Preliminaries

1. Some preliminary notations and definitions

We consider as given:

- a perfect field k,
- a univariate polynomial f of degree n whose coefficients belong to k,
- $n+2$ indeterminates $x_1, \ldots, x_n, T$ and x.

1.1. General notations.

Let g be a univariate polynomial over k of degree n.

- $\hat{k}$ is an algebraic closure of the field k;
- $k[x_1, \ldots, x_n]$ is the ring of polynomials in the variables $x_1, \ldots, x_n$ with coefficients in the field k;
- $k(x_1, \ldots, x_n)$ is the fraction field of $k[x_1, \ldots, x_n]$;
- $\mathfrak{S}_n$ is the symmetric group of degree n;
- I_n is the identity group of $\mathfrak{S}_n$;
- $\Delta(g)$ is the discriminant of g;
- Ω_g is an ordered set, included in $\hat{k}^n$, containing the n roots of g; assume that $\Omega_g = (\beta_1, \ldots, \beta_n)$;
- $k[\Omega_g] = k[\beta_1, \ldots, \beta_n]$;
- $k(\Omega_g) = k(\beta_1, \ldots, \beta_n)$ is the splitting field of g;
- for $P \in k[x_1, \ldots, x_n]$, $P(\Omega_g) = P(\beta_1, \ldots, \beta_n)$;
- for $\sigma \in \mathfrak{S}_n$, $\sigma \circ \Omega_g = (\beta_{\sigma(1)}, \ldots, \beta_{\sigma(n)})$;
- $\alpha_1, \ldots, \alpha_n$ are the n roots of the polynomial f in $\hat{k}$;
- $\Omega = \Omega_f = (\alpha_1, \ldots, \alpha_n)$.

1.2. Actions of groups.

Definition 1.1. The action of the symmetric group $\mathfrak{S}_n$ on the field $k(x_1, \ldots, x_n)$ is defined by:

$$\begin{array}{rcl} \mathfrak{S}_n \times k(x_1, \ldots, x_n) & \longrightarrow & k(x_1, \ldots, x_n) \\ (\sigma, P) & \mapsto & \sigma.P(x_1, \ldots, x_n) = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \end{array}$$

The notation $\sigma.P(\Omega_g)$ is not ambiguous : $\sigma.P(\Omega_g) = (\sigma.P)(\Omega_g)$. However, the following lemma refines this notation:

LEMMA 1.2. *Let $\sigma, \tau \in \mathfrak{S}_n$ and $P \in k[x_1, \ldots, x_n]$, then $(\sigma.P)(\tau \circ \Omega_g) = P(\tau\sigma \circ \Omega_g)$.*

PROOF. Let $\sigma, \tau \in \mathfrak{S}_n$ and P be a polynomial in $k[x_1, \ldots, x_n]$. Then

$$\begin{aligned}(\sigma.P)(x_1, \ldots, x_n)(\tau \circ \Omega_g) &= P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}) \\ &= P(\tau\sigma \circ \Omega_g) \quad ,\end{aligned}$$

because the evaluation of x_j is $\alpha_{\tau(j)}$ for all $j \in [1, n]$ and then one of the $x_{\sigma(i)}$ is $\alpha_{\tau\sigma(i)}$ for all $i \in [1, n]$ (setting $j := \sigma(i)$). □

Now, let L be a subgroup of $\mathfrak{S}_n$ and $\Theta \in k(x_1, \ldots, x_n)$.

Definition 1.3. The *orbit of Θ under the action of L*, denoted by $L.\Theta$, is defined by:

$$L.\Theta = \{\sigma.\Theta \mid \sigma \in L\} \quad .$$

Definition 1.4. The fraction Θ is called an *invariant of L* (or an *L-invariant*) if $L.\Theta = \{\Theta\}$.

Notation 1.5. The field of L-invariants is denoted by $k(x_1, \ldots, x_n)^L$.

Definition 1.6. The *stabilizer of Θ on L*, denoted by $\mathrm{Stab}_L(\Theta)$, is defined by:

$$\mathrm{Stab}_L(\Theta) = \{\sigma \in L \mid \Theta = \sigma.\Theta\} \quad .$$

Notation 1.7. The *stabilizer of a subgroup H of L* will be denoted by $\mathrm{Stab}_L(H)$.

Definition 1.8. Let H be a subgroup of $\mathfrak{S}_n$ and $\sigma_1 H, \ldots, \sigma_e H$ (resp. $H\sigma_1, \ldots, H\sigma_e$) the left (resp. right) cosets of H in $\mathfrak{S}_n$. Then the set $\{\sigma_1, \ldots, \sigma_n\}$ is called a *left* (resp. *right*) *transversal* of $\mathfrak{S}_n \mod H$.

1.3. Ideals and Ω-relations.

Definition 1.9. Let $\alpha \in \hat{k}^n$. A polynomial $P \in k[x_1, \ldots, x_n]$ is called an *α-relation* if $P(\alpha) = 0$.

Definition 1.10. . Let L be a subset of $\mathfrak{S}_n$. We denote by I_Ω^L the *ideal of L-invariant Ω-relations* defined by:

$$I_\Omega^L = \{R \in k[x_1, \ldots, x_n] \mid (\forall \sigma \in L)\ \sigma.R(\Omega) = 0\} \quad .$$

Definition 1.11. The *ideal of Ω-relations*, denoted by I_Ω, is defined by:

$$I_\Omega \overset{I_n}{=}_\Omega = \{R \in k[x_1, \ldots, x_n] \mid R(\Omega) = 0\} \quad . \tag{1.1}$$

Definition 1.12. The ideal $I_\Omega^{\mathfrak{S}_n}$ is called the *ideal of symmetric relations among the roots of the polynomial f*.

Remark 1. As the ideal $I_\Omega^{\mathfrak{S}_n}$ does not depend on the order of the roots of f it can be denoted by $I_f^{\mathfrak{S}_n}$.

2. The Galois group and the direct Galois problem

Since the roots of the univariate polynomial f are algebraic over k, by induction we have $k[\Omega] \cong k(\Omega)$, the splitting field of f.

We will be interested in the algebraic numbers $P(\Omega)$ of $k(\Omega)$ such that P is a polynomial of $k[x_1, \ldots, x_n]$.

The symmetric group $\mathfrak{S}_n$ acts faithfully on $k(x_1, \ldots, x_n)$. For $\sigma \in \mathfrak{S}_n$ and two fractions $P, Q \in k(x_1, \ldots, x_n)$, the equality $P = Q$ implies that $\sigma.P = \sigma.Q$. But, for P and $Q \in k[x_1, \ldots, x_n]$, the equality $P(\Omega) = Q(\Omega)$ does not necessarily imply that $\sigma.P(\Omega) = \sigma.Q(\Omega)$. In other words, the group $\mathfrak{S}_n$ does not act necessarily faithfully on the field $k(\Omega)$.

Example 2.1. Set $f := (x-1)(x-j)(x-j^2) = (x-1)(x^2+x+1)$, $P := x_2^2$, $Q := x_3$, and $\sigma := (1,2)$, then $P(\Omega) = j^2 = Q(\Omega)$ and $\sigma.P(\Omega) = 1^2 \neq \sigma.Q(\Omega) = j^2$.

Thus, the fundamental question of Galois theory is the following:

Which is the biggest subset G_Ω of $\mathfrak{S}_n$ such that for all $P, Q \in k[x_1, \ldots, x_n]$ and for all $\sigma \in G_\Omega$

$$P(\Omega) = Q(\Omega) \qquad \text{implies} \qquad \sigma.P(\Omega) = \sigma.Q(\Omega) \ ?$$

This question is equivalent to the following:

Which is the biggest subset G_Ω of $\mathfrak{S}_n$ such that for all $R \in k[x_1, \ldots, x_n]$ and for all $\sigma \in G_\Omega$

$$R(\Omega) = 0 \qquad \text{implies} \qquad \sigma.R(\Omega) = 0 \ ?$$

In order to answer at this last question we consider the ideal I_Ω of Ω-relations. Thus, G_Ω is a group (see Lemma 2.2 in Chapter 4) explicitly given by:

Definition 2.2. The *Galois group of* Ω, denoted by G_Ω, is defined by:

$$G_\Omega = \{\sigma \in \mathfrak{S}_n \mid \ (\forall R \in I_\Omega)\ \sigma.R \in I_\Omega\} \qquad . \tag{2.1}$$

In other words, the Galois group G_Ω is the group which leaves invariant the Ω-relations.

Remark 2. Often, the Galois group of Ω is called the *Galois group of* f.

Therefore, there is a faithful action of G_Ω on the quotient ring $A_{I_\Omega} := k[x_1, \ldots, x_n]/I_\Omega$ which is defined by:

$$\begin{array}{rcl} G_\Omega \times A_{I_\Omega} & \longrightarrow & A_{I_\Omega} \\ (\sigma, P) & \mapsto & \sigma.P(\Omega) = P(\sigma \circ \Omega) \end{array} \qquad .$$

Now, consider the surjective k-algebra morphism of evaluation given by:

$$\begin{array}{rcl} k[x_1, \ldots, x_n] & \longrightarrow & k(\Omega) \\ P & \mapsto & P(\Omega) \end{array}$$

having I_Ω as kernel. Then the quotient ring A_{I_Ω} is k-isomorphic to the field $k(\Omega)$. (The ideal I_Ω is a maximal ideal of $k[x_1, \ldots, x_n]$ because $k(\Omega)$ is a field.) We will denote by Φ the induced k-isomorphism between A_{I_Ω} and $k(\Omega)$:

$$\begin{array}{rccc} \Phi & : & A_{I_\Omega} & \longrightarrow & k(\Omega) \\ & & P & \mapsto & P(\Omega) \end{array} .$$

From the k-isomorphism Φ, a faithful action $\star$ of G_Ω on $k(\Omega)$ is induced by the one of G_Ω on A_{I_Ω}:

$$\begin{array}{ccc} G_\Omega \times k(\Omega) & \longrightarrow & k(\Omega) \\ (\sigma, p) & \mapsto & \sigma \star p := (\sigma.P)(\Omega) \end{array} ,$$

where $P = \Phi^{-1}(p)$.

The effective problem of Galois theory is to compute the Galois group G_Ω and the ideal I_Ω of Ω-relations.

CHAPTER 2

Ideals and endomorphisms of quotient rings

This part is devoted to results about radical ideals in dimension 0 (i.e. the associated algebraic variety is finite).

1. Definitions and notations

Let I be an ideal of $k[x_1, \ldots, x_n]$ of dimension 0 and let Θ be a polynomial of $k[x_1, \ldots, x_n]$. We adopt the following notations:

- A_I is the quotient ring $k[x_1, \ldots, x_n]/I$;
- $\mathrm{End}(A_I)$ is the set of endomorphisms of A_I;
- $V(I)$ is the algebraic variety of $\hat{k} \bigotimes_k I$ in $\hat{k}$:
$$V(I) = \{\beta \in \hat{k}^n \mid (\forall P \in I)\ P(\beta) = 0\} \quad ;$$
- $\overline{\Theta}$ denotes the class of Θ in A_I;
- $\overline{\Theta}.A_I = \{\overline{\Theta}.P \mid P \in A_I\}$;
- $\hat{\Theta}$ is the endomorphism induced by the multiplication by $\overline{\Theta}$ in A_I as follows:
$$\begin{array}{rccc} \hat{\Theta} : & A_I & \longrightarrow & A_I \\ & P & \mapsto & \overline{\Theta}.P \end{array} \quad ;$$
- $\hat{\Theta}A_I = \overline{\Theta}.A_I$;
- $C_{\Theta,I}$ is the *characteristic polynomial* of the endomorphism $\hat{\Theta}$ belonging to $\mathrm{End}(A_I)$;
- $M_{\Theta,I}$ is the *minimal polynomial* of $\hat{\Theta}$;
- $SF_{\Theta,I}$ is the monic polynomial whose roots are those of $C_{\Theta,I}$ not counted with their multiplicities.

Remark 3. The polynomial $SF_{\Theta,I}$ is the square free form of the characteristic polynomial $C_{\Theta,I}$. As the field k is perfect, the coefficients of $SF_{\Theta,I}$ belong to k.

Definition 1.1. A set of ideals $\mathcal{A}_1, \ldots, \mathcal{A}_m$ in a field R is said *pairwise comaximal* if each $\mathcal{A}_i \neq R$ and
$$\mathcal{A}_i + \mathcal{A}_j = R \qquad \text{for } i \neq j \quad .$$
If $n = 2$, we simply say that $\mathcal{A}_1$ and $\mathcal{A}_2$ are comaximal.

Definition 1.2. An ideal I is said *radical* if it equals its radical $\sqrt{I}$ given by:
$$\sqrt{I} = \{P \in k[x_1, \ldots, x_n] \mid (\exists m \in \mathbb{N})\ P^n \in I\} \quad .$$

2. Results about radical ideals

Stickelberger's Theorem gives $C_{\Theta,I}$ in the following form:

$$C_{\Theta,I}(T) = \prod_{\beta \in V(I)} (T - \Theta(\beta))^{\mu(\beta)} \in k[T] \quad , \tag{2.1}$$

where $\mu(\beta)$ is the multiplicity of β. The degree $d := \sum_{\beta \in V(I)} \mu(\beta)$ of the characteristic polynomial $C_{\Theta,I}$ is naturally $\dim_k(A_I) = \dim_{\hat{k}}(\hat{k} \bigotimes_k A_I)$. The multiplicity $\mu(\beta)$ is the one of the maximal ideal $J = (x_1 - \beta_1, \ldots, x_n - \beta_n)$ in the ring $\hat{k} \bigotimes_k k[x_1, \ldots, x_n]/I$.

LEMMA 2.1. *If I is radical then for all $\beta \in V(I)$ its multiplicity $\mu(\beta)$ equals one and*

$$C_{\Theta,I}(T) = \prod_{\beta \in V(I)} (T - \Theta(\beta)) \in k[T] \quad . \tag{2.2}$$

PROOF. Because $\mathrm{card}(V(I)) = \dim_k(A_I) = d$, the degree of the characteristic polynomial. □

THEOREM 2.2. *(Yokoyama-Noro-Takeshima) Let $Q \in k[x_1, \ldots, x_n]$. Then*

$$A_{I+(Q)} \cong A_I / \hat{Q} A_I \tag{2.3}$$

and A_I is isomorphic to End(A_I).

PROOF. See **[67]**. □

COROLLARY 2.3. *Let $P \in k[T]$.*

$$A_{I+(P(\Theta))} \cong A_I / P(\hat{\Theta}) A_I \tag{2.4}$$

so that $P(\Theta) \in I$ if and only if $P(\hat{\Theta}) = 0$.

PROOF. Apply Equality (2.3). □

THEOREM 2.4. *(Yokoyama-Noro-Takeshima) The ideal I is radical if and only if every minimal polynomial $M_{x_i,I}$ ($i \in [1, n]$) is square free because the radical of I is given by:*

$$\sqrt{I} = (SF_{x_1,I}(x_1), \ldots, SF_{x_n,I}(x_n)) + I \quad . \tag{2.5}$$

PROOF. See **[67]**. □

Now the minimal polynomial $M_{\Theta,I}$ is the monic polynomial in $k[T]$ of smaller degree such that $M_{\Theta,I}(\hat{\Theta}) = 0$. We can also say that $M_{\Theta,I}$ is the monic polynomial in $k[T]$ of smaller degree such that $M_{\Theta,I}(\Theta) \in I$. On the other hand, the polynomial $SF_{\Theta,I}$ is the square free form of $C_{\Theta,I}$ which belongs to $k[T]$.

LEMMA 2.5. *The polynomial $SF_{\Theta,I}$ is a factor of the polynomial $M_{\Theta,I}$.*

PROOF. For $F \in k[T]$, the condition $F(\hat{\Theta}) = 0$ is equivalent to $F(\Theta) \in I$ and then $F(\hat{\Theta}) = 0$ implies that for all $\beta \in V(I)$ there exists a root ρ of F in $\hat{k}$ such that $\Theta(\beta) = \rho$ (by definition of $V(I)$, the converse is true if $I = \sqrt{I}$). Then all roots of $SF_{\Theta,I}$ are also roots of F : $SF_{\Theta,I}$ is a factor of F. Applying this last result to $F = M_{\Theta,I}$ the lemma is proved. □

The following lemma gives a sufficient and necessary condition for which $SF_{\Theta,I} = M_{\Theta,I}$.

LEMMA 2.6. *The condition $SF_{\Theta,I} = M_{\Theta,I}$ is equivalent to $SF_{\Theta,I}(\Theta) \in I$.*

PROOF. Let $F \in k[T]$. The definition of $M_{\Theta,I}$ implies that $F(\hat{\Theta}) = 0$ if and only if F is a multiple of $M_{\Theta,I}$. On the other hand, the polynomial $SF_{\Theta,I}$ is a factor of $M_{\Theta,I}$. As $M_{\Theta,I}$ and $SF_{\Theta,I}$ are monic, the lemma is proved. □

LEMMA 2.7. *The ideal I is radical if and only if each $\Theta \in k[x_1, \ldots, x_n]$ satisfies $SF_{\Theta,I} = M_{\Theta,I}$.*

PROOF. Assume that $I = \sqrt{I}$. As the polynomial $SF_{\Theta,I}(\Theta)$ vanishes at each $\beta \in V(I)$, it belongs to I and therefore $SF_{\Theta,I} = M_{\Theta,I}$. The converse is provided by the Yokoyama-Noro-Takeshima's theorem (see Theorem 2.4). □

Example 2.8. Let L be a subset of $\mathfrak{S}_n$. Let us prove that the ideal I_Ω^L (see Definition 1.10 of Chapter 1) is radical. It is sufficient to prove that $SF_{\Theta,I_\Omega^L}(\Theta) \in I_\Omega^L$. By definition of I_Ω^L the set $\{l \circ \Omega \mid l \in L\}$ is included in $V(I_\Omega^L)$ and then $(\forall l \in L)\ l.\Theta(\Omega)$ is a root of SF_{Θ,I_Ω^L} which actually belongs to the ideal I_Ω^L.

CHAPTER 3

Invariants

1. Primitive Invariants

Definition 1.1. Let L be a subgroup of $\mathfrak{S}_n$ and H be a subgroup of L. A polynomial $\Theta \in K[x_1, \ldots, x_n]$ is said to be *L-primitive H-invariant* if

$$H = \mathrm{Stab}_L(\Theta) = \{\sigma \in L \mid \sigma.\Theta = \Theta\} \qquad .$$

If $L = \mathfrak{S}_n$ the polynomial Θ is said a *primitive H-invariant.*

Example 1.2. The Vandermond determinant $\delta_n = \prod_{1 \leq i < j \leq j}^{n} (x_i - x_j)$ is a primitive invariant of the alternating subgroup A_n of $\mathfrak{S}_n$.

Example 1.3. Let $\mathcal{D}_4$ be the dihedral subgroup of $\mathfrak{S}_4$. The polynomial $x_1x_2 + x_3x_4$ is a $\mathfrak{S}_4$-primitive $\mathcal{D}_4$-invariant.

Example 1.4. The polynomials

$$\begin{array}{ll} x_1 + 2x_2 + \cdots (n-1)x_{n-1} & \text{and} \\ x_1 x_2^2 \cdots x_{n-1}^{n-1} & \end{array}$$

are $\mathfrak{S}_n$-primitive I_n-invariants.

LEMMA 1.5. *Let H and L be two subgroups of $\mathfrak{S}_n$ such that L contains H and let Θ be an L-primitive H-invariant. Then for each $\tau \in L$ the polynomial $\tau.\Theta$ is an L-primitive $(\tau H \tau^{-1})$-invariant.*

PROOF. Take $\tau \in L$ and set $A := \{\sigma \in L \mid \ \sigma \in \tau H \tau^{-1}\}$. We have

$$\begin{array}{rcl} A & = & \{\sigma \in L \mid \ \tau^{-1}\sigma\tau \in H\} \\ A & = & \{\sigma \in L \mid \ \tau^{-1}\sigma\tau.\Theta = \Theta\} \\ A & = & \{\sigma \in L \mid \ \sigma.(\tau.\Theta) = \tau.\Theta\} \qquad . \end{array}$$

□

The computation of invariants can be performed by Kemper's package (see [**39**]) or by Abdeljaouad's package (see [**1**]).

2. Separable primitive invariants

Definition 2.1. Let H and L be two subgroups of $\mathfrak{S}_n$ such that $H \subset L$. An L-primitive H-invariant, Θ, is said *L-separable for Ω* if

$$H = \{\sigma \in L \mid \ \sigma.\Theta(\Omega) = \Theta(\Omega)\} \qquad .$$

We say also that Θ is an *L-primitive H-invariant separable for Ω.*

A separable $\mathfrak{S}_n$-primitive H-invariant is simply said a *separable primitive L-invariant.*

Remark 4. For each subgroup L of $\mathfrak{S}_n$, a separable $\mathfrak{S}_n$-primitive H-invariant always is an L-primitive H-invariant separable for Ω.

Remark 5. An L-primitive H-invariant separable for Ω is not necessarily separable for $\tau \circ \Omega$, where $\tau \in L$.

Remark 6. When L contains the Galois group G_Ω, Θ is L-separable for Ω if and only if $\Theta(\Omega)$ is a simple root of the resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$ (see Section 5.2 Chapter 9).

LEMMA 2.2. *Assume that f is a separable polynomial and k is infinite. There exists a separable primitive I_n-invariant.*

PROOF. Let $T_1, \ldots, T_n$ be n independent variables and $V(T)(X) = \sum_{i=1}^n T_i x_i$. For all $\sigma \in \mathfrak{S}_n$, if $\sigma \neq id$ then $V(T)(\Omega) \neq \sum_{i=1}^n T_i \alpha_{\sigma(i)} = V(T)(\sigma \circ \Omega)$ and, as k is infinite, there exist $t_1, \ldots, t_n \in k$ such that $V(t_1, \ldots, t_n)(\Omega) \neq V(t_1, \ldots, t_n)(\sigma \circ \Omega)$ (equality occurs for a finite number of $t_i \in k(\Omega)$). The polynomial $V(t_1, \ldots, t_n)(X)$ is an I_n-invariant and is separable. □

LEMMA 2.3. *Assume that f is a separable polynomial and the field k is infinite. There exists a separable primitive H-invariant in $k[x_1, \ldots, x_n]$ for any subgroup H of $\mathfrak{S}_n$.*

PROOF. Let V be a separable primitive I_n-invariant. Consider the separable polynomial

$$C(T) = \prod_{\sigma \in \mathfrak{S}_n} (T_\sigma . V(\Omega)) \qquad .$$

Let $\tau_1 = id, \ldots, \tau_e$ be a left transversal of $\mathfrak{S}_n \mod H$. For $i \in [1, e]$, we set

$$R_i(T) = R_i(T)(x_1, \ldots, x_n) := \prod_{\sigma \in H} (T - \tau_i \sigma . V) \qquad .$$

We get $C = \prod_{i=1}^e R_i(T)(\Omega)$. As V is I_n-separable, $(\forall i \in [2, e]\ )\ R_1(T)(\Omega_f) \neq R_i(T)(\Omega_f)$ so that there exists $u \in k$, which is infinite, such that $R_1(u)(\Omega_f) \neq R_i(u)(\Omega_f)$. Now, let $\tau \in \mathfrak{S}_n$. If $\tau \in H$ then $\tau.R_1(u) = R_1(u)$ else there exists $i \in [2, e]$ such that $\tau.R_1(u) = R_i(u)$. Thus polynomial $R_1(u)$ is a separable primitive H-invariant . □

In **[22]** is given another method for computing separable primitive invariants.

There exists polynomials which are separable for any univariate separable polynomial. The Vandermonde determinant is a such invariant.

Example 2.4. Let $\mathcal{M}_5$ the metacyclic group of $\mathfrak{S}_5$. Assume that the polynomial f is a separable polynomial of degree 5. The Cayley's invariant

$$(x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - (x_1x_3 + x_3x_5 + x_5x_2 + x_2x_4 + x_4x_1))^2$$

is a separable primitive $\mathcal{M}_5$-invariant (see **[19]** and **[7]**).

3. Lagrange's theorem

For H a subgroup of $\mathfrak{S}_n$, we denote by $k[x_1, \ldots, x_n]^H$ the algebra of polynomial invariants of H:

$$k[x_1, \ldots, x_n]^H = \{P \in k[x_1, \ldots, x_n] \mid (\forall \sigma \in H)\ \sigma.P = P\} \quad .$$

THEOREM 3.1 (Lagrange-Colin). *Let two subgroups H and G of $\mathfrak{S}_n$ such that $H \subset G$. Let Θ be a G-primitive H-invariant, $\Theta_1, \ldots, \Theta_e$ be the distinct elements of the G-orbit of Θ and*

$$\Delta_\Theta = \prod_{1 \leq i < j \leq n} (\Theta_i - \Theta_j)^2 \quad .$$

The polynomial Δ_Θ is the discriminant of the minimal polynomial of Θ over the field $k(x_1, \ldots, x_n)^G$ (see 9.3 Chapter 5). Then $k[x_1, \ldots, x_n]^H$ is a $k[x_1, \ldots, x_n]^G$-algebra given by:

$$k[x_1, \ldots, x_n]^H \subset \frac{1}{\Delta_\Theta} k[x_1, \ldots, x_n]^G[\Theta] \quad . \tag{3.1}$$

PROOF. see **[41]**, **[6]** and **[25]**, Remark 3.11. □

CHAPTER 4

The ideals of Ω-relations and of symmetric relations

We have $\Omega \in \hat{k}^n$ containing the n roots of the polynomial f.

In Chapter 1 are defined the ideals fixed by sets of permutations. Two of them play a particular rule. They are the ideal of symmetric relations among the roots of the polynomial f:

$$I_f^{\mathfrak{S}_n} = \{R \in k[x_1, \ldots, x_n] \mid \ (\forall \sigma \in \mathfrak{S})\ \sigma.R(\Omega) = 0\}$$

and the ideal of the Ω-relations:

$$I_\Omega = \{R \in k[x_1, \ldots, x_n] \mid \ R(\Omega) = 0\} \qquad .$$

This chapter is devoted to these particular ideals.

The Galois group G_Ω of Ω has been defined as follows:

$$G_\Omega = \{\sigma \in \mathfrak{S}_n \mid \ (\forall R \in I_\Omega)\ \sigma.R(\Omega) = 0\}.$$

1. Definition of particular symmetric relations

Definition 1.1. A polynomial s of $k[x_1, \ldots, x_n]$ is said a *symmetric polynomial* if $\mathrm{Stab}_{\mathfrak{S}_n}(s) = \mathfrak{S}_n$.

All symmetric polynomials belong to the ideal of symmetric relations $I_f^{\mathfrak{S}_n}$. But $f(x_1)$ is not symmetric and belongs to the ideal $I_f^{\mathfrak{S}_n}$.

Definition 1.2. Let $i \in \mathbb{N}$. Set $e_i := e_i(x_1, \ldots, x_n)$, the *$i$-th elementary symmetric function on $x_1, \ldots, x_n$* is given by:

$$x^n + \sum_{i=1}^{n} e_i x^{n-i} = \prod_{k=1}^{n} (x + x_k) \qquad .$$

For $s > 0$, the *complete symmetric function*, denoted by $h_i(x_1, \ldots, x_s)$, is the sum of the monomials $x_1^{i_1} \cdots x_s^{i_s}$ of degree $i = i_1 + \cdots + i_s$ and $h_0(x_1, \ldots, x_s) = 1$.

Remark 7. The elementary symmetric functions of the roots of a monic univariate polynomial g are, up to a sign, its coefficients:

$$g(x) = x^n - e_1(\Omega_g)x^{n-1} + \cdots + (-1)^n e_n(\Omega_g) \qquad .$$

Notation 1.3. Denote by $\mathcal{J}_f$ the ideal generated by the following n symmetric polynomials:

$$\mathcal{J}_f = (e_1 - e_1(\Omega), \ldots, e_n - e_n(\Omega)) \qquad .$$

Definition 1.4. The n polynomials defined by induction as follows:

$$\begin{aligned} f_n(x) &= f(x) \\ f_i(x) &= f_i(x, x_{i+1}, \ldots, x_n) = \frac{f_{i+1}(x) - f_{i+1}(x_{i+1})}{x - x_{i+1}} \qquad \text{for } 1 \leq i \leq n-1 \end{aligned}$$

are called the *interpolating functions.*

The interpolating functions, introduced by Ampère (see **[3]**), satisfy:

$$f_i(x_i) \in k[x_i, x_{i+1}, \ldots, x_n] \qquad \text{and} \qquad \deg_{x_i}(f_i(x_i)) = i \qquad .$$

2. Varieties

PROPOSITION 2.1. *The variety of $I_f^{\mathfrak{S}_n}$ in $\hat{k}^n$ is given by:*

$$V(I_f^{\mathfrak{S}_n}) = \{\sigma \circ \Omega \mid \sigma \in \mathfrak{S}_n\} = \mathfrak{S}_n \circ \Omega \qquad , \tag{2.1}$$

the $\mathfrak{S}_n$-orbit of Ω. If f is separable then card$(V(I_f^{\mathfrak{S}_n})) =$ card$(\mathfrak{S}_n) = n!$.

PROOF. Set $\mathcal{W} := \{\sigma \circ \Omega \mid \sigma \in \mathfrak{S}_n\}$. We have $f(x) = x^n - e_1(\Omega)x^{n-1} + \cdots + (-1)^n e_n(\Omega) = \prod_{i=1}^n (x - \alpha_i)$. Then $\beta \in \mathcal{W}$ if and only if $e_i(\beta) - e_i(\Omega) = 0$ for $i \in [1, \ldots, n]$. In other words, $\mathcal{W} = V(e_1 - e_1(\Omega), \ldots, e_n - e_n(\Omega))$. As for $i \in [1, n]$ the polynomial $e_i - e_i(\Omega)$ belongs to the ideal $I_f^{\mathfrak{S}_n}$, $V(I_f^{\mathfrak{S}_n}) \subset \mathcal{W}$. Conversely, take $\sigma \in \mathfrak{S}_n$ and $R \in I_f^{\mathfrak{S}_n}$; we have $R(\sigma \circ \Omega) = \sigma.R(\Omega) = 0$, by definition of $I_f^{\mathfrak{S}_n}$. Thus $\mathcal{W} \subset V(I_f^{\mathfrak{S}_n})$. □

PROPOSITION 2.2. *The variety in $\hat{k}^n$ of the ideal of the Ω-relations is given by:*

$$V(I_\Omega) = \{\sigma \circ \Omega \mid \sigma \in G_\Omega\} = G_\Omega \circ \Omega \qquad , \tag{2.2}$$

the G_Ω-orbit of Ω. If f is a separable polynomial then card$(V(I_\Omega)) =$ card(G_Ω).

PROOF. By definition of G_Ω, we have $G_\Omega \circ \Omega \subset V(I_\Omega)$. Conversely, as $I_f^{\mathfrak{S}_n} \subset I_\Omega$,

$$V(I_\Omega) = \{\sigma \circ \Omega \mid \ (\forall R \in I_\Omega)\ R(\sigma \circ \Omega) = 0\} \ .$$

Let $\sigma \in \mathfrak{S}_n$. By definition of the Galois group G_Ω, if $(\forall R \in I_\Omega)\ \sigma.R(\Omega) = 0$ then $\sigma \in G_\Omega$. Thus $V(I_\Omega) \subset G_\Omega \circ \Omega$. □

3. Characteristic and minimal polynomials

Assume that the roots of the polynomial f are distinct (i.e. f is separable).

For a radical ideal of $k[x_1,\ldots,x_n]$, the expressions of the characteristic and the minimal polynomials of endomorphisms in $\mathrm{End}(k[x_1,\ldots,x_n]/I)$ are given in Chapter 2. Let $\Theta \in k[x_1,\ldots,x_n]$. As the variety of the ideals of Ω-relations is $G_\Omega \circ \Omega$, the characteristic and the minimal polynomials of the endomorphism $\hat{\Theta}$ of $k[x_1,\ldots,x_n]/I_\Omega$ are respectively given by:

$$C_{\Theta,I_\Omega} = \prod_{\sigma\in G_\Omega} (T - \sigma.\Theta(\Omega)) \tag{3.1}$$

$$M_{\Theta,I_\Omega} = \prod_{\psi\in\{\sigma.\Theta(\Omega)|\sigma\in G_\Omega} (T-\psi) = \prod_{\psi\in G_\Omega\star\theta} (T-\psi) \tag{3.2}$$

where $\star$ is the action of the Galois group G_Ω on $k(\Omega)$ and $\theta = \Theta(\Omega)$. The polynomials C_{Θ,I_Ω} and M_{Θ,I_Ω} belong to $k[T]$ because the maximal ideal I_Ω is radical (see Chapter 2).

In the same manner:

$$C_{\Theta,I_\Omega^{\mathfrak{S}_n}} = \prod_{\sigma\in\mathfrak{S}_n} (T - \sigma.\Theta(\Omega)) \tag{3.3}$$

LEMMA 3.1. *If Θ is a primitive G_Ω-invariant then $\Theta(\Omega)$ belongs to k.*

PROOF. Let $\theta := \Theta(\Omega)$. By hypothesis $C_{\Theta,I_\Omega} = (T-\theta)^{\mathrm{card}(G_\Omega)} \in k[T]$. As k is a perfect field the proof is finish. □

4. Generators of $I_f^{\mathfrak{S}_n}$ and Cauchy moduli

Recall the historical theorem of Cauchy (see **[17]**):

THEOREM 4.1. *(Cauchy) Soit $F(x_1,\ldots,x_n)$ un polynôme à coefficients dans $\mathcal{R}$ et symétrique en les variables $x_1,\ldots,x_n$. Pour éliminer $x_n,\ldots,x_1$ dans le polynôme F, il suffit de diviser successivement F par les divers termes de la suite*

$$f_1(x_1), f_2(x_2), \ldots, f_n(x_n)\ ,$$

en considérant chaque f_i comme une fonction de x_i. Le dernier reste obtenu sera indépendant de $x_1,\ldots,x_n$ et donnera la valeur $F(\alpha_1,\ldots,\alpha_n)$ en fonction des coefficients de f.

Definition 4.2. The polynomials $f_1(x_1), f_2(x_2), \ldots, f_n(x_n) = f(x_n)$ are called the *Cauchy moduli of the polynomial f.*

Remark 8. The Cauchy moduli are used for efficient computations of resolvents (see Chapter 9).

LEMMA 4.3. *For $0 \leq r < n$, the r-th Cauchy modulus associated with f is given by:*

$$f_r(x_r) = \sum_{i=0}^{r} (-1)^i e_i(\Omega) h_{r-i}(x_r, \ldots, x_n) \qquad . \tag{4.1}$$

In particular $f_n(x_n) = \sum_{i=0}^{n} (-1)^i e_i(\Omega) h_{n-i}(x_n) = f(x_n)$ and $f_1(x_1) = h_1(x_1, \ldots, x_n) - e_1(\Omega)$.

Remark 9. Cauchy gives the formula for $n = 4$.

In modern terms Theorem 4.1 rounds as follows:

THEOREM 4.4. *The set of Cauchy moduli is a reduced Gröbner basis of the ideal $\mathcal{J}_f$ for lexicographic order.*

PROOF. The set of Cauchy moduli is a triangular set, it yields a reduced Gröbner basis for the lexicographic order of the ideal $\mathcal{I}$ it generates. By Cauchy's Theorem $\mathcal{J}_f \subset \mathcal{I}$. Let be the generic polynomial $F(x_1, \ldots, x_n)(x) = \prod_{i=1}^{n}(x - x_i) = x^n - e_1 x^{n-1} + \cdots + (-1)^n e_n$ and set $u_i := e_i - e_i(\Omega)$. Denote by $F_r(x_1, \ldots, x_n)(x)$ the r-th interpolating function of $F(x_1, \ldots, x_n)$. We have $F_r(x_r) = F_r(x_1, \ldots, x_n)(x_r, \ldots, x_n) = 0$ and $F_r(\Omega)(x_r, \ldots, x_n) = f_r(x_r, \ldots, x_n)$. By Lemma 4.3,

$$\begin{aligned} f_r(x_r, \ldots, x_n) &= F_r(\Omega)(x_r, \ldots, x_n) - F_r(x_1, \ldots, x_n)(x_r, \ldots, x_n) \\ &= \sum_{i=0}^{r} (-1)^i u_i h_{r-i}(x_r, \ldots, x_n) \in \mathcal{J}_f \qquad . \end{aligned}$$

Then $\mathcal{I} \subset \mathcal{J}_f$ and the theorem is proved. □

THEOREM 4.5. *Let $\mathcal{J}_f$ be the ideal defined as above then*

$$I_f^{\mathfrak{S}_n} = \sqrt{\mathcal{J}_f}$$

and $I_f^{\mathfrak{S}_n} = \mathcal{J}_f$ if and only if f is separable.

Example 4.6. Let $\overline{f}$ be the square free form of f. Let $g(x) = x - 1 = \overline{f}(x)$ with $f(x) = g(x)^2 = x^2 - 2x + 1$. We have $g(x_1), g(x_2) \in \sqrt{\mathcal{J}_f}$. Setting $u_1 := x_1 + x_2 - 2$ and $u_2 = x_1 x_2 - 1$, the ideal $\mathcal{J}_f$ is given by $\mathcal{J}_f = (u_1, u_2)$ and a Gröbner basis for the lexicographic order is $(f(x_2), \frac{f(x_1) - f(x_2)}{x_1 - x_2}) = (f(x_2), u_1)$ (it is clear that $f(x_2) = -u_2 + x_2 u_1$ is in a Gröbner basis). The reduction of $g(x_1)$ by this Gröbner basis gives: $g(x_1) = 0.f(x_2) + u_1 + (-x_2 + 1) = u_1 + g(x_2)$. Since $g(x_2) \neq 0$, the polynomial $g(x_1)$ is not included in $\mathcal{J}_f$, and similarly $g(x_2) \notin \mathcal{J}_f$. We conclude that $\mathcal{J}_f \neq (u_1, u_2, g(x_1), g(x_2)) \subset \sqrt{\mathcal{J}_f}$.

This example gives a hint for the following proof.

PROOF. The ideal $\mathcal{J}_f$ is included in the ideal $I_f^{\mathfrak{S}_n}$ since its generators are symmetric relations. We have also $V(I_f^{\mathfrak{S}_n}) \subset V(\mathcal{J}_f)$. Now, let $\beta \in V(\mathcal{J}_f)$, then, by definition of varieties, for all $i \in [1, \ldots, n]$ $e_i(\beta) - e_i(\Omega) = 0$. By definition of elementary symmetric functions, we have $\prod_{i=1}^{n}(x - \beta_i) = \prod_{i=1}^{n}(x - \alpha_i)$ so that $\beta \in V(I_f^{\mathfrak{S}_n})$. We have proved

$I_f^{\mathfrak{S}_n} = \sqrt{\mathcal{J}_f}$ because $V(\mathcal{J}_f) = V(I_f^{\mathfrak{S}_n})$. By Yokoyama-Noro-Takeshima Theorem, since $\mathcal{J}_f$ and $I_f^{\mathfrak{S}_n}$ have the same variety we obtain:

$$\sqrt{\mathcal{J}_f} = (\overline{f}(x_1), \ldots, \overline{f}(x_n)) + \mathcal{J}_f = I_f^{\mathfrak{S}_n} \quad .$$

Now, assume that f is a separable polynomial. Then $\overline{f} = f$, and it is sufficient to prove that $f(x_1) \in \mathcal{J}_f$; this is the case by Theorem 4.4. Conversely, assume that f is not separable. We know that if f is not separable we have $\overline{f}(x_1)$ not in $\mathcal{J}_f$, since a triangular Gröbner basis of $\mathcal{J}_f$ contains $f(x_i)$ and $\overline{f}(x_1)$ does not divides $f(x_i)$ for all $i \in [1, n]$. □

Remark 10. Theorem 4.5 gives a simple proof that the set $\{x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} \mid 0 \leq k_i \leq n - i\}$ is a basis of the k-vector-space $k[x_1, \ldots, x_n]/\mathcal{J}_f$. Actually, the monomials of this set are those that are under the staircase of the initials monomials of the Cauchy moduli (for the lexicographic order).

5. Decomposition of the symmetric relations ideal

The results of this section provide from **[6]**.

5.1. Decomposition of variety $V(I_f^{\mathfrak{S}_n})$.

Since the ideal of Ω-relations, I_Ω, is prime (it is maximal), then its variety $V(I_\Omega)$ is irreducible. We suppose that f is separable.

Let $u_1, \ldots, u_n$ be n independent variables and set $F(U, X) := (u_1 x_1 + \cdots + u_n x_n)$.

Definition 5.1. The *fundamental form* $\ominus_V(T, U)$ of a variety V is:

$$\ominus_V(T, U) = \prod_{\beta \in V} (T - F(U, \beta)) \quad .$$

(Note the analogy between the fundamental form and the characteristic polynomial.)

When the polynomial f is separable the respective fundamental forms associated with the symmetric relations ideal and the Ω-relations ideal are given by:

$$\ominus_{V(I_f^{\mathfrak{S}_n})}(T, U) = \prod_{\sigma \in \mathfrak{S}_n} (T - F(U, \sigma \circ \Omega)) \quad \text{and} \tag{5.1}$$

$$\Psi_{V(I_\Omega)}(T, U) = \prod_{\sigma \in G_\Omega} (T - F(U, \sigma \circ \Omega)) \quad . \tag{5.2}$$

PROPOSITION 5.2. *Let $\tau_1, \ldots, \tau_e$ be a right transversal of $\mathfrak{S}_n \mod G_\Omega$. If f is separable, then the factorization of the fundamental form of $V(I_f^{\mathfrak{S}_n})$ into irreducible factors over k is given by:*

$$\ominus_{V(I_f^{\mathfrak{S}_n})} = \prod_{i=1}^{e} \Psi_{V(I_{\tau_i \circ \Omega})} \quad ,$$

Consequently, the decomposition of the variety $V(I_f^{\mathfrak{S}_n})$ into irreducible varieties is:

$$V(I_f^{\mathfrak{S}_n}) = \bigcup_{i=1}^{e} V(I_{\tau_i \circ \Omega}) \qquad . \tag{5.3}$$

PROOF. Set $P_\Omega := \Psi_{V(I_\Omega)}$. For all $\tau \in \mathfrak{S}_n$, we have $\tau G_{\tau\circ\Omega} = G_\Omega \tau$. The definition of fundamental form and Lemma 4.2 imply:

$$\begin{aligned} P_{\tau\circ\Omega} &= \prod_{\sigma \in G_{\tau\circ\Omega}} (T - F(U, \tau\sigma \circ \Omega)) = \prod_{\sigma \in \tau^{-1} G_\Omega \tau} (T - F(U, \tau\sigma \circ \Omega)) \qquad , \\ &= \prod_{\tau\sigma \in G_\Omega \tau\, , \sigma \in \mathfrak{S}_n} (T - F(U, \tau\sigma \circ \Omega)) = \prod_{c \in G_\Omega \tau} (T - F(U, c \circ \Omega)) \qquad . \end{aligned}$$

The fundamental form $P_{\tau\circ\Omega}$ is irreducible over k since each ideal $I_{\tau\circ\Omega}$ is prime.

A direct proof of the decomposition of $V(I_f^{\mathfrak{S}_n})$ is the following:

$$\begin{aligned} \bigcup_{i=1}^{e} V(I_{\tau_i\circ\Omega}) &= \bigcup_{i=1}^{e} \{\tau_i\sigma \circ \Omega \mid \ \sigma \in \tau_i^{-1} G_\Omega \tau_i\} \\ &= \bigcup_{i=1}^{e} \{\tau_i\sigma \circ \Omega \mid \ \tau_i\sigma \in G_\Omega \tau_i\} = V(I_f^{\mathfrak{S}_n}) \qquad . \end{aligned}$$

□

5.2. Decomposition of the ideal $I_f^{\mathfrak{S}_n}$.

The general properties used in this section can be found in the book of P. Samuel and O. Zariski (see [**57**] Chap. III Section 13).

Let $\tau_1, \ldots, \tau_e$ be a right transversal of $\mathfrak{S}_n \mod G_\Omega$.

When our polynomial f is separable, it is clear that the e maximal ideals $I_{\tau_i\circ\Omega}$ are distinct (since their varieties are disjoint) and then the set $\mathcal{A} = \{I_{\tau_1\circ\Omega}, \ldots, I_{\tau_e\circ\Omega}\}$ is pairwise comaximal (see Definition 1.1 Chapter 2).

Decomposition (5.3) of the variety $V(I_f^{\mathfrak{S}_n})$ into irreducible varieties gives the irreducible primary decomposition of the ideal $I_f^{\mathfrak{S}_n}$:

$$I_f^{\mathfrak{S}_n} = \bigcap_{i=1}^{e} I_{\tau_i\circ\Omega} \qquad . \tag{5.4}$$

(The fact that each $I_{\tau_i\circ\Omega}$ is prime gives a new proof that $I_f^{\mathfrak{S}_n}$ equals its radical.) As the set $\mathcal{A}$ is pairwise maximal, identity (5.4) becomes

$$I_f^{\mathfrak{S}_n} = \prod_{i=1}^{e} I_{\tau_i\circ\Omega} \tag{5.5}$$

and for all $l \in \mathbb{N}$ the set $\{I^l_{\tau_1 \circ \Omega}, I_{\tau_2 \circ \Omega} \ldots, I_{\tau_e \circ \Omega}\}$ is also pairwise comaximal and then $I^l_{\tau_1 \circ \Omega}$ is comaximal with $\bigcap_{i=2}^{e} I_{\tau_i \circ \Omega}$ and with $\prod_{i=2}^{e} I_{\tau_i \circ \Omega}$. (Here the notation I^l is the standard notation for a power of an ideal I.)

6. Generators of the ideal I_Ω of Ω-relations

Let $\Omega = (\alpha_1, \ldots, \alpha_n) \in \hat{k}^n$ containing the n roots of the univariate polynomial f.

6.1. Factorizing in successive extensions.

This section sketches the algorithm described in **[61]** (Chapter III) and in **[2]** which computes for the ideal I_Ω a Gröbner basis for the lexicographic order.

We suppose that the polynomial f is separable (its roots are distinct).

Consider the following successive extensions fields of k:

$$k,\ k_n := k(\alpha_n),\ k_{n-1} := k(\alpha_{n-1}, \alpha_n),\ \ldots,\ k_1 := k(\alpha_1, \ldots, \alpha_n) \qquad .$$

We will define recursively the polynomials

$$g_n(x_n), g_{n-1}(x_{n-1}, x_n), \ldots, g_1(x_1, \ldots, x_n)$$

belonging to the ring $k[x_1, \ldots, x_n]$. Let g_n an irreducible factor over k of the polynomial f such that $g_n(\alpha_n) = o$. The polynomial $g_n(x_n)$ is called the *first fundamental modulus of the polynomial* f. The field k_n is k-isomorphic to the field $k[x]/(g_n(x))$. Now, suppose that for some $i \in [1, n-1]$:

1) the polynomials $g_n(x_n), \ldots, g_{i+1}(x_{i+1}, \ldots, x_n)$ are known;

2) the field $k[x_{i+1}, \ldots, x_n]/(g_{i+1}, \ldots, g_n)$ is k-isomorphic to the field k_{i+1} and

3) $g_j(\alpha_j, \ldots, \alpha_n) = 0$ for each $j \in [i+1, n]$.

Let $g_i(x, \alpha_{i+1}, \ldots, \alpha_n)$ be the polynomial which is an irreducible factor of the polynomial $f(x)$ over $k_{i+1}[x]$ such that α_i is one of its roots. The polynomial

$$g_i(x_i, x_{i+1}, \ldots, x_n)$$

is called the *i-th fundamental modulus of the polynomial* f. The field k_i is k-isomorphic to the quotient rings $k[x_i, \ldots, x_n]/(g_i, \ldots, g_n)$.

For $i \in [2, n+1]$, α_{i-1} is a k_i-primitive element of the field k_{i-1} and its minimal polynomial over k_i is the polynomial $g_{i-1}(x, \alpha_i, \ldots, \alpha_n)$.

Remark 11. As soon as all factors are linear, the inductive method for computing the fundamental modulus can be stopped.

The factorizations of the polynomial f over the fields k_i can be replaced by the one of the interpolating functions $f_n(x_n), \ldots, f_1(x_1, \ldots, x_n)$ (see Definition 1.4) over the quotient rings $k[x_i, \ldots, x_n]/(g_i, \ldots, g_n)$. In **[2]** an efficient algorithm for this factorizations is given.

THEOREM 6.1. *The set of the fundamental moduli* $\{g_1(x_1,\ldots,x_n),\ldots,g_n(x_n)\}$ *is a reduced Gröbner basis for the lexicographic order of the ideal of relations* I_Ω. *In particular, we have:*

$$k(\alpha_1,\ldots,\alpha_n) \cong k[x_1,\ldots,x_n]/(g_1,\ldots,g_n) \quad .$$

PROOF. see **[2]**. □

COROLLARY 6.2. $card(G_\Omega) = \prod_{i=1}^{n} deg_{x_i}(g_i)$.

PROOF. Because card(G_Ω) =card($V(I_\Omega)$). □

6.2. Computation of a generating system of the ideal of Ω-relations.

Factorizations in extension fields are very expensive because the degrees depend on the cardinality of the Galois group G_Ω of the polynomial f. It is preferable to determine G_Ω and compute such a Gröbner basis using generating system of the ideal of Ω-relations I_Ω given by the following theorem:

THEOREM 6.3. *(Arnaudiès-Avb) Let* Ω *be an ordered set of roots of a separable univariate polynomial* f *of* $k[x]$. *Let* G_Ω *be the Galois group of* Ω *and let* $\tau_1 \ldots \tau_e$ *be a right transversal of* $\mathfrak{S}_n \mod G_\Omega$. *Set* $J := \bigcup_{i=2}^{e} I_{\tau_i \circ \Omega}$ *and let* $g \in I_\Omega \backslash J$. *Then*

$$\begin{aligned} I_\Omega &= I_\Omega^{\mathfrak{S}_n} + < g > \quad , \\ &= < f_1,\ldots,f_n,g > \quad . \end{aligned}$$

where $f_1,\ldots,f_n$ *are the Cauchy moduli of* f.

PROOF. (see **[6]**) We first prove that the varieties are equal: It is clear that $V(I_\Omega) \subset V(I_\Omega^{\mathfrak{S}_n} + < g >)$. Let $\beta \in V(I_\Omega^{\mathfrak{S}_n} + < g >)$; we have $\beta = \tau \circ \Omega$ and as $g(\tau \circ \Omega) = 0$, the polynomial g vanishes over each irreducible variety $V(I_{\tau\circ\Omega})$ so that $g \in I_{\tau\circ\Omega} = I(V(I_{\tau\circ\Omega}))$. By the choice of g we have $I_{\tau\circ\Omega} = I_\Omega$ so that $\tau \in G_\Omega$. As the varieties of I_Ω and $I_\Omega^{\mathfrak{S}_n} + < g >$ are equal and the ring $k[x_1,\ldots,x_n]$ is Noetherian then there exists $l \in \mathbb{N}$ such that

$$I_\Omega^l \subset I_\Omega^{\mathfrak{S}_n} + < g > \subset I_\Omega \quad .$$

Now since J and I_Ω^l are comaximal (see Section 5.2), there exist $u \in I_\Omega^l$ and $v \in J$ such that $u+v=1$. For $x \in I_\Omega^l$ we have $x = xu + xv$, the polynomial xu is in $I_\Omega^l \subset I_\Omega^{\mathfrak{S}_n} + < g >$ and $xv \in I_\Omega J = \prod_{i=1}^{e} I_{\tau_i\circ\Omega} = \bigcap_{i=1}^{e} I_{\tau_i\circ\Omega} = I_f^{\mathfrak{S}_n} \subset I_\Omega^{\mathfrak{S}_n} + g$ (see Equality (5.5)). □

Example 6.4. Let $\Theta_{G_\Omega} \in k[x_1,\ldots,x_n]$ such that $\mathrm{Stab}_{\mathfrak{S}_n}(\Theta_{G_\Omega}) = G_\Omega$ (i.e. a primitive G_Ω-invariant). Set $\theta := \Theta_{G_\Omega}(\Omega)$; by Lemma 3.1 the algebraic number θ belongs to k. If Θ_{G_Ω} verify $G_\Omega = \{\sigma \in \mathfrak{S}_n) \mid \sigma.\Theta_{G_\Omega}(\Omega) = \theta\}$ (i.e. Θ_{G_Ω} is separable). then the polynomial $R_{G_\Omega} = \Theta_{G_\Omega} - \theta \in k[x_1,\ldots,x_n]$ is convenient for Theorem 6.3.

In Chapter 6 this result is generalized to every ideal I_Ω^L where L is a subgroup of the symmetric group $\mathfrak{S}_n$. More precisely, Chapter 6 describes an inductive method designed to compute a generating system of I_Ω, the ideal of Ω-relations.

CHAPTER 5

Fields and groups

We will suppose in all this chapter that the polynomial f is separable (its roots are pairwise distinct). We set

$$f := \prod_{i=1}^{n}(x - \alpha_i) \in k[x] \qquad \text{where } \alpha_i \in \hat{k}$$

and $\Omega := (\alpha_1, \ldots, \alpha_n) \in \hat{k}^n$.

1. Recalls about ideals and groups

We recall some notations and results providing from previous chapters.
The ideal of Ω-relations is:

$$I_\Omega = \{R \in k[x_1, \ldots, x_n] \mid R(\Omega) = 0\}$$

and the Galois group of Ω over k is:

$$G_\Omega = \{\sigma \in \mathfrak{S}_n \mid \sigma(I_\Omega) = I_\Omega\} \qquad .$$

Put $\underline{X} = (x_1, \ldots, x_n)$. The splitting field $k(\Omega)$ of the polynomial f is k-isomorphic to the quotient ring $k[\underline{X}]/I_\Omega$ by the following k-isomorphism (see Section 2 Chapter 1):

$$\begin{array}{rccc} \Phi \ : & k[\underline{X}]/I_\Omega & \longrightarrow & k(\Omega) \\ & P & \mapsto & P(\Omega) \end{array} \qquad .$$

The Galois group G_Ω acts faithfully on $k(\Omega)$:

$$\begin{array}{rcl} G_\Omega \times k(\Omega) & \longrightarrow & k(\Omega) \\ (\sigma, p) & \mapsto & \sigma \star p := (\sigma.P)(\Omega) \end{array} \qquad ,$$

where $P = \Phi^{-1}(p)$.

The variety of the maximal ideal I_Ω is given by:

$$\begin{array}{rcll} V(I_\Omega) & = & G_\Omega \circ \Omega & \text{and} \\ \text{card}(V(I_\Omega)) & = & \text{card}(G_\Omega) & \end{array}$$

because the polynomial f is separable.

Let $\Theta \in k[\underline{X}]$ and $\theta = \Theta(\Omega)$. The characteristic and minimal polynomials associated with Θ in $k[\underline{X}]/I_\Omega$ and in $k[\underline{X}]/I_\Omega^{\mathfrak{S}_n}$ are the following polynomials of $k[T]$:

$$C_{\Theta,I_\Omega} = \prod_{\sigma\in G_\Omega} (T - \sigma.\Theta(\Omega)) \quad , \tag{1.1}$$

$$M_{\Theta,I_\Omega} = \prod_{\psi\in\{\sigma.\Theta(\Omega)|\sigma\in G_\Omega\}} (T-\psi) = \prod_{\psi\in G_\Omega\star\theta} (T-\psi) \quad \text{and} \tag{1.2}$$

$$C_{\Theta,I_\Omega^{\mathfrak{S}_n}} = \prod_{\sigma\in Sigma_n} (T - \sigma.\Theta(\Omega)) \quad . \tag{1.3}$$

2. Algebraic numbers

Remark 12. If K is a field and L is a finite algebraic extension of K, then L is included in the field $K(\Omega_g)$, where g is the polynomial over K of smaller degree such that the generators of L over K are the roots of g. Thus we can expose the standard results over the fields using the fields between k and $k(\Omega)$. Moreover, as k is a perfect field, all finite extensions of k are separable.

Definition 2.1. Let $\theta \in k(\Omega)$. The *minimal polynomial of θ over k* is the irreducible monic univariate polynomial over k having θ as root. This polynomial will be denoted by $\mathrm{Min}_{\theta,k}$. The roots of $\mathrm{Min}_{\theta,k}$ are called the *conjugates of θ over k*.

LEMMA 2.2. *Let $g \in k[x]$ and θ be a root of g in $\hat{k}$. Then the minimal polynomial of θ over k is a factor of the polynomial g.*

PROOF. Denote by m the minimal polynomial of θ over k. Let h be the monic polynomial of smaller degree having θ as root. There exist two polynomials q and r of $k[x]$ such that $m = hq+r$ with $\deg(r) <\deg(h)$. The polynomial r equals zero because $r(\theta) = 0$. As m is irreducible over k, it equals h. Now, if $g \in k[x]$ such that $g(\theta) = 0$ then the degree of the polynomial m is less than the one of g. Thus $g = qm + r$ where $q, r \in k[x]$ and $\deg(r) <\deg(m)$. As $r(\theta) = 0$ and the degree of m is minimal then $r = 0$. □

Definition 2.3. Let F be an algebraic extension of k. An algebraic number θ is a *k-primitive element of F* if $F = k(\theta)$.

LEMMA 2.4. *An algebraic number θ over k satisfies:*

$$k[\theta] = k(\theta) \cong k[x]/(Min_{\theta,k}(x)) \quad . \tag{2.1}$$

PROOF. Let $m \in k[x]$ be the minimal polynomial of θ over k. The principal ideal (m) is the kernel of the surjective k-morphism:

$$\begin{array}{ccc} k[x] & \longrightarrow & k[\theta] \\ P & \mapsto & P(\theta) \end{array}$$

and as (m) is principal it is maximal in $k[x]$ and $k[x]/(m)$ is a field. □

LEMMA 2.5. *Let $\theta \in k(\Omega)$. The degree of the minimal polynomial of θ over k equals $dim_k k(\theta)$.*

PROOF. Let d be the degree of the minimal polynomial of θ over k. Then $1, x, \ldots, x^{d-1}$ is a k-vector space basis of $k[x]/(\mathrm{Min}_{\theta,k}(x))$. □

3. Minimal polynomials

We show that the minimal polynomial of an algebraic number β of $k(\Omega)$ over k coincides with the minimal polynomial of the endomorphism in $\mathrm{End}(k[\underline{X}]/I_\Omega)$ associated with the image of β by Φ^{-1}.

PROPOSITION 3.1. *Take α a root of the polynomial f and consider g its minimal polynomial over k. Set $I := \{i \in [1, \ldots, n] \mid \alpha_i = \alpha\}$. Then, for each $i \in I$, the polynomial g is the square free form of the characteristic polynomial C_{x_i,I_Ω}. Hence there exists $m \in \mathbb{N}$ such that*

$$g(t)^m = C_{x_i,I_\Omega} \quad \textit{and} \tag{3.1}$$

$$g(t) = \prod_{\beta \in \{\alpha_{\sigma(i)} | \sigma \in G_\Omega\}} (t - \beta) \quad . \tag{3.2}$$

If f is irreducible, then $g = f$ and the integer m equals card$(G_\Omega)/n$.

PROOF. Take $i \in I$. Since C_{x_i,I_Ω} is a polynomial over k and has α_i as a root (G_Ω contains the identity), the minimal polynomial g of α_i is a factor of C_{x_i,I_Ω}. Choose an order of the roots such that $\Omega_g \subset \Omega_{C_{x_i,I_\Omega}} = (\alpha_{\sigma(i)} \mid \sigma \in G_\Omega)$. As g is irreducible and k is perfect the roots of g are distinct. Setting $\hat{g}(x_1, \ldots, x_n) := g(x_i)$ we have $\hat{g}(\Omega) = 0 \Rightarrow (\forall \sigma \in G_\Omega)\ (\sigma.\hat{g})(\Omega) = g(\alpha_{\sigma(i)}) = 0$, by definition of the Galois group G_Ω. This proves that the set $\{\alpha_{\sigma(i)} \mid \sigma \in G_\Omega\}$ is a subset of the distinct roots of g and therefore equals the set of the roots of g. □

Remark 13. Let g_i be the irreducible factor of f having α_i as a root. The polynomial $g_i(x_i)$ belongs to the ideal I_Ω since $g_i(\alpha_i) = g_i(x_i)(\Omega) = 0$ and by the Yokoyama–Noro-Takeshima's Theorem (see Chapter 2), $g_i(x_i) \in I_\Omega$ implies $I_\Omega = \sqrt{I_\Omega}$ and $g_i = M_{x_i,I_\Omega}$.

More generally, we have

THEOREM 3.2. *Let $\Theta \in k[x_1, \ldots, x_n]$ and $\theta = \Theta(\Omega) \in \hat{k}$. Then*

$$M_{\Theta,I_\Omega} = Min_{\theta,k}$$

so that

$$Min_{\theta,k} = \prod_{\psi \in \{\Theta(\sigma \circ \Omega) \mid \sigma \in G_\Omega\}} (T - \psi) = \prod_{\psi \in G_\Omega \star \theta} (T - \psi) \quad .$$

PROOF. Since θ is a roots of M_{Θ,I_Ω}, the set of the roots of the irreducible polynomial $\mathrm{Min}_{k,\theta}$ is a subset of the set of the roots of M_{Θ,I_Ω} which is $\{\Theta(\sigma\circ\Omega) \mid \sigma\in G_\Omega\}$. Now set $P := \mathrm{Min}_{\theta,k}(\Theta)$. We have $P(\Omega) = \mathrm{Min}_{\theta,k}(\Theta(\Omega)) = 0$ and then, by definition of G_Ω, $(\forall\sigma\in G_\Omega)\ 0 = \sigma.P(\Omega) = \mathrm{Min}_{\theta,k}(\Theta(\sigma\circ\Omega))$. Hence $(\forall\sigma\in G_\Omega)\ \sigma.\Theta(\Omega)$ is a root of $\mathrm{Min}_{\theta,k}$ so that the set of roots of $\mathrm{Min}_{\theta,k}$ is $\{\Theta(\sigma\circ\Omega) \mid \sigma\in G_\Omega\}$. As the roots of M_{Θ,I_Ω} are distinct, the theorem is proved. □

COROLLARY 3.3. *Let θ be an algebraic number over k. Then*

$$deg(Min_{\theta,k}) = card(G_\Omega\star\theta) \quad .$$

LEMMA 3.4. *Let $\theta\in k(\Omega)$ and $\Theta = \Phi^{-1}(\theta)\in k[x_1,\ldots,x_n]/I_\Omega$ (then $\theta=\Theta(\Omega)$). The set of conjugates of θ over k equals the set $\{\sigma.\Theta(\Omega)\mid\sigma\in G_\Omega\}$.*

PROOF. See Theorem 3.2. □

4. Primitive element theorem

THEOREM 4.1. *Let K be a field and let L be a separable finite extension of K. Then there exists $\theta\in K$ such that $L = K[\theta]$.*

PROOF. First suppose that the field K is finite. So that L is a finite field and the multiplicative group L^* is cyclic. Any generator of L^* is a K-primitive element of the extension L of K.

Now, suppose that K is infinite. The following proof is that of Lagrange (see **[41]**, Paragraph 100). As the field k is perfect and M is a separable extension of K, we can put $k := K$ and suppose that

$$L = k(\alpha_1,\ldots,\alpha_m)$$

where $m\le n$ and $\Omega = (\alpha_1,\ldots,\alpha_n)$ is the n-tuple of the n distinct roots of the polynomial f of $k[x]$.

Let $H = I_m\times\mathfrak{S}_{n-m}$ and $(\lambda_1,\ldots,\lambda_m)\in k^n$ such that

$$W = \lambda_1x_1+\cdots+\lambda_mx_m$$

is a primitive H-invariant. As the perfect field k is infinite and the polynomial f is separable, the invariant W can be supposed such that the polynomial

$$\mathcal{L}_{W,f} = \prod_{\Psi\in\mathfrak{S}_n.W}(T - Psi(\Omega))$$

is a separable polynomial (it is the absolute resolvent of f by W) (see Section 2 Chapter 3). Put $e := n!/(n-m)!$, the index of the group H in the symmetric group $\mathfrak{S}_n$ which equals the degree of the polynomial $\mathcal{L}_{W,f}$. Choose the order of the orbit $\mathfrak{S}_n.W = \{W_1,\ldots,W_e\}$ such that for $j\in[1,e]$ and $i\in[i_{j-1}+1,i_j]$ (with $i_0=0$ and $i_m=e$)

$$\sigma_i\in\mathfrak{S}_n \ ,\ W_i = \sigma_i.W \ ,\ W_1 = W \quad\text{and}\quad \sigma_i.x_j = x_j \quad .$$

For $j \in [0, e-1]$, denote by A_j the orbit $\mathfrak{S}_n.(W^j x_1)$ of the polynomial $W^j x_1$. As $\mathrm{card}(\mathfrak{S}_n.W) = e$, for $j \in]0, e-1]$

$$\mathrm{card}(A_j) = e$$

and $\mathrm{card}(A_0) = n$. By the fundamental theorem of symmetric functions, for $j \in [0, e-1]$ there exists $\mu_j \in k$ such that

$$\mu_j = \sum_{P \in A_j} P(\Omega) \qquad .$$

Now, let $Y_1, \ldots, Y_{e-1}$ be $e-1$ indeterminated and be the polynomials:

$$F(T, Y) = 1 + Y_1 T + \cdots + Y_{e-1} T^{e-1} \qquad \text{and}$$
$$M(Y) = e/n\mu_1 + \mu_1 Y_1 + \cdots + \mu_{e-1} Y_{e-1} \qquad .$$

We have:

$$\begin{aligned} M(Y) &= \alpha_1 \sum_{j=1}^{i_1} F(W_j(\Omega), Y_1, \ldots, Y_{e-1}) \\ &= \alpha_2 \sum_{j=i_1+1}^{i_2} F(W_j(\Omega), Y_1, \ldots, Y_{e-1}) \\ &\vdots \\ &= \alpha_n \sum_{j=i_{n-1}+1}^{e} F(W_j(\Omega), Y_1, \ldots, Y_{e-1}) \qquad . \end{aligned}$$

By interpolation, there exists $y = (y_1, \ldots, y_{e-1}) \in k^n$ such that the polynomial $F(T, y)$ of degree $e-1$ satisfies the e equations:

$$\begin{aligned} F(W_j(\Omega), y) &= 0 \qquad \text{for } j \in [2, e] \text{ and} \\ F(W(\Omega), y) &\neq 0 \end{aligned}$$

because the determinant $\prod_{1 \leq i < j \leq e} (W_j(\Omega) - W_j(\Omega))$ of the absolute resolvent $\mathcal{L}_{W,f}$ does not equal zero. Thus

$$\alpha_1 = \frac{M(y)}{F(W(\Omega), y)} \qquad .$$

For $\alpha_2, \ldots, \alpha_m$, we choose $x_i W^j$ instead of $x_1 W^j$ for $i \in [2, e]$ and $j \in [0, e-1]$. □

5. Dimension and primitive elements of $k(\Omega)$

We will suppose that the field k is infinite.

Let L be an algebraic extension of k and θ be a k-primitive element of L. Then

$$\dim_k L = \deg(\mathrm{Min}_{\theta,k}) = \mathrm{card}(G_\Omega \star \theta) \qquad . \tag{5.1}$$

Let $(\lambda_1, \ldots, \lambda_n) \in k^n$ such that the polynomial

$$V = \lambda_1 x_1 + \cdots + \lambda_n x_n$$

is a primitive I_n-invariant and the characteristic polynomial $C_{V,I_\Omega^{\mathfrak{S}_n}}$ $(=\mathcal{L}_{V,f})$ is a separable polynomial. Set

$$v := V(\Omega).$$

By the proof of the theorem of the primitive element, the algebraic number v is a k-primitive element of $k(\Omega)$. Thus

$$k(\Omega) = k(v) \cong k[x]/(\mathrm{Min}_{v,k}) \quad . \tag{5.2}$$

As the polynomial f is separable and $\mathrm{card}(G_\Omega \star v) = \mathrm{card}(G_\Omega)$, we have

$$\dim_k(k(\Omega)) = \mathrm{card}(G_\Omega) = \deg(\mathrm{Min}_{v,k}) \quad . \tag{5.3}$$

Remark 14. We also can use another arguments. As the ideal I_Ω is radical the dimension $\dim_k(k(\Omega)) = \dim_k k[x_1, \ldots, x_n]/I_\Omega$ equals the cardinality of the variety $V(I_\Omega)$. Thus, since the polynomial f is separable:

$$\dim_k k(\Omega) = \mathrm{card}(G_\Omega) \quad . \tag{5.4}$$

Let V, as above. As

$$\dim_k k(v) = \mathrm{card}(G_\Omega)$$

and $v \in k(\Omega)$ we have

$$k(v) = k(\Omega) \quad .$$

Thus the algebraic number v is a k-primitive element of $k(\Omega)$.

LEMMA 5.1. *Let V and v be as above. Then*

$$C_{V,I_\Omega} = M_{V,I_\Omega} = Min_{v,k} \quad .$$

PROOF. First proof. The set of roots of C_{V,I_Ω} is $S := \{\sigma.V(\Omega) \mid \sigma \in G_\Omega\}$. As V is invariant only by the identity and $C_{V,I_\Omega^{\mathfrak{S}_n}}$ is separable, all roots of C_{V,I_Ω} are distinct and $C_{V,I_\Omega} = M_{V,I_\Omega}$ and $M_{V,I_\Omega} = \mathrm{Min}_{v,k}$ by Theorem 3.2.

Second proof. (Without using Theorem 3.2) The set of roots of $\mathrm{Min}_{v,k}$ contains the elements $R := (\sigma.V(\Omega) \mid \sigma \in G_\Omega)$ because $\mathrm{Min}_{v,k}(V) \in I_\Omega$ and the variety of I_Ω is $G_\Omega \circ \Omega$. As V is invariant only by the identity and $C_{V,I_\Omega^{\mathfrak{S}_n}}$ is separable, all elements of R are distinct. As $\mathrm{card}(R) = \mathrm{card}(G_\Omega)$ equals the degree of $\mathrm{Min}_{v,k}$, the set R equals the set of the roots of $\mathrm{Min}_{v,k}$. It is also the set of the roots of C_{V,I_Ω} (see Identity 3.1 Chapter 4). □

THEOREM 5.2. *Suppose that the polynomial f is separable. An algebraic number θ is a k-primitive element of the extension field $k(\Omega)$ of k if and only if its minimal polynomial over k is given by:*

$$Min_{\theta,k}(T) = \prod_{\sigma \in G_\Omega} (T - \sigma.\Theta(\Omega)) = C_{\Theta,I_\Omega}(T) \quad , \tag{5.5}$$

where $\Theta = \Phi^{-1}(\theta)$.

PROOF. Let θ be a primitive element of the splitting field $k(\Omega)$ of f and v as above. First, as $v \in k(\Omega)$, it can be written $v = g(\theta)$ where g is an univariate polynomial with coefficients in k so that, by definition of G_Ω, $(\forall \sigma \in G_\Omega)\ \sigma.V(\Omega) = g(\sigma.\Theta(\Omega))$. Second, if C_{Θ,I_Ω} is not separable then $\sigma.\Theta(\Omega) = \sigma'.\Theta(\Omega)$ for some σ and σ' two distinct permutations in G_Ω. Consequently $\sigma.V(\Omega) = \sigma'.V(\Omega)$ which is impossible because V is chosen such that C_{V,I_Ω} is separable. We have proved that the characteristic polynomial C_{Θ,I_Ω} is separable; thus

$$C_{\Theta,I_\Omega} = M_{\Theta,I_\Omega} = \mathrm{Min}_{\theta,k} \quad .$$

Conversely, if $\mathrm{Min}_{\theta,k} = C_{\Theta,I_\Omega}$ then θ is a primitive element of the extension field $k(\Omega)$ of k since the degree of its minimal polynomial over k equals $\mathrm{card}(G_\Omega)$ the degree of the extension field $k(\Omega)$ of k and $\theta \in k(\Omega)$. □

6. Results of Galois

We prove the historical result of E. Galois (see **[32]**):

"*Il existe un groupe de substitutions tel que toute fonction des racines dont les substitutions n'altèrent pas les valeurs numériques, soit rationnellement exprimable et réciproquement.*"

We will suppose that the field k is infinite.

Now we consider a polynomial V of $k[x_1, \ldots, x_n]$ such that $\mathrm{Stab}_{\mathfrak{S}_n}(V)$ is the identity group and such that $C_{V,I_\Omega^{\mathfrak{S}_n}}$ is a separable polynomial (see Section 5). Set $v := V(\Omega)$ which is a k-primitive element of the field $k(\Omega)$.

Notation 6.1. For $u \in k(\Omega)$ and $U = \Phi^{-1}(u) \in k[x_1, \ldots, x_n]/I_\Omega$ we denote by R_u the polynomial of $k[T]$ such that $u = R_u(v)$ and its degree is strictly less than the degree of $\mathrm{Min}_{v,k}$. We have

$$u = U(\Omega) = R_u(V(\Omega)) \quad .$$

LEMMA 6.2. *(Galois) Let $v \in k(\Omega)$ as above and $u \in k(\Omega)$. The condition*

$$u = R_u(V(\Omega)) \in k$$

is equivalent to

$$(\forall g \in G_\Omega)\ \ R_u(V(g \circ \Omega)) = R_u(V(\Omega)) = u \quad .$$

PROOF. We prove this lemma using only the subset H of $\mathfrak{S}_n$ such that the set of conjugates of v is the set $\{\sigma.V(\Omega) \mid \sigma \in H\}$. (We omit that $H = G_\Omega$ by Lemma 3.4.) Let d be the degree of $\mathrm{Min}_{v,k}$. Set $R := R_u$ and

$$W(t) := R(t) - R(V(\Omega))$$

which is a univariate polynomial of $k(\Omega)[t]$. Now suppose that $(\forall h \in H)\ R(V(h \circ \Omega)) = R(V(\Omega)) = u$; then $W(h.V(\Omega)) = 0$. Since f is separable, the polynomial W whose degree is strictly less than d, has at least d distinct roots. The polynomial W is obviously zero

so that $u = R(V(\Omega)) = R(1) \in k$. Conversely if $u \in k$ then $W \in k[t]$. As $V(\Omega)$ is a root of $W \in k[t]$, the polynomial W has the same roots as $\mathrm{Min}_{v,k}$ (since it is irreducible) and therefore $(\forall h \in H)\ R(V(h \circ \Omega)) = R(V(\Omega)) = u$. In order to finish, as $H = G_\Omega$, the lemma is proved. □

Remark 15. Part of Lemma 6.2 has been proved by Galois as follows: let $\theta \in k$; if $(\forall h \in H)\ R_\theta(V(h \circ \Omega)) = R_\theta(V(\Omega))$ then

$$R(V(\Omega)) = \prod_{\tau \in H} P(\tau.V(\Omega))/\mathrm{card}(H) \in k$$

by the fundamental theorem of symmetric functions.

Remark 16. We know that $H = G_\Omega$ by the essential equality $M_{V,I_\Omega} = \mathrm{Min}_{v,k}$.

THEOREM 6.3. *(Galois) Let $u \in k(\Omega)$. We have $u \in k$ if and only if $(\forall \sigma \in G_\Omega)$ $\sigma \star u = u$.*

PROOF. Let $U = \Phi^{-1}(u)$; we have $\sigma \star u = \sigma.U(\Omega)$. If $\sigma \in G_\Omega$ then $R_u(V(\Omega)) = U(\Omega)$ is equivalent to $R_u(V(\sigma \circ \Omega)) = U(\sigma \circ \Omega)$. Thus, by Lemma 6.2, $u = U(\Omega) \in k$ if and only if $(\forall \sigma \in G_\Omega)\ \sigma.U(\Omega) = U(\Omega) = u$. □

7. Galois extensions and automorphism groups

In this section the polynomial f is supposed to be separable (its roots are pairwise distinct).

we will prove that the action $\star$ of G_Ω over $k(\Omega)$ is the same as that of the group $\mathrm{Aut}_k(k(\Omega))$ of the k-automophisms over $k(\Omega)$.

Notation 7.1. The group of the k-automorphisms of an algebraic extension field E of k is denoted by $\mathrm{Aut}_k(E)$.

Consider the k-automorphism:

$$\begin{array}{rccc} \Phi\ :\ k[x_1,\ldots,x_n]/I_\Omega & \longrightarrow & k(\Omega) \\ P & \mapsto & P(\Omega) \end{array}$$

and for $\sigma \in \mathfrak{S}_n$, define the k-automorphism Ψ_σ by

$$\begin{array}{rccc} \Psi_\sigma\ :\ k[x_1,\ldots,x_n] & \longrightarrow & k[x_1,\ldots,x_n] \\ P & \mapsto & \sigma.P \quad . \end{array}$$

LEMMA 7.2. *Let $\sigma \in G_\Omega$. Then the morphism $\tilde{\Psi}_\sigma$, defined by:*

$$\begin{array}{rccc} \tilde{\Psi}_\sigma\ :\ k[x_1,\ldots,x_n]/I_\Omega & \longrightarrow & k[x_1,\ldots,x_n]/I_\Omega \\ P & \mapsto & \sigma.P \quad , \end{array}$$

is a k-automorphism. Consequently the morphism $\Phi\tilde{\Psi}_\sigma\Phi^{-1}$ is a k-automorphism of $k(\Omega)$ which satisfies $\Phi\tilde{\Psi}_\sigma\Phi^{-1}(\alpha_i) = \alpha_{\sigma(i)}$.

PROOF. As the Galois group G_Ω is the decomposition group of I_Ω, the condition $\sigma \in G_\Omega$ is equivalent to $\sigma(I_\Omega) = I_\Omega$. Hence the k-automorphism Ψ_σ induces the k-automorphism $\tilde{\Psi}_\sigma$ of $k[x_1, \ldots, x_n]/I_\Omega$. □

Notation 7.3. We denote by ϕ_σ the k-automorphism $\Phi\tilde{\Psi}_\sigma\Phi^{-1}$.

LEMMA 7.4. *Set $\Omega := (\alpha_1, \ldots, \alpha_n)$. If $\phi \in Aut_k(k(\Omega))$ then there exists $\sigma \in \mathfrak{S}_n$ such that $\phi(\alpha_i) = \alpha_{\sigma(i)}$ for $i \in [1, n]$. The k-automorphism ϕ will be denoted by ϕ_σ.*

PROOF. For $i \in [1, n]$ we have $\phi(e_i(\Omega)) = e_i(\Omega) \in k$ where e_i is the i-th elementary symmetric function (see Definition 1.2 Chapter 4). Thus

$$\prod_{i=1}^{n}(x - \phi(\alpha_i)) = f(x) = \prod_{i=1}^{n}(x - \alpha_i) \qquad .$$

□

THEOREM 7.5. *Set $\Omega := (\alpha_1, \ldots, \alpha_n)$. The group $Aut_k(k(\Omega))$ of the k-automorphisms of $k(\Omega)$ is isomorphic to the Galois group G_Ω of f by:*

$$\begin{array}{ccc} G_\Omega & \longrightarrow & Aut_k(k(\Omega)) \\ \sigma & \mapsto & \phi_\sigma \end{array} \qquad ,$$

where $\phi_\sigma(\alpha_i) = \alpha_{\sigma(i)}$ for $i \in [1, n]$.

If $r \in k(\Omega)$ and $R = \Phi^{-1}(r)$ (i.e. $R(\Omega) = r$) then

$$\forall\, \sigma \in G_\Omega \qquad \phi_\sigma(r) = R(\sigma \circ \Omega) = \sigma \star r \qquad . \tag{7.1}$$

PROOF. If $\phi \in \mathrm{Aut}_k(k(\Omega))$, then by Lemma 7.4, there exists $\sigma \in \mathfrak{S}_n$ such that $\phi = \phi_\sigma$. For this σ and for any $R \in I_\Omega$ we have $\sigma.R(\Omega) = r(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = R(\phi(\alpha_1), \ldots, \phi(\alpha_n)) = \phi(R(\alpha_1, \ldots, \alpha_n)) = \phi(0) = 0$, since ϕ is a k-automorphism of $k(\Omega)$ and $R \in I_\Omega$. Then $\phi = \phi_\sigma$ with $\sigma \in G_\Omega$. Conversely if $\sigma \in G_\Omega$, by Lemma 7.2, ϕ_σ is a k-automorphism of $k(\Omega)$. As $\phi_\sigma \in \mathrm{Aut}_k(k(\Omega))$, we have $\phi_\sigma(r) = \phi_\sigma(R(\Omega)) = R(\phi_\sigma(\alpha_1), \ldots, \phi_\sigma(\alpha_n)) = R(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = R(\sigma \circ \Omega) = \sigma \star r$. □

Remark 17. By Theorem 7.5, when $\sigma \in G_\Omega$ it is possible to write $\phi_\sigma.R(\Omega)$ or $\sigma(r)$ instead of $\phi_\sigma(R(\Omega))$. This convention is strictly reserved to the elements of the Galois group of f.

We give the standard definition of Galois groups of field extensions:

Definition 7.6. (**Galois group**) When an algebraic extension E of a field K is the splitting field of a polynomial with coefficients in K, E is said a *normal extension of K*. If, moreover, the extension E is separable then E is said *a Galois extension of K*, the group $\mathrm{Aut}_K(E)$ is denoted by $\mathrm{Gal}_K(E)$ and is called the *Galois group of the extension E over K*.

Remark 18. When K is perfect, E is always separable.

Definition 7.7. Let E be a Galois extension of a field K and g be a polynomial of $K[x]$ such that the field E is the splitting field of g. The Galois group of E over K is said the *Galois group of* g and is denoted by $\mathrm{Gal}_K(g)$.

Theorem 7.5 indicates that if E is a Galois extension of a field K, which is the splitting field of an univariate polynomial g with coefficients in K, then, for each ordered set Ω_g of the roots of g, the Galois group $\mathrm{Gal}_K(E)$ is isomorphic to the Galois group G_{Ω_g} associated with the Ω_g-relations ideal $I_{\Omega_g} = \{R \in K[x_1, \ldots, x_n] \mid \ R(\Omega_g) = 0\}$.

Remark 19. A k-automorphism is completely defined by a unique element of $B(\Omega, \Omega)$, the set of bijections of Ω in Ω.We have

$$I_\Omega = I_f^{\mathfrak{S}_n}$$

if and only if each element of $B(\Omega, \Omega)$ defines an element of $\mathrm{Aut}_k(k(\Omega))$. This means that if there exists a relation among the roots of f which is not symmetric then some bijection in $B(\Omega, \Omega)$ does not define a k-automorphism of $k(\Omega)$.

Example 7.8. Set $f := (x-1)(x-j)(x-j^2) = x^3 - 1$. Set $\Omega := (1, j, j^2)$. The Cauchy moduli of f are: $f_1 = x_3 + x_2 + x_1, f_2 = x_3^2 + x_2x_3 + x_2^2, f_3 = x_3^3 - 1$. The polynomial $R = x_2^2 - x_3$ is an Ω-relation. The remainder of the division of R by $f(x_2)$ is $-x_3^2 - x_2x_3 - x_3$. As this remainder depends on x_2, the Ω-relation R is not symmetric and therefore the Galois group of f is not $\mathfrak{S}_3$. Actually, it is obvious that the Galois group of f is $\mathfrak{S}_1 \times \mathfrak{S}_2$.

LEMMA 7.9. *Let E be a normal extension of a field K, then all minimal polynomials of elements of E split into linear factors in E.*

PROOF. (due to M. Artin) By hypothesis, there exists a polynomial $g \in K[x]$ such that $E = K(\Omega_g)$, where Ω_g is an ordered set of the roots of g. Let $\theta \in E$. Then there exists $\Theta \in k[x_1, \ldots, x_n]$ such that $\theta = \Theta(\Omega_g)$. The coefficients of the polynomial

$$C(T) = \prod_{\sigma \in \mathfrak{S}_n} (T - \sigma.\Theta(\Omega_g))$$

belong to the field K by the fundamental theorem of symmetric functions and its roots belong to E. Thus the minimal polynomial of θ over the field K is a factor of the polynomial C and its roots belong to E. □

8. Galois duality

We refer also to Arnaudiès-Bertin's or Artin's books for Galois duality and other results on the fields (see **[5]** and **[11]**).

We take K a Galois extension of k. Recall that $\Omega \in \hat{k}^n$ contains the n roots of the univariate polynomial f of $k[x]$.

Notation 8.1. Let H be a subgroup of the k-automorphisms group of K. The set of the elements of K which are H-invariant is a subfield of K. We will denote it by $\mathrm{Inv}_K(H)$:

$$\mathrm{Inv}_K(H) = \{P \in K \mid (\forall \phi \in H)\ \phi(P) = P\} \quad .$$

Notation 8.2. Let H be a subgroup of the Galois group G_Ω. The subfield of $k(\Omega)$ of elements invariant by H is denoted by $k(\Omega)^H$:

$$k(\Omega)^H = \{r \in k(\Omega) \mid (\forall \sigma \in H)\ \sigma \star r = r\} \quad .$$

If H is a subgroup of G_Ω and H' its image in $\mathrm{Gal}_k(k(\Omega))$ (see Theorem 7.5). We have:

$$\mathrm{Inv}_{k(\Omega)}(H') = k(\Omega)^H \quad .$$

THEOREM 8.3. *(Galois duality) Suppose that K is a Galois extension of k. We have*

(1) *Let E be an extension of k in K. Then there exists a subgroup H of $Gal_k(K)$ such that $E = Inv_K(H)$.*

(2) *Let H be a subgroup of the Galois group $Gal_k(K)$. Then $k \subset Inv_K(H) \subset K$.*

PROOF. Set $G := \mathrm{Gal}_k(K) = \mathrm{Aut}_k(K)$.

(1) K is a Galois extension of E because it is one of k. Therefore, by Theorem 6.3, $E = \mathrm{Inv}_K(H)$, where $H = \mathrm{Aut}_E(K) = \mathrm{Gal}_E(K)$. Now, as $k \subset E$, the group $\mathrm{Aut}_E(K)$ is a subgroup of $\mathrm{Aut}_k(K)$ (i.e. each E-automorphism is trivially a k-automorphism).

(2) Let H be a subgroup of G. We choose a polynomial f such that $K = k(\Omega)$, where Ω is a set of roots of f. By the isomorphism between $\mathrm{Aut}_k(k(\Omega))$ and G_Ω, H can be view as a subgroup of G_Ω and $k(\Omega)^H \subset k(\Omega)$. Let $u \in k$; as $(\forall \sigma \in G_\Omega)$ we have $\sigma \star u = u$, it is true in particular for all $\tau \in H$. Thus $k \subset k(\Omega)^H$. □

LEMMA 8.4. *Let f be a polynomial of $k[x]$. Let H be a subgroup of G_{Ω_f} and let $E = k(\Omega_f)^H$. Let θ be a k-primitive element of E: $E = k(\theta)$. We have:*
(i) $H = \{\sigma \in G_{\Omega_f} \mid \sigma \star \theta = \theta\}$;
(ii) the minimal polynomial of θ over k is given by:

$$Min_{\theta,k} = \prod_{i=1}^{e} (T - \tau_i \star \theta) \quad , \tag{8.1}$$

where $\tau_1, \ldots, \tau_e$ is a left transversal of $G_{\Omega_f} \mod H$;
(iii) the degree of the extension field E over k is the index of H in G_{Ω_f}.

PROOF. *(i)* We have $u \in E$ if and only if $(\forall \sigma \in H)\ \sigma \star u = u$ and $\sigma \in H$ if and only if $(\forall u \in E)\ \sigma \star u = u$. Let $\sigma \in H$ such that $\sigma \star \theta = \theta$. For each $u \in E$ there exists a polynomial $P \in k[x]$ such that $u = P(\theta)$. Thus $\sigma \star u = \sigma \star P(\theta) = P(\sigma \star \theta) = P(\theta) = u$, and $\sigma \in H$.
(ii) We have

$$\mathrm{Min}_{\theta,k} = \prod_{\phi \in G_{\Omega_f} \star \theta} (T - \phi) \quad .$$

Let $\tau_1, \ldots, \tau_e$ be a left transversal of $G_\Omega \mod H$. For all $i, j \in [1, e]$ we have $\tau_i h \star \theta = \tau_i \star \theta$ and $\tau_i \star \theta = \tau_j \star \theta$ is equivalent to $\tau_j^{-1}\tau_i \in H$ because $\tau_j^{-1} \in G_{\Omega_f}$ and by (i). We have the result because $\tau_j^{-1}\tau_i \in H$ if and only if $\tau_i = \tau_j$.
(iii) The degree of an algebraic extension extension over k is the one of the minimal polynomial over k of its k-primitive elements. □

COROLLARY 8.5. *Let H and L be two subgroups of $Gal_k(K)$ such that $H \subset L$. Then the degree of the extension field $Inv_K(H)$ of $Inv_K(L)$ equals the $[L : H]$, the index of H in L. If θ is an $Inv_K(L)$-primitive polynomial of the field $Inv_K(H)$ then:*

$$Min_{\theta,k} = \prod_{i=1}^{e} (T - \tau_i \star \theta) \qquad , \tag{8.2}$$

where $\tau_1, \ldots, \tau_e$ is a left transversal of $L \mod H$.

PROOF. Let Ω be the set of the roots of an univariate polynomial such that $K = k(\Omega)$. As K also is a Galois extension of $\mathrm{Inv}_K(L)$, we can use Lemma 8.4 with L instead of $\mathrm{Gal}_k(K)$ (or G_Ω) and $\mathrm{Inv}_K(L)$ instead of $k = \mathrm{Inv}_K(\mathrm{Gal}_k(K))$. □

THEOREM 8.6. *Suppose that K is a Galois extension of k. Let H be a subgroup of $Gal_k(K)$ and let $E = Inv_K(H)$. Then*

(a) E is a Galois extension of k if and only if H is a normal subgroup of $Gal_k(K)$;

(b) in this case the Galois group of the extension field E/k is isomorphic to the group $Gal_k(K)/H$.

PROOF. As K is a Galois extension of k, there exists a separable polynomial $f \in k[x]$ such that $K = k(\Omega)$, where Ω is a set of the distinct roots of f. Let θ be a k-primitive element of E.

(a) the field E is a Galois extension of k if and only if $(\forall \tau \in G_\Omega)\ \tau \star \theta \in E$. This is equivalent to $(\forall \tau \in G_\Omega)\ (\forall \sigma \in H)\ \sigma\tau \star \theta = \tau \star \theta$. As $\tau^{-1} \in G_\Omega$, this is equivalent to $(\forall \tau \in G_\Omega)\ (\forall \sigma \in H)\ \tau^{-1}\sigma\tau \star \theta = \theta$, which in turn is equivalent to $(\forall \tau \in G_\Omega)\ (\forall \sigma \in H)$ $\tau^{-1}\sigma\tau \in H$ because θ is a k-primitive element (see (i) of Lemma 8.4). Thus E is a Galois extension if and only if H is a normal subgroup of G_Ω.

(b) As H is a normal subgroup of G_Ω, then the set of left cosets of $G_\Omega \mod H$ is the group denoted by G_Ω/H. Thus, by (ii) of Lemma 8.4, we have:

$$\mathrm{Min}_{\theta,k} = \prod_{\tau \in G_\Omega/H} (T - \tau \star \theta) \qquad . \tag{8.3}$$

But as θ is a k-primitive element of E which is also the splitting field of its minimal polynomial, the Galois group of $\mathrm{Min}_{\theta,k}$ is isomorphic to G_Ω/H by Theorem 5.2. □

9. Invariants and fields

Definition 9.1. Put $K = k(\Omega)$. Let $\theta \in K$ and L, H be two subgroups of G_Ω such that $H \subset L$. If $H = \mathrm{Stab}_L(\theta)$ then θ is said an *L-primitive H-invariant for Ω*.

Applying the definition with $k(x_1, \ldots, x_n)^{\mathfrak{S}_n}$ instead of k and $\Omega = (x_1, \ldots, x_n)$ (i.e $G_\Omega = \mathfrak{S}_n$), an L-primitive H-invariant for Ω is an L-primitive H-invariant.

Let L and H be two subgroups of G_Ω such that $H \subset L$. If $\Theta \in k[x_1, \ldots, x_n]$ is an L-primitive H-invariant separable for Ω (see Section 2 Chapter 3) then $\Theta(\Omega)$ is an L-primitive H-invariant for Ω.

THEOREM 9.2. *Let L and H be two subgroups of G_Ω such that $H \subset L$. An algebraic number $\theta \in k(\Omega)$ is an L-primitive H-invariant for Ω if and only if θ is a primitive element of the field extension $k(\Omega)^H$ over $k(\Omega)^L$.*

PROOF. Let $\tau_1, \ldots, \tau_e$ be a left transversal of $L \mod H$. If $\theta \in k(\Omega)$ is an L-primitive H-invariant for Ω then $\theta \in k(\Omega)^H$ and the conjugates of θ over $k(\Omega)^L$ are the distinct elements of $L\star\theta$ by Galois theory. This conjugates are the e elements $\tau_i\star\theta$, $i \in [1, n]$. Thus θ is a primitive element of the field extension $k(\Omega)^H$ over $k(\Omega)^L$ because $e = [L : H]$ equals the degree of the extension $k(\Omega)^H$ of the field $k(\Omega)^L$. Conversely, if the conjugates of an element θ of $k(\Omega)^H$ are the e distinct elements $\tau_i \star \theta$, $i \in [1, n]$ then $\mathrm{Stab}_L(\theta) = H$. □

COROLLARY 9.3. *Let $K = k(x_1, \ldots, x_n)^{\mathfrak{S}_n}$ and let Θ be an L-primitive H-invariant. The minimal polynomial of Θ over the field $K_L := K(x_1, \ldots, x_n)^L$ is the L-relative resolvent by Θ, denoted by $\mathcal{L}^L_\Theta$, and*

$$Min_{\Theta, K_L} = \mathcal{L}^L_\Theta = \prod_{i=1}^{e} (x - \sigma_i.\Theta) \in K(x_1, \ldots, x_n)^L[x] \qquad , \tag{9.1}$$

where $\sigma_1, \ldots, \sigma_e$ is a left transversal of L mod H.

PROOF. See the proof of Theorem 9.2 : we have $\mathrm{Min}_{\Theta, K_L} = \mathcal{L}^L_\Theta$, by definition of generic resolvents (see Definition 5.6 of Chapter 6). □

CHAPTER 6

Ideals and groups

We take $f \in k[x]$ a polynomial of degree n and $\Omega \in \hat{k}^n$ containing the n roots of the polynomial f.

For L be a subset of the symmetric group $\mathfrak{S}_n$, the ideal of L-invariant Ω-relations is given by

$$I_\Omega^L \quad = \quad \{R \in k[x_1, \ldots, x_n] \ \mid \ (\forall \sigma \in L)\ \sigma.R(\Omega) = 0\} \qquad .$$

LEMMA 0.4. *The ideal I_Ω^L is radical: $I_\Omega^L = \sqrt{I_\Omega^L}$.*

PROOF. First Proof. Let $n \in \mathbb{N}$ and $P \in k[x_1, \ldots, x_n]$ such that $P^n \in I_\Omega^L$. Let $\sigma \in L$; then $(\sigma.P^n) = (\sigma.P)^n$ and $0 = (\sigma.P)^n(\Omega) = (\sigma.P(\Omega))^n$. Since k is a field we have $\sigma.P(\Omega) = 0$ and then $P \in I_\Omega^L$.

Second Proof. See Example 2.8 Chapter 2. □

1. First inclusions

LEMMA 1.1. *If L contains the identity then*

$$I_\Omega^L \subset I_\Omega \qquad .$$

LEMMA 1.2. *Let H and L be two subsets of $\mathfrak{S}_n$ such that $H \subset L$. Then $I_\Omega^L \subset I_\Omega^H$.*

PROOF. Let $R \in I_\Omega^L$. If $H \subset L$ and $\sigma.R \in I_\Omega$ for all $\sigma \in L$ then $\sigma.R \in I_\Omega$. This occurs in particular for all $\sigma \in H$ and therefore $R \in I_\Omega^H$. □

Remark 20. The converse of Lemma 1.2 is not always true.

We have $I_\Omega^{\mathfrak{S}_n} \neq I_\Omega$ when there exists $\sigma \in \mathfrak{S}_n$ such that $I_\Omega \neq I_{\sigma\circ\Omega}$. The following proposition gives links between $I_{\sigma\circ\Omega}$ and I_Ω.

PROPOSITION 1.3. *Let σ be a permutation in $\mathfrak{S}_n$ and let L be a subset of $\mathfrak{S}_n$, we have:*

$$(i) \qquad I_{\sigma\circ\Omega}^L = I_\Omega^{\sigma L} \qquad ,$$

$$(ii) \qquad I_\Omega^{\mathfrak{S}_n} \subset I_\Omega^L \qquad ,$$

$$(iii) \qquad I_{\sigma\circ\Omega}^{\mathfrak{S}_n} = I_\Omega^{\mathfrak{S}_n} \text{ and}$$

$$(iv) \quad \text{if } L \text{ contains the identity then } I_\Omega^{\sigma L} = I_{\sigma\circ\Omega}^L \subset I_{\sigma\circ\Omega} \qquad .$$

PROOF. (i) Let $R \in k[x_1, \ldots, x_n]$. We have $R \in I_{\sigma\circ\Omega}^{\sigma^{-1}L}$ if and only if for all $l \in L$ then $l.R(\Omega) = \sigma^{-1}l.R(\sigma \circ \Omega) = 0$. The other relations are trivial. □

Remark 21. The previous proposition shows that the ideal of symmetric relations $I_\Omega^{\mathfrak{S}_n} = I_f^{\mathfrak{S}_n}$ does not depend on the choice of the order of the roots of f.

2. The stabilizer and the decomposition group

LEMMA 2.1. *A subset of $\mathfrak{S}_n$ stable by composition is a group.*

LEMMA 2.2. *Let I be an ideal of $k[x_1, \ldots, x_n]$ and H be the following set of permutations:*

$$H := \{\sigma \in \mathfrak{S}_n \mid \sigma(I) \subset I\} \quad .$$

Then H is a group and $H = \{\sigma \in \mathfrak{S}_n \mid \sigma(I) = I\}$. In particular, the Galois group G_Ω is actually a group.

PROOF. For σ, $\tau \in H$ $\tau\sigma \in H$ since $\tau\sigma.I \subset \tau.I \subset I$. Then H is a stable by composition and, by Lemma 2.1, it is a group. □

LEMMA 2.3. *Let $\mathcal{H}$ be a set of subsets of $\mathfrak{S}_n$, then*

$$I_\Omega^{\bigcup_{H\in\mathcal{H}} H} = \bigcap_{H\in\mathcal{H}} I_\Omega^H \quad . \tag{2.1}$$

PROOF.

$$\begin{aligned} P \in I_\Omega^{\bigcup_{H\in\mathcal{H}} H} &\Leftrightarrow (\forall \sigma \in \bigcup_{H\in\mathcal{H}} H)\ \sigma.P(\Omega) = 0 \\ &\Leftrightarrow (\forall H \in \mathcal{H})\ (\forall \sigma \in H)\ \sigma.P(\Omega) = 0 \\ &\Leftrightarrow P \in \bigcap_{H\in\mathcal{H}} I_\Omega^H \quad . \end{aligned}$$

□

Let $E_L = \{H \in \mathfrak{S}_n \mid I_\Omega^H = I_\Omega^L\}$. Then by Lemma 2.3 the largest element of E_L exists and equals the set $\bigcup_{H\in E_L} H$.

Definition 2.4. Let L be a set of permutations. The *stabilizer of the ideal* I_Ω^L, denoted by $\mathrm{Max}(I_\Omega^L)$, is the largest subset of $\mathfrak{S}_n$ satisfying:

$$I_\Omega^L = I_\Omega^{\mathrm{Max}(I_\Omega^L)} \quad . \tag{2.2}$$

Definition 2.5. The *decomposition group*, $\mathrm{Gr}(I)$, *of an ideal* $I \subset k[x_1, \ldots, x_n]$ is defined by:

$$\mathrm{Gr}(I) = \{\sigma \in \mathfrak{S}_n \mid \sigma(I) = I\} \quad . \tag{2.3}$$

PROPOSITION 2.6. *Let L be a subgroup of $\mathfrak{S}_n$. Then*

$$L \subset Gr(I_\Omega^L) \quad \textit{and obviously} \tag{2.4}$$

$$I_\Omega^{Gr(I_\Omega^L)} \subset I_\Omega^L \quad . \tag{2.5}$$

PROOF. In order to prove (2.4), suppose that $\tau \in L$ and $R \in I_\Omega^L$. By Lemma 2.2, it is sufficient to prove that $\tau(I_\Omega^L) \subset I_\Omega^L$. For all $\sigma \in L$ $\sigma\tau.R \in I_\Omega$ since $\sigma\tau \in L$. Thus $\tau.R \in I_\Omega^L$ (i.e. $\tau \in \mathrm{Gr}(I_\Omega^L)$). □

The stabilizer $\mathrm{Max}(I_\Omega^L)$ is not necessarily a group. Further, Proposition 3.9 of Chapter 7 gives necessary and sufficient conditions for which $\mathrm{Max}(I_\Omega^L)$ is a group. At this step, we have:

LEMMA 2.7.

$$G_\Omega = Max(I_\Omega) = Gr(I_\Omega) \qquad and \tag{2.6}$$

$$\mathfrak{S}_n = Max(I_\Omega^{\mathfrak{S}_n}) = Gr(I_\Omega^{\mathfrak{S}_n}) \quad . \tag{2.7}$$

The ideals I_Ω and $I_\Omega^{\mathfrak{S}_n}$ are equal if and only if $G_\Omega = \mathfrak{S}_n$.

PROOF. Obvious. □

But what happens for other subgroups of $\mathfrak{S}_n$?

PROPOSITION 2.8. *Let I be an ideal of $k[x_1, \ldots, x_n]$. If $I \subset I_\Omega$ then*

$$I \subset I_\Omega^{Gr(I)} \tag{2.8}$$

and in particular if $I = I_\Omega^L$, where L is a subgroup of $\mathfrak{S}_n$, then

$$I = I_\Omega^L = I_\Omega^{Gr(I)} = I_\Omega^{Max(I)} \tag{2.9}$$

and $L \subset Gr(I) \subset Max(I)$. Moreover, if $Max(I_\Omega^L)$ is a group then $Gr(I_\Omega^L) = Max(I_\Omega^L)$.

PROOF. First, take $R \in k[x_1, \ldots, x_n]$. If $R \in I$ then, by definition of the decomposition group, $(\forall \sigma \in \mathrm{Gr}(I))$ we have $\sigma.R \in I \subset I_\Omega$ and finally $R \in I_\Omega^{\mathrm{Gr}(I)}$. Now, let L be a subgroup of $\mathfrak{S}_n$ and set $I := I_\Omega^L \subset I_\Omega$ (since L contains the identity). By the inclusion (2.8), $I_\Omega^L \subset I_\Omega^{\mathrm{Gr}(I_\Omega^L)}$.Conversely, since L is stable by composition, by Proposition 2.6 the group L is a subgroup of $\mathrm{Gr}(I_\Omega^L)$ and then $I_\Omega^{\mathrm{Gr}(I_\Omega^L)} \subset I_\Omega^L$ by Lemma 1.2. Now if $\mathrm{Max}(I)$ is a group, then Proposition 2.6, applied with $\mathrm{Max}(I)$ instead of L, gives $\mathrm{Max}(I) \subset \mathrm{Gr}(I)$, and by definition of $\mathrm{Max}(I)$ and using (2.9) the inverse inclusion is proved. □

The Galois group depends on the choice of Ω for the set of the roots of f:

PROPOSITION 2.9. *Let $\tau \in \mathfrak{S}_n$, the Galois group of $\tau \circ \Omega$ is given by:*

$$G_{\tau\circ\Omega} = \tau^{-1} G_\Omega \tau \quad , \tag{2.10}$$

$$G_{\tau\circ\Omega} = \{\sigma \in \mathfrak{S}_n \mid (\forall P \in I_{\tau\circ\Omega}) \ P(\tau\sigma \circ \Omega) = 0\} \quad . \tag{2.11}$$

PROOF. Set $G := G_\Omega$. We have $\tau \in \sigma^{-1} G \sigma$ if and only if $\sigma\tau\sigma^{-1} \in G$. Let $\tau \in \sigma^{-1} G \sigma$ and $R \in I_{\sigma\circ\Omega}$. We have $\sigma.R(\Omega) = 0$ and then $\sigma.R \in I_\Omega$. Since $\sigma\tau\sigma^{-1} \in G$, we have $0 = (\sigma\tau\sigma^{-1})\sigma.R(\Omega) = \sigma\tau.R(\Omega) = \tau.R(\sigma \circ \Omega)$ and then $\tau \in G_{\sigma\circ\Omega}$. Conversely suppose that $\tau \in G_{\sigma\circ\Omega}$. Let $R \in I_\Omega$ then $\sigma.(\sigma^{-1}.R)(\Omega) = 0$ and since $\tau \in G_{\sigma\circ\Omega}$, we have $0 = \tau.(\sigma^{-1}.R)(\sigma \circ \Omega) = \sigma\tau\sigma^{-1}.R(\Omega)$ and then $\tau \in \sigma^{-1} G \sigma$. Prove identity (2.11): by

definition of $G_{\tau\circ\Omega}$ we have $G_{\tau\circ\Omega} = \{\sigma \in \mathfrak{S}_n \mid (\forall P \in I_{\tau\circ\Omega}) \ (\sigma.P)(\tau \circ \Omega) = 0\}$ and the result follows from Lemma 1.2. □

At present it is possible to give a partial correspondence between groups and ideals; it will be completed in Theorem 3.7:

THEOREM 2.10. *If L and H are two subsets of $\mathfrak{S}_n$ we have:*

$$\text{if } H \subset L \quad \text{then} \quad I_\Omega^L \subset I_\Omega^H \qquad \text{and} \tag{2.12}$$

$$\text{if } I_\Omega^L \subset I_\Omega^H \quad \text{then} \quad Max(I_\Omega^H) \subset Max(I_\Omega^L) \qquad . \tag{2.13}$$

PROOF. Equation (2.12) provide from Lemma 1.2. Now, let $\sigma \in \mathrm{Max}(I_\Omega^H)$ and $R \in I_\Omega^L$. We will prove (2.13). By hypothesis $R \in\subset I_\Omega^H$. Thus $\sigma.R(\Omega) = 0$ and $\sigma \in \mathrm{Max}(I_\Omega^L)$ by definition of $\mathrm{Max}(I_\Omega^L)$. □

Remark 22. We have $H \subset \mathrm{Max}(I_\Omega^L)$ if, and only if, $\mathrm{Max}(I_\Omega^H) \subset \mathrm{Max}(I_\Omega^L)$.

COROLLARY 2.11. *Let H be a subset of $\mathfrak{S}_n$ which contains the identity. If $H \subset G_\Omega$ then*

$$I_\Omega^H = I_\Omega = I_\Omega^{G_\Omega} \qquad , \tag{2.14}$$

$$Max(I_\Omega^H) = Gr(I_\Omega^H) = G_\Omega. \tag{2.15}$$

If H is a group and $Gr(I_\Omega^H) = G_\Omega$ then $H \subset G_\Omega$.

PROOF. As H contains the identity, then $I_\Omega^H \subset I_\Omega = I_\Omega^{I_n}$. If $H \subset G_\Omega$ then $I_\Omega = I_\Omega^{G_\Omega} \subset I_\Omega^H$ and therefore $I_\Omega^H = I_\Omega = I_\Omega^{G_\Omega}$. If $H \neq G_\Omega$ then $H \neq G_\Omega = \mathrm{Max}(I_\Omega^H) = \mathrm{Gr}(I_\Omega^H)$. Now, suppose that H is a group and $\mathrm{Gr}(I_\Omega^H) = G_\Omega$. Then by Proposition 2.6 $H \subset \mathrm{Gr}(I_\Omega^H) = G_\Omega$. □

Remark 23. Corollary 2.11 gives an example in which $\mathrm{Max}(I_\Omega^H) \neq H \neq \mathrm{Gr}(I_\Omega^H)$.

3. Identification of the stabilizer and primitive polynomials of ideals

We suppose that the field k is infinite.

We start with the following standard result (see, for example **[60]**):

LEMMA 3.1. *Let M be a subgroup of $\mathfrak{S}_n$ such that $G_\Omega \subset M$, L a subgroup of M and Θ_L be an M-primitive L-invariant. We have the following:*
(i) if $G_\Omega \subset L$ then $\Theta_L(\Omega) \in k$;
(ii) if $\Theta_L(\Omega) \in k$ and if Θ_L is M-separable for Ω then $G_\Omega \subset L$.

PROOF. *(i)* holds because the minimal polynomial M_{Θ,I_Ω} which belongs to $k[T]$ equals $T - \Theta_L$.
(ii). If $\theta = \Theta_L(\Omega) \in k$ then $R_L := \Theta_L - \theta \in I_\Omega^L \subset I_\Omega$ since L contains the identity. Let $\sigma \in G_\Omega$ such that $\sigma \notin L$; then $\sigma.R_L(\Omega) = \sigma.\Theta_L - \theta \neq 0$, since $\sigma \in M$ and Θ is M-separable for Ω. Thus $R_L \notin I_\Omega^{G_\Omega} = I_\Omega$. □

Remark 24. If one of hypothesis of *i* or *ii* of Lemma 3.1 is valid then $L = \mathrm{Max}(I_\Omega^L)$. Because, when k is infinite, we always can choose a separable primitive L-invariant Θ_L and the polynomial $R_L := \Theta_L - \Theta_L(\Omega)$ belongs to the ideal I_Ω^L.

But what can we say in case in which G_Ω is not contained in L ? The following sheds some light on this general situation.

LEMMA 3.2. *Let M be a subgroup of $\mathfrak{S}_n$ and let H be a subset of $\mathfrak{S}_n$. Suppose that $G_\Omega \subset M$. Then there exists $R_M \in I_\Omega^M$ such that $R_M \in I_\Omega^H$ if and only if $H \subset M$.*

PROOF. Pick Θ_M a separable primitive M-invariant which exists (see Lemma 2.3 Chapter 3). By hypothesis, the polynomial $R_M = \Theta_M - \Theta_M(\Omega)$ belongs to $k[x_1, \ldots, x_n]$. Let $\sigma \in \mathfrak{S}_n$, if $\sigma \notin M$ then $\sigma.\Theta_M \neq \Theta_M$ and $\sigma.\Theta_M(\Omega) \neq \Theta_M(\Omega)$ since Θ_M is separable. □

PROPOSITION 3.3. *Let M be a subgroup of $\mathfrak{S}_n$ such that $G_\Omega \subset M$ and let H be a subset of $\mathfrak{S}_n$.*
(i) If $I_\Omega^M \subset I_\Omega^H$ then $H \subset Max(I_\Omega^H) \subset M$.
(ii) If, moreover, H is a subgroup of $\mathfrak{S}_n$ then $Gr(I_\Omega^H) \subset M$.

PROOF. It is sufficient to prove $H \subset M$ since $I_\Omega^H = I_\Omega^{\mathrm{Max}(I_\Omega^H)}$ and if H is a subgroup of $\mathfrak{S}_n$: $I_\Omega^H = I_\Omega^{\mathrm{Gr}(I_\Omega^H)}$. Let R_M be as in Lemma 3.2. By hypothesis, $R_M \in I_\Omega^H$ so that $H \subset M$. □

Let $\Theta \in k[x_1, \ldots, x_n]$ and $\theta := \Theta(\Omega)$. Recall the expression of the minimal polynomial M_{Θ, I_Ω} of the endomorphism $\hat{\Theta}$ of $k[x_1, \ldots, x_n]/I_\Omega$:

$$M_{\Theta, I_\Omega} = \prod_{\phi \in G_\Omega \star \theta} (T - \phi) = \prod_{\phi \in \{\tau.\Theta(\Omega) | \tau \in G_\Omega\}} (T - \phi) \quad . \tag{3.1}$$

By Theorem 3.2 Chapter 5 we have:

$$\mathrm{Min}_{\theta,k} = M_{\Theta, I_\Omega} \quad .$$

THEOREM 3.4. *Let L and M be two subgroups of $\mathfrak{S}_n$ such that L and G_Ω are included in M. Let Θ be an M-primitive L-invariant separable for Ω. Put $R_{L,M} := M_{\Theta, I_\Omega}(\Theta)$. Then the polynomial $R_{L,M}$ satisfies the following:*

a) $R_{L,M} \in I_\Omega^L$;

b) $G_\Omega L = \{\sigma \in M \mid \sigma.R_{L,M}(\Omega) = 0\}$;

PROOF. a) For $\sigma \in L$, as Θ is a primitive L-invariant we have:

$$\sigma.R_{L,M} = M_{\Theta, I_\Omega}(\sigma.\Theta) = M_{\Theta, I_\Omega}(\Theta) = R_{L,M} \quad .$$

Therefore, $\sigma.R_{L,M}(\Omega) = M_{\Theta, I_\Omega}(\Theta(\Omega)) = 0$.

b) Put $A := \{\sigma \in M \mid \ \sigma.R_{L,M}(\Omega) = 0\}$. By (3.1),

$$\begin{aligned} A &= \{\sigma \in M \mid \ (\exists\, \tau \in G_\Omega)\ \sigma.\Theta(\Omega) = \tau.\Theta(\Omega)\} \\ &= \{\sigma \in M \mid \ (\exists\, \tau \in G_\Omega)\ \tau^{-1}\sigma.\Theta(\Omega) = \Theta(\Omega)\} \end{aligned}$$

since $\tau^{-1} \in G_\Omega$. Eventually, as Θ is M-separable for Ω and $\tau^{-1}\sigma \in M$,

$$A = \{\sigma \in M \mid \ (\exists\, \tau \in G_\Omega)\ \tau^{-1}\sigma \in L\} = G_\Omega L \qquad .$$

□

COROLLARY 3.5. *The stabilizer is given by*

$$Max(I_\Omega^L) = G_\Omega L \qquad .$$

PROOF. Let $r \in I_\Omega^L$, $\tau \in G_\Omega$ and $l \in L$. Since $l.r \in I_\Omega$ and by definition of G_Ω, $\tau.(l.r) \in I_\Omega$ and by consequence $\tau l \in \mathrm{Max}(I_\Omega^L)$. Conversely, let $\sigma \in \mathrm{Max}(I_\Omega^L)$. By Proposition 3.3 $\mathrm{Max}(I_\Omega^L) \subset M$. By a) of Theorem 3.4, $\sigma.R_{L,M}(\Theta)(\Omega) = 0$. Finally, by b) of Theorem 3.4, we have $\sigma \in G_\Omega L$. □

Theorem 3.4 and Corollary 3.5 prove that there exists a polynomial $R_{L,M}$ which characterizes the ideal I_Ω^L.

Definition 3.6. Let M and L be two subgroups of $\mathfrak{S}_n$ such that $L \subset M$ and M contains the Galois group G_Ω. A polynomial F satisfying

$$G_\Omega L = \{\sigma \in M \mid \ \ \sigma.F(\Omega) = 0\}$$

is called an *M-primitive polynomial of the ideal I_Ω^L*. In case $M = \mathfrak{S}_n$, the polynomial F will be called a *primitive polynomial of the ideal I_Ω^L*.

When k is infinite, the polynomial $R_{L,M}$ of Theorem 3.4 is an M-primitive polynomial of the ideal I_Ω^L.

This following theorem is the same correspondence given in Theorem 2.10:

THEOREM 3.7 (Correspondence between Stabilizers and Ideals). *Under the same hypothesis of Theorem 3.4 and if H a subgroup of the symmetric group $\mathfrak{S}_n$, then*

$$H \subset G_\Omega L \qquad \textit{if and only if} \qquad I_\Omega^L \subset I_\Omega^H.$$

Note that $H \subset G_\Omega L$ if and only if $G_\Omega H \subset G_\Omega L$.

The decomposition group of an ideal is not necessary equal to the maximal set $G_\Omega L$. It is so case when $G_\Omega \subset \mathrm{Gr}(I_\Omega^L)$ and L is a group because $L \subset \mathrm{Gr}(I_\Omega^L)$. The following proposition gives a condition for which equality holds:

PROPOSITION 3.8. *Let L be a subgroup of $\mathfrak{S}_n$. If L is contained in the normalizer of G_Ω in $\mathfrak{S}_n$ then $G_\Omega \subset Gr(I_\Omega^L)$ and consequently $Max(I_\Omega^L) = G_\Omega L$ is a group equal to $Gr(I_\Omega^L)$.*

PROOF. Suppose that L is as in the hypothesis of Proposition 3.8. Let $\sigma \in G_\Omega$, $r \in I_\Omega^L$; we prove that $\sigma.r \in I_\Omega^L$. For $l \in L$ we have $l.(\sigma.r) = l\sigma.r = \sigma' l.r$, where $\sigma' \in G_\Omega$ because L is included in the normalizer of $G_\Omega \in \mathfrak{S}_n$. We have $l.r(\Omega) = 0$ and the definition of the Galois group G_Ω gives $0 = \sigma'.(l.r)(\Omega) = l.(\sigma.r(\Omega))$. The first assertion is proved.

When L is group the decomposition group $\mathrm{Gr}(I_\Omega^L)$ is always included in $\mathrm{Max}(I_\Omega^L) = G_\Omega L$. By hypothesis, G_Ω and L are contained in $\mathrm{Gr}(I_\Omega^L)$, which is a group, $G_\Omega L$ is in turn contained in $\mathrm{Gr}(I_\Omega^L)$. □

The following proposition gives necessary and sufficient conditions in which $G_\Omega L$ is a group:

PROPOSITION 3.9. *There exists a group G such that $I_\Omega^G = I_\Omega^L$ and G contains the Galois group G_Ω if, and only if, one of the following equivalent conditions is satisfied:*
(i) $G_\Omega L$ is a group ;
(ii) $LG_\Omega \subset G_\Omega L$; (this holds under the hypothesis of Proposition 3.8 of Chapter 6);
(iii) $Gr(I_\Omega^L) = G_\Omega L$;
(iv) $G_\Omega \subset Gr(I_\Omega^L)$.
In particular, G_Ω is a subgroup of the decomposition group $Gr(I_\Omega^L)$ when G_Ω is a subgroup of L.

PROOF. As $\mathrm{Gr}(I_\Omega^L)$ contains all subgroup G such that $I_\Omega^G = I_\Omega^L$, the hypothesis of the proposition is equivalent to *(iv)*.

We must prove that *(i)* is equivalent to *(ii)*. If *(i)* holds then the group $G_\Omega L$ is stable under composition and contains G_Ω: we have $(G_\Omega L)G_\Omega \subset G_\Omega L$ and as G_Ω is a group then $LG_\Omega \subset G_\Omega L$ and *(ii)* holds. Now, suppose that *(ii)* holds; then $(G_\Omega L)(G_\Omega L) \subset G_\Omega(G_\Omega L)L \subset G_\Omega L$. We are left with proving that *(iv)* implies *(iii)*, the equality between the decomposition group and the stabilizer of the ideal I_Ω^L. As $L \subset \mathrm{Gr}(I_\Omega^L)$, $G_\Omega L \subset G_\Omega \mathrm{Gr}(I_\Omega^L) = \mathrm{Gr}(I_\Omega^L)$, when *(iv)* holds. If L is a group then we always have $\mathrm{Gr}(I_\Omega^L) \subset \mathrm{Max}(I_\Omega^L) = G_\Omega L$. The other equivalences holds (see Proposition 2.8 Chapter 6). □

COROLLARY 3.10. *If a subgroup H of $\mathfrak{S}_n$ contains the Galois group G_Ω then*

$$G_\Omega H = Gr(I_\Omega^H) = H \ .$$

4. Varieties

In Chapter 4 the following is proved:

$$V(I_f^{\mathfrak{S}_n}) = \{\sigma \circ \Omega \mid \sigma \in \mathfrak{S}_n\} = \mathfrak{S}_n \circ \Omega \qquad , \tag{4.1}$$

PROPOSITION 4.1. *Let L be a subset of $\mathfrak{S}_n$. The variety in $k(\Omega)^n$ of its associated ideal is given by:*

$$V(I_\Omega^L) = \{\sigma \circ \Omega \mid \sigma \in Max(I_\Omega^L)\} = Max(I_\Omega^L) \circ \Omega = G_\Omega L \circ \Omega \qquad , \tag{4.2}$$

the $G_\Omega L$-orbit of Ω. In particular

$$V(I_\Omega) = \{\sigma \circ \Omega \mid \sigma \in G_\Omega\} = G_\Omega \circ \Omega \qquad . \tag{4.3}$$

PROOF. Let $\beta \in V(I_\Omega^L)$. Then $\beta = \sigma \circ \Omega$, where $\sigma \in \mathfrak{S}_n$, since $V(I_\Omega^L) \subset V(I_\Omega^{\mathfrak{S}_n})$. Let $\sigma \in \mathfrak{S}_n$. By definition of $\mathrm{Max}(I_\Omega^L)$, the condition $(\forall P \in I_\Omega^L)\ \sigma.P(\Omega) = 0$ is equivalent to $\sigma \in \mathrm{Max}(I_\Omega^L)$. □

The variety of the ideals $I_{\tau\circ\Omega}$ where $\tau \in \mathfrak{S}_n$ is given by:

LEMMA 4.2. *For $\tau \in \mathfrak{S}_n$*

$$V(I_{\tau\circ\Omega}) \;=\; \{\tau\sigma \circ \Omega \;\mid\; \sigma \in G_{\tau\circ\Omega}\} = \{\sigma \circ \Omega \;\mid\; \sigma \in G_\Omega\tau\} = G_\Omega\tau \circ \Omega \qquad ,$$

where $G_\Omega\tau \circ \Omega$ is the orbit of Ω under the action of $G_\Omega\tau$.

PROOF. The variety $V(I_\Omega)$ is given in Proposition 4.1. Now $\sigma \in G_\Omega \Leftrightarrow \forall P \in I_\Omega\ \sigma.P(\Omega) = 0 \Leftrightarrow \sigma \circ \Omega \in V(I_\Omega^{G_\Omega})$. Now, by definition $V(I_{\tau\circ\Omega}) = \{\rho \circ \Omega \mid \rho \in \mathfrak{S}_n \text{ and } \forall P \in I_{\tau\circ\Omega}\ P(\rho \circ \Omega) = 0\}$. Let $\sigma_\rho \in \mathfrak{S}_n$ such that $\rho = \tau\sigma_\rho$, we have $V(I_{\tau\circ\Omega}) = \{\tau\sigma_\rho \circ \Omega \mid \sigma_\rho \in \mathfrak{S}_n \text{ and } \forall P \in I_{\tau\circ\Omega}\ P(\tau\sigma_\rho \circ \Omega) = 0\}$. By Proposition 2.9 and Equality (2.11) the lemma is proved. □

5. Endomorphism of the quotient ring $k[x_1, \ldots, x_n]/I_\Omega^L$

In this section, L is supposed a subset of $\mathfrak{S}_n$.

5.1. Characteristic and minimal polynomials.

We refer to notations and definitions of Chapter 2. For L a subset of $\mathfrak{S}_n$, we set

$$A_{I_\Omega^L} := k[x_1, \ldots, x_n]/I_\Omega^L \qquad .$$

PROPOSITION 5.1. *Take $\Theta \in k[x_1, \ldots, x_n]$. Let the endomorphism $\hat{\Theta} \in End(A_{I_\Omega^L})$ associated with Θ. The characteristic polynomial of $\hat{\Theta}$ is given by:*

$$\begin{aligned} C_{\Theta,I_\Omega^L} &= \prod_{\sigma\circ\Omega \in Max(I_\Omega^L)\circ\Omega} (T - \Theta(\sigma \circ \Omega)) \\ &= \prod_{\sigma \in G_\Omega L} (T - \sigma.\Theta(\Omega)) \qquad \textit{because } f \textit{ is separable.} \end{aligned} \tag{5.1}$$

The minimal polynomial of $\hat{\Theta}$ is given by:

$$\begin{aligned} M_{\Theta,I_\Omega^L} = SF_{\Theta,I_\Omega^L} &= \prod_{\psi \in \{\sigma.\Theta(\Omega) \mid \sigma \in Max(I_\Omega^L)\}} (T - \psi) = \\ &= \prod_{\psi \in \{\sigma.\Theta(\Omega) \mid \sigma \in G_\Omega^L\}} (T - \psi) \qquad . \end{aligned} \tag{5.2}$$

PROOF. This is because the ideal I_Ω^L is radical (see Lemmas 2.1 and 2.7 Chapter 2) and $V(I_\Omega^L) = \mathrm{Max}(I_\Omega^L) \circ \Omega$. □

LEMMA 5.2. *Let L be a subgroup of $\mathfrak{S}_n$ and $\Psi \in k[x_1,\ldots,x_n]$ such that $L.\Psi = \{\Psi\}$. Then the minimal polynomials of Ψ relative to I_Ω^L and of $\psi = \Psi(\Omega)$ over k are equal:*

$$M_{\Psi,I_\Omega^L} = M_{\Psi,I_\Omega} = Min_{\psi,k} = \prod_{\phi \in G_\Omega \star \psi} (T - \phi) \quad . \tag{5.3}$$

PROOF. Obvious. □

Remark 25. We have seen that, by linear algebra and since k is perfect, this two above polynomials belong to $k[T]$. However, this also follows from the fact that their coefficients are invariant under the Galois group G_Ω.

LEMMA 5.3. *Let L be a subgroup of $\mathfrak{S}_n$. If $G_\Omega \subset L$ then $L = Max(I_\Omega^L) \circ \Omega$.*

PROOF. Let Θ_L be a separable primitive L-invariant. If $G_\Omega \subset L$ then $G_\Omega.\Theta_L = \{\Theta_L\}$. The minimal polynomial M_{Θ_L,I_Ω} belongs to $k[T]$ and equals $T - \Theta_L(\Omega)$. Thus $\Theta_L(\Omega) \in k$ and the polynomial $\Theta_L - \Theta_L(\Omega)$ belongs to I_Ω^L. By the separability of Θ_L we have $L = \mathrm{Max}(I_\Omega^L)$. □

Suppose that there exists methods for testing if a group contains the Galois group. By the previous theorem we know that, if L is a subgroup containing the Galois group G_Ω, we have all elements for computing the characteristic polynomial C_{Θ,I_Ω^L}. But, if the Galois group is not known it is not possible to compute the minimal polynomial M_{Θ,I_Ω^L} for any polynomial Θ.

The following lemma shows that we need compute a characteristic polynomial for testing the inclusion of G_Ω in a group.

LEMMA 5.4. *Suppose that there exists a known group L containing the Galois group G_Ω (by example $L = \mathfrak{S}_n$) and a group H. Let Θ_H be an L-primitive H-invariant. Then*

(i) If $G_\Omega \subset H$ then $\Theta_H(\Omega) \in k$.

(ii) If Θ_H is L-separable for Ω and $\Theta_H(\Omega) \in k$ then $G_\Omega \subset H$.

The H-invariant Θ_H is L-separable for Ω if the multiplicity of the root $\Theta_H(\Omega)$ of C_{Θ,I_Ω^L} equals card(H).

PROOF. *(i)* See Proof of Lemma 5.3 or by Galois Theorem (see Theorem 6.3 Chapter 5).

(ii) If Θ_H is L-separable for Ω and $\Theta_H(\Omega) \in k$ then $H = \mathrm{Max}(I_\Omega^H)$ (see proof of Lemma 5.3). As H is a group, then $I_\Omega^H \subset I_\Omega$ so that $G_\Omega \subset \mathrm{Max}(I_\Omega^H)$.
For the test of the separability, see Lemma 5.5. □

LEMMA 5.5. *Let be a group L containing the Galois group G_Ω (by example $L = \mathfrak{S}_n$) and a group H. Let Θ_H be an L-primitive H-invariant. Then*

$$C_{\Theta,I_\Omega^L} = \prod_{i=1}^{e}(T - \tau_i.\Theta_H(\Omega))^{card(H)} = \prod_{\Psi\in L.\Theta}(T - \Psi(\Omega))^{card(H)}$$

where $\tau_1, \ldots, \tau_e$ is a left transversal of $l \mod H$. Moreover, for $i \in [1, e]$, the polynomial $\tau_i.\Theta_H$ is an L-primitive $\tau_i H \tau_i^{-1}$-invariant.

PROOF. Exercise. □

Lemma 5.5 and Lemma 5.4 give the following informations:
- If the characteristic polynomial C_{Θ_H,I_Ω^L} has a linear simple factor then a conjugate of H in L contains the Galois group;
- It is sufficient to compute the following polynomial of $k[T]$ (because k is a perfect field):

$$\prod_{\Psi\in L.\Theta}(T - \Psi(\Omega)) \qquad .$$

This previous polynomial is called the Lagrange resolvent. When a characteristic polynomial can be computed, it is possible to compute a Lagrange resolvent and not necessary a minimal polynomial.

5.2. Resolvents.

The resolvent was introduced by Lagrange in [**41**]. In this section is given a new presentation of this fundamental tool of Galois theory.

Take $\Theta \in k[x_1, \ldots, x_n]$ and L a subgroup of $\mathfrak{S}_n$. Set $K := k(x_1, \ldots, x_n)^{\mathfrak{S}_n}$.
The standard definition of the generic resolvent is the following:

Definition 5.6. The *L-relative resolvent by* Θ is the univariate polynomial $\mathcal{L}_\Theta^L$ defined by:

$$\mathcal{L}_\Theta^L(T) = \prod_{\Psi\in L.\Theta}(T - \Psi) \qquad , \tag{5.4}$$

Remark 26. The generic resolvent $\mathcal{L}_\Theta^L$ is the minimal polynomial of Θ over the field $K(x_1, \ldots, x_n)^L$ because L is the Galois group of the extension field $K(x_1, \ldots, x_n)$ of $K(x_1, \ldots, x_n)^L$. (See also Section 9 Chapter 5.)

PROPOSITION 5.7. *Let H be a subgroup of L. The L-relative resolvent by Θ belongs to the field $K(x_1, \ldots, x_n)^L[x]$ and if Θ is an L-primitive H-invariant then the L-relative resolvent by Θ satisfies:*

$$\mathcal{L}_\Theta^L(T) = \prod_{i=1}^{e}(T - \sigma_i.\Theta) \qquad , \tag{5.5}$$

where $\sigma_1, \ldots, \sigma_e$ is a left transversal of L mod H.

PROOF. Exercise. □

Definition 5.8. The *resolvent by* Θ *associated with the ideal* I_Ω^L is the univariate polynomial $\mathcal{L}_{\Theta,I_\Omega^L}$ defined by:

$$\mathcal{L}_{\Theta,I_\Omega^L} = \prod_{\Psi\in \mathrm{Max}(I_\Omega^L).\Theta} (T-\Psi(\Omega)) \qquad . \tag{5.6}$$

Remark 27. If the group L contains the Galois group then the invariant Θ is L-separable for Ω if, and only if, $\Theta(\Omega)$ is a simple root of the resolvent $\mathcal{L}_{\Theta,I_\Omega^L}$.

LEMMA 5.9. *Let the group* H=$Stab_{Max(I_\Omega^L)}(\Theta)$ *which is the stabilizer of* Θ *on the stabilizer of the ideal* I_Ω^L. *Set* d =*card(H). Then*

$$C_{\Theta,I_\Omega^L} = \mathcal{L}^d_{\Theta,I_\Omega^L} \tag{5.7}$$

and $\mathcal{L}_{\Theta,I_\Omega^L} \subset k[T]$.

PROOF. The set H is a group because it is finite and is stable by composition. The equality is obvious. The resolvent belongs to $k[T]$ because k is a perfect field. □

LEMMA 5.10. *If the resolvent* $\mathcal{L}_{\Theta,I_\Omega^L}$ *is a separable polynomial then it equals the minimal polynomial* M_{Θ,I_Ω^L}.

PROOF. Because M_{Θ,I_Ω^L} is the square free form of the characteristic polynomial (the ideal I_Ω^L is radical and k is a perfect field). □

PROPOSITION 5.11. *Assume that the stabilizer* $Max(I_\Omega^L)$ *is a group and choose* L *such that* $L = Max(I_\Omega^L)$. *Let* $H = Stab_L(\Theta)$ *(i.e. the polynomial* Θ *is an* L*-primitive* H*-invariant). We have:*

$$\mathcal{L}_{\Theta,I_\Omega^L} = \prod_{i=1}^{l} (T-\sigma_i.\Theta(\Omega)) \qquad , \tag{5.8}$$

where $\sigma_1,\ldots,\sigma_l$ *is a left transversal of* $L \mod H$.

PROOF. See Proposition 5.7. □

Definition 5.12. The resolvent $\mathcal{L}_{\Theta,I_f^{\mathfrak{S}_n}}$, which were introduced by Lagrange, is called the *absolute resolvent of* f *by* Θ. We will denote it by $\mathcal{L}_{\Theta,f}$. When $L = \mathfrak{S}_{n_1}\times\cdots\times\mathfrak{S}_{n_d}$ is a product of symmetric groups, the resolvent $\mathcal{L}_{\Theta,I_\Omega^L}$ is called the *absolute multi-resolvent of* Ω *by* Θ.

The multi-resolvents has been introduced in **[35]**. They are used for reducible polynomials (see Chapter 8).

Notation 5.13. Suppose that $f = f_1\cdots f_d$ where f_i is a polynomial of $k[x]$ of degree $n_i > 0$ for $i \in [1,d]$. Set $L := \mathfrak{S}_{n_1}\times\cdots\times\mathfrak{S}_{n_d}$. The absolute multi-resolvent $\mathcal{L}_{\Theta,I_\Omega^L}$ is denoted by $\mathcal{L}_{\Theta,(f_1,\ldots,f_d)}$.

Remark 28. For all $i \in [1,n]$,

$$\mathcal{L}_{x_i,I_\Omega^{\mathfrak{S}_n}} = f(T) \qquad \text{so that} \tag{5.9}$$

$$M_{x_i,I_\Omega^{\mathfrak{S}_n}} = SF_{x_i,I_\Omega^{\mathfrak{S}_n}} = \overline{f}(T) \qquad , \tag{5.10}$$

where $\overline{f}$ is the square free form of f.

5.3. Examples of resolvents.

Example 5.14. Let V be a $\mathfrak{S}_n$-primitive I_n-invariant. The absolute resolvent $\mathcal{L}_{V,f}$ is called a *Galois resolvent* of the polynomial f. Galois used it for proving the existence of the Galois group (see **[32]**). We can choose:

$$\begin{aligned} V &= x_1 + 2x_2 + \cdots (n-1)x_{n-1} \qquad \text{or} \\ V &= x_1 x_2^2 \cdots x_{n-1}^{n-1} \qquad . \end{aligned}$$

Example 5.15. Let $\mathcal{D}_4$ be the dihedral subgroup of $\mathfrak{S}_4$ whose $\Psi = x_1x_2 + x_3x_4$ is a $\mathfrak{S}_4$-primitive $\mathcal{D}_4$-invariant. The resolvent

$$\mathcal{L}_{\Psi,f} = (T - (\alpha_1\alpha_2 - \alpha_3\alpha_4))(T - (\alpha_1\alpha_3 - \alpha_2\alpha_4))(T - (\alpha_1\alpha_4 - \alpha_2\alpha_4))$$

is known under the name of the *dihedral resolvent* of the polynomial f.

Example 5.16. Suppose that the polynomial f is monic and denote by $\Delta(f)$ its discriminant. Choose $M = \mathfrak{S}_n$ and $L = \mathcal{A}_n$, the alternating subgroup of $\mathfrak{S}_n$. The Vandermonde determinant, $\delta_n = \prod_{1\le i<j\le n}(x_i - x_j)$, is a $\mathfrak{S}_n$-primitive $\mathcal{A}_n$-invariant. We have

$$\mathcal{L}_{\delta_n,f} = (x^2 - \Delta(f)) \qquad .$$

This resolvent is separable when the polynomial f is separable.

Example 5.17. Let $\xi \neq 1$ be a primitive unit n-th root. Set $\Theta = \xi x_1 + \xi^2 x_2 + \cdots + \xi^{n-1}x_{n-1} + x_n$. The absolute resolvent $\mathcal{L}_{\Theta,f}$ is called the *Vandermonde-Lagrange resolvent*

6. Generators of the ideal I_Ω^L

We suppose that the field k is infinite for existence of separable primitive invariants.

We take a subgroup M of $\mathfrak{S}_n$ containing a group L and the Galois group G_Ω (for example $M = \mathfrak{S}_n$). We have the following situation:

$$I_f^{\mathfrak{S}_n} \subset I_\Omega^M \subset I_\Omega^L \subset I_\Omega \qquad .$$

Let Θ be an M-primitive L-invariant. We denote by Δ_Θ the discriminant of the generic resolvent $\mathcal{L}_\Theta^M$. The discriminant of the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$ equals $\Delta_\Theta(\Omega)$. We have (see Theorem 3.1 Chapter 3):

$$k[x_1,\ldots,x_n]^L \subset \frac{1}{\Delta_\Theta} k[x_1,\ldots,x_n]^M[\Theta] \qquad . \tag{6.1}$$

Set

$$R_{L,M} := M_{\Theta,I_\Omega^M}(\Theta)$$

(see Proposition 5.1). When Θ is M-separable for Ω the polynomial $R_{L,M}$ is an M-primitive polynomial of the ideal I_Ω^L (see Definition 3.6).

Remark 29. The minimal polynomial of $\Theta(\Omega)$ over k equals M_{Θ,I_Ω^M} and is an irreducible factor over k of the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$ (see Lemma 5.2).

For computing the resolvents and consequently the Galois group G_Ω and the ideal I_Ω, we must determine a generating system of the ideal I_Ω^L.

Recall that if Ψ is separable primitive G_Ω-invariant then (see Theorem 6.3 of Chapter 4)

$$I_\Omega = I_\Omega^{\mathfrak{S}_n} + (\Psi - \Psi(\Omega)) = I_\Omega^M + (\Psi - \Psi(\Omega)) \quad .$$

The following lemma gives a first approach:

LEMMA 6.1. *If F be an M-primitive polynomial of the ideal I_Ω^L then*

$$I_\Omega^L = \sqrt{I_\Omega^M + (F)} \quad . \tag{6.2}$$

PROOF. We have $\sqrt{I_\Omega^L} = \sqrt{I_\Omega^M + (F)}$ because they are the same variety, by definition of M-primitive polynomials and the ideal I_Ω^L is radical. □

LEMMA 6.2. *If $Q \in k[x_1, \ldots, x_n]^M$ then $Q(\Omega) \in k$ and*

$$Q = Q(\Omega) \mod I_\Omega^M$$

PROOF. We have $Q(\Omega) \in k$ because $G_\Omega \subset M$. Therefore $Q - Q(\Omega)$ belongs to the ideal I_Ω^M. □

LEMMA 6.3. *Let Θ be an M-primitive L-invariant such that the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$ is a separable polynomial. Let us a polynomial P in I_Ω^L which is M-separable for Ω (i.e. $Stab_M(P) = \{\sigma \in M \mid \sigma.P(\Omega) = P(\Omega)\}$). Then*

$$P \in I_\Omega^M + < R_{L,M} > \quad .$$

PROOF. Let $H :=\mathrm{Stab}_M(P)$. Since the polynomial P is M-separable for Ω and for all $l \in L$ we have $l.P(\Omega) = P(\Omega)$ $(= 0)$, then $L \subset H$. Thus (see Theorem 3.1 Chapter 3):

$$k[x_1, \ldots, x_n]^H \subset k[x_1, \ldots, x_n]^L \subset \frac{1}{\Delta_\Theta} k[x_1, \ldots, x_n]^M[\Theta] \quad .$$

There exists a polynomial $F(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]^M[T]$ such that

$$\Delta_\Theta.P = F(x_1, \ldots, x_n)(\Theta) \quad .$$

As $G_\Omega \subset M$, there exists a polynomial $g \in k[T]$ such that $F(\Omega)(T) = g(T)$. Moreover, $P(\Omega) = 0$ because $P \in I_\Omega^L \subset I_\Omega$. Then

$$F(\Omega)(\Theta(\Omega)) = g(\Theta(\Omega)) = 0 \quad .$$

Thus g is a multiple of the minimal polynomial of $\theta = \Theta(\Omega)$ over k which equals the minimal polynomial M_{Θ,I_Ω}. Thus the polynomial $R_{L,M}$ is a factor of $g(\Theta)$. Denote by $\overline{U}$ the class of a polynomial U in the quotient ring $A_{I_\Omega^M} = k[x_1,\ldots,x_n]/I_\Omega^M$. By Lemma 6.2, $\overline{\Delta_\Theta} = \Delta_\Theta(\Omega) = \lambda \in k$. As the coefficients of F belong to $k[x_1,\ldots,x_n]^M$, we have (see Lemma 6.2):

$$\lambda.\overline{P} = \overline{\Delta_\Theta.P} = \overline{g(\Theta)} = \overline{R_{L,M}.Q}$$

where $Q \in k[x_1,\ldots,x_n]$. As $\lambda \neq 0$ we have

$$\overline{P} = \overline{R_{L,M}}.Q$$

where $Q \in k[x_1,\ldots,x_n]$. For every ideal I we have

$$k[x_1,\ldots,x_n]/(I+(R)) = A_I/\hat{R}A_I$$

where $A_I = k[x_1,\ldots,x_n]/I$ (see Equality (2.3) Chapter 2). Thus

$$\overline{P} = 0 \mod \overline{R_{L,M}}A_{I_\Omega^M}$$

and finally $P \in I_\Omega^M + < R_{L,M} >$. □

But the previous lemma does not give information about the no separable polynomial of the ideal I_Ω^L. The following theorem gives this information:

THEOREM 6.4. *Suppose that the polynomial f is separable. Let L and M be two subgroups of $\mathfrak{S}_n$ such that*

$$G_\Omega \subset Gr(I_\Omega^L) \subset M \quad .$$

Let F be an M-primitive polynomial of I_Ω^L (i.e. $G_\Omega L = \{\sigma \in M \mid \sigma.F(\Omega) = 0\}$). Then

$$I_\Omega^L = I_\Omega^M + < F > \quad . \tag{6.3}$$

In particular, if $L \subset G_\Omega$ then

$$I_\Omega = I_\Omega^L = I_\Omega^M + < F > \quad . \tag{6.4}$$

PROOF. If the theorem is valid with $\mathrm{Gr}(I_\Omega^L) = L$ then it holds also for each subgroup L which verifies the hypothesis of theorem because $I_\Omega^L = I_\Omega^{\mathrm{Gr}(I_\Omega^L)}$. Thus we can suppose that $\mathrm{Gr}(I_\Omega^L) = L$, so that $L = G_\Omega L$ because the Galois group G_Ω is supposed a subgroup of the decomposition group $\mathrm{Gr}(I_\Omega^L)$.

Let $\tau_1 = id, \ldots, \tau_e$ be a right transversal of $M \mod L$ and set

$$I := I_\Omega^L \text{ and } J := \bigcup_{i=2}^{e} I_\Omega^{L\tau_i} = I_\Omega^{\bigcap_{i=2}^{e} L\tau_i} \quad .$$

Using Lemma 6.5, the ideals I and J are comaximal because the ideals $I_\Omega^{L\tau_1}, \ldots, I_\Omega^{L\tau_e}$ are pairwise comaximal. A polynomial g is an M-primitive polynomial of I_Ω^L if and only $g \in I \backslash J$.

By Lemma 6.1, there exists an integer $l > 0$ such that

$$I^l \subset I_\Omega^M + < F > \subset I \quad .$$

As the ideals I and J are comaximal, the ideals I^l and J are too. Now, let $x \in I$ then there exist $u \in I^l$ and $v \in J$ such that

$$x = xu + xv \qquad .$$

We have $xu \in I_\Omega^M + < F >$ and $xv \in IJ = M$ because the ideals $I_\Omega^{L\tau_1}, \ldots, I_\Omega^{L\tau_e}$ are pairwise comaximal so that:

$$IJ = \prod_{i=1}^{e} I_\Omega^{L\tau_i} = \bigcap_{i=1}^{e} I_\Omega^{L\tau_i} = M \qquad .$$

□

LEMMA 6.5. *Let $\tau_1, \ldots, \tau_e$ be a right transversal of $M \mod L$ and L such that $G_\Omega L = L$. If f is separable then the ideals $I_\Omega^{L\tau_1}, \ldots, I_\Omega^{L\tau_e}$ are pairwise comaximal.*

PROOF. Let $i, j \in [1, n]$. We have $V(I_\Omega^{L\tau_i}) = L\tau_i \circ \Omega$ because $G_\Omega L = L$. If f is separable then $V(I_\Omega^{L\tau_i} + I_\Omega^{L\tau_j}) = V(I_\Omega^{L\tau_i}) \bigcap V(I_\Omega^{L\tau_j}) = \emptyset$. □

CHAPTER 7

Computational Galois theory

This chapter explores recent techniques for computing the ideal of Ω-relations I_Ω and the Galois group G_Ω. For existence of separable primitive invariants we must suppose that k is infinite and f is a separable polynomial.

1. The Ideals I_Ω^L and resolvent roots

In using resolvents, we search relations among the roots of a minimal polynomial $\mathrm{Min}_{\theta,k}$, where $\theta \in \hat{k}$.

In this section we suppose that M and L are two subgroups of $\mathfrak{S}_n$ such that M contains L and the Galois group G_Ω. In this situation, the stabilizer $\mathrm{Max}(I_\Omega^M)$ equals the group M.

Let $id = \tau_1, \ldots, \tau_l$ be a left transversal of $M \mod L$.

Notation 1.1. The set $\{\tau_1 L, \ldots, \tau_l L\}$ of the left cosets of $M \mod L$ will be denoted by $(M/L)_g$.

Let Θ_L be an M-primitive L-invariant separable for Ω (see Definition 2.1 Chapter 3) and set $\theta_L := \Theta_L(\Omega)$. Denote by e the degree of the minimal polynomial $\mathrm{Min}_{\theta_L,k}$. As $\mathrm{Min}_{\theta_L,k} = M_{\Theta_L, I_\Omega^L}$ is a (simple) factor of the resolvent $\mathcal{L}_{\Theta_L, I_\Omega^M}$, we can choose an order of the transversal such that $\tau_1, \ldots, \tau_e$ (where $e \leq l$) is as follows (see Proposition 5.7 Chapter 6 and Lemma 5.2 Chapter 6):

$$\mathrm{Min}_{\theta_L,k} = \prod_{i=1}^{e} (T - \tau_i.\Theta_L(\Omega)) = \prod_{\phi \in G_\Omega \star \theta_L} (T - \phi) \quad . \tag{1.1}$$

LEMMA 1.2. *For $i \in [1, e]$ we have $\tau_i \in G_\Omega L$. We can choose $\tau_i \in G_\Omega$ so that $\cup_{i=1}^{e} \tau_i L \subset G_\Omega L$.*

PROOF. By definition of $\tau_1, \ldots, \tau_e$ and by Equality (1.1), for each $i \in [1, e]$ there exists $g \in G_\Omega$ such that $\tau_i.\Theta_L(\Omega) = g.\Theta_L(\Omega)$. As g^{-1} belongs to G_Ω, it is equivalent to $g^{-1}\tau_i.\Theta(\Omega) = \Theta_L(\Omega)$. Now, this is equivalent to $g^{-1}\tau_i \in L$, since Θ_L is a separable M-primitive L-invariant and $g^{-1}\tau_i$ belongs to M. □

LEMMA 1.3. *For $i \in [1, e]$ the M-primitive $(\tau_i L \tau_i^{-1})$-invariant $\tau_i.\Theta$ is M-separable for Ω as well as Θ.*

PROOF. Exercise. Recall that for $V, U \in k[x_1, \ldots, x_n]$ and $\sigma \notin G_\Omega$, the equality $V(\Omega) = U(\Omega)$ does not imply that $\sigma.V(\Omega) = \sigma.U(\Omega)$. □

Recall the following lemma proved in Chapter 6:

LEMMA 1.4. *Let $\mathcal{H}$ be a set of subgroups of $\mathfrak{S}_n$. Then*

$$I_\Omega^{\bigcup_{H\in\mathcal{H}} H} = \bigcap_{H\in\mathcal{H}} I_\Omega^H \qquad . \tag{1.2}$$

PROPOSITION 1.5. *Let M and L be two subgroups of $\mathfrak{S}_n$ such that M contains L and G_Ω. Let Θ_L be an M-primitive L-invariant separable for Ω and $\theta_L = \Theta_L(\Omega)$. Setting $R_{L,M} := Min_{\theta_L,k}(\Theta_L) = \prod_{i=1}^{e}(\Theta - \tau_i.\Theta_L(\Omega))$ we have*

$$R_{L,M} \in I_\Omega^{\bigcup_{i=1}^{e}\tau_i L} = \bigcap_{i=1}^{e} I_\Omega^{\tau_i L} = \bigcap_{i=1}^{e} I^L_{\tau_i\circ\Omega} \qquad . \tag{1.3}$$

More precisely, for $\sigma \in M$, $\sigma \in \bigcup_{i=1}^{e}\tau_i L$ if and only if $\sigma.R_{L,M}(\Omega) = 0$.

PROOF. We chose the permutations $\tau_1, \ldots, \tau_e$ such that they belong to the Galois group G_Ω. It is possible by Lemma 1.2. Set $A := \{\sigma \in M \mid \sigma.R_{L,M}(\Omega) = 0\}$. By definition of the polynomial $R_{L,M}$ we have

$$A = \{\sigma \in M \mid (\exists i \in [1, e])\, \sigma.\Theta(\Omega) = \tau_i.\Theta(\Omega)\} \qquad .$$

As $\tau_i \in G_\Omega$ and Θ_L is M-separable for Ω:

$$\begin{aligned} A &= \{\sigma \in M \mid (\exists i \in [1, e])\, \tau_i^{-1}\sigma.\Theta = \Theta\} \qquad , \\ &\quad \{\sigma \in M \mid (\exists i \in [1, e])\, \sigma \in \tau_i L\} \end{aligned}$$

since Θ is an M-primitive L-invariant. □

The polynomial $R_{L,M}$ in Proposition 1.5 is an M-primitive polynomial of the ideal I_Ω^L (see Definition 3.6 Chapter 6). For Θ a separable primitive L-invariant we obtain the following equality:

$$G_\Omega L = \bigcup_{i=1}^{e} \tau_i L \qquad , \tag{1.4}$$

where $\tau_1.\Theta(\Omega), \ldots, \tau_e.\Theta(\Omega)$ are the conjugates of $\Theta(\Omega)$ over k. In other words $\{\tau_1 L, \ldots, \tau_e L\}$ is the G_Ω-orbit of L in $(M/L)_g$, the left cosets of $M \mod L$.

THEOREM 1.6. *Let M and L be two subgroups of $\mathfrak{S}_n$ such that M contains L and G_Ω (in particular $G_\Omega L \subset M$). Let $\tau_1, \ldots, \tau_l$ be a left transversal of $M \mod L$ and $\tau_1, \ldots, \tau_e$ in G_Ω ($e \leq l$) such that $G_\Omega L = \bigcup_{i=1}^{e}\tau_i L$. Then $\tau_1, \ldots, \tau_e$ is a left transversal of $G_\Omega \mod L \cap G_\Omega$, i.e. G_Ω is the following disjoint union:*

$$G_\Omega = \tau_1(L \cap G_\Omega) + \cdots + \tau_e(L \cap G_\Omega) \qquad . \tag{1.5}$$

The set $\{\tau_1 L, \ldots, \tau_e L\}$ is the G_Ω-orbit of L in $(M/L)_g$.

PROOF. By definition of a transversal we have $G_\Omega = M \cap G_\Omega = \bigcup_{i=1}^{l}(\tau_i L \cap G_\Omega)$ and this union is disjoint for the no empty subset. As $G_\Omega \subset \bigcup_{i=1}^{e} \tau_i L = G_\Omega L$, we have $G_\Omega = \bigcup_{i=1}^{e}(\tau_i L \cap G_\Omega)$. Now, for each $i \in [1, e]$, since $\tau_i G_\Omega = G_\Omega$, $\tau_i L \cap G_\Omega = \tau_i(L \cap G_\Omega) \neq \emptyset$ because L and G_Ω are groups. □

THEOREM 1.7 (Preservation of the primitive element). *(Arnaudiès-Avb) Let M and L be two subgroups of $\mathfrak{S}_n$ such that M contains L and G_Ω and let Θ a M-primitive L-invariant separable for Ω. Then $\theta = \Theta(\Omega)$ is a G_Ω-primitive $(L \cap G_\Omega)$-invariant relative to Ω. In other words, if Θ is M-separable for Ω and is a primitive element of the extension field $K(x_1, \ldots, x_n)^L$ of $K(x_1, \ldots, x_n)^M$, where $K = k(x_1, \ldots, x_n)^{\mathfrak{S}_n}$, then θ is a primitive element of the extension field $E = k(\Omega)^{L \cap G_\Omega}$ of k. It follows that, the Galois group of $k(\Omega)$ over E is $L \cap G_\Omega$.*

PROOF. As $k = k(\Omega)^{G_\Omega}$, θ is a primitive element of the extension $k(\Omega)^{L \cap G_\Omega}$ of the field k if $L \cap G_\Omega = \{\sigma \in G_\Omega \mid \sigma \star \theta = \theta\}$. As Θ is an M-primitive L-invariant and $G_\Omega \subset M$ we have:

$$\begin{aligned} G_\Omega \cap L &= \{\tau \in G_\Omega \mid \tau.\Theta = \Theta\} \\ &\quad \{\tau \in G_\Omega \mid \tau.\Theta(\Omega) = \Theta(\Omega)\} \end{aligned}$$

because Θ is M-separable for Ω. Finally, $G_\Omega \cap L = \{\tau \in G_\Omega \mid \tau \star \theta = \theta\}$. □

Remark 30. Let Θ be an M-primitive L-invariant. This invariant is M-separable for Ω if and only if the minimal polynomial of $\Theta(\Omega)$ is a simple factor of the resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$.

THEOREM 1.8. *(Arnaudiès-Avb) Let M and L be two subgroups of $\mathfrak{S}_n$ such that M contains L and G_Ω and Θ be an M-primitive L-invariant separable for Ω. Then the degree of the minimal polynomial of $\Theta(\Omega)$ over k is the index of $L \cap G_\Omega$ in G_Ω which is also the cardinality of the G_Ω-orbit of the class of L in $(M/L)_g$. If $\{\tau_1 L, \ldots, \tau_e L\}$ is this orbit then $\tau_1.\Theta(\Omega), \ldots, \tau_e.\Theta(\Omega)$ are the conjugates of $\Theta(\Omega)$ over k.*

We have now the following fundamental theorem:

THEOREM 1.9. *(Arnaudiès-Avb) Let M and L be two subgroups of $\mathfrak{S}_n$ such that M contains L and G_Ω and Θ be an M-primitive L-invariant. If the resolvent $\mathcal{L}_{\Theta, I_\Omega^M}$ is separable, then the degrees of its irreducible factors over k are the cardinalities of the G_Ω-orbits of $(M/L)_g$. More precisely, for each simple root $\theta_i := \tau_i.\Theta(\Omega)$ of this resolvent, the degree of its minimal polynomial is the length of the G_Ω-orbit of $\tau_i L$ in $(M/L)_g$ which equals the index of $(\tau_i L \tau_i^{-1}) \cap G_\Omega$ in G_Ω. The Galois group of the extension field $k(\Omega)$ of $k(\theta_i)$ is $(\tau_i L \tau_i^{-1}) \cap G_\Omega$.*

PROOF. The result of Theorem 1.8 holds for each $\tau.\Theta_L$ where $\tau \in \mathcal{T} := \{\tau_1, \ldots, \tau_l\}$ is our left transversal of $M \mod L$ whose the order is not fixed at this moment. The set $\{\tau_1.\Theta(\Omega), \ldots, \tau_l.\Theta(\Omega)\}$ is the set of the roots of the resolvent $\mathcal{L}_{\Theta_L, I_\Omega^M}$ counted with their multiplicities. We investigated the minimal polynomial of $\tau.\Theta(\Omega) = \Theta(\sigma \circ \Omega)$ for $\tau \in M$.

For that, consider the ideal $I_{\tau\circ\Omega}$ instead of I_Ω. If Θ is M-separable for $\tau\circ\Omega$ (see Definition 2.1 Chapter 3), by (1.4) there exists an order of the transversal of M $modL$ such that:

$$\bigcup_{i=1}^{r}\tau_i L = G_{\tau\circ\Omega}L \qquad ,$$

where $\tau_1 = id$ and $\{\tau_1.\Theta(\tau\circ\Omega),\ldots,\tau_r.\Theta(\tau\circ\Omega)\} = \{\tau\tau_1.\Theta(\Omega),\ldots,\tau\tau_r.\Theta(\Omega)\}$ are the distinct conjugates of $\Theta(\tau\circ\Omega)$ over k. As $G_{\tau\circ\Omega} = \tau^{-1}G_\Omega\tau$ we have

$$\bigcup_{i=1}^{r}\tau\tau_i L = G_\Omega\tau L \qquad .$$

Now since $\tau M = M$,

$$\bigcup_{j=1}^{r}\sigma_j L = G_\Omega\tau L \qquad ,$$

where $\sigma_1 = \tau$, $\{\sigma_1.\Theta(\Omega),\ldots,\sigma_r.\Theta(\Omega)\}$ are the conjugates of $\tau.\Theta(\Omega)$ over k and the set of r distinct classes $\{\sigma_j L \mid j\in[1,e]\}$ is the G_Ω-orbit of τL in $(M/L)_g$. □

Definition 1.10. Let F be a polynomial of $k[T]$ of degree m. The list of its irreducible factors over k ordered in increasing order is called the *partition of the polynomial* F. This is a partition of the integer m. This partition will be denoted by $\mathrm{part}(F)$.

Example 1.11. Let us $k=\mathbb{Q}$ and $F(T) = (x^2+1)(x^7+2)(x+1)^3(x^4+1)^3(x^4+2)^2$. The partition of F can be written in the two following manners:

$$\mathrm{part}(F) = (1,1,1,2,4,4,4,7) = (1^3,2,4^3,7) \qquad .$$

Remark 31. Let $P = \sum_{i=1}^{e} t_1\tau_i.\Theta_L$, where $t_1,\ldots,t_n$ are distinct permutations. If $\sigma.P = P$ then for all $i\in[1,e]$ we have $\sigma\in\tau_i L\tau_i^{-1}$ and then $\sigma\in\bigcap_{i=1}^{e}\tau_i L\tau_i^{-1}$. If P is separable then $P(\Omega)$ is a primitive element of the field extension $k(\Omega)^H$ of k where $H=\bigcap_{i=1}^{e}\tau_i L\tau_i^{-1}\cap G_\Omega$. Since $k(\Omega)^H$ is the splitting field of $\mathrm{Min}_{\theta,k}$ the polynomial P is a primitive element over k of this splitting field.

2. Partition Matrices

All the results of this section are from the papers **[6]** and **[7]**. The first partial partition matrices were introduced in **[13]** (see also **[9]**, **[14]**, **[16]**, **[31]**, **[33]**, **[51]**, **[52]**, **[59]** and **[65]**).

Consider a subgroup L of $\mathfrak{S}_n$ and two subgroups G, H of L.

2.1. Solving direct Galois problem using partition matrices.

Let L, G, H be subgroups of $\mathfrak{S}_n$ such that L contains the groups H and G.

LEMMA 2.1. *The G-orbits of $(L/H)_g$ only depend on the conjugacy classes of G and H in L.*

PROOF. (see [7]) □

Notation 2.2. Let $\mathcal{G}$ and $\mathcal{H}$ be the conjugacy classes of G and H in L, respectively. We denote by $\mathcal{O}_L(G,H)$ or $\mathcal{O}_L(\mathcal{G},\mathcal{H})$ the set of the G-orbits of $(L/H)_g$.

Now, we give an order for the set of conjugacy classes of subgroups of L:

$$L = \mathcal{C}_1, \ldots, \mathcal{C}_r = Id$$

by decreasing cardinality (for the same cardinality we choose an arbitrary ordering). Recall that the degree of an L-relative H-resolvent is the index $[L:H]$.

Definition 2.3. Let the r conjugacy classes of subgroups of L ordered as bellow. The *partition matrix relative to* L is the $r \times r$ matrix $\mathcal{P}^L$ such that for each $i,j \in [1,r]$

$$\mathcal{P}^L_{i,j} = \{\text{card}(O) \mid O \in \mathcal{O}_L(\mathcal{C}_i,\mathcal{C}_j)\} \quad , \tag{2.1}$$

where $\text{card}(O)$ is the cardinality of the orbit O. The list of integers $\mathcal{P}^L_{i,j}$ is ordered in increasing order and is called a *partition* of the index $[L:H]$ where H is any group of the class $\mathcal{C}_j$.

Definition 2.4. In the partition matrix $\mathcal{P}^L$ the conjugacy classes of groups indexing the columns ($\mathcal{C}_j$ in (2.1)) are called the *testing classes* and the conjugacy classes of groups indexing the rows ($\mathcal{C}_i$ in (2.1)) are called *candidate classes*. A group of a testing class is called a *testing group* and a group of a candidate class is called a *candidate group*.

LEMMA 2.5. *The rows of the partition matrix relative to L are pairwise distinct.*

PROOF. (see [7]) □

THEOREM 2.6. *Suppose that G_Ω is a subgroup of the group L. Then the partition matrix $\mathcal{P}^L$ is sufficient in order to determine the Galois group G_Ω. In particular, it is always possible to determine G_Ω with absolute resolvents.*

PROOF. Let L be a subgroup of $\mathfrak{S}_n$. For each subgroup H of L there exists an L-primitive H-invariant Θ such that the resolvent $F_H := \mathcal{L}_{\Theta, I^L_\Omega}$ is separable (see Lemma 2.3 Chapter 3). If G_Ω is included in L we can apply Theorem 1.9. If the partition of the matrix $\mathcal{P}^L$, computed with a candidate group G and the testing group H, does not equal the partition $\text{part}(F_H)$ (see Definition 1.10) then the group G and all other groups of its conjugacy class in L can not be the Galois group G_Ω. Computing a separable L-relative H-resolvents for each H in the set of testing groups of matrix $\mathcal{P}^L$, we determine the Galois group G_Ω since the rows of this matrices are pairwise distinct by Lemma 2.5.
In particular the Galois group is always included in $\mathfrak{S}_n$. □

Remark 32. In practice, it is not necessary to compute an H-resolvent for each subgroup representing a conjugacy class in the group L for determining the Galois group G_Ω. Firstly, it suffice to consider the smallest submatrix of $\mathcal{P}^L$ containing the testing groups with largest cardinality (with small index in L) such that its rows are pairwise distinct. Secondly, if we determine a subgroup L_1 of L containing the Galois group G_Ω,

we can change of partition matrix. We use then the matrix $\mathcal{P}^{L_1}$. Hence the degrees of the resolvents are smaller than the degrees of resolvents necessary in order to use the matrix $\mathcal{P}^L$: the degree of a resolvent relative to a group M is majored by $\mathrm{card}(M)$ and it must be computed and factorised.

2.2. Computation in GAP.

The logicial `Groups Algorithms and Programming` (see [**36**]) is very useful for computing with groups. In `GAP`, left actions becomes right actions.

The computation of partition $\mathcal{O}_L(G,H)$ can be realized by `GAP`-function `Partitions`:

```
Partitions := function(L,G,H)
              local orbits;
              orbits:=Orbits(G,Right-Cosets(L,H), On-Right);
              return List(orbits,D->Length(D));
              end;
```

But it is also possible to compute the partition $\mathcal{O}_L(G,H)$ using each index $[G : G \cap \tau_i H \tau_i^{-1}]$ for $\tau_1, \ldots, \tau_e$ a left transversal of $L \mod H$:

```
Partitions := function(L,G,H)
              local transversale, lesconj,lesindices;
              tranversale := List(RightCosets(L,H),
                                  rc->Representative(rc));
              lesconj := List(transversale,tau->H^tau);
              lesindices:=List(lesconj,
                               Hi->Index(G,Intersection(G,Hi)));
              return    List(Collected(lesindices),
                             doublet ->[doublet[1],
                                        doublet[2]/doublet[1]]);
              end;
```

where `lesconjs` is the list of the conjugates $\tau_i H \tau_i^{-1}$ of H ($i \in [1,e]$). This conjugates are not necessarily distinct.

3. group matrices

We introduce a new matrix containing information about the Galois groups of the factors (irreducible or not) of resolvents over k. This new matrix contains the informations

of the partition matrix. It can be use for computing some polynomials with a Galois group which is a given group.

We denote by Ω_f n-tuple of the roots of the polynomial f. We take L and H two subgroups of $\mathfrak{S}_n$ such that L contains the group H and the Galois group G_{Ω_f} of the polynomial f.

3.1. The Galois group of a resolvent factor.

We will find the Galois group of a factor irreducible over k of an H-resolvent $\mathcal{L}_{\Theta,I^L_{\Omega_f}}$ in function of the Galois group G_{Ω_f} of f and of the group H associated with the invariant Θ.

Let
- $\mathcal{L} := \{\tau_1 H, \ldots, \tau_e H\}$ be the G_{Ω_f}-orbit of H in $(L/H)_g$;
- Θ_H be an L-primitive H-invariant separable for Ω_f;
- $\theta_i := \tau_i.\Theta_H(\Omega_f)$ for $i \in [1, e]$;
- $g = \mathrm{Min}_{\theta_1,k}$.

The polynomial g is an irreducible simple factor over k of the resolvent $\mathcal{L}_{\Theta_H,I^L_{\Omega_f}}$.

As Θ_H is L-separable for Ω_f, the left action of G_{Ω_f} on $\{\theta_1, \ldots, \theta_e\}$ is the same as that on the G_{Ω_f}-orbit $\mathcal{L}$. We have:

$$g = \mathrm{Min}_{\theta_1,k} = \prod_{i=1}^{e}(T - \tau_i.\Theta_H(\Omega_f)) = \prod_{i=1}^{e}(T - \theta_i) \qquad .$$

We choose $\Omega_g := (\theta_1, \ldots, \theta_e)$ and e indeterminated $X_1, \ldots, X_e$. The ideal I_{Ω_g} of $k[X_1, \ldots, X_e]$ containing the Ω_g-relations is:

$$\begin{aligned} I_{\Omega_g} &= \{P \in k[X_1, \ldots, X_e] \mid P(\theta_1, \ldots, \theta_e) = 0\} \\ &= \{P \in k[X_1, \ldots, X_e] \mid P(\tau_1.\Theta_H(\Omega_f), \ldots, \tau_e.\Theta_H(\Omega_f)) = 0\} \qquad . \end{aligned}$$

Now, define a k-morphism ξ by:

$$\begin{aligned} \xi : k[X_1, \ldots, X_e] &\longrightarrow k[x_1, \ldots, x_n] \\ X_i &\mapsto \tau_i.\Theta(x_1, \ldots, x_n) \qquad . \end{aligned}$$

We have $\xi(I_{\Omega_g}) \subset I_{\Omega_f}$ because

$$P(\theta_1, \ldots, \theta_e) = \xi(P)(\alpha_1, \ldots, \alpha_n) \qquad . \tag{3.1}$$

Then the k-morphism ξ induces an injective k-morphism $\overline{\xi}$ of $k[X_1, \ldots, X_e]/I_{\Omega_g}$ into $k[x_1, \ldots, x_n]/I_{\Omega_f}$. The k-morphism $\overline{\xi}$ induces a natural injection of $k(\Omega_g)$, the splitting field of the polynomial g, into $k(\Omega_f)$ given by identity (3.1).

Define the morphism ρ between the Galois group G_{Ω_f} and $\mathfrak{S}_e$ the symmetric group of degree e. Let $\sigma \in G_{\Omega_f}$, its image $\rho(\sigma)$ by ρ is the permutation of $\mathfrak{S}_e$ defined by: for $i, j \in [1, e]$

$$\rho(\sigma)(i) = j \qquad \text{if} \qquad \sigma\tau_i L = \tau_j L \qquad .$$

Recall that for $\sigma \in G_{\Omega_f}$ then $\sigma\tau_i L = \tau_j L$ is equivalent to $\sigma \star \theta_i = \theta_j$. We have for $i \in [1, e]$

$$\tau_{\rho(\sigma)(i)}.\Theta_H = \sigma.(\tau_i.\Theta_H) \qquad . \tag{3.2}$$

Then for all $\sigma \in G_{\Omega_f}$ and $P \in k[X_1, \ldots, X_e]$ we have

$$\begin{aligned} \sigma.\xi(P) &= P(\sigma\tau_1.\Theta_H, \ldots, \sigma\tau_n.\Theta_H) \\ &= (\rho(\sigma).P)(\tau_1.\Theta_H, \ldots, \tau_n.\Theta_H) \qquad . \end{aligned}$$

Finally:

$$\sigma.\xi(P) = \xi(\rho(\sigma).P) \qquad \text{so that} \tag{3.3}$$

$$(\sigma.\xi(P))(\Omega_f) = (\rho(\sigma).P)(\Omega_g) \qquad . \tag{3.4}$$

PROPOSITION 3.1. *We have:*
(a) $\rho(G_{\Omega_f}) = G_{\Omega_g}$*;*
(b) the left action of G_{Ω_f} *on* $\mathcal{L}$ *is the same as the one of* G_{Ω_g} *on* $\theta_1, \ldots, \theta_e$*;*
(c) let $U = \bigcap_{i=1}^{e} Stab_{G_{\Omega_f}}(\tau_i L) = \bigcap_{i=1}^{e}(G_{\Omega_f} \cap \tau_i H \tau_i^{-1})$*; then* $U = Ker(\rho)$ *and* G_{Ω_f}/U *is isomorphic to* G_{Ω_g}*.*

PROOF. (b) is a direct consequence of (a).
(a) $\rho(G_{\Omega_f}) \subset G_{\Omega_g}$ because $\xi(I_{\Omega_g}) \subset I_{\Omega_f}$. Let $V \in k[X_1, \ldots, X_e]$ be a separable primitive I_e-invariant and set $v := V(\Omega_g)$. We have $v = \xi(V)(\Omega_f)$ by (3.1). By the choice of V, we have:

$$C_{V,I_{\Omega_g}} = \mathrm{Min}_{v,k} = \prod_{t \in G_{\Omega_g}} (T - t.V(\Omega_g)) \tag{3.5}$$

and as $v \in k(\Omega_f)$

$$\mathrm{Min}_{v,k} = \prod_{\phi \in G_{\Omega_f} \star v} (T - \phi) \qquad . \tag{3.6}$$

Thus, for all $t \in G_{\Omega_g}$ there exists $\sigma \in G_{\Omega_f}$ such that $t.V(\Omega_g) = \sigma \star v$. But $v = \xi(V)(\Omega_f)$ and for $\sigma \in G_{\Omega_f}$, identity (3.4) applied to $P := V$ implies:

$$\sigma \star v = \rho(\sigma).V(\Omega_g) \qquad . \tag{3.7}$$

Therefore for all $t \in G_{\Omega_g}$ there exists $\sigma \in G_{\Omega_f}$ such that $t.V(\Omega_g) = \rho(\sigma).V(\Omega_g)$. Now, as t^{-1} belongs to the Galois group G_{Ω_g}, the equality $t.V(\Omega_g) = \rho(\sigma).V(\Omega_g)$ is equivalent to $V(\Omega_g) = t^{-1}\rho(\sigma).V(\Omega_g)$. The assumption of the separability of V which is invariant only

under the identity implies that $t = \rho(\sigma)$ and part (a) of our proposition is proved.
(c) For each $\tau \in \mathfrak{S}_n$, G and H subgroups of $\mathfrak{S}_n$, we have $\mathrm{Stab}_G(\tau H) = G \cap \tau H \tau^{-1}$ so that

$$\bigcap_{i=1}^{e} G \cap \tau_i H \tau_i^{-1} = \bigcap_{i=1}^{e} \mathrm{Stab}_G(\tau_i H) \qquad . \tag{3.8}$$

First proof. ρ is not injective. Let $g \in G_{\Omega_f}$, the equality $\rho(g) = id$ is equivalent to $(\forall i \in [1, e])\ g\tau_i H = \tau_i H$ if and only if $g \in \bigcap_{i=1}^{e} \mathrm{Stab}_{G_{\Omega_f}}(\tau_i L)$.

Second proof. For $i \in [1, e]$„ θ_i is a k-primitive element of $k(\Omega)^{G_{\Omega_f} \cap \tau_i H \tau_i^{-1}}$ (see Theorem 1.7 Chapter 6). Then the splitting field of g is $k(\Omega)^U$ (see Equality (3.8)). This splitting field is a Galois extension of k, U is normal subgroup of $\mathfrak{S}_n$ and by the Galois correspondence, the Galois group of g is isomorphic to G_{Ω_f}/U. □

COROLLARY 3.2. *(Arnaudiès-avb) Suppose that $n \neq 4$ and let H be a proper subgroup of $\mathfrak{S}_n$ which is not the alternating subgroup $\mathcal{A}_n$. Let Θ be a separable primitive H-invariant (i.e. the absolute resolvent $\mathcal{L}_{\Theta,f}$ is separable). Then the splitting field of the absolute resolvent $\mathcal{L}_{\Theta,f}$ is the same as that of f. In other words, the Galois group of $\mathcal{L}_{\Theta,f}$ is isomorphic to the one of f.*

PROOF. For $n \neq 4$ the only subgroup of $\mathfrak{S}_n$ which are normal in $\mathfrak{S}_n$ are $\mathfrak{S}_n$, $\mathcal{A}_n$ and the identity group. The Galois group of $\mathcal{L}_{\Theta,f}$ is isomorphic to G_{Ω_f}/U, where $U = \bigcap_{i=1}^{e}(G_{\Omega_f} \cap \tau_i H \tau_i^{-1})$ and $\tau_1, \ldots, \tau_e$ is a left transversal of $\mathfrak{S}_n \mod H$. As U is a normal subgroup of H not equal to $\mathfrak{S}_n$ and $\mathcal{A}_n$ it is the identity group. □

Remark 33. Proposition 3.1 indicates how to compute a priori the Galois group of a factor of a resolvent which is irreducible over k. In order to compute the Galois group of any factor over k (i.e. not necessary irreducible) it suffices to consider the unions of G_{Ω_f}-orbits.

3.2. The group matrix and computation in GAP.

Definition 3.3. The *group matrix relative to L*, denoted by $\mathcal{G}^L$, is defined as follows: let $\mathcal{C}_i$ and $\mathcal{C}_j$ be two conjugacy classes in L of two subgroups G and H of L respectively. Then $\mathcal{G}^L_{i,j}$ is the list of Galois groups of irreducible factors over k of any L-relative H-resolvent separable for Ω_h of a polynomial h of $k[x]$ having G as Galois group over k.

In order to compute the element $\mathcal{G}^L_{i,j}$ of the group matrix, we have following function of GAP given by C. Quitté:

```
Groups := function(L,G,H)
          local orbits;
          orbits:=Orbits(G,RightCosets(L,H), OnRight);
          return List(orbits,
```

```
                D->AsSubgroup(SymmetricGroup(Length(D),
                              Operation(G,D,OnRight));
        end;
```

The group matrix $\mathcal{G}^L$ contains all the informations of the partition matrix $\mathcal{P}^L$. The Galois group of f can be determined not only from the degrees, but also from the computation of the Galois groups of its factors. This is useful in the cases in which the degree of a factor of a resolvent is smaller than the one of f or when it is sufficient to compute the discriminant of f (see Chapter 11).

4. Inductive construction of the Ω-relations ideal

We want to find an algorithm computing a generating system of the ideal I_Ω of Ω-relations.

An ideal I_Ω^L is said *known* when a generating system of this ideal is known.

Example 4.1. The ideal $I_\Omega^{\mathfrak{S}_n}$ of symmetric relations is known. The set of polynomials $e_1 - e_1(\Omega), \ldots, e_n - e_n(\Omega)$ is a generating system of $I_\Omega^{\mathfrak{S}_n}$. Moreover, the set of the n Cauchy moduli of polynomial f is a reduced Gröbner basis for lexicographic order of the ideal $I_\Omega^{\mathfrak{S}_n}$ (see Section 4 Chapter 4).

There exist finite increasing chains of ideals:

$$I_\Omega^{\mathfrak{S}_n} = I_1 \subset I_2 \subset \cdots \subset I_m = I_\Omega$$

where each ideal I_j ($j \in [1, m]$) has the form I_Ω^H with H a subset of $\mathfrak{S}_n$.

We search to construct one such chain by an inductive computation of generating systems of ideals $I_2, \ldots, I_m$. Recall Theorem 6.4 of Chapter 6:

THEOREM 4.2. *Let L and M be two subgroups of $\mathfrak{S}_n$ such that*

$$G_\Omega \subset GR(I_\Omega^L) \subset M$$

and let F be an M-primitive polynomial of I_Ω^L. Then

$$I_\Omega^L = I_\Omega^M + (F) \qquad . \tag{4.1}$$

In particular, when $L \subset G_\Omega$

$$I_\Omega = I_\Omega^L = I_\Omega^M + (F) \qquad . \tag{4.2}$$

4.1. Hypothesis.

Suppose that M is a subgroup of $\mathfrak{S}_n$ containing the Galois group G_Ω (i.e. which verifies the hypothesis of Theorem4.2) and such that the ideal I_Ω^M is known. At beginning the only known ideal is $I_\Omega^{\mathfrak{S}_n}$ and the Galois group is effectively included in $\mathfrak{S}_n$.

Let L be a subgroup of M. We have the following situation:

$$I_f^{\mathfrak{S}_n} \subset I_\Omega^M \subset I_\Omega^L \subset I_\Omega \qquad . \tag{4.3}$$

Choose Θ an M-primitive L-invariant separable for Ω and set

$$R_{L,M} := M_{\Theta,I_\Omega^M}(\Theta)$$

which is an M-primitive polynomial of I_Ω^L (see Definition 3.6 Chapter 6). The minimal polynomial of $\Theta(\Omega)$ over k is an irreducible (simple) factor of the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$. As the ideal I_Ω^M is known, this resolvent can be computed (see Chapter 9).

4.2. Theoretical results.

We search the conditions in which the construction of the chain (4.3) can be continued.
By Theorem 4.2, if $G_\Omega L$ is a group then the ideal I_Ω^L is known with:

$$I_\Omega^L = I_\Omega^M + < R_{L,M} > \qquad .$$

Proposition 3.9 Chapter 6 gives sufficient and necessary conditions for which $G_\Omega L$ is a group.

PROPOSITION 4.3. *Let Θ be an M-primitive L-invariant separable for Ω. There is an equivalence between the following conditions:*
(i) $I_\Omega^L = I_\Omega^M$
(ii) $G_\Omega L = M$*; and in this case* $Gr(I_\Omega^L) = G_\Omega L$*;*
(iii) the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$ *is irreducible over* k*; and in this case equals* $Min_{\Theta(\Omega),k}$.

Suppose that L is a maximal subgroup of M. One conjugate H of L in M is such that $G_\Omega H$ is a group if, and only if, one of the following conditions holds:
(a) the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$ *is irreducible over* k *; and in this case* $Gr(I_\Omega^L) = G_\Omega L = M$*;*
(b) the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$ *has a simple factor which is linear in* $k[x]$.

PROOF. Prove the first three equivalences. If $I_\Omega^L = I_\Omega^M$ then $G_\Omega L = G_\Omega M = M$ (and $\mathrm{Gr}(I_\Omega^L) = \mathrm{Gr}(I_\Omega^M) = M$). Conversely, if $G_\Omega L = M$ then, by definition of the stabilizer, $I_\Omega^L = I_\Omega^M$. Therefore (i) is equivalent to (ii). If $G_\Omega L = M$ then

$$\mathcal{L}_{\Theta,I_\Omega^M} = \mathcal{L}_{\Theta,I_\Omega^L} = \mathrm{Min}_{\Theta(\Omega),k}$$

because Θ is M-separable for Ω. Conversely, if (iii) holds then

$$G_\Omega \star \Theta(\Omega) = \{\Psi(\Omega) \mid \Psi \in M.\Theta\} \qquad .$$

Let $m \in M$. There exists $g_m \in G_\Omega$ such that $g_m.\Theta(\Omega) = m.\Theta(\Omega)$. As $g_m^{-1} \in G_\Omega$, $g_m^{-1}m.\Theta(\Omega) = \Theta(\Omega)$. We have $m \in G_\Omega L$ since the M-primitive L-invariant Θ is M-separable for Ω and $g_m^{-1}m \in M$. Thus $G_\Omega L = M$ because the inverse inclusion always is true. Therefore (ii) is equivalent to (iii).

Now, suppose that L is a maximal subgroup of M.
We know that $\mathrm{Gr}(I_\Omega^L) = G_\Omega L = M$ is equivalent to (a) for all subgroup L of M.

Suppose that $\mathrm{Gr}(I_\Omega^L) = G_\Omega L \neq M$. As $L \subset \mathrm{Gr}(I_\Omega^L) \subset M$ and L is a maximal subgroup of M, $L = \mathrm{Gr}(I_\Omega^L) = G_\Omega L$. Then $G_\Omega \subset L$ and (b) holds. Conversely, if (b) is valid then $G_\Omega \subset \tau L \tau^{-1}$ with $\tau \in M$ (see Lemma 3.1 Chapter 6). □

In case in which the group L is not a maximal subgroup of M, if the resolvent $\mathcal{L}_{\Theta, I_\Omega^M}$ reducible over k and has no simple linear factor over $k[x]$ then it is not possible to test one of conjugates of L in M verifies the condition of Theorem 4.2. But omit this problem and search to exploit the computation of the resolvent $\mathcal{L}_{\Theta(\Omega), I_\Omega^M}$.

Let $\tau_1, \ldots, \tau_e$ be permutations of the left transversal of $M \mod L$ such that:

$$\mathcal{O} = (\tau_1.\Theta, \ldots, \tau_e.\Theta)$$

is the G_Ω-orbit of Θ and

$$\mathcal{L} = (\tau_1 L, \ldots, \tau_e L)$$

is the G_Ω-orbit of L (the correspondence between these two sets has be given for the first time by Berwick in [**13**]). The e distinct elements

$$\tau_1.\Theta(\Omega), \ldots, \tau_e.\Theta(\Omega)$$

of $\hat{k}$ are the conjugates of $\Theta(\Omega)$ over k (i.e. the roots of the minimal polynomial of $\Theta(\Omega)$ over k). Recall that the G_Ω-orbit of $\Theta(\Omega)$ is the following:

$$G_\Omega \star \Theta(\Omega) = (\tau_1.\Theta(\Omega), \ldots, \tau_e.\Theta(\Omega)) \quad .$$

Set

$$S := \mathrm{Stab}_M(\mathcal{O}) = \mathrm{Stab}_M(\mathcal{L}) = \mathrm{Stab}_M(G_\Omega L) \quad .$$

In [**6**] for $M = \mathfrak{S}_n$ it is proved that :

$$G_\Omega \subset S \subset \bigcup_{i=1}^{e} \tau_i L = \bigcup_{L_i \in \mathcal{L}} L_i \quad .$$

The following lemma extends this result to a group M containing the Galois group G_Ω.

LEMMA 4.4. *If L is a group, then $G_\Omega \subset S \subset G_\Omega L$ and:*

$$I_\Omega^L = I_\Omega^{G_\Omega L} \subset I_\Omega^S \subset I_\Omega \quad . \tag{4.4}$$

On the other hand, $L \subset Gr(I_\Omega^L) \subset G_\Omega L$ and $S = Gr(I_\Omega^S) = G_\Omega S$, since $Max(I_\Omega^S) = S$ is a group.

PROOF. As $G_\Omega.\mathcal{L} = \mathcal{L}$ then $G_\Omega \subset S$, by definition of S, so that $G_\Omega S = \mathrm{Gr}(I_\Omega^S) = S$. And $S \subset G_\Omega L$ because L is a group and $SL \subset SG_\Omega L \subset G_\Omega L$, by definition of S. □

Complete Proposition 3.9 Chapter 6 for testing hypothesis of Theorem and for constructing the chain (4.3):

PROPOSITION 4.5. *The stabilizer $G_\Omega L$ is a group if, and only if, one of the following equivalences holds:*

(1) $L \subset S$;
(2) $I_\Omega^L = I_\Omega^S$;
(3) $G_\Omega L = S$ *(we always have* $G_\Omega S = S$*)* ;
(4) $S = Gr(I_\Omega^L)$.

PROOF. Obvious. □

Remark 34. We have $G_\Omega L = M$ if, and only if, $S = M$. Thus, by Proposition 4.3, the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$ is irreducible over k if, and only if, $S = M$. If L is a maximal subgroup of M then it is possible to test the equality $I_\Omega^L = I_\Omega^S$ (or $S = G_\Omega L$): either the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$ is irreducible over k and, in this case, $S = M$ or it has a linear factor over k and, in this case, S equals L (for an order of Ω). In case for which L is not a maximal subgroup of M it is possible that $G_\Omega L$ is a group and the group S does not equal M or L. Effectively, suppose that the polynomial f does not split over k (G_Ω is not the identity group) and choose $M = \mathfrak{S}_n \neq G_\Omega$. Take for L the identity group. Then $I_\Omega^L = I_\Omega^{G_\Omega} = I_\Omega$ and $S = G_\Omega$. Thus $S \neq M$ and $S \neq L$.

This remark introduces the following proposition useful to stop our construction:

PROPOSITION 4.6. *The following assertions are equivalent:*

(i) $G_\Omega = S = G_\Omega L$;
(ii) $L \subset G_\Omega$;
(iii) $I_\Omega = I_\Omega^M + (R_{L,M})$.

The equivalence between (i) and (iii) of Proposition 4.6 has been proved for $S = \mathfrak{S}_n$ *in* **[6]**.

PROOF. The condition $G_\Omega L = \mathrm{Max}(I_\Omega^L) = G_\Omega$ is equivalent to $I_\Omega = I_\Omega^L = I_\Omega^M + (R_{L,M})$ which is equivalent to $L \subset G_\Omega$. □

Remark 35. If V be a separable primitive I_n-invariant (where I_n is the identity group in $\mathfrak{S}_n$) then:

$$I_\Omega = I_f^{\mathfrak{S}_n} + (\mathrm{Min}_{V(\Omega),k}(V)) \quad . \tag{4.5}$$

However, the problem is to compute $\mathcal{L}_{V,I_f^{\mathfrak{S}_n}}$, the Galois's resolvent whose degree is $n!$.

We have the following equality (see **[6]** for $M = \mathfrak{S}_n$)

$$[S : G_\Omega] = [S \cap L : G_\Omega \cap L] \quad . \tag{4.6}$$

We have:

$$I_\Omega^M \subset I_\Omega^L \subset I_\Omega^S = I_\Omega^M + < F > \subset \cdots \subset I_\Omega \ , \tag{4.7}$$

where F is an M-primitive polynomial of I_Ω^S. Set $A_G = k[x_1, \ldots, x_n]/I_\Omega^G$ for each subset G of $\mathfrak{S}_n$. The chain (4.7) induces the following about the quotiented algebras:

$$A_{\mathfrak{S}_n} \supset A_M \supset A_S \supset A_{G_\Omega} \cong k(\Omega)$$

with, by Theorem 2.2 Chapter 2,:

$$A_S \;=\; k[x_1,\ldots,x_n]/(I_\Omega^M + < F >) \cong A_M/\hat{F}A_M \quad .$$

If the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$ has a simple linear factor $(T-\lambda)$ over k, we can choose an order of Ω such that $S = G_\Omega L = L$ and

$$I_\Omega^L = I_\Omega^S = I_\Omega^M + < \Theta - \lambda > \qquad .$$

Otherwise, we must compute an M-primitive polynomial of the ideal I_Ω^L using the resolvent $\mathcal{L}_{\Theta,I_\Omega^L}$.

Let $\Theta_{S,M}$ be an M-primitive S-invariant which is M-separable for Ω. As the minimal polynomial of $\Theta_{S,M}(\Omega)$ over k is $T - \Theta_{S,M}(\Omega)$ (we have $G_\Omega \subset S$), the polynomial

$$R_{S,M} = \Theta_{S,M} - \Theta_{S,M}(\Omega)$$

is an M- primitive polynomial of our new ideal I_Ω^S. In order to compute an M-primitive S-invariant, A. Colin take for $\Theta_{S,M}$ a symmetric functions on $\mathcal{O}$ the G_Ω-orbit of Θ (see **[24]**). As $\Theta_{S,M}(\Omega)$ is a symmetric polynomial of the roots of the minimal polynomial $\mathrm{Min}_{\Theta(\Omega),k}$, its computation is carried out using the fundamental theorem of symmetric functions with coefficients of $\mathrm{Min}_{\theta,k}$ (see **[24]** and **[64]** for computation of symmetric polynomials). There exists an elementary symmetric function and a power symmetric function which give an M-primitive L-invariant $\Theta_{S,M}$ which is M-separable for Ω (see **[46]**).

Putting $\underline{x} = (x_1,\ldots,x_n)$ and $K = k(x_1,\ldots,x_n)^{\mathfrak{S}_n}$ the field point of view is the following (see **[24]**):

$$K \subset K(\underline{x})^M \;\subset\; K(\underline{x})^M(\Theta_{S,M}) = K(\underline{x})^S \subset K(\underline{x})^{G_\Omega} \tag{4.8}$$

and such that $\Theta_{S,M}(\Omega)$ is known as a value in k.

4.3. First Algorithm.

For the sake clarity, this first algorithm, called `GaloisIdeal1`, is given without partition and group matrices.

The algorithm `GaloisIdeal1` is presented under the form of a recursive function. It starts with

`GaloisIdeal1(f,n,`$\mathfrak{S}_n$`,Generators)`

where
- `n` is the degree n of polynomial f represented by `f` ;
- `Generators` is a list containing the symmetric group $\mathfrak{S}_n$ and the n Cauchy moduli of polynomial f.

In each recursive call

`GaloisIdeal1(f,n,M,Generators)` ,

- `M` is a subgroup of $\mathfrak{S}_n$ containing the Galois group G_Ω;
- `Generators` is a list containing the Cauchy moduli of f, distinct subgroups

$$M_1 = \mathfrak{S}_n \supset M_2 \supset \cdots \supset M_m$$

of $\mathfrak{S}_n$ and polynomials $R_2, \ldots, R_m$ of $k[x_1, \ldots, x_n]$ such that for $i \in [2, m]$ the polynomial R_i is an $M_{(i-1)}$-primitive polynomial of the ideal $I_\Omega^{M_i}$.

The result of the function `GaloisIdeal1` is the list `Generators` such that

$$I_\Omega^{M_m} = I_\Omega$$

with $M_m \subset G_\Omega$.

Define two functions used in the algorithm.
- The function `Return` returns a result and ends the algorithm. For this reason the alternation `Else` does not appear.
- Let S be the group $\mathrm{Stab}_M(G_\Omega L)$ and V the minimal polynomial of $\Theta(\Omega)$ over k; the function `R(M,`S`,`V`)` computes an `M`-primitive polynomial of the ideal I_Ω^S using the fundamental theorem of symmetric functions with the coefficients of polynomial V.

```
Function GaloisIdeal1(f, n, M, Generators)
```

```
(A) Choose L a subgroup of M
*   Compute Θ an M-primitive L-invariant
    Compute And factorize F the M-relative L-resolvent L_{Θ,I_Ω^M}
    (suppose that F is separable)
**  IfF is irreducible (case G_Ω L=M)
      Then Choose another subgroup L of M
(B)          Ifall subgroups L of M are tested
               Then Return Generators (we have G_Ω =M)
             Go to * with L
    Choose V an irreducible factor of F over k
    If L is a subgroup of the Galois group (L = I_n)
      Then Add V(Θ) to the list Generators and Return Generators
*** If the degree of V is 1
      Then Add L and V(Θ) to the list Generators
           GaloisIdeal1(f,n,L,Generators)
           (an exit will be produced)
(C) Compute the orbit associated with the polynomial V
(D) Compute S the stabilizer of this orbit
    Add S and R(M,S) to the list Generators
    GaloisIdeal1(f,n,S,Generators)
```

Comments about algorithm `GaloisIdeal1`

(A) When a Galois resolvent is computable, we apply Proposition 4.6 in order to stop the algorithm : the identity group is chosen. Otherwise the group `L` is chosen such that the algorithm converges on I_Ω with few steps and with easy computation and factorization of resolvents. In order to have few steps, the cardinality of the group `L` must be small and, for rapid computations and factorizations of resolvents, this cardinality must be big. Recall that two subgroups of the same conjugacy class in m give the same results. Then only one subgroup by conjugacy class will be used.

(B) In this case $I_\Omega^M = I_\Omega^L = I_\Omega^S$ (i.e. the resolvent is irreducible). If `M`$\neq G_\Omega$ then there is the group `L`$= G_\Omega$ of `M` which does not satisfy this equality.

(C) The elements of the orbit associated with `V` are the classes $\tau_{i_1}L, \ldots, \tau_{i_e}L$ of $(M/L)_g$ such that $\tau_{i_1}.\Theta(\Omega), \ldots, \tau_{i_e}.\Theta(\Omega)$ are the roots of the factor `V`.

(D) The union of elements of the orbit is: $U = \bigcup_{j=1}^{e} \tau_{i_j}L = G_\Omega L$ the union of the orbit associated with `V`; if U is a group, then `S`$= U$ else me must compute the stabilizer `S`; when the polynomial `V` is linear or the polynomial `F` is irreducible over k, S$= U$. These cases are traited in ** and in ***. When L is a maximal subgroup of `M` and if `F` is not irreducible over k or has not a linear factor over k, we are sure that for each conjugate H of L in M the stabilizer $G_\Omega H$ is not a group and $S \neq G_\Omega H$.

When `V` is not linear and `F` is not irreducible over k, the unknown Galois group G_Ω is necessary for computing the stabilizer `S`. However, in order to avoid many candidate groups, we can perform it using partition and group matrices. More about this in the follows section.

4.4. Second Algorithm.

We have a first algorithm `GaloisIdeal1` which needs the impossible computation of a G_Ω-orbit. We search a new algorithm.

Suppose that the group M contains the Galois group G_Ω and we know a generating system of the ideal I_Ω^M. We have chosen a subgroup L of M and we have compute the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$ where Θ is an M-primitive L-invariant separable for Ω.

Suppose that we have computed a set $\mathcal{S}_M$ of groups which are candidate for the Galois group (only one by conjugacy class in M). By example, when $M = \mathfrak{S}_n$ and none resolvent has been computed, the set $\mathcal{S}_{\mathfrak{S}_n}$ is the conjugacy classes of subgroups of $\mathfrak{S}_n$. As the Galois group is included in the group M, the $\mathcal{S}_M$ contains only subgroups of M.

By partition matrices and using the factorization of the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$ we determine a set $\mathcal{S}$ of groups of $\mathcal{S}_M$ which are candidate for the Galois group G_Ω. Let G be the minimal subgroup of M which contains the union of groups of $\mathcal{S}$ and let H be the intersection of

the groups of $\mathcal{S}$:

$$G =< \bigcup_{H' \in \mathcal{S}} H' > \text{ and } H = \bigcap_{H' \in \mathcal{S}} H' \quad .$$

As the set $\mathcal{S}$ is known, the groups G and H too and they satisfy:

$$H \subset G_\Omega \subset G \quad .$$

Proposition 4.6 will be applied in order to stop our algorithm: if there exists a subgroup H' of H such that an H'-resolvent can be computed rapidly then the algorithm is stopped using:

$$I_\Omega = I_\Omega^M + < R_{H',M} > \quad .$$

Remark 36. As the group G is known and contains the Galois group, it is possible to apply Theorem 4.2 with G at the place of M. But in this case, an M-relative G-resolvent (or $\Theta_G(\Omega)$) must be computed. Unless a such resolvent can be computed quickly, it is preferable to use the resolvent $\mathcal{L}_{\Theta, I_\Omega^M}$ which is already computed.

Take the idea of algorithm `GaloisIdeal1`. As the groups G and L are known, the set $GL = \{gl \mid g \in G \ , l \in L\}$ is also known and it is possible to compute the group $\mathrm{Stab}_M(GL)$, the stabilizer of GL in the group M. Set $S' :=\mathrm{Stab}_M(GL)$. The group S' contains the Galois group G_Ω (see Figure (4.9)). It is then possible to apply Theorem 4.2 with the group S' at the place of the group M.

We will replace the group $S =\mathrm{Stab}_M(G_\Omega L)$ of Algorithm `GaloisIdeal1` which is not always computable by the group S'. The point of view of groups is the following:

$$\begin{array}{ccccccc} L & \subset & G_\Omega L & \subset & GL & \subset & M \\ & & \cup & & \cup & & \\ & & S = \mathrm{Stab}_M(G_\Omega L) & \subset & S' = \mathrm{Stab}_M(GL) & & \\ & & \cup & & \cup & & \\ H & \subset & G_\Omega & \subset & G & & \end{array} \tag{4.9}$$

where H, G, L, M and S' are known subgroups of $\mathfrak{S}_n$.

The considered chains of ideals are as the following:

$$I_\Omega^{\mathfrak{S}_n} \subset \cdots \subset I_\Omega^M \subset I_\Omega^{S'} \subset I_\Omega^G \subset \cdots \subset I_\Omega = I_\Omega^H \quad .$$

Now, it is necessary to find an M-primitive polynomial of the ideal $I_\Omega^{S'}$ as we have found an M-primitive polynomial of the ideal I_Ω^S.

Let $G.L$ the G-orbit of L in $(M/L)_g$:

$$G.L = \{\tau_1 L, \ldots, \tau_s L\} \subset (M/L)_g \quad .$$

Define W the univariate polynomial associated with this orbit:

$$W(T) = \prod_{i=1}^{s} (T - \tau_i.\Theta(\Omega)) \quad . \tag{4.10}$$

As $G_\Omega \subset G \subset M$, the polynomial W is a factor of the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$ and its coefficients, invariant under the group G_Ω, belong to the field k. As the invariant Θ is separable for Ω, we have:

$$\mathcal{L}_{\Theta,I_\Omega^L} = \prod_{\Psi \in G_\Omega L.\Theta} (T - \Psi(\Omega)) = \mathcal{L}_{\Theta,I_\Omega} = M_{\Theta,I_\Omega} = \mathrm{Min}_{\Theta(\Omega),k} \quad . \tag{4.11}$$

We have $G_\Omega L \subset GL$. Then the resolvent $\mathcal{L}_{\Theta,I_\Omega^L}$ is a (simple) factor of the polynomial W and is irreducible over the field k.

But if GL and $G_\Omega L$ are not identical then the polynomial W is different to the resolvent $\mathcal{L}_{\Theta,I_\Omega^L}$ and is not irreducible over k. Give an example where the stabilizer $G_\Omega L$ does not equal the set GL:

Example 4.7. Suppose that G and M are equal so that $GL = M$. If $M = GL = G_\Omega L$ then

$$\mathcal{L}_{\Theta,I_\Omega^M} = \mathcal{L}_{\Theta,I_\Omega^L} = \mathrm{Min}_{\Theta(\Omega),k}$$

by (4.11). This situation happens only if the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$ is irreducible over the ground field k. In this case the stabilizer $G_\Omega L$ of the ideal I_Ω^L is a group acting transitively on $(M/L)_g$, the left classes of $M \mod L$. But, it is possible that the testing group L gives any information (i.e. $G = M$) and that the separable M-relative L-resolvents are not irreducible over the field k.

The G-orbit $G.L$ is known and correspond with the polynomial W of $k[T]$, a factor over k of the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$. The stabilizer in M of the G-orbit $G.L$ is supposed computed. It rests to identify the polynomial W. In case in which the Galois groups of factors of the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$ gives any information, we have the proposition 4.8:

PROPOSITION 4.8. *Suppose that the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$ is separable and V one of its factors. Then the condition $V = W$ is equivalent to $V(\Theta) \in I_\Omega^G$.*

PROOF. By definition of W we have $W(\Theta) \in I_\Omega^G$. Now, suppose that $V(\Theta) \in I_\Omega^G$. Then $(\forall \tau \in G)\ V(\tau.\Theta(\Omega)) = 0$ and there exists $i \in [1, e]$ such that $\tau.\Theta(\Omega) = \tau_i.\Theta(\Omega)$. As $\tau_i.\Theta(\Omega)$ is a simple root of the resolvent, we have $\tau.\Theta = \tau_i.\Theta$. Now, as $\tau_i^{-1}\tau \in M$ and Θ is an M-primitive L-invariant we have $\tau_i \in \tau L$. Finally $\tau_i \in GL$. □

But as the ideal I_Ω^G is unknown, this proposition is not useful.

Now, an M-primitive polynomial of the ideal $I_\Omega^{S'}$ is computable using the polynomial W in the same manner than for the ideal I_Ω^S using the polynomial $\mathrm{Min}_{\theta,k}$.

All elements are given in order to describe the algorithm `GaloisIdeal` derived from the algorithm `GaloisIdeal1`.

The algorithm `GaloisIdeal` is presented under the form of a recursive function. It can be executed by calling:

`GaloisIdeal(f,n,`$\mathfrak{S}_n$`,Generators,Candidates)`

where
- `n` is the degree n of the polynomial f represented by `f`;
- `Generators` is a list containing the symmetric group $\mathfrak{S}_n$ and the n Cauchy moduli of the polynomial f generating the ideal $I_\Omega^{\mathfrak{S}_n}$;
- `Candidates` contains all conjugacy classes of subgroups of $\mathfrak{S}_n$.

In each recursive call

`GaloisIdeal(f,n,M,Generators,Candidates)` ,

- `M` is a subgroup of $\mathfrak{S}_n$ containing the Galois group G_Ω;
- `Generators` is a list containing the Cauchy moduli of the polynomial f, distinct subgroups

$$M_1 = \mathfrak{S}_n \supset M_2 \supset \cdots \supset M_m$$

of $\mathfrak{S}_n$ and polynomials $R_2, \ldots, R_m$ of $k[x_1, \ldots, x_n]$ such that for each $i \in [2, m]$ the polynomial R_i is an $M_{(i-1)}$-primitive polynomial of the ideal $I_\Omega^{M_i}$;
- `Candidates` is a list of subgroups of M containing the groups which are candidate for the Galois group G_Ω (only one group by conjugacy class in M).

At each call of the algorithm, the list `Candidates` decreases and the list `Generators` increases. The first one converges to the Galois group by elimination of conjugacy classes and the second one converges to the maximal ideal of Ω-relations by construction of an ascending chain of ideals. The result of the algorithm is the list `Generators`. The smaller group M_m containing in the result `Generators` verifies:

$$I_\Omega = I_\Omega^{M_m}$$

with $M_m \subset G_\Omega$. When $M_m \neq G_\Omega$, it is easy to deduce the Galois group G_Ω from the ideal I_Ω (see Proposition 5.1.

We now define two functions used in algorithm.
- The function `Return` stops the execution of the function `GaloisIdeal` returning a result. For this reason, the alternation `Else` is absent in the tests `If-Then-Else`.
- Let S' be the group $\mathrm{Stab}_M(GL)$ and W the polynomial defined in (4.10); the function `R(M,`S'`,`W`)` compute an `M`-primitive polynomial of the ideal $I_\Omega^{S'}$ applying the fundamental theorem of symmetric function over the coefficients of the polynomial W.

Hypothesis. In the first step, it is to expensive to compute an absolute I_n-resolvent (I_n is the identity group in $\mathfrak{S}_n$). This resolvent, called the *Galois resolvent* determines immediately the ideal I_Ω (see Proposition 4.6).

Function GaloisIdeal(f, n, M, Generators, Candidates)

```
(A) Choose L a subgroup of M
*   Compute Θ an M-primitive L-invariant
    Compute And factorize F the M-relative L-resolvent L_{Θ,I_Ω^M}
    (suppose F is separable)
    Choose V a factor of F irreducible over k
    If L is a subgroup of the Galois group
      Then Add V(Θ) to Generators And Return Generators
    Take back from the list Candidates the excluded groups
                        (by group matrices or other methods)
    If Candidates contains only one group G (i.e.  G=G_Ω)
      Then If M=G Then Return Generators
      Compute P an M-primitive polynomial of the ideal of Ω-relations
      Add P and G to Generators And Return Generators
    Let H be the intersection of groups of the list Candidates
    If for a subgroup SH of H
      it is easy to compute an M-relative SH-resolvent
      Then L:=SH And Goto * with L (L is a subgroup of G_Ω)
    Compute G a minimal subgroup of M containing the groups of Candidates
    If G=M (the testing group L is not a good choice)
(B)   Then Choose another subgroup L of M
           Goto * with L (an exit will be produced)
    Compute the G-orbits of (M/L)_g (we have G≠ M)
**  Choose a G-orbit Or
(C) Determine the factor W of F corresponding to Or
    If it is not possible
      Then Change the orbit
           If all orbits are tested
(B)          Then Choose another subgroup L of M
                  Goto * with L
           Goto ** with the new orbit
(D) Compute S the stabilizer of Or in M
    If S=M for each orbit Or
(B)   Then Choose another subgroup L of M
           Goto * with L
    Add R(M,S,W) And S to the list Generators
(E) Change the conjugacy classes of groups in Candidates
    GaloisIdeal(f,n,S,Generators,Candidates)
```

PROOF. The algorithm finishes because it includes the one of group matrices. □

Comments about the algorithm `GaloisIdeal`

- (A) The good choice of a subgroup `L` of `M` depends on the complexity of the computation of `M`-relatives resolvents, on the informations given by the group matrix relative to the group `M` and on the length on the chain of ideals which must be small as much as possible.
- (B) It is not possible that all subgroups of `M` have been used as testing groups because before the Galois group is determined. Effectively, when all subgroups of `M` are used as testing groups, the group matrices relative to `M` suffices in order to determine the Galois group.
- (C) In order to determine the factor associated with an orbit, it must use the degree or the Galois groups of the factors or Proposition 4.8.
- (D) The stabilizer `S` of the orbit equals the union of groups of this orbit if this union is a group.
- The step (E) is indispensable since two conjugate subgroups in the group `M` are not necessary conjugate in its subgroup `S`.

Variant of algorithm `GaloisIdeal`.

The computation of a relative resolvent needs a Gröbner basis (see Chapter 9). Therefore, before to replace the group M by its subgroup S, it is possible to use many testing groups in M because the Gröbner basis of the ideal I_Ω^M is already computed. The advantage of the subgroup S is that the degrees of the S-relative resolvents is smaller than the degrees of the M-relative resolvents.

5. Compute the decomposition group of an ideal

PROPOSITION 5.1. *Let $(f_1, \ldots, f_m)$ be n-variate polynomials over the field k generating an ideal I of $k[x_1, \ldots, x_n]$. Suppose that $Gr(I)$, the decomposition group of the ideal I, is included in a subgroup M of the symmetric group $\mathfrak{S}_n$ (it is always included in $\mathfrak{S}_n$). Then $Gr(I)$ is the subgroup of M such that for each generator τ of $Gr(I)$ and for each $i \in [1, m]$ we have $\tau.f_i \in I$.*

PROOF. Obvious. □

6. Galois inverse problem

The group matrices can be used for computing polynomials for a given group (see **[65]**). Consider $\mathcal{C}_i$ and $\mathcal{C}_j$ two conjugacy classes in L such that: $\mathcal{C}_i$ is the conjugacy class of the Galois group of a known univariate polynomial f and $\mathcal{C}_j$ is the conjugacy class of a subgroup H of L. When computing an L-relative H-resolvent of f, the Galois groups of its separable irreducible factors over k are given by $\mathcal{G}_{i,j}^L$. In **[34]** polynomials of degree 12 using group matrices are computed. As it is noted in remark 33 it is possible to consider also the non transitive subgroups associated to the factors over k which are not irreducible.

An explicit example is given in Section 4.4 Chapter 9.

CHAPTER 8

Reducible polynomials

In all this chapter we will suppose that the field k is infinite.

1. Inclusion of Galois group of a reducible polynomial

In the following all is well known.

The Galois group over k of a univariate polynomial is transitive if, and only if, it is irreducible over k. In this section, we precise the type of non transitive Galois groups. The transitive subgroups of $\mathfrak{S}_n$ can be characterized by the following lemma:

LEMMA 1.1. *A subgroup of $\mathfrak{S}_n$ is transitive if, and only if, it is not contained in the direct product of two symmetric groups.*

PROOF. If $G \subset \mathfrak{S}_m \times \mathfrak{S}_{n-m}$, G acts on $[1, m]$ and $[m+1, n-m]$, no one element of G can take a digit of $[1, m]$ into one of $[m+1, n-m]$. Conversely, if one orbit of G is of size m, then G acts separately on $[1, m]$ and $[m+1, n-m]$, i.e. $G \subset \mathfrak{S}_m \times \mathfrak{S}_{n-m}$. □

LEMMA 1.2. *For g and h two distinct separable polynomials of respective degrees m and p, we have $G_{(\Omega_g, \Omega_h)} \subset \mathfrak{S}_m \times \mathfrak{S}_p$.*

PROOF. Set $f := gh$ and $\Omega_f = (\Omega_g, \Omega_h)$. Let $\sigma \in G_{\Omega_f}$, if $\sigma \notin \mathfrak{S}_m \times \mathfrak{S}_p$ then there exists $i \in [1, m]$ such that $\sigma(i) \notin [1, m]$. We have $g(x_i) \in I_{\Omega_f}$ and $\sigma.g(x_i) \in I_{\Omega_f}$. Since f is separable and $\alpha_{\sigma(i)} \notin \Omega_g$, it is impossible that $\sigma.g(x_i) \in I_{\Omega_f}$. Thus $\sigma \in \mathfrak{S}_m \times \mathfrak{S}_p$. □

THEOREM 1.3. *We have the following assertions:*

1. *Let g and h be two distinct separable polynomials. Then*

$$G_{(\Omega_g, \Omega_h)} \subset G_{\Omega_g} \times G_{\Omega_h} .$$

2. *Let f be a separable polynomial of $k[x]$. If there exist two groups $G \subset \mathfrak{S}_m$ and $H \subset \mathfrak{S}_p$ such that $G_{\Omega_f} \subset G \times H$ then there exist two polynomials g and h over k of respective degrees m and p such that $f = gh$ and, up to a permutation, $G_{\Omega_g} \subset G \subset \mathfrak{S}_m$ and $G_{\Omega_h} \subset H \subset \mathfrak{S}_p$.*

PROOF. 1. Set $f := gh$ and $\Omega_f = (\Omega_g, \Omega_h)$. Let $R \in I_{\Omega_g}$, as polynomial in $k[x_1, \ldots, x_n]$, the polynomial R also belongs to the ideal $I_{\Omega_g, \Omega_h} = I_{\Omega_f}$. Let $\sigma \in G_{\Omega_f}$. By Lemma 1.2, since f is a separable polynomial, we have $\sigma = (\tau, \tau')$ where $\tau \in \mathfrak{S}_m$ and $\tau' \in \mathfrak{S}_p$. As $\sigma.R(\Omega_g, \Omega_h) = 0$ for all $R \in I_{\Omega_f}$, we have in particular $\tau.R(\Omega_g) = 0$ for all $R \in I_{\Omega_g}$. Thus

$\sigma \in G_{\Omega_g} \times \mathfrak{S}_p$. By the same process we have $\sigma \in \mathfrak{S}_m \times G_{\Omega_h}$. Thus $\sigma \in G_{\Omega_g} \times G_{\Omega_h}$. (We can also use the theorems about the group and partition matrices).

2. We set $H := \mathfrak{S}_1 \times \mathfrak{S}_{n-1}$ and we assume that

$$G_{\Omega_f} \subset G \times H \subset \mathfrak{S}_m \times \mathfrak{S}_p$$

Each $(\mathfrak{S}_m \times \mathfrak{S}_p)$-orbit of $\mathfrak{S}_n \mod H$ contains a G_{Ω_f}-orbit of $\mathfrak{S}_n \mod H$. Thus, the separable absolute H-resolvent f has two factors g and h over k of respective degrees m and p. Let U be the union of G_{Ω_f}-orbits of $\mathfrak{S}_n \mod H$ associated with the polynomial g. With an adequate order of the G_{Ω_f}-orbits of $\mathfrak{S}_n \mod H$, the action of $G \times H$ on U equals the action of G on U and, on the other hand, the action of G_{Ω_g} on $[1, m]$ equals the action of G_{Ω_f} on U Therefore $G_{\Omega_g} \subset G$ because $G_{\Omega_f} \subset G \times H$. In the same way $G_{\Omega_h} \subset H$. □

Now, if $f = gh$ is reducible over k with $\deg(g) = m$ and $\deg(h) = p$ then the Galois group of f is included in $L = \mathfrak{S}_m \times \mathfrak{S}_p$. Thus it is sufficient to compute absolute multi-resolvents of degree $[L : H]$ instead of absolute resolvents of degree $[\mathfrak{S}_n : H]$. As, the computation of (absolute) multi-resolvents is quick, the case in which f is a reducible polynomial over k is a very nice situation. The computation of Galois groups G and H of g and h can also be used for computing the Galois of f with Theorem 3.4 given in Section 3. Effectively, for computing $(G \times H)$-relative resolvents of (Ω_g, Ω_h), a Gröbner basis of the ideal $I^{G\times H}_{(\Omega_g,\Omega_h)}$ must be computed (see **[12]**). With Theorem 3.4, we deduce this Gröbner basis from the Gröbner basis of the ideals $I^G_{\Omega_g}$ and $I^H_{\Omega_h}$ (see **[30]** for fast computations of Gröbner basis).

2. Primitive polynomial

Let L and H be two subgroups of $\mathfrak{S}_n$ such that L contains the group H and the Galois group G_Ω of the univariate polynomial f.

Notation 2.1. Let E be set of polynomials in $k[x_1, \ldots, x_m]$ $(m \in [1, n])$, the ideal generated by E in $k[x_1, \ldots, x_n]$ will be denoted by $< E >$.

Give Theorem 6.4 of Chapter 6:

THEOREM 2.2. *If the decomposition group $Gr(I^H_\Omega)$ contains the Galois group G_Ω then there exists a polynomial $R_{L,H}$ in the polynomial ideal I^H_Ω such that*

$$I^H_\Omega = I^L_\Omega + < R_{L,H} > \quad . \tag{2.1}$$

Such a polynomial verifies:

$$Gr(I^H_\Omega) = \{\sigma \in L \mid \ \sigma.R_{L,H}(\Omega) = 0\} \quad .$$

The polynomial $R_{L,H}$ of Theorem 2.2 is called an *L-primitive polynomial of the ideal* I^H_Ω.

Notation 2.3. Let $\theta \in k(\Omega)$, the polynomial $\mathrm{Min}_{\theta,k}$ is the minimal polynomial of θ over k.

When the field k is infinite, a construction of primitive elements is as follows: let Θ be an L-primitive H-invariant separable for Ω (which exists because k is infinite) and $\theta = \Theta(\Omega)$; the polynomial $R_{L,H} = \mathrm{Min}_{\theta,k}(\Theta)$ is an L-primitive polynomial of the ideal I_Ω^H.

LEMMA 2.4. *Let $g, h \in k[x]$ of respective degrees m and p. Let two subgroups $G \subset \mathfrak{S}_m$ and $H \subset \mathfrak{S}_p$ be given such that*

$$G_{\Omega_g} \subset G \qquad \text{and} \qquad G_{\Omega_h} \subset H \ .$$

If $R_G \in k[x_1, \ldots, x_m]$ is a $\mathfrak{S}_m$-primitive polynomial of the ideal $I_{\Omega_g}^G$ then R_G, as a polynomial in $k[x_1, \ldots, x_{m+p}]$, is a $(\mathfrak{S}_m \times H)$- primitive polynomial of the ideal $I_{(\Omega_g,\Omega_h)}^{G\times H}$.

PROOF. As $G_{\Omega_g} \subset G$ and $G_{\Omega_h} \subset H$, we have $G_{(\Omega_g,\Omega_h)} \subset G \times H$ (see Theorem 1.3). Thus $\mathrm{Gr}(I_{\Omega_g}^G) = G$ and $\mathrm{Gr}(I_{(\Omega_g,\Omega_h)}^{G\times H}) = G \times H$. Let $R_G \in k[x_1, \ldots, x_m]$ be a $\mathfrak{S}_m$-primitive polynomial of the ideal $I_{\Omega_g}^G$. Then $(\forall \sigma \in \mathfrak{S}_m)$ the condition $\sigma.R_G(\Omega_g) = 0$ is equivalent to $\sigma \in G$ (see Theorem 2.2). Now, let $\tau \in \mathfrak{S}_m \times H$, we can write $\tau = (\tau_1, \tau_2)$ where $\tau_1 \in \mathfrak{S}_m$ and $\tau_2 \in H$. As $\tau.R_G = \tau_1.R_G$, the condition $\tau.R_G(\Omega_g, \Omega_h) = 0$ is equivalent to the condition $\tau \in G \times H$. Therefore R_G is a $(\mathfrak{S}_m \times H)$- primitive polynomial of the ideal $I_{(\Omega_g,\Omega_h)}^{G\times H}$. □

3. Ideals and groups

In **[21]** it is proved that for g and h two univariate polynomials over k there is

$$G_{\Omega_{gh}} = G_{\Omega_g} \times G_{\Omega_h} \qquad \text{if, and only if,} \qquad I_{\Omega_{gh}} = < I_{\Omega_g}, I_{\Omega_h} > \qquad . \tag{3.1}$$

This section generalizes this equivalence.

Notation 3.1. For E a subset of $k[x_1, \ldots, x_n]$, we will denote by $< E >$ the ideal generated in $k[x_1, \ldots, x_n]$ by the polynomials of E.

LEMMA 3.2. *Let g and h be two univariate polynomials over k of respective degree m and p and $n = m+p$. Assume that $I_{\Omega_g} \subset k[x_1, \ldots, x_m]$ and $I_{\Omega_h} \subset k[x_{m+1}, \ldots, x_{m+p}]$. Put $\Omega_{gh} := (\Omega_g, \Omega_h)$. Then each subgroups $G \subset \mathfrak{S}_m$ and $H \subset \mathfrak{S}_p$ verify:*

$$< I_{\Omega_g}^G, I_{\Omega_h}^H > \subset \ I_{\Omega_{gh}}^{G\times H} \qquad . \tag{3.2}$$

PROOF. Set $B := < I_{\Omega_g}^G, I_{\Omega_h}^H > = k[x_1, \ldots, x_n]I_{\Omega_g}^G + k[x_1, \ldots, x_n]I_{\Omega_h}^H$. Let $\sigma \in G \times H$. We embed $k[x_1, \ldots, x_m]$ in $k[x_1, \ldots, x_n]$. For all $r \in I_{\Omega_g}^G$, by definition of $I_{\Omega_g}^G$, we have $\sigma.r(\Omega_g, \Omega_h) = \sigma.r(\Omega_g) = 0$. Therefore, for all $r \in k[x_1, \ldots, x_n]I_{\Omega_g}^G$ we also have $\sigma.r(\Omega_g, \Omega_h) = 0$. In the same way, if $r \in k[x_1, \ldots, x_n]I_{\Omega_h}^H$ then $\sigma.r(\Omega_g, \Omega_h) = 0$. Thus, if $r \in B$ then $\sigma.r(\Omega_g, \Omega_h) = 0$ so that $r \in I_{(\Omega_g,\Omega_h)}^{G\times H}$. □

LEMMA 3.3. *Let g and h be two univariate polynomials over k of respective degree m and p and $n = m + p$. Assume that $I_{\Omega_g} \subset k[x_1, \ldots, x_m]$ and $I_{\Omega_h} \subset k[x_{m+1}, \ldots, x_{m+p}]$. Set $\underline{x} := (x_1, \ldots, x_m)$, $\underline{y} := (x_{m+1}, \ldots, x_n)$,*

$$\mathcal{J}_g :=< e_1(\underline{x}) - e_1(\Omega_g), \ldots, e_m(\underline{x}) - e_m(\Omega_g) > \qquad \textit{and}$$
$$\mathcal{J}_h :=< e_1(\underline{y}) - e_1(\Omega_h), \ldots, e_p(\underline{y}) - e_p(\Omega_h) >$$

where e_i denotes the i-th elementary symmetric function (see Definition 1.2 Chapter 4). Then

$$\begin{aligned} I_{(\Omega_g,\Omega_h)}^{\mathfrak{S}_m \times \mathfrak{S}_p} &= < I_{\Omega_g}^{\mathfrak{S}_m}, I_{\Omega_h}^{\mathfrak{S}_p} > \\ &= k[x_1, \ldots, x_n]\sqrt{\mathcal{J}_g} + k[x_1, \ldots, x_n]\sqrt{\mathcal{J}_h} \qquad . \end{aligned}$$

If, moreover, gh is a separable polynomial then

$$I_{(\Omega_g,\Omega_h)}^{\mathfrak{S}_m \times \mathfrak{S}_p} = k[x_1, \ldots, x_n]\mathcal{J}_g + k[x_1, \ldots, x_n]\mathcal{J}_h \qquad .$$

PROOF. Put $B :=< I_{\Omega_g}^{\mathfrak{S}_n}, I_{\Omega_h}^{\mathfrak{S}_p} >$, and $\Omega_{gh} = (\Omega_g, \Omega_h)$. By Lemma 3.2 it is enough to prove that $I_{\Omega_{gh}}^{\mathfrak{S}_m \times \mathfrak{S}_p} \subset B$. Let us the polynomials

$$P = \prod_{i=1}^{n}(x - x_i) \quad , \quad Q = \prod_{i=1}^{m}(x - x_i) \qquad \text{and} \qquad R = P/Q \qquad .$$

As $P = QR$

$$\sum_{k=0}^{n}(-1)^k e_k(x_1, \ldots, x_n)x^{n-k} = \sum_{k=0}^{n}(-1)^k x^{n-k} \sum_{i+j=k} e_i(\underline{x})e_j(\underline{y})x^{n-k} \qquad .$$

Thus, for $k = 1, \ldots, n$:

$$e_k(x_1, \ldots, x_n) - e_k(\Omega_f) = \sum_{i+j=k}(e_i(\underline{x})e_j(\underline{y}) - e_i(\Omega_g)e_j(\Omega_h)) \qquad .$$

We have $e_k(x_1, \ldots, x_n) - e_k(\Omega_f) \in B$ because for $i \in [1, m]$ and $j \in [1, p]$ $e_i(\underline{x})e_j(\underline{y}) - e_i(\Omega_g)e_j(\Omega_h) = (e_i(\underline{x}) - e_i(\Omega_g))e_j(\underline{y}) + (e_j(\underline{y}) - e_j(\Omega_h))e_i(\Omega_g)$. Thus $I_{\Omega_{gh}}^{\mathfrak{S}_n} \subset B$ (see Section 4 Chapter 4). Now, as k is infinite and gh is separable, there exists Θ a $\mathfrak{S}_n$-primitive $(\mathfrak{S}_m \times \mathfrak{S}_p)$-invariant separable for Ω_{gh}. By fundamental theorem of symmetric functions, we have $\lambda = \Theta(\Omega_{gh}) \in k$ and the minimal polynomial of Θ over k is $T - \lambda$ so that $R = \Theta - \lambda$ is a primitive polynomial of the ideal $I_{\Omega_{gh}}^{\mathfrak{S}_m \times \mathfrak{S}_p}$ (see Definition 3.6 Chapter 6). The primitive polynomial R belongs to the ideal B because it is symmetric in variables of $\underline{x}$ and of the variables of $\underline{y}$ and $R(\Omega_{gh}) = 0$. In other words $I_{\Omega_{gh}}^{\mathfrak{S}_m \times \mathfrak{S}_p} = I_{\Omega_{gh}}^{\mathfrak{S}_n} + < R > \subset B$. □

Remark 37. The Galois group $G_{(\Omega_g,\Omega_h)}$ of gh is included in $\mathfrak{S}_m \times \mathfrak{S}_p$ because the separable resolvent $\mathcal{L}_{\Theta,gh}$ has $T - \lambda$ as simple linear factor over k (see Proof of Lemma 3.3).

Since the group $\mathfrak{S}_m \times \mathfrak{S}_p$ and its subgroup $G_{\Omega_g} \times G_{\Omega_h}$ contain the identity, we have

$$I_{(\Omega_g,\Omega_h)}^{\mathfrak{S}_m \times \mathfrak{S}_p} \subset I_{(\Omega_g,\Omega_h)}^{G_{\Omega_g} \times G_{\Omega_h}} \subset I_{(\Omega_g,\Omega_h)} \quad . \tag{3.3}$$

Now, the following theorem generalizes the result given in (3.1):

THEOREM 3.4. *Let g and h be two univariate polynomials over k of respective degree m and p and $n = m + p$. Put $\Omega_{gh} := (\Omega_g, \Omega_h)$. Assume that the product gh is a separable polynomial, $I_{\Omega_g} \subset k[x_1, \ldots, x_m]$ and $I_{\Omega_h} \subset k[x_{m+1}, \ldots, x_{m+p}]$. Then all subgroups $G \subset \mathfrak{S}_m$ and $H \subset \mathfrak{S}_p$ such that $\mathfrak{S}_m \times H$ or $G \times \mathfrak{S}_p$ contains the Galois group $G_{\Omega_{gh}}$ verify:*

$$I_{(\Omega_g,\Omega_h)}^{G \times H} =< I_{\Omega_g}^G, I_{\Omega_h}^H >$$

and in particular $I_{(\Omega_g,\Omega_h)}^{G_{\Omega_g} \times G_{\Omega_h}} =< I_{\Omega_g}, I_{\Omega_h} > \subset I_{(\Omega_g,\Omega_h)}$.

PROOF. Put $B =< I_{\Omega_g}^G, I_{\Omega_h}^H >$ and $\Omega_{gh} = (\Omega_g, \Omega_h)$. Lemma 3.2 gives the inclusion $B \subset I_{\Omega_{gh}}^{G \times H}$. Conversely, suppose that $\mathfrak{S}_m \times H$ contains the Galois $G_{\Omega_{gh}}$. Let R_G be a primitive polynomial of the ideal $I_{\Omega_g}^G$ and R_H be a primitive polynomial of the ideal $I_{\Omega_h}^H$. Using at first Lemma 2.4 and at last Lemma 3.3, we have

$$\begin{aligned} I_{\Omega_{gh}}^{G \times H} &= < I_{\Omega_{gh}}^{\mathfrak{S}_m \times H}, R_G > \\ &= < I_{\Omega_{gh}}^{\mathfrak{S}_m \times \mathfrak{S}_p}, R_H, R_G > \\ &= < I_{\Omega_g}^{\mathfrak{S}_m}, I_{\Omega_h}^{\mathfrak{S}_p}, R_H, R_G > \\ &= B \end{aligned}$$

by definition of the polynomials R_G and R_H. □

Therefore (3.1) is a consequence of Theorem 3.4:

COROLLARY 3.5. *For g and h two univariate polynomials over k the condition $I_{(\Omega_g,\Omega_h)} = I_{\Omega_{(\Omega_g,\Omega_h)}}^{G_{\Omega_g} \times G_{\Omega_h}}$ is equivalent to $G_{(\Omega_g,\Omega_h)} = G_{\Omega_g} \times G_{\Omega_h}$.*

PROOF. Set $\Omega := (\Omega_g, \Omega_h)$. We always have $I_\Omega = I_\Omega^{G_{\Omega_g} \times G_{\Omega_h}}$ when $G_\Omega = G_{\Omega_g} \times G_{\Omega_h}$. Conversely, the inclusion $G_\Omega \subset G_{\Omega_g} \times G_{\Omega_h}$ is given by lemma 1.2 and the reverse inclusion is given by the definition of the Galois group G_Ω, which is the maximal subgroup of $\mathfrak{S}_n$ stabilizing I_Ω. □

COROLLARY 3.6. *Under the same hypothesis as Theorem 3.4, a Gröbner basis for the lexicographic order of the ideal $I_{(\Omega_g,\Omega_h)}^{G \times H}$ is the union of the Gröbner basis for the lexicographic order of the ideals $I_{\Omega_g}^G$ and $I_{\Omega_h}^H$.*

PROOF. Let L be a subgroup of $\mathfrak{S}_n$ and Ω be a list of the roots of an univariate polynomial over k of degree n. A Gröbner basis for the lexicographic order of the ideal I_Ω^L of $k[x_1, \ldots, x_n]$ is a triangular system $f_1(x_1), \ldots, f_n(x_1, \ldots, x_n)$ where, for lexicographic order, the leading monomial of each polynomial f_i ($i \in [1, n]$) has the form $x_i^{\mu_i}$ with $\mu_i > 0$ (see **[12]**). □

4. Groups, ideals and fields

The following theorem is a collection of well known results:

THEOREM 4.1. *Let f be a separable polynomial of $k[x]$ of degree n such that $f = f_{n_1} \dots f_{n_d}$ and $\Omega_f = (\Omega_{f_{n_1}}, \dots, \Omega_{f_{n_d}})$. Set $G_{\Omega_{f_{n_i}}} := G_{n_i}$ and $D_i := k(\Omega_{f_{n_i}})$ for $i \in [1,d]$. The following conditions are equivalent:*

(1) *card*(G_{Ω_f}) =*card*$(G_{n_1}) \times \dots \times$ *card*(G_{n_d});
(2) $G_{\Omega_f} = G_{n_1} \times \dots \times G_{n_d}$;
(3) $D_i \cap k(\Omega_{f_{n_1}}, \dots, \Omega_{f_{n_{i-1}}}) = k$ *for all* $i \in [2,d]$;
(4) $I_{\Omega_f} = I_{\Omega_f}^{G_{\Omega_f}} = I_{\Omega_f}^{G_{n_1} \times \dots \times G_{n_d}}$.

PROOF. Equivalence between 1. and 2. : Theorem 1.3.

Equivalence between 4. and 2. : see Corollary 3.5

Equivalence between 3. and 2. : suppose that $d = 2$; we have $k(\Omega_{f_{n_1}}, \Omega_{f_{n_2}}) = D_1 \cup D_2$; but $D_1 \cap D_2 = k$ if, and only if, $[k : D_1 \cup D_2] = [k : D_1] \times [k : D_2]$; by the Galois correspondence, it is equivalent to write

$$\mathrm{card}(\mathrm{Gal}_k(D_1 \cup D_2)) = \mathrm{card}(D_1) \times \mathrm{card}(D_2) \ .$$

We conclude by induction on d. □

5. Multi-resolvents

Let $f_1, \dots, f_d$ be several polynomial of $k[x]$ of respective degrees $n_1, \dots, n_d$ strictly greater that 1 and such that the polynomial f is the product $f_1 \cdots f_d$.

For $i \in [1,d]$, we choose Ω_{f_i} an ordering of the roots of the polynomial f_i. Set $\Omega_f = (\Omega_{f_1}, \dots, \Omega_{f_d})$. Let L be a subgroup of $\mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_d}$. The resolvent by $\Theta \in k[x_1, \dots, x_n]$ associated with $I_{\Omega_f}^L$ is following polynomial:

$$\mathcal{L}_{\Theta, I_{\Omega_f}^L} = \prod_{\Psi \in L.\Theta} (T - \Psi(\Omega_{f_1}, \dots, \Omega_{f_d})) \qquad . \tag{5.1}$$

If the group L contains the direct product $G_{\Omega_{f_1}} \times G_{\Omega_{f_d}}$ of the Galois groups of $f_1, \dots, f_d$ then the resolvent $\mathcal{L}_{\Theta, I_{\Omega_f}^L}$ belongs to $k[T]$ because L contains the Galois group G_{Ω_f}.

When $L = \mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_d}$, the resolvent $\mathcal{L}_{\Theta, I(\Omega_{f_1}, \dots, \Omega_{f_d})^L}$ does not depend on the order of the roots of each polynomial f_i $(i \in [1,d])$.

Definition 5.1. The resolvent $\mathcal{L}_{\Theta, I_{(\Omega_{f_1}, \dots, \Omega_{f_d})}^{\mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_d}}}$ is denoted $\mathcal{L}_{\Theta, (f_1, \dots, f_d)}$ and called the *multi-resolvent of* $(f_1, \dots, f_d)$ *by* Θ.

The computation of multi-resolvents is a simple generalization of the one of resolvents. When $f = f_1 \cdots f_d$ is a reducible polynomial over k the partition and group matrices relative to $\mathcal{S} = \mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_d}$ are sufficient for computing the Galois group of f because it is containing in L. But the efficiency of the computation of the Galois group of a

polynomial depends on the degree of resolvents. The computation of the Galois group of f requires computations of multi-resolvents of degree $[\mathcal{S} : H]$, where H is a subgroup of $\mathcal{S}$, instead of resolvents of degree $[\mathfrak{S}_n : H]$ for an irreducible polynomial.

Example 5.2. We suppose that the polynomials are monic. Let $L = \mathfrak{S}_2 \times \mathfrak{S}_2 \subset \mathfrak{S}_4$. Suppose that f is a monic reducible separable polynomial of degree 4: $f = f_1 f_2$, where f_1 and f_2 are irreducible univariate polynomials over k of degree 2. Choose the order of roots of f such that $\Omega_f = (\Omega_{f_1}, \Omega_{f_2})$. If f_1 and f_2 are irreducible over k then the Galois group G_{Ω_f} is L or a conjugate of $H = [I_4, (1,2)(3,4)]$ in L. Now, an L-relative H-resolvent separable for Ω_f is irreducible if and only if the Galois group of f is L. The polynomial $\Theta = (x_1 - x_2)(x_3 - x_4)$ is an L-primitive H-invariant. The multi-resolvent of (f_1, f_2) by Θ is $\mathcal{L}_{\Theta,(f_1,f_2)} = (x^2 - \Delta(f_1)\Delta(f_2))$ where $\Delta(f_i)$ is the discriminant of f_i $(i = 1, 2)$. Thus the Galois group of f is L if and only if the product $\Delta(f_1)\Delta(f_2)$ is a square. The advantage of the multi-resolvent is clear: the computation of the multi-resolvent is instantaneous and its degree is 2 whereas the degree of an absolute H-resolvent is 12. This difference of degrees between resolvents and multi-resolvents increases with the degree of the polynomial f. Moreover, The polynomial f_1 is irreducible in D_{f_2} if and only if the Galois group of f_1 over D_{f_2} is $\mathfrak{S}_2$ and this is the case if and only if the Galois group of f is L.

Let L be a subgroup of $\mathfrak{S}_n$. Two subgroups which are conjugate in $\mathfrak{S}_n$ are not necessarily conjugate in L. This remark has a consequence for relative resolvents. For the candidate groups, this problem appears when f has two factors of the same degree. For a testing group this problem appears only when it is included in a product of more than two symmetric groups. Example 1.1 of Chapter 11 explains a method which allows one to avoid this problem for the candidate groups.

6. One factor has an alternating Galois group : Gal$(f) \subset \mathfrak{S}_2 \times \mathcal{A}_m$

LEMMA 6.1. *Denote by $\mathcal{A}_m$ the alternating group in $\mathfrak{S}_m$. Let $m \geq 3$, let h be a polynomial whose Galois group is $\mathcal{A}_m$ and let g be an irreducible polynomial of degree 2. Then the Galois group of hg is $\mathfrak{S}_2 \times \mathcal{A}_m$.*

PROOF. If $m \geq 5$: If this is not the case, g splits into two linear factors in D_h and D_g, the splitting field of g is a field between k and D_h. Thus the Galois group of g is a proper normal subgroup of $\mathcal{A}_m$. Contrary to the fact that $\mathcal{A}_m$ is simple for $m \geq 5$. For $m < 5$ see Sections concerning degrees 5 and 6 in Chapter 11. □

CHAPTER 9

Computation of resolvents

1. Different methods

The computation of resolvents can be done in many ways:

- using invariants (see **[13]** and **[23]**))
- by interpolation (see **[33]**)
- by successive resultants (see **[41]** and **[59]**)
- by Gröbner basis and successive resultants in $k[x_1, \ldots, x_n]/I_\Omega^L$ (see **[55]**, **[48]** and **[12]**)
- by generating functions (see **[18]**)
- by symmetric functions (see **[42]** and **[63]**)
- by linear algebra and trace (see **[4]** and **[22]**)
- by numerical methods (see **[60]** and **[27]**)

We will explain the method with linear algebra and trace (see Section 2), the method with triangular sets (see Section 3), the computation of some particular resolvents (see Section 4) and the computation of multi-resolvents (see Section 5).

In this chapter, we consider f a univariate polynomial of $k[x]$ of degree n and Ω an ordered set of its roots.

2. By linear algebra and traces

Let M_0, M and L be three subgroups of $\mathfrak{S}_n$ such that:

$$G_\Omega \subset L \subset M \subset M_0 \qquad .$$

Set $K := k(x_1, \ldots, x_n)^{\mathfrak{S}_n}$, $K_{M_0} := K(\underline{x})^{M_0}$, $K_M := K_{M_0}(\underline{x})^M$ and $u := [M_0 : M]$. Assume that Ψ is a K-primitive element of the field K_M such that the value $\Psi(\Omega)$ of k is already computed (the polynomial Ψ is an M_0-primitive M-invariant). The set $(1, \Psi, \ldots, \Psi^{u-1})$ is a K_{M_0}-vector space basis of K_M.

If Θ is an M-primitive L-invariant, then the coefficients of the generic resolvent $\mathcal{L}_\Theta^M$ belong to K_M (see Definition 5.6 Chapter 6). We search to compute their evaluation at Ω for computing the resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$.

Let $F \in K_M$ which can be do a coefficient of the resolvent $\mathcal{L}_\Theta^M$. Then F is a linear combination of the Ψ^i and its evaluation $F(\Omega)$ depends on that of the Ψ^i. Thus, the problem is to compute the coefficients of this linear combination.

A method is the following: Let $B_1, \ldots, B_u$ be a K_{M_0}-vector space basis of K_M. We search u values $y_1, \ldots, y_u$ in K_{M_0} such that:

$$F = y_1 B_1 + \cdots + y_u B_u \qquad . \tag{2.1}$$

Denote by Tr:=$\mathrm{Tr}_{M_0,M}$ the trace function of K_M over K_{M_0} and, for each $i, j \in [1, u]$, set c_j :=$\mathrm{Tr}(FB_j)$ and $a_{i,j}$:=$\mathrm{Tr}(B_i B_j)$. Equality (2.1) induces

$$c_j = y_1 a_{1,j} + \cdots + y_u a_{u,j} \tag{2.2}$$

which produces the linear system $C = AY$, where $C = (c_j)_{j\in[1,u]}$, $A = (a_{i,j})_{1\le i,j\le u}$ and the unknown vector $Y = (Y_i)_{i\in[1,u]}$. This system which has only one solution $(y_1, \ldots, y_u)$ and can be solved by linear algebra.

However, as the resolvent has $u = [M_0 : M]$ coefficients, it is much more efficient to make a precomputation of an orthogonal basis by Gram-Schmidt classical algorithm. Then for a such basis, $\mathrm{Tr}(FB_j) = c_j = y_j a_{j,j} = y_j \mathrm{Tr}(B_j, B_j)$ so that

$$F = \sum_{j=0}^{u} c_j . B_j / a_{j,j} \qquad . \tag{2.3}$$

3. Gröbner basis and successive resultants

Let M and L be two subgroups of $\mathfrak{S}_n$ such that $G_\Omega \subset \mathrm{Gr}(I_\Omega^L) \subset M$. Let F be an M-primitive polynomial of the ideal I_Ω^L. By Theorem 6.4 of chapter 6, we have:

$$I_\Omega^L = I_\Omega^M + < F > \qquad .$$

Then if a generating system of the ideal I_Ω^M is computed, it is possible to compute a Gröbner basis of the ideal I_Ω^L. We will suppose that $L = \mathrm{Gr}(I_\Omega^L)$.

This section shows how it is possible to compute the characteristic polynomial C_{Θ,I_Ω^L}, where Θ is an L-primitive invariant of a subgroup of L when some Gröbner basis of the ideal I_Ω^L is computed. The computation of the resolvent $\mathcal{L}_{\Theta,I_\Omega^L}$ is deduced from the one of the characteristic polynomial from reductions in the quotient ring

$$A_{I_\Omega^L} = k[x_1, \ldots, x_n]/I_\Omega^L$$

and by computations of some r-th roots.

Notation 3.1. The resultant of two polynomials $u(x)$ and $v(x)$ in the variable x will be denoted by $\mathrm{Res}_x(u(x), v(x))$.

3.1. Case $L = \mathfrak{S}_n$.

Denote by $f_1, \ldots, f_n$ the Cauchy moduli of the polynomial f (see Definition 4.2 Chapter 4).

THEOREM 3.2. *For $r \in [0, n-1]$, define the polynomials $\Psi_r \in k[T][x_{r+1}, \ldots, x_n]$ and $\Psi_n \in k[T]$ for Ψ_n) by induction:*

$$\Psi_0 := T - \Theta \tag{3.1}$$

$$\Psi_r := Res_{x_r}(f_r(x_r, \ldots, x_n), \Psi_{r-1}(x_r, \ldots, x_n)) \quad . \tag{3.2}$$

Then

$$\Psi_n = C_{\Theta, I_\Omega^{\mathfrak{S}_n}} \quad .$$

PROOF. see **[55]**. □

In **[48]** is given the algorithm extracted from Theorem 3.2 for computing the absolute resolvent $\mathcal{L}_{\Theta, I_\Omega^{\mathfrak{S}_n}}$. If the algorithm of **[48]** is realized in the quotient ring $A_{I_\Omega^{\mathfrak{S}_n}}$ then it computes a polynomial a power of which is the absolute resolvent (see **[55]**). The computation in $A_{I_\Omega^{\mathfrak{S}_n}}$ is much more efficient because it avoids computations of a few resultants and bounds the degree of each variable x_i by i, the degree of x_i in the i-th Cauchy modulus ($i \in [1, n]$).

3.2. General case.

The method described in Section 3.1 can be generalized for any subgroup L of $\mathfrak{S}_n$ which contains the Galois group G_Ω (see **[12]**). The complete proof of the result is not given because it contains many technical notations and definitions.
Let $E = \{f_1(x_1), \ldots, f_n(x_1, \ldots, x_n)\}$ be a set of polynomials in $k[x_1, \ldots, x_n]$.

Let K be a field extension of k such that $K \cap k[x_1, \ldots, x_n] = k$. Take Ψ a polynomial in $K[x_1, \ldots, x_n]$ and define recursively the $n+1$ polynomials $\Psi_0, \Psi_1, \ldots, \Psi_n$ relative as follows:

$$\begin{aligned} \Psi_n &:= \Psi \in K[x_1, \ldots, x_n] \qquad \text{and for } i \in [1, n-1] \\ \Psi_{i-1} &:= \mathrm{Res}_{x_i}(f_i(x_1, \ldots, x_i), \Psi_i(x_1, \ldots, x_i)) \in K[x_1, \ldots, x_{i-1}] \quad . \end{aligned} \tag{3.3}$$

For I an ideal of $k[x_1, \ldots, x_n]$, its algebraic variety $V(I)$ in $\hat{k}^n$ and $i \in [1, n]$, we set $V_i := V(I) \cap \hat{k}^i$ (we have $V_n = V(I)$).

The following theorem gives the computation of the characteristic polynomial $C_{\Theta, I}$ for some particular ideals:

THEOREM 3.3. *(Aubry-Avb) Let I be a zero-dimensional radical ideal of $k[x_1, \ldots, x_n]$. Suppose that there exist n polynomials $f_1(x_1), \ldots, f_n(x_1, \ldots, x_n)$ of I such that*

$$V_i = Z_{\hat{k}^i}(f_1(x_1), \ldots, f_i(x_1, \ldots, x_i)) \quad \textit{for each } i \in [1, n]$$

and such that for each $\beta = (\beta_1, \ldots, \beta_{i-1}) \in V_{i-1}$, *the polynomial* $f_i(\beta_1, \ldots, \beta_{i-1}, x_i)$ *as polynomial in* $\hat{k}[x_i]$ *is monic and has no multiple root. Let* Ψ_0 *defined as in 3.3. Then*

$$\Psi_0 = \prod_{\beta \in V(I)} \Psi(\beta) \quad . \tag{3.4}$$

In particular, when $\Theta \in k[x_1, \ldots, x_n]$ *and* $\Psi = (T - \Theta) \in k[T][x_1, \ldots, x_n]$, *we have*

$$\Psi_0 = C_{\Theta,I}(T) \quad . \tag{3.5}$$

PROOF. Start with $\Psi_0 = \mathrm{Res}_{x_1}(f_1(x_1), \Psi_1(x_1)) = \prod_{\beta_1 \in V_1} \Psi_1(\beta_1)$. By induction, we prove that for each $j \in [1, n]$

$$\Psi_0 = \prod_{\beta \in V_j} \Psi_j(\beta_1, \ldots, \beta_j) \quad .$$

Supposing that our assertion holds for $j = i - 1$, we have

$$\Psi_0 = \prod_{\beta \in V_{i-1}} \Psi_{i-1}(\beta_1, \ldots, \beta_{i-1}) \qquad (\star) \quad .$$

By definition of Ψ_{i-1}, identity $(\star)$ becomes

$$\Psi_0 = \prod_{\beta \in V_{i-1}} \mathrm{Res}_{x_i}(f_i(\beta_1, \ldots, \beta_{i-1}, x_i), \Psi_i(\beta_1, \ldots, \beta_{i-1}, x_i)) \quad .$$

Since $V_i = Z_{\hat{k}^i}(f_1, \ldots, f_i)$ and $f_i(\beta_1, \ldots, \beta_{i-1}, x_i)$ is separable in $\hat{k}[x_i]$, the result follows. □

If I satisfies the conditions of Theorem 3.3 then a reduced Gröbner basis for the lexicographic order of the ideal I is a set of polynomials $f_1, \ldots, f_n$ which satisfies the conditions.

When $I = I_\Omega^L$, where L is a subgroup of $\mathfrak{S}_n$ which contains the Galois group G_Ω then I satisfies the conditions of Theorem 3.3 (see **[12]**). As the case of $L = \mathfrak{S}_n$, the algorithm given in **[48]** realized in the quotient field $k[x_1, \ldots, x_n]/I_\Omega^L$ computes a polynomial $S(T)$ such that the resolvent $\mathcal{L}_{\Theta, I_\Omega^L} = S^m$ where $m \in \mathbb{N}^*$. In the case $m \neq 1$, any factor of the resolvent is separable and the polynomial S is not useful for the computation of Galois group G_Ω.

In Chapter 10, an explicit example will illustrate the computation of resolvents.

4. Compute Particular absolute resolvents

There exists many formulas for computing particular resolvents. For example, the product resolvent (the invariant is a product $x_1 \cdots x_r$) can be rapidly computed using resultants. For this section, we choose to explain the computation of absolute resolvents which depend on the Vandermonde determinant because their are not famous but very useful for the determination of Galois group.

For $r \in [1, n]$, we denote by $\delta_r(x_{u_1}, \ldots, x_{u_r})$ the Vandermonde determinant:

$$\delta_r(x_{u_1}, \ldots, x_{u_r}) = \prod_{1 \leq i < j \leq r} (x_{u_i} - x_{u_j})$$

and we set $\delta_r := \delta_r(x_1, \ldots, x_r)$. The Vandermonde determinant δ_n is a $\mathfrak{S}_n$-primitive $\mathcal{A}_n$-invariant, where $\mathcal{A}_n$ is the alternating subgroup of the symmetric group $\mathfrak{S}_n$.

Notation 4.1. For $P \in k[x_1, \ldots, x_n]$, we set $\tilde{P} := P(\Omega)$.

4.1. Computation with invariants $\delta_n\Theta$.

THEOREM 4.2. *Let f be an univariate polynomial with leading coefficient a_n and let $Disc(f)$ be its discriminant. Let $\Theta \in k[x_1, \ldots, x_n]$ such that $\sigma.\Theta \neq -\Theta$ for all $\sigma \in \mathfrak{S}_n$. The resolvent $\mathcal{L}_{\delta_n\Theta,f}$ is given by the following resultant:*

$$\mathcal{L}_{\delta_n\Theta,f}(y) = Res_x(\mathcal{L}_{\Theta,f}(x), y^2 - x^2 \frac{Disc(f)}{a_n^{2(n-1)}}) \quad , \tag{4.1}$$

and its degree is twice the degree of the resolvent $\mathcal{L}_{\Theta,f}$.

PROOF. Let $\theta_1, \ldots, \theta_s$ be the s roots of $\mathcal{L}_{\Theta,f}$, each being repeated as many times as its multiplicity. We have

$$\begin{aligned} \mathcal{L}_{\delta_n\Theta,f}(y) &= \prod_{i=1}^{s} (y - \tilde{\delta_n}\theta_i)(y + \tilde{\delta_n}\theta_i) \\ &= \prod_{i=1}^{s} (y^2 - \widetilde{\Delta_n}\theta_i^2) \\ &= \mathrm{Res}_x(\mathcal{L}_{\Theta,f}(x), y^2 - x^2\widetilde{\Delta_n}) \quad , \end{aligned}$$

where $\Delta_n = \delta_n^2$ satisfies $\mathrm{Disc}(f) = a_n^{2(n-1)}\widetilde{\Delta_n}$. □

Remark 38. Theorem 4.2 allows to compute the resolvent $\mathcal{L}_{\delta_n\Theta,f}$ very fast, since it is obtained directly from an ordinary resultant.

Remark 39. Since the computation is obtained from a resultant, the factorization of $\mathcal{L}_{\Theta,f}$ gives a partial factorization of the resolvent $\mathcal{L}_{\delta_n\Theta,f}$. We even can compute only the needed factors of this last resolvent. Namely, let q be a factor of $\mathcal{L}_{\Theta,f}$; then $\mathrm{Res}_x(q(x), y^2 - a_n^{2(1-n)}x^2\mathrm{Disc}(f))$ is a factor of $\mathcal{L}_{\delta_n\Theta,f}$. This remark is very important, since to search the Galois group of a polynomial, it is not always necessary to know all the factors of the considered resolvent. It will generally be sufficient to study some irreducible factors which are minimal polynomials of primitive elements of intermediate fields between k and the splitting field of f (see **[7]**,**[65]** and the examples at the end of this paper).

Remark 40. If the polynomial Θ is a primitive invariant of $\mathfrak{S}_m \times \mathfrak{S}_{n-m}$ (for example $\Theta = x_1 \cdots x_m$), then $\delta_n\Theta$ and $\delta_m^i\delta_{n-m}(x_{m+1}, \ldots, x_n)$ ($i = 1$ or $i = -1$) are primitive invariants of the same group. (See **[62]** for the computation of symmetric resolvents.)

Remark 41. If the polynomial Θ is a primitive invariant of $I_m \times \mathfrak{S}_{n-m}$ (for example $\Theta = x_1 x_2^2 \cdots x_m^m$), then $\delta_n\Theta$ is a primitive invariant of $I_m \times \mathcal{A}_{n-m}$. (See **[18]** or **[59]** or **[62]** for the computation of monomial and linear resolvents.)

The following theorem gives another formula for our resolvent:

THEOREM 4.3. *Under the same assumptions as in Theorem 4.2, denoting by g the resolvent of $\mathcal{L}_{\Theta,f}$ by x_1^2, we get*

$$\mathcal{L}_{\delta_n\Theta,f} = \widetilde{\Delta_n}^n g(\frac{y^2}{\widetilde{\Delta_n}}) \qquad , \tag{4.2}$$

where $Disc(f) = a_n^{2(n-1)}\widetilde{\Delta_n}$.

PROOF. The proof of Theorem 4.2 implies

$$\begin{aligned} \mathcal{L}_{\delta_n\Theta,f}(y) &= \prod_{i=1}^{s}(y^2 - \widetilde{\Delta_n}\theta_i^2) \\ &= \widetilde{\Delta_n}^n \prod_{i=1}^{s}(\frac{y^2}{\widetilde{\Delta_n}} - \theta_i^2) \qquad . \end{aligned}$$

□

This formula also works for the factorization, since $g = \mathrm{Res}_x(\mathcal{L}_{\Theta,f}, y - x^2)$.

Remark 42. Let us recall that a polynomial and any of its separable Tschirnhaus resolvent have the same Galois group. We also know that the Galois group of a simple factor of an H-resolvent of a polynomial g is determinated, up to conjugation, only by H and by the Galois group of g (see **[65]**). Let $\mathcal{L} = \mathcal{L}_{\Theta,f}$; since $\mathcal{L}_{\delta_n\Theta,f} = \mathcal{L}_{\delta_n x_1,\mathcal{L}}$, we may transform L rather than f by a Tschirnhaus resolvent when an interesting factor g of $\mathcal{L}_{\delta_n\Theta,f}$ is not square free. It will be sufficient to compute the Tschirnhaus resolvent of the factor of $\mathcal{L}_{\Theta,f}$ corresponding to the factor g of $\mathcal{L}_{\delta_n\Theta,f}$.

THEOREM 4.4. *Let f be an univariate polynomial with leading coefficient a_n and let $Disc(f)$ be its discriminant. Let $\Psi \in k[x_1, \ldots, x_n]$ for which there exists $\sigma \in \mathfrak{S}_n \backslash \mathcal{A}_n$ such that $\sigma.\Psi = -\Psi$ (see remark 45). Let F be the polynomial such that $F(x^2) = \mathcal{L}_{\Psi,f}(x)$, the resolvent $\mathcal{L}_{\delta_n\Psi,f}$ is given by the following resultant:*

$$\mathcal{L}_{\delta_n\Theta,f}(y) = Res_x(F(x), y^2 - \frac{xDisc(f)}{a_n^{2(n-1)}}) \tag{4.3}$$

and it has the same degree as the resolvent $\mathcal{L}_{\Psi,f}$.

PROOF. Suppose that the degree of $\mathcal{L}_{\Psi,f}(x)$ is $2s$ and let $\psi_1, -\psi_1, \ldots, \psi_s, -\psi_s$ be its roots (by assumption this resolvent is even). We have $F(x) = \prod_{i=1}^{n}(x - \psi_i^2)$, thus

$$\begin{aligned}\mathcal{L}_{\delta_n\Psi,f}(y) &= \prod_{i=1}^{s}(y - \psi_i\tilde{\delta_n})(y + \psi_i\tilde{\delta_n}) \\ &= \prod_{i=1}^{s}(y^2 - \psi_i^2\widetilde{\Delta_n}) \\ &= \mathrm{Res}_x(F(x), y^2 - x\widetilde{\Delta_n}) \quad .\end{aligned}$$

□

Remark 43. We also may apply remark 39 concerning the invariant $\delta_n\Theta$. The invariant $\delta_n\Psi$ generates a resolvent which can be computed and factorized quickly. But in this case we use a polynomial Q such that $Q(x^2)$ is a factor of $\mathcal{L}_{\Psi,f}(x)$. Hence if the resolvent $\mathcal{L}_{\Psi,f}(x)$ has an irreducible factor q_1 which is not even, we must multiply q_1 by other irreducible factors $q_2, \ldots, q_r$ of this resolvent in order to obtain an even factor $q = q_1 \cdots q_s$. Next we put $Q(x^2) = q(x)$ and we obtain a factor of the resolvent $\mathcal{L}_{\delta_n\Theta,f}$ using the following resultant:

$$\mathcal{L}_{\delta_n\Theta,f}(y) = \mathrm{Res}_x(Q(x), y^2 - \frac{x\mathrm{Disc}(f)}{a_n^{2(n-1)}}) \quad . \tag{4.4}$$

Remark 44. Suppose that $m > 1$ and that $\Psi = \delta_m = \prod_{i=1}^{m}(x_i - x_j)$. The polynomial δ_m is a primitive invariant of $\mathcal{A}_m \times \mathfrak{S}_m$ (of index $\binom{n}{m}$ in $\mathfrak{S}_n$), and $\delta_n\delta_m$ is a primitive invariant of $\mathcal{A}_{n-m} \times \mathfrak{S}_m$. This remark is very important. For example, for $n > 4$ it is much easier to compute the resolvent associated with $\delta_2 = x_1 - x_2$ than to compute the resolvent associated with δ_{n-2}. By Theorem 4.4 it is possible to compute an $(\mathcal{A}_{n-2} \times \mathfrak{S}_2)$-resolvent.

The following theorem gives another formula for computing our resolvent:

THEOREM 4.5. *Under the same hypothesis as in Theorem 4.4, denoting by g the resolvent of $\mathcal{L}_{x_1^2,F}$, we have:*

$$\mathcal{L}_{\delta_n\Psi,f} = \widetilde{\Delta_n}^n g(\frac{y^2}{\widetilde{\Delta_n}}) \quad , \tag{4.5}$$

where $Disc(f) = a_n^{2(n-1)}\widetilde{\Delta_n}$.

PROOF. clear □

Remark 45. If we have $\sigma.\Psi \neq -\Psi$ for all $\sigma \in \mathfrak{S}_n \backslash \mathcal{A}_n$ and if there exists $\sigma \in \mathcal{A}_n$ such that $\sigma.\Psi = -\Psi$, then Ψ is a primitive invariant of $\mathcal{A}_n$ and $\delta_n\Psi$ is a symmetrical polynomial in $x_1, \ldots, x_n$. In this case, we have $\mathcal{L}_{\delta_n\Psi,f} = (x - \widetilde{\delta_n\Psi})$.

THEOREM 4.6. *Let f be an univariate polynomial with leading coefficient a_n and $Disc(f)$ be its discriminant. Let $i \in \mathbb{N}^*$ and g be the univariate polynomial $g(z) = \prod_{k=1}^{n}(z - \frac{1}{f'^2(\alpha_k)})$, where $\alpha_1, \ldots, \alpha_n$ denote the roots of f. Then*

$$\mathcal{L}_{\frac{\delta_{n-i}(x_{i+1},\ldots,x_n)}{\delta_i},f}(y) = C^{\binom{n}{i}}\mathcal{L}_{x_1\cdots x_i,g}(\frac{y^2}{C}) \qquad , \tag{4.6}$$

where $C = \frac{Disc(f)}{a_n^{2(n-i-1)}}$.

PROOF. Consider the generic polynomial $F(x) = A_n \prod_{i=1}^{n}(x - x_i)$, where A_n denotes a new variable. The notation F' stands for the derivative of F relative to the variable x. The following identity:

$$\delta_{n-i}(x_{i+1}, \ldots, x_n)F'(x_1)F'(x_2)\cdots F'(x_i) = (-1)^{\frac{i(i-1)}{2}}A_n^i\delta_n\delta_i$$

shows that we can use the result of Theorem 4.3; so we obtain:

$$\mathcal{L}_{\frac{\delta_{n-i}(x_{i+1},\ldots,x_n)}{\delta_i},f}(y) = (a_n^{2i}\widetilde{\Delta_n})^{\binom{n}{i}}\mathcal{L}_{x_1\cdots x_i,g}(\frac{y^2}{a_n^{2i}\widetilde{\Delta_n}}) \qquad .$$

□

Remark 46. We also can use Theorem 4.2 and deduce a similar formula to compute this resolvent.

To compute the polynomial g the method is follows: the polynomial φ whose roots are the squares of the values of f' at the roots of f may be written as:

$$\varphi(y) = \prod_{k=1}^{n}(y - f'^2(\alpha_k)) = \mathrm{Res}_x(f(x), y - f'^2(x)) \qquad . \tag{4.7}$$

Taking $c = \varphi(0)$, we obtain: $g(z) = (-1)^n\frac{z^n}{c}\varphi(1/z)$.

Remark 47. For $i \in \mathbb{N}^*$, the functions $\frac{\delta_{n-i}(x_{i+1},\ldots,x_n)}{\delta_i}$, $\delta_{n-i}(x_{i+1}, \ldots, x_n)\delta_i$ and $\delta_n x_1 \ldots x_i$ are primitive invariants of the same group.

4.2. The invariants $\delta_n x_1$ and δ_{n-1}.

These two polynomials are primitive invariants of $\mathcal{A}_{n-1} \times \mathfrak{S}_1$, a subgroup of index $2n$ in $\mathfrak{S}_n$.

With $\Theta = x_1$, formula (4.1) of Theorem 4.2 entails

$$\mathcal{L}_{\delta_n x_1,f}(y) = \mathrm{Res}_x(f(x), y^2 - x^2\frac{\mathrm{Disc}(f)}{a_n^{2(n-1)}}) \qquad . \tag{4.8}$$

In the other hand, since $\delta_1(x_n) = 1$, with $i = 1$ the Formula (4.6) of Theorem 4.6 implies that

$$\mathcal{L}_{\delta_{n-1},p}(y) = C^n g(\frac{y^2}{C}) \qquad , \tag{4.9}$$

where $C = \frac{\mathrm{Disc}(f)}{a^{2n-4}}$ and $g(z) = \prod_{k=1}^{n}(z - \frac{1}{f'^2(\alpha_k)})$.

Now, give examples taken from **[65]**. The notation T_i^j corresponds to the group T_i of $\mathfrak{S}_j$ given in **[16]**. In our examples, we suppose that the resolvents are all square free. Otherwise, we use a Tschirnhaus transformation (see Remark 42).

4.3. Example for the direct Galois problem.

Our family of resolvents is useful in many situations. In the following example, we apply the Theorem 4.2.

Let $i, j \in \mathbb{N}$. For a subgroup of the symmetric group $\mathfrak{S}_j$, the notation $T_i(j)$ refer to the classification of **[16]**.

Let f be an irreducible monic polynomial of degree 10 such that its discriminant D is a square and whose resolvent $\mathcal{L}_{x_1x_2,f}$ of degree 45 has an irreducible factor h of degree 5 and two irreducible factors of degree 20. Suppose that the Galois group of h is the group $T_2^{(5)}$. Then the one of f is the group $T_{16}^{(10)}$ or the group $T_{23}^{(10)}$. Now with our method we compute directly the factor g of degree 10 of $\mathcal{L}_{x_1x_2,f}$ by the formula $g(y) = \mathrm{Res}_x(h(x), y^2 - x^2\,\mathrm{Disc}(f))$. If the Galois group of g is the group $T_2^{(10)}$ then the Galois group of f is the group $T_{16}^{(10)}$, if it is the group $T_2^{(10)}$ the Galois group of g is the group $T_{23}^{(10)}$. To determine the Galois group of g, it suffice to compute the resolvent $\mathcal{L}_{x_1x_2,g}$. If this resolvent has more than one irreducible factors of degree 5 the Galois group of g is the group $T_3^{(10)}$ otherwise it is the group $T_2^{(10)}$.

4.4. Example for the inverse Galois problem.

We have many examples where our family of resolvents are useful to compute polynomial of degree 12 with a fixed Galois group. We now give an example in degree 10 applying the Theorem 4.4.

Note H the subgroup of $\mathfrak{S}_{10}$ such that $\delta_{10}(x_1 - x_2)$ is a primitive invariant of it. From **[65]** we have the following result: if f is a polynomial of degree 10 whose the Galois group is the group $T_{29}^{(10)}$, then the Galois group of the simple irreducible factor of an H-resolvent of f is the group $T_{24}^{(10)}$. The Galois group of $f(x) = x^{10} + 10x^8 + 10x^7 + 20x^6 + 26x^5 + 30x^4 + 20x^3 + 20x^2 + 10x + 2$ is the group $T_{29}^{(10)}$. With `SYM` we compute in only 15 seconds the resolvent $\mathcal{L}_{x_1-x_2,p}$ (of degree 90) whose the simple irreducible factor of degree 10 is $q(y) = y^{10} + 20y^8 + 140y^6 + 120y^4 - 560y^2 + 1052$. We compute instantly π the simple irreducible factor of degree 10 of the resolvent $\mathcal{L}_{\delta_{10}(x_1-x_2),p}$ by our formulae:

$\pi(z) = \text{Resultant}_y(\text{subst}(y, y^2, q), z - y\text{Disc}(f))$. We obtain

$$\begin{aligned}\pi(z) \;=\; & z^{10} - 82716975622228439828906929500160z^8 + \\ & 23947343196309168966405701015245260150976691558521271636040089 60z^6 \\ & -84893648716553297860791415569795434646216702599856530145726010984 \\ & 10375126326842911582784061440z^4 \\ & -16385007033194715574406726257596460439383567504154799723346385793369 86 \\ & 12003791515766457278325594574926373458639645365250293760z^2 \\ & -12730310492466239998665754739410742256267540852760625851689045402252 8 \\ & 72502946473816198741843546882041265978460340564331835401231811995475512 30 \\ & 530390050471936\end{aligned}$$

The polynomial π has $T_{24}^{(10)}$ as Galois group (it can be simplified, but it isn't the preoccupation for our example).

5. Computation of multi-resolvents

Suppose that f is a reducible polynomial:

$$f = f_1 \cdots f_d$$

with $\deg_{x_i}(f_i) = n_i \neq 0$ and $n = n_1 + \cdots + n_d$. Set

$$\Omega_f := (\Omega_{f_1}, \ldots, \Omega_{f_d}) \qquad \text{and} \tag{5.1}$$

$$L := \mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_d} \subset \mathfrak{S}_n \qquad . \tag{5.2}$$

We have $G_\Omega \subset L$ (see Chapter 8).

The computation of the multi-resolvent $\mathcal{L}_{\Theta, I_\Omega^L} = \mathcal{L}_{\Theta,(f_1,\ldots,f_d)}$ (see Definition 5.12 Chapter 6). is a generalization of computation of absolute resolvent.

For example, in order to compute a multi-resolvent of (f_1, f_2) we must consider that we compute, at first, an absolute resolvent of f_1 with coefficients in $k(\Omega_{f_2})$ and after an absolute resolvent of f_2 (see **[62]**, **[35]** or **[55]** for explicit algorithms). The following example illustrates the algorithm using Cauchy moduli:

Example 5.1. Suppose that $n = 6$ and $f = uv$ where u and v are polynomials of degree 3 over k. The polynomial $t_6 = x_1x_4 + x_2x_5 + x_3x_6$ is a $(\mathfrak{S}_3 \times \mathfrak{S}_3)$-primitive T_{21}-invariant (see Section 5 Chapter 11). The absolute multi-resolvent $\mathcal{L}_{t_6,(u,v)}$ can be computed as an absolute resolvent using Cauchy moduli (see Section 3.1): let $u_1(x_1), u_2(x_1, x_3)$ and $u_3(x_1, x_2, x_3)$ be the Cauchy moduli of u and $v_1(x_4), v_2(x_4, x_5)$ and $v_3(x_4, x_5, x_6)$ those of v; let

$$U(x_1, x_2, x_3, T) = \text{Res}_{x_4}(v_1, \text{Res}_{x_5}(v_2, \text{Res}_{x_6}(v_3, T - t_6))) \qquad ,$$

and let be W given by $W^2(x_1, T) = \text{Res}_{x_2}(u_2, \text{Res}_{x_3}(u_3, U))$. Then we have

$$\mathcal{L}^3_{t_6,(u,v)} = \text{Res}_{x_1}(u_1, W) \qquad .$$

We have powers of the polynomial W and of the resolvent. Those powers are removed by using a specific algorithm (see **[48]**). In practice, the computation of resultants are realized modulo the ideal $I^{\mathfrak{S}_3\times\mathfrak{S}_3}_{(\Omega_u,\Omega_v)} =< u_1,u_2,u_3,v_1,v_2,v_3 >$.

We will describe some methods for computing particular multi-resolvents.

5.1. Projection.

Suppose that $f = gh$ where $g,h \in k[x]$ and $\deg(g) = m$. Set $\Omega_f = (\Omega_g,\Omega_h)$. Let $\Theta \in k[x_1,\ldots,x_n]$, be such that it depends only on the variables $x_1,\ldots,x_m$. Let G be a subgroup of $\mathfrak{S}_m$ and H be a subgroup of $\mathfrak{S}_{n-m}$. Then

$$L_{\Theta,I^{G\times H}_{\Omega_f}} = L_{\Theta,I^{G}_{\Omega_g}} \quad . \tag{5.3}$$

5.2. Product of discriminants.

Suppose that $f = f_1\cdots f_d$ such that each f_i is a monic polynomial of $k[x]$ of degree $n_i > 0$ for $i \in [1,d]$. Let us consider the following invariant:

$$\Theta = \delta_{1,n_1}\delta_{n_1+1,n_1+n_2}\cdots\delta_{n_1+\cdots+n_{d-1}+1,n}$$

where, for $i < j \leq n$, $\delta_{i,j} = \prod_{i\leq p<q\leq j}(x_p - x_q)$ is a Vandermonde determinant. Then the multi-resolvent of $(f_1,\ldots,f_d)$ by Θ is:

$$\mathcal{L}_{\Theta,(f_1,\ldots,f_d)} = (x^2 - \Delta(f_1)\Delta(f_2)\cdots\Delta(f_d)) \quad , \tag{5.4}$$

where $\Delta(g)$ denotes the discriminant of a univariate polynomial g.

5.3. Product by a Vandermonde.

Suppose that f can be factored as $f = gh$ where g and h are monic univariate polynomial over k of respective degree m and p. Putting $\Omega_f := (\Omega_g,\Omega_h)$ we have $G_{\Omega_f} \subset \mathfrak{S}_m\times\mathfrak{S}_p$. Let $\Theta \in k[x_{m+1},\ldots,x_n]$ and let H be a subgroup of $\mathfrak{S}_p$ which contains G_{Ω_h}. We want to compute the relative $(\mathfrak{S}_m\times H)$-resolvent $\mathcal{L}_{\delta_m\Theta,I^{\mathfrak{S}_m\times H}_{\Omega_f}}$.

Case $(-\Theta)$ does not belong to the orbit $H.\Theta$.

We have:

$$L_{\delta_m\Theta,I^{\mathfrak{S}_m\times H}_{\Omega_f}}(y) \;=\; \mathrm{Res}_x(\mathcal{L}_{\Theta,I^{H}_{\Omega_h}}(x), y^2 - \Delta(g)x^2) \tag{5.5}$$

Indeed:

$$\begin{aligned}\mathcal{L}_{\delta_m\Theta,I^{\mathfrak{S}_m\times H}_{\Omega_f}}(y) &= \prod_{\Psi\in H.\Theta}(y-\delta_m\Psi)(y+\delta_m\Psi)\\ &= \prod_{\Psi\in H.\Theta}(y^2-\delta_m^2\Psi^2) \quad .\end{aligned}$$

The degree of the resolvent $L_{\delta_m\Theta,I_{\Omega_f}^{\mathfrak{S}_m\times H}}$ is twice of the degree of the resolvent $L_{\Theta,I_{\Omega_h}^H}$.

Case $(-\Theta)$ belongs to the orbit $H.\Theta$.

The resolvent $\mathcal{L}_{\Theta,I_{\Omega_h}^H}$ is even. Suppose that its roots are given by: $L_{\Theta,I_{\Omega_h}^H}(y) = \prod_{i=1}^m (y^2-\theta_i^2)$, where $\theta_i \in \hat{k}$ and set $F(y^2) = L_{\Theta,I_{\Omega_h}^H}(y)$. We have:

$$\mathcal{L}_{\delta_m\Theta,I_{\Omega_f}^{\mathfrak{S}_m\times H}}(y) = \mathrm{Res}_x(F(x), y^2-\Delta(g)x) \tag{5.6}$$

Indeed:

$$L_{\delta_m\Theta,I_{\Omega_f}^{\mathfrak{S}_m\times H}}(y) = \prod_{i=1}^m (y-\delta_m\theta_i)(y+\delta_m\theta_i) \prod_{\Psi\in H.\Theta} (y^2-\delta_m^2\theta_i^2) \quad .$$

The degree of the resolvent $\mathcal{L}_{\delta_m\Theta,I_{\Omega_f}^{\mathfrak{S}_m\times H}}$ equals the one of the resolvent $\mathcal{L}_{\Theta,I_{\Omega_h}^H}$.

Example 5.2. Let $f = h_2h_4$ and $\Theta = \delta_2(x_3x_4 - x_5x_6)$. Setting $\Psi_1 = x_3x_4 - x_5x_6$, $\Psi_2 = x_3x_5 - x_4x_6$, $\Psi_3 = x_3x_6 - x_4x_5$ and $F(z^2) = \mathcal{L}_{\Psi_1,h_4}(z)$, the multi-resolvent of (h_2,h_4) by Θ is given by:

$$\begin{aligned}\mathcal{L}_{\Theta,(h_2,h_4)} &= (x^2-\Delta(h_2)\Psi_1^2)(x^2-\Delta(h_2)\Psi_2^2)(x^2-\Delta(h_2)\Psi_3^2)\\ &= \mathrm{Res}_z(F(z), x^2-z\Delta(h_2)) \quad .\end{aligned}$$

Partial Computation.

If the resolvent $\mathcal{L}_{\Theta,I_{\Omega_h}^H}$ is partially factorized, we can compute only some factors of the resolvent $\mathcal{L}_{\delta_m\Theta,\mathfrak{S}_m\times H,\Omega_f}$ since it is computed using a resultant.

CHAPTER 10

An explicit example

We give an example in which a relations ideal is computed. The motivation of this example is essentially the illustration of
- the method of Section 3 Chapter 9 for computing resolvents;
- the algorithm `GaloisIdeal` of Chapter 7 for computing the Galois Ideal.

Notation 0.3. For a subset $E \subset \mathbb{Q}[x_1, \ldots, x_n]$, we will denote by $< E >$ the ideal generated by E in $\mathbb{Q}[x_1, \ldots, x_n]$.

We consider the polynomial $f = x^6 + 2$ which is irreducible over $\mathbb{Q}$. Denote by Ω an ordered set containing the 6 roots of f. We will compute the ideal I_Ω of the Ω-relations by computing an increasing chain of ideals between $I_\Omega^{\mathfrak{S}_6}$, the ideal of symmetric relations among the roots of f and I_Ω.

The first step consists in computing a triangular set which generates the ideal I_Ω^M for $M = \mathfrak{S}_6$. This set is given by the Cauchy moduli of the polynomial f:

$$\begin{aligned} I_\Omega^{\mathfrak{S}_6} \;=\; & < x_6 + x_5 + x_4 + x_3 + x_2 + x_1, \\ & x_5^2 + x_4x_5 + x_3x_5 + x_2x_5 + x_1x_5 + x_4^2 + x_3x_4 + x_2x_4 + x_1x_4 \\ & + x_3^2 + x_2x_3 + x_1x_3 + x_2^2 + x_1x_2 + x_1^2, \\ & x_4^3 + x_3x_4^2 + x_2x_4^2 + x_1x_4^2 + x_3^2x_4 + x_2x_3x_4 + x_1x_3x_4 + x_2^2x_4 + x_1x_2x_4 + x_1^2x_4 \\ & + x_3^3 + x_2x_3^2 + x_1x_3^2 + x_2^2x_3 + x_1x_2x_3 + x_1^2x_3 + x_2^3 + x_1x_2^2 + x_1^2x_2 + x_1^3, \\ & x_3^4 + x_2x_3^3 + x_1x_3^3 + x_2^2x_3^2 + x_1x_2x_3^2 + x_1^2x_3^2 + x_2^3x_3 + x_1x_2^2x_3 \\ & + x_1^2x_2x_3 + x_1^3x_3 + x_2^4 + x_1x_2^3 + x_1^2x_2^2 + x_1^3x_2 + x_1^4, \\ & x_2^5 + x_1x_2^4 + x_1^2x_2^3 + x_1^3x_2^2 + x_1^4x_2 + x_1^5, x_1^6 + 2 > \qquad . \end{aligned}$$

Choose $L = \mathfrak{S}_1 \times \mathfrak{S}_5$. The polynomial $\Theta_1 = x_1$ is a primitive L-invariant. The absolute resolvent $\mathcal{L}_{\Theta_1, f}$ equals f. As f is irreducible over $\mathbb{Q}$, its Galois group is transitive. Thus, the candidate groups are the transitive subgroups of $\mathfrak{S}_6$.

Choose $L = \mathcal{A}_6$, the alternating subgroup of $\mathfrak{S}_6$. Denote by Θ_2 the Vandermonde determinant which is a primitive $\mathcal{A}_6$-invariant. Since the discriminant of f is not a square, the Galois group of f is not contained in $\mathcal{A}_6$.

Now, let $L =$PGL$_2(5)$ be the transitive maximal subgroup of $\mathfrak{S}_n$ of degree 120. We denote by Θ_3 the primitive L-invariant given in **[33]** (this invariant is very big). The

computation of the absolute resolvent of f by Θ_3 is realized by the method of **[55]** (see Theorem 3.2 Chapter 9). Its factorization over $\mathbb{Q}$ is the following:

$$\mathcal{L}_{\Theta_3,I_f^{\mathfrak{S}_6}} = \mathcal{L}_{\Theta_3,f} = (T-42)(T-24)^2(T+6)^3 \quad .$$

In this case, the partition matrix method (see **[7]** or Section 2 Chapter 7) indicates that the Galois group of f is one of the following groups: $\mathrm{PGL}_2(5)$, $\mathrm{PSL}_2(5)$, the dihedral group $\mathcal{D}_6$ or the cyclic group $\mathcal{C}_6$ which are included in $\mathrm{PGL}_2(5)$. By Theorem 6.4 of Chapter 6, we have

$$I_\Omega^L = I_f^{\mathfrak{S}_6} + < \Theta_3 - 42 >$$

where 42 is the value given by the linear factor over $\mathbb{Q}$ of the resolvent $\mathcal{L}_{\Theta_3,f}$. The logicial FGb (see **[30]**) computes the triangular set which generates the ideal I_Ω^L:

$$\begin{aligned} I_\Omega^L \;=\; & < 24x_6 + x_3^3x_2^3x_1 + 8x_3^3x_2^2x_1^2 + 6x_3^3x_2x_1^3 + 5x_3^3x_1^4 + 8x_3^2x_2^3x_1^2 + 4x_3^2x_2^2x_1^3 + 8x_3^2x_2x_1^4 \\ & + 6x_3x_2^3x_1^3 + 8x_3x_2^2x_1^4 - 4x_3x_2x_1^5 + 12x_3 + 5x_2^3x_1^4 + 12x_2 + 14x_1, \\ & 24x_5 - 5x_3^3x_2^4 - 7x_3^3x_2^3x_1 - 16x_3^3x_2^2x_1^2 - 7x_3^3x_2x_1^3 - 5x_3^3x_1^4 - 8x_3^2x_2^4x_1 - 12x_3^2x_2^3x_1^2 \\ & - 12x_3^2x_2^2x_1^3 - 8x_3^2x_2x_1^4 - 12x_3x_2^4x_1^2 - 16x_3x_2^3x_1^3 - 12x_3x_2^2x_1^4 + 8x_3 - 5x_2^4x_1^3 \\ & - 5x_2^3x_1^4 - 2x_2 - 2x_1, \\ & 24x_4 + 5x_3^3x_2^4 + 6x_3^3x_2^3x_1 + 8x_3^3x_2^2x_1^2 + x_3^3x_2x_1^3 + 8x_3^2x_2^4x_1 + 4x_3^2x_2^3x_1^2 + 8x_3^2x_2^2x_1^3 \\ & + 12x_3x_2^4x_1^2 + 10x_3x_2^3x_1^3 + 4x_3x_2^2x_1^4 + 4x_3x_2x_1^5 + 4x_3 + 5x_2^4x_1^3 + 14x_2 + 12x_1, \\ & x_3^4 + x_3^3x_2 + x_3^3x_1 + x_3^2x_2^2 + x_3^2x_2x_1 + x_3^2x_1^2 + x_3x_2^3 \\ & + x_3x_2^2x_1 + x_3x_2x_1^2 + x_3x_1^3 + x_2^4 + x_2^3x_1 + x_2^2x_1^2 + x_2x_1^3 + x_1^4, \\ & x_2^5 + x_2^4x_1 + x_2^3x_1^2 + x_2^2x_1^3 + x_2x_1^4 + x_1^5, x_1^6 + 2 > \quad . \end{aligned}$$

Denote by f_i the generator of I_Ω^L given in the previous formula; $f_i \in k[x_1,\ldots,x_i]$ and derivative$(f_i,x_i) \neq 0$.
Now, set $M :=\mathrm{PGL}(2,5)$ and choose $L = \mathcal{D}_6$. The situation is the following:

$$I_f^{\mathfrak{S}_6} \subset I_\Omega^{\mathrm{PGL}(2,5)} \subset I_\Omega^{\mathcal{D}_6} \subset I_\Omega \quad .$$

The polynomial primitive $\mathcal{D}_6$-invariant

$$\Theta_4 = x_1x_4 + x_4x_5 + x_5x_2 + x_2x_3 + x_3x_6 + x_6x_1$$

is a fortiori a $\mathrm{PGL}(2,5)$-primitive $\mathcal{D}_6$-invariant. We must compute a $\mathrm{PGL}(2,5)$-relative resolvent of f by Θ_4 whose degree is 10 the index of the group L in the group M. Let

$$V_0(T,x_1,\ldots,x_6) := T - \Theta_4 \quad .$$

The reduction of V_0 modulo the ideal I_Ω^M (given by successive Euclidian divisions) eliminates the variables x_6, x_5 and x_4 in V_0. Let $W_0(T,x_1,x_2,x_3)$ be the result of this reduction and

$$V_1(T,x_1,x_2) := \mathrm{Res}_{x_3}(f_3,W_0) \quad .$$

The reduction of V_1 modulo the ideal I_Ω^M does not eliminate the variables x_1 and x_2 of respective degree 32 and 28 in V_1 but produces a new polynomial $W_1(T, x_1, x_2)$ of degree 4 in each variable x_1 and x_2.
The elimination of the variable x_2 is given by

$$V_2(T, x_1) := \mathrm{Res}_{x_2}(f_2, W_1) \quad .$$

The reduction of V_2 modulo the ideal I_Ω^M produces a univariate polynomial of degree 20 whose factorization (in fact the square free form) is the following polynomial :

$$T^2(T^3-2)^2(T^3+2)^4 \quad .$$

Then the factorization over $\mathbb{Q}$ of the $\mathcal{D}_6$-resolvent is:

$$\mathcal{L}_{\Theta_4, I_\Omega^M} = T(T^3-2)(T+2)^2 \quad .$$

The partition matrix relative to M indicates that the Galois group of f is $\mathcal{D}_6$ or $\mathcal{C}_6$. The ideal fixed by $\mathcal{D}_6$ is given by:

$$I_\Omega^{\mathcal{D}_6} = I_\Omega^{\mathrm{PGL}(2,5)} + < \Theta_4 - 0 > \ ,$$

where 0 is the value given by the simple linear factor over $\mathbb{Q}$ of the resolvent $\mathcal{L}_{\Theta_4, I_\Omega^M}$. A triangular set of generators of our ideal, computed by FGb, is the following:

$$I_\Omega^{\mathcal{D}_6} =< x_6 - x_3 - x_1, x_5 + x_3 + x_1, x_4 + x_3, x_3^2 + x_1x_3 + x_1^2, x_2 + x_1, x_1^6 + 2 > \quad .$$

Now, set $M := \mathcal{D}_6$ and choose $L = \mathcal{C}_6$. Let

$$\Theta_5 = x_4x_5^2 + x_3x_6^2 + x_5x_2^2 + x_2x_3^2 + x_6x_1^2 + x_1x_4^2$$

be an M-primitive L-invariant. The degree of an M-relative L-resolvent is 2, the index of $\mathcal{C}_6$ in $\mathcal{D}_6$. The reduction of Θ_5 modulo the ideal $I_\Omega^{\mathcal{D}_6}$ produces the value 0. We are in a degenerated case: the resolvent equals T^2 and the computation of the resolvent modulo the ideal $I_\Omega^{\mathcal{D}_6}$ produces the polynomial T. Many $\mathcal{D}_6$-primitive $\mathcal{C}_6$-invariants computed by Abdeljaouad's package are in this case. In order to find a $\mathcal{D}_6$-primitive $\mathcal{C}_6$-invariant which is not degenerated, we adopt the Colin's method (see **[22]**). We replace the invariant $\Theta_5(x_1, \ldots, x_6)$ by the invariant

$$\Psi = \Theta(p(x_1), \ldots, p(x_6))$$

where $p(x) = x^2 + 1$. The computation of the $\mathcal{D}_6$-relative resolvent of f by Ψ is realized using two reductions modulo the ideal $I_\Omega^{\mathcal{D}_6}$ and one resultant. It is the following irreducible polynomial:

$$\mathcal{L}_{\Psi, I_\Omega^{\mathcal{D}_6}} = T^2 - 24T + 252 \quad .$$

Since this resolvent is irreducible over $\mathbb{Q}$, the Galois group of f over $\mathbb{Q}$ is $\mathcal{D}_6$ and the ideal I_Ω of relations among the roots of f is $I_\Omega^{\mathcal{D}_6}$.

CHAPTER 11

Computation of Galois groups up to degree 7

We consider f a *separable* monic univariate polynomial over the field k of degree $n \in [3, 7]$.

In the present chapter are presented the results of a complete investigation of partition and group matrices carried out for the purpose of computing the Galois group of the polynomial f over k.

The matrices of partitions and of groups are computed using the software `GAP` ([**36**]).

Previous results about irreducible polynomials are included in our tables. The references are the following: in [**52**] the linear resolvents are used for irreducible polynomials of degree less than 7 and [**13**], [**14**], [**31**] and [**33**] use maximal groups as testing groups for irreducible polynomials of degree respective 5,6,7, and 6. The given partition matrices relative to the symmetric groups are taken from [**9**].

The research is completed by some considerations about factorizations in extension fields.

The computation of Galois groups for degrees bigger than 7 is possible (see [**9**], for example for irreducible polynomials) but a presentation on a paper will be very complicated.

1. The problem of the conjugacy classes

Let L be a subgroup of $\mathfrak{S}_n$. Two subgroups which are conjugate in $\mathfrak{S}_n$ are not necessarily conjugate in L. For the candidate groups, this problem appears when f has two factors of the same degree. For a testing groups this problem appears only when L is a product of more than two symmetric groups. Example 1.1 explains a method which allows one to avoid this problem for the candidate groups. For testing groups there is an example in Remark 48.

Example 1.1. Suppose that $n = 6$ (see Section 5). The groups $T_{25}^1 = [(1,2),(3,4)(5,6)]$, $T_{25}^2 = [(3,4),(1,2)(5,6)]$ and $T_{25}^3 = [(5,6),(1,2)(3,4)]$ are conjugate in $\mathfrak{S}_6$ and not in $T_{23} = \mathfrak{S}_2 \times \mathfrak{S}_2 \times \mathfrak{S}_2$. If f splits over k into three irreducible factors f_1, f_2 and f_3 of degree

2:

$$f = f_1 f_2 f_3$$

then the three testing groups T_{25}^1, T_{25}^2 and T_{25}^3 induce the same partitions and each polynomial

$$\mathcal{L}_i(x) = (x^2 - \Delta(f_j)\Delta(f_k))$$

$(i \neq j \neq k \neq i)$ is a T_{23}-relative T_{25}^i-resolvent. In order to know if G_{Ω_f} is included in one of the groups T_{25}^i, it is necessary to compute the three products $\Delta(f_j)\Delta(f_k)$ and check if one of them is a square. After this computation, it is still possible to partially fix an ordering of the roots of f. For example, if $\Delta(f_1)\Delta(f_2)$ is a square then the Galois group G_{Ω_f} is included in T_{25}^3 and $\Omega_f = (\Omega_{f_j}, \Omega_{f_k}, \Omega_{f_3})$ with $j, k = 1, 2$ (i.e. the evaluation of x_5, x_6 must be performed at the roots of f_3).

Another example is the group $T_{19} \subset \mathfrak{S}_3 \times \mathfrak{S}_3$ in $\mathfrak{S}_6$ (see Section 5).

2. Notations for tables

The decomposition field of a polynomial h will be denoted by D_h.

The alternating group in $\mathfrak{S}_n$ is denoted by $\mathcal{A}_n$ and $\mathcal{D}_n$ and $\mathcal{C}_n$ denote respectively a conjugate of the dihedral and the cyclic groups in $\mathfrak{S}_n$.

Let $1 \leq i < j$, the *Vandermonde determinant* in the variables $x_i, x_{i+1}, \ldots x_j$ is denoted by $\delta_{i,j}$:

$$\delta_{i,j} = \delta_{j-i+1}(x_i, x_{i+1}, \ldots, x_j) = \prod_{i \leq u < v \leq j} (x_u - x_v)$$

and we set $\delta_j := \delta_{1,j}$. The discriminant of f, denoted by $\Delta(f)$, equals $\delta_n(\Omega_f)^2$.

The *dihedral invariant* is denoted by b_i:

$$b_i = x_1x_2 + x_2x_3 + \cdots + x_{i-1}x_i + x_ix_1 \ .$$

In general H is the generic name for testing groups, Θ denotes a primitive H-invariant. In our partition and group matrix the location of the testing groups is variable: if we have an entry with " H: ", then the testing groups are in the same row as " H:", if it is " H " then the testing groups are in the same column as " H ".

We identify a subgroup of $\mathfrak{S}_n$ and its conjugacy classes in $\mathfrak{S}_n$. In a submatrix of the group matrix relative to a proper subgroup of L, we refer to example 1.1 for the candidate groups and we notify the chosen conjugate if it is necessary for the testing groups.

The notations $i_1, H_{j_2}^{(i_2)}, H_{j_3}^{(i_3)} \times H_{j_4}^{(i_4)}$ for the factors of a resolvent has this meaning: our resolvent has 3 factors over k, one irreducible of degree i_1, one of degree i_2 and of Galois group $H_{j_2}^{(i_2)}$ and one reducible factor of degree $i_3 + i_4$ and of Galois group $H_{j_3}^{(i_3)} \times H_{j_4}^{(i_4)}$.

For $i \in \mathbb{N}$, the polynomial h_i is a monic irreducible univariate polynomial over k.

3. Degrees 3 and 4

There exist 11 conjugacy classes of subgroups in $\mathfrak{S}_4$ and the case of degree 4 includes the one of degree 3. At first we have this following submatrix of group matrix relative to $\mathfrak{S}_4$ in which the candidate groups are in the first row, their types in the second one and the testing groups are T_3, T_4 and T_6.

	T_5	T_4	T_3	T_2	T_1	T_6	T_7	T_8	T_9	T_{10}	T_{11}
	$\mathfrak{S}_4$	$\mathcal{A}_4$	$\mathcal{D}_4$	$\mathcal{C}_4$	V_4	$I_1 \times \mathfrak{S}_3$	$\mathfrak{S}_2 \times \mathfrak{S}_2$	$\mathcal{A}_3 \times Id$	$\mathfrak{S}_2$	$Id_2 \times \mathfrak{S}_2$	I_4
T_6	T_5	T_4	T_3	T_2	T_1	$1, \mathfrak{S}_3$	2^2	$1, \mathcal{A}_3$	2^2	$1^2, 2$	1^4
T_4	2	1^2	2	2	1^2	2	2	1^2	1^2	2	1^2
T_3	$\mathfrak{S}_3$	$\mathcal{A}_3$	$1, 2$	$1, 2$	1^3	$\mathfrak{S}_3$	$1, 2$	$\mathcal{A}_3$	1^3	$1, 2$	1^3

The polynomials δ_4, b_4 and x_1 are primitive invariants of T_4, T_3 and T_6, respectively.

This submatrix of partitions in $\mathfrak{S}_4$ is not sufficient for determining the groups T_3 and T_2, T_7 and T_9.

A separable T_3-relative T_2-resolvent is irreducible if and only if $G_{\Omega_f} = T_3$ and otherwise $G_{\Omega_f} = T_2$. A closed formula of the discriminant of a T_3-relative T_2-resolvent is given in **[5]** (see also **[22]** or **[12]** for an automatic computation). This relative resolvent is always separable.

Now, if $f = h_2^1 h_2^2$ with $\Omega_f = (\Omega_{h_2^1}, \Omega_{h_2^2})$, then the Galois group of f is T_7 or T_9. There are two more ways for determining the Galois group of f. The first is by computing of a T_7-primitive T_9-resolvent and the second by factorizing in an extension (see Example 5.2).

Using a resolvent a T_7-primitive T_9-resolvent: Let $\Theta_9 = \delta_{1,2}\delta_{3,4}$ which is a T_7-primitive T_9-invariant. We have the following multi-resolvent (see Section 5 of Chapter 9):

$$\mathcal{L}_{\Theta_9,(h_2^1,h_2^2)} = (x^2 - \Delta(h_2^1)\Delta(h_2^2)) \qquad .$$

If the product of the discriminant of h_2^1 and h_2^2 is a square then the Galois group of f is T_9, otherwise it is T_7.

Using a factorization in algebraic extension: we have $D_{h_2^1} = D_{h_2^2}$ if and only if $G_{\Omega_f} = T_9$ and $D_{h_2^1} \cap D_{h_2^2} = k$ if and only if $G_{\Omega_f} = T_7$.

4. Degree 5

There exist 19 conjugacy classes of subgroups in $\mathfrak{S}_5$ with 5 classes of transitive subgroups. If f has a linear factor, we go back to the degree 4.

Case $f = h_5$ is irreducible.

We have the following submatrix of the partition matrix relative to $\mathfrak{S}_5$ in which the candidate groups are in the first row and the testing groups are in the first column with an associated invariant in the second column:

H	Θ	T_5	T_4^+	T_3	T_2^+	T_1^+
$I_1 \times \mathfrak{S}_{n-1}$	x_1	T_5	T_4^+	T_3	T_2^+	T_1^+
$\mathcal{M}_5$	Θ_5	6	6	$1, 5$	$1, 5$	$1, 5$
$I_2 \times \mathfrak{S}_3$	δ_2	20	$4^2, 12$	20	10^2	5^4
$\mathcal{A}_3 \times \mathfrak{S}_2$	δ_3	20	20	20	5^4	10^2

where Θ_5 is a T_3-primitive invariant given by: $(x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - (x_1x_3 + x_3x_5 + x_5x_2 + x_2x_4 + x_4x_1))^2$ (see **[19]**). This resolvent computed by Cayley and tabulated in `SYM` is obtained instantaneously (its computation using Cauchy moduli needs 20 seconds and many hours by symmetric functions). In order to distinguish the dihedral and the cyclic groups (resp. $T_2 = \mathcal{D}_5$ and $T_1 = \mathcal{C}_5$), it is also possible to compute an T_2-relative T_1-resolvent of degree 2 (T_1 is a subgroups of T_2).

Case $f = h_2h_3$ and $\Omega_f = (\Omega_{h_2}, \Omega_{h_3})$.

The Galois group of f is either $T_6 = \mathfrak{S}_2 \times \mathfrak{S}_3$, or $T_7^+ = [(3, 4, 5), (1, 2)(4, 5)]$ or $T_8 = \mathfrak{S}_2 \times \mathcal{A}_3$.

The partition matrix relative to the group T_6 gives the following: if $\Delta(h_3)$ is a square then $G_{\Omega_f} = T_8$ else if the product $\Delta(h_2)\Delta(h_3)$ is a square then $G_{\Omega_f} = T_7$ else it is T_6. We remark that the computation of the discriminant of f is not necessary.

Instead of using the partition matrix, the following lemma can be applied:

LEMMA 4.1. *If G_{Ω_f} is T_7 then f has an irreducible factor over k of degree 3 which can only be $\mathcal{A}_3$. Thus, if the Galois group of a polynomial $h \in k[x]$ of degree 3 is $\mathcal{A}_3$ and if g is an irreducible polynomial over k of degree 2 then the Galois of the polynomial gh is $T_8 = \mathfrak{S}_2 \times \mathcal{A}_3$.*

PROOF. If h_3 and h_2 are irreducible factors over k of degrees 3 and 2 of f then the Galois group of f must be T_6,T_7 or T_8. If the Galois group of h_3 is the alternating group, then the Galois group of f must be do a subgroup of $T_8 = \mathfrak{S}_2 \times \mathcal{A}_3$. The group T_7 which has the same order of T_8 is not a subgroup as T_8. □

We can also use factorization in an algebraic extension : $D_{h_2} \cap D_{h_3} = \emptyset$ if, and only if, G_{Ω_f} is T_6 or T_8. Hence $D_{h_2} \subset D_{h_3}$ if and only if G_{Ω_f} is T_7. We have $D_{h_2} \subset D_{h_3}$ if and only if h_3 is reducible over D_{h_2}.

5. Degree 6

There exist 56 conjugacy classes in $\mathfrak{S}_6$.

When f has one linear factor over k, its Galois group is determinated by the degrees less than 6.

Case $f = h_6$ is irreducible.

The group matrix shows that a T_{14}-resolvent of degree 6 solves the problem for all but 4 transitive subgroups of $\mathfrak{S}_6$ using the resolution of reducible polynomials. (Therefore, this resolvent can be also used for computing many polynomials of degree 6 whose Galois group is not transitive.) The formal computation of an T_{14}-resolvent is quick using Noether normalization (see **[23]**) and primitive invariants are computed by **[33]** or Berwick or Abdeljaouad's package.

The part of the group matrix of $\mathfrak{S}_6$ concerning T_{14} as testing group is the following:

Candidates :	T_1	T_2	T_3	T_5	T_6	T_8	T_9	T_{11}
T_{14} :	$1, T_8^{(5)}$	$1^3, \mathfrak{S}_3$	$1, T_6^{(5)}$	T_{19}	T_{29}	$1^2, \mathfrak{S}_4$	T_{17}	T_{27}
Candidates :	T_{13}	T_{14}	T_{16}	T_4^+	T_7^+	T_{10}^+	T_{12}^+	T_{15}^+
T_{14} :	T_{13}	$1, \mathfrak{S}_5$	T_{16}	$1^2, \mathcal{A}_4$	T_{28}	T_{10}	$1, \mathcal{A}_5$	T_{15}

For the groups T_{10}^+, T_{13}, T_{15}^+ and T_{16} we have the following result: if a T_{13}-resolvent of f is irreducible then G_{Ω_f} is T_{15}^+ or T_{16} and otherwise its partition is $1, 9$ and the Galois group of f is T_{10}^+ or T_{13}. The T_{13}-resolvent $\mathcal{L}_{b_6,f}$ can be computed using formulae given in **[8]**. As a T_{15}-relative T_{10}-resolvents has the same degree than a T_{13}-resolvent, it is not necessary to compute this relative resolvent.

Case $f = h_3^1 h_3^2$ and $\Omega_f = (\Omega_{h_3^1}, \Omega_{h_3^2})$.

The possible Galois groups of f are given in the first column of the following table. The third column gives the types of the factors of f. The next two give the partitions with T_{18} and T_{21} as testing groups and the last column gives informations about the splitting fields:

candidates	order	factors	T_{18}	T_{21}	splitting fields
T_{17}	36	$\mathfrak{S}_3 \times \mathfrak{S}_3$	2	6	$D_{h_3^1} \cap D_{h_3^2} = k$
T_{18}^+	18	$\mathfrak{S}_3, \mathfrak{S}_3$	1^2	3^2	$D_{h_3^i} \neq D_{h_3^1} \cap D_{h_3^2} \neq k$
T_{19}	18	$\mathcal{A}_3 \times \mathfrak{S}_3$	2	6	$D_{h_3^1} \cap D_{h_3^2} = k$
T_{21}^+	6	$\mathfrak{S}_3, \mathfrak{S}_3$	1^2	$1, 2, 3$	$D_{h_3^1} = D_{h_3^2}$
T_{20}^+	9	$\mathcal{A}_3 \times \mathcal{A}_3$	1^2	3^2	$D_{h_3^1} \cap D_{h_3^2} = k$
T_{22}^+	3	$\mathcal{A}_3, \mathcal{A}_3$	1^2	$1^3, 3$	$D_{h_3^1} = D_{h_3^2}$

The third column also gives the types of the groups which are direct products of groups. The generators of three groups which are not product of groups are:

$$\begin{aligned} T_{18}^{+} &= [(4,5,6),(1,2,3),(2,3)(5,6)] \quad , \\ T_{21}^{+} &= [(1,2,3)(4,5,6),(2,3)(5,6)] \text{ and} \\ T_{22}^{+} &= [(1,2,3)(4,5,6)] \quad . \end{aligned}$$

The polynomial $\Theta_{18} = \delta_3(x_1,x_2,x_3).\delta_3(x_4,x_5,x_6)$ is a T_{17}-primitive T_{18}-invariant and the associated multi-resolvent is

$$\mathcal{L}_{\Theta_{18},(h_3^1,h_3^2)}(x) = (x^2 - \Delta(h_3^1)\Delta(h_3^2)) \quad .$$

In order to compute a T_{17}-relative T_{21}-resolvent, we fix the choice of h_3^1: if one of the factors of f has $\mathcal{A}_3$ as Galois group then we denote it by h_3^1. The polynomial $t_6 = x_1x_4+x_2x_5+x_3x_6$ is a T_{17}-primitive T_{21}-invariant. (See Example 5.1 Chapter 9 for the computation of the associated resolvent.)

Case $f = h_2^1h_2^2h_2^3$ and $\Omega_f = (\Omega_{h_2^1},\Omega_{h_2^2},\Omega_{h_2^3})$.

In the following table, the first column contains the candidate groups, the second their respective orders, the third the type of the factorization of f and the last one gives informations about the splitting fields:

Candidates	O	factors of f	splitting fields
T_{23}	8	$\mathfrak{S}_2 \times \mathfrak{S}_2 \times \mathfrak{S}_2$	$D_{h_2^i} \cap D_{h_2^j} = k$ for $1 \le i < j \le 3$ and $D_{h_2^3} \not\subset D_{h_2^1} \cup D_{h_2^2}$
T_{24}^{+}	4	$\mathfrak{S}_2, \mathfrak{S}_2, \mathfrak{S}_2$	$D_{h_2^i} \cap D_{h_2^j} = k$ and $D_{h_2^3} \subset D_{h_2^1} \cup D_{h_2^2}$
T_{25}	4	$T_9^{(4)} \times \mathfrak{S}_2$	$D_{h_2^3} \cap D_{h_2^i} = k$ for $i = 1,2$ and $D_{h_2^1} = D_{h_2^2}$
T_{26}	2	$T_9^{(4)}, \mathfrak{S}_2$	$D_{h_2^1} = D_{h_2^2} = D_{h_2^3}$

We have $T_{24} = [(3,4)(5,6),(1,2)(5,6)]$ and $T_{26} = [(1,2)(3,4)(5,6)]$.

In the case in which the Galois group of f is included in one of the conjugate of $T_{25} = T_9^{(4)} \times \mathfrak{S}_2$, the factor of degree 4 of f whose Galois group is included in $T_9^{(4)}$ must be identified (see Example 1.1). In the following table, the first column contains our candidate groups, the last column contains the partitions associated with the absolute $I_1 \times \mathcal{A}_5$-resolvents and the others the partitions associated with T_{23}-relative resolvents:

H :	T_{24}	T_{25}	$T_7^{(4)} \times Id_2$	T_{26}	$T_9^{(4)} \times Id_2$	$I_1 \times \mathcal{A}_5$
Θ :	$\delta_{1,2}\delta_{3,4}\delta_{5,6}$	$\delta_{1,2}\delta_{3,4}$	$x_1x_2x_5x_6$	$x_1x_3x_5 + x_2x_4x_6$	$\delta_{1,2}\delta_{3,4}x_5$	δ_6x_1
T_{23}	2	2	2	4	4	2^6
T_{24}	1^2	2	2	4	2^2	2^6
T_{25}	2	1^2	2	2^2	4	$2^2, 4^2$
T_{26}	2	1^2	2	1^4	2^2	2^6

The computation of an $(Id \times \mathcal{A}_5)$-resolvent with the invariant $\delta_6 x_1$ is preferable to a T_{23}-relative $(T_9^{(4)} \times Id_2)$-resolvent because the $(Id \times \mathcal{A}_5)$-resolvent can be computed and factored easily as follows:

$$\mathcal{L}_{\delta_6 x_1, f}(x) = \mathrm{Res}_y(h_2^1(y), x^2 - \Delta(f).y^2)\mathrm{Res}_y(h_2^2(y), x^2 - \Delta(f).y^2)\mathrm{Res}_y(h_2^3(y), x^2 - \Delta(f).y^2) \quad .$$

Putting $h_2^3 = x^2 - g_1 x + g_2$ we have the following multi-resolvents:

$$\begin{aligned}
\mathcal{L}_{\Theta_{24},(h_1,h_2,h_3)} &= (x^2 - \Delta(h_2^1)\Delta(h_2^2)\Delta(h_2^3)) \\
\mathcal{L}_{\Theta_{25},(h_1,h_2,h_3)} &= (x^2 - \Delta(h_2^1)\Delta(h_2^2)) \text{ with } D_{h_2^1} = D_{h_2^2} \text{ if } G_{\Omega_f} \subset T_{25} \\
\mathcal{L}_{\delta_{1,2}\delta_{3,4}x_5,(h_1,h_2,h_3)} &= x^4 - \Delta(h_2^1)\Delta(h_2^2)(g_1^2 - 2g_2)x^2 + (\Delta(h_2^1)\Delta(h_2^2)g_2)^2 \quad .
\end{aligned}$$

Case $f = h_2 h_4$ and $\Omega_f = (\Omega_{h_2}, \Omega_{h_4})$.

The possible Galois groups of f are given in the first column of the following table. The table gives groups and partitions associated with the testing groups $I_1 \times \mathfrak{S}_5$ and $I_1 \times \mathcal{A}_5$ with respective invariants x_1 and $\delta_6 x_1$.

candidates	O	$I_1 \times \mathfrak{S}_5$	$I_1 \times \mathcal{A}_5$	splitting fields
T_{27}	48	$\mathfrak{S}_2 \times \mathfrak{S}_4$	4,8	$D_{h_2} \cap D_{h_4} = k$
T_{28}^+ = [(3,4)(5,6),(3,5)(4,6),(4,5,6),(1,2)(5,6)]	24	$2, \mathfrak{S}_4$	$2^2, 4^2$	$D_{h_2} \subset D_{h_4}$
T_{29}	24	$\mathfrak{S}_2 \times \mathcal{A}_4$	$2^2, 8$	$D_{h_2} \cap D_{h_4} = k$
T_{30}	16	$\mathfrak{S}_2 \times \mathcal{D}_4$	4,8	$D_{h_2} \cap D_{h_4} = k$
T_{31} =[(3,4)(5,6),(3,5,4,6),(1,2)(5,6)]	8	$2, \mathcal{D}_4$	$4, 4^2$	$D_{h_2} \subset D_{h_4}$
T_{32}^+ =[(3,4)(5,6),(3,5)(4,6),(1,2)(5,6)]	8	$2, \mathcal{D}_4$	$2^2, 4^2$	$D_{h_2} \subset D_{h_4}$
T_{33}	8	$\mathfrak{S}_2 \times \mathcal{C}_4$	4,8	$D_{h_2} \cap D_{h_4} = k$
T_{34}	8	$\mathfrak{S}_2 \times V_4$	$2^2, 4^2$	$D_{h_2} \cap D_{h_4} = k$
T_{35} =[(5,6),(3,4),(1,2)(3,5)(4,6)]	8	$2, \mathcal{D}_4$	4,8	$D_{h_2} \subset D_{h_4}$
T_{36}^+= [(3,4)(5,6),(1,2)(3,5,4,6)]	4	$2, \mathcal{C}_4$	$2^2, 4^2$	$D_{h_2} \subset D_{h_4}$
T_{37} = [(3,4)(5,6),(1,2)(3,5)(4,6)]	4	$2, V_4$	$2^2, 4^2$	$D_{h_2} \subset D_{h_4}$

The group T_{29} is determined by the Galois group of h_4. For the other candidate groups, factorization of the T_{27}-relative T_{28}-resolvent $\mathcal{L}_{\delta_{1,2}\delta_{5,6},\Omega_f,T_{27}} = (x^2 - \Delta(h_2)\Delta(h_4))$ is given by:

Candidates :	T_{27}	T_{28}^+	T_{30}	T_{31}	T_{32}^+	T_{35}	T_{33}	T_{36}^+	T_{34}	T_{37}
T_{10} :	2	1^2	2	2	1^2	2	2	1^2	2	2

The computation of the product of the discriminant of h_2 and h_4 is better than the computation of the discriminant of f.

We now complete our work with this submatrix of the partition matrix relative to T_{27}:

H:	T_{31}	T_{35}	$T_7^{(5)} \times Id$	$I_3 \times \mathfrak{S}_3$
Θ:	Θ_{31}	$\delta_2(x_3x_4 - x_5x_6)$	$\delta_{1,2}\delta_{5,6}$	x_1x_3
T_{30}	$2, 4$	$2, 4$	8	8
T_{31}	$1^2, 4$	$2, 4$	4^2	8
T_{35}	$2, 4$	$1^2, 4$	8	4^2

Here $\Theta_{31} = x_2x_4x_6^2 + x_1x_6x_4^2 + x_2x_6x_3^2 + x_1x_3x_6^2 + x_2x_5x_4^2 + x_1x_4x_5^2 + x_2x_3x_5^2 + x_1x_5x_3^2$ has been computed by Abdeljaouad's package. For computation of the multi-resolvent of (h_2, h_4) by Θ_{35} and $\delta_{1,2}\delta_{5,6}$ see Section 5 of Chapter 9).

6. Degree 7

There exist 96 conjugacy classes of subgroups in $\mathfrak{S}_7$. We avoid subgroups for which f has one factor of degree 1.

Case $f = h_7$ is irreducible.

We have the following submatrix of the partition matrix of $\mathfrak{S}_7$ in which the testing groups are in the first row and the candidate groups are in first column:

H:	$I_1 \times \mathcal{A}_6$	T_{26}	T_{27}	T_8	T_5
Θ:	δ_6	x_1x_2	$\delta_7x_1x_2$	$x_1x_2x_3$	Θ_5
T_7	14	21	42	35	30
T_6^+	7^2	21	21^2	35	15^2
T_5^+	7^2	21	21^2	7,28	1,7,8,14
T_4	14	21	42	14,21	$2, 14^2$
T_3^+	7^2	21	21^2	$7^2, 21$	$1^2, 7^4$
T_2	14	7^3	14^3	$7^3, 14$	$2, 14^2$
T_1^+	7^2	7^3	7^6	7^5	$1^2, 7^4$

(The columns of T_8 and T_{26} have been computed by **[51]**.) For the invariant Θ_5 we can choose the one computed in **[31]**. If the Galois group of f is T_5 or T_3 a T_5-relative T_3-resolvent of degree 8 is sufficient for determining it: the Galois of f is T_3 if and only if this resolvent has a linear (separable) factor.

Case $f = h_4h_3$ and $\Omega_f = (\Omega_{h_4}, \Omega_{h_3})$.

At first there are five groups which can be identified only by the type of the factorization of f: $T_{21} = \mathfrak{S}_4 \times \mathcal{A}_3$, $T_{22} = \mathcal{A}_4 \times \mathfrak{S}_3$, $T_{23} = D_4 \times \mathcal{A}_3$, $T_{24} = C_4 \times \mathcal{A}_3$ and $T_{25}^+ = V_4 \times \mathcal{A}_3$.

For the other cases, the Galois group of f is one of the subgroups given at first column in the following table. The second column gives the Galois groups of factors of an $(Id \times \mathfrak{S}_6)$-resolvent (the polynomial f is one of them) and the third column gives the partitions of an $(Id \times \mathcal{A}_6)$-resolvent. The others columns give a submatrix of the partition

matrix of T_8 with the testing groups T_9,T_{10},T_{39},T_{12},T_{14} and T_{40}. In order to choose the testing groups in the partition matrix of T_8, we have taken the testing groups of index less than 9 in T_8 and we have avoided the groups which do not give useful results.

H:	$I_1 \times \mathfrak{S}_6$	$I_1 \times \mathcal{A}_6$	T_9	T_{10}	T_{19}	T_{12}	T_{14}	T_{41}
Θ:	x_1	$\delta_7 x_1$	$\delta_{1,4}\delta_{5,7}$	Θ_{10}	$\delta_4+\delta_{5,7}$	Θ_{12}	$\delta_{5,7}(x_1x_2-x_3x_4)$	x_5b_4
T_8	$\mathfrak{S}_4 \times \mathfrak{S}_3$	6,8	2	6	4	6	6	9
T_9^+	$\mathfrak{S}_4, \mathfrak{S}_3$	$3^2, 4^2$	1^2	3^2	2^2	6	6	9
T_{10}^+	$\mathfrak{S}_4, \mathfrak{S}_3$	$3^2, 4^2$	1^2	$1, 2, 3$	2^2	6	6	$3, 6$
T_{11}	$D_4 \times \mathfrak{S}_3$	$6, 8$	2	6	4	$2, 4$	$2, 4$	$3, 6$
T_{12}	$D_4, \mathfrak{S}_3$	$4^2, 6$	2	6	4	$1^2, 4$	$2, 4$	$3, 6$
T_{13}^+	$D_4, \mathfrak{S}_3$	$3^2, 4^2$	1^2	3^2	2^2	$2, 4$	$2, 4$	$3, 6$
T_{14}	$D_4, \mathfrak{S}_3$	$6, 8$	2	6	4	$2, 4$	$1^2, 4$	$3, 6$
T_{15}	$C_4 \times \mathfrak{S}_3$	$6, 8$	2	6	4	$2, 4$	$2, 4$	$3, 6$
T_{16}^+	$C_4, \mathfrak{S}_3$	$3^2, 4^2$	1^2	3^2	2^2	$2, 4$	$1^2, 4$	$3, 6$
T_{17}	$V_4 \times \mathfrak{S}_3$	$6, 8$	2	6	2^2	2^3	2^3	3^3
T_{18}	$V_4, \mathfrak{S}_3$	$4^2, 6$	2	6	2^2	$1^2, 2^2$	$1^2, 2^2$	3^3
T_{19}^+	$\mathcal{A}_4 \times \mathcal{A}_3$	$3^2, 4^2$	1^2	3^2	1^4	6	6	9
T_{20}^+	$\mathcal{A}_4, \mathcal{A}_3$	$3^2, 4^2$	1^2	$1^3, 3$	1^4	6	6	3^3

Where
$T_{41} = Id \times \mathfrak{S}_2 \times D_4$,
$T_9 = [(1,2)(3,4),(1,4)(2,3),(2,3,4)(5,6,7),(2,3,4),(3,4)(6,7)]$,
$T_{10} = [(1,2)(3,4),(1,4)(2,3),(2,3,4)(5,6,7),(3,4)(6,7)]$,
$T_{12} = [(5,6,7),(3,4)(6,7),(1,2)(6,7),(1,3)(2,4)(6,7)]$,
$T_{13} = [(5,6,7),(3,4)(6,7),(1,2)(6,7),(1,3)(2,4)]$,
$T_{14} = [(1,2),(3,4),(5,6,7),(6,7)(1,3)(2,4)]$,
$T_{16} = [(5,6,7),(1,2)(3,4),(1,3,2,4)(6,7)]$,
$T_{18} = [(5,6,7),(1,2)(3,4),(1,3)(2,4)(6,7)]$
and $T_{20} = [(4,5)(6,7),(4,6)(5,7),(1,2,3)(5,6,7)]$.

The following invariants are computed using Abdeljaouad's package:

$$\begin{aligned}
\Theta_{10} &= x_3x_4x_5 + x_2x_4x_6 + x_2x_3x_7 + x_1x_4x_7 + x_1x_3x_6 + x_1x_2x_5 \qquad \text{and} \\
\Theta_{12} &= x_2x_6x_4^2x_7^2 + x_4x_7x_2^2x_6^2 + x_2x_7x_4^2x_5^2 + x_4x_5x_2^2x_7^2 + x_2x_5x_4^2x_6^2 + x_4x_6x_2^2x_5^2 \\
&\quad + x_2x_7x_3^2x_6^2 + x_3x_6x_2^2x_7^2 + x_2x_5x_3^2x_7^2 + x_3x_7x_2^2x_5^2 + x_2x_6x_3^2x_5^2 + x_3x_5x_2^2x_6^2 \\
&\quad + x_1x_7x_4^2x_6^2 + x_4x_6x_1^2x_7^2 + x_1x_5x_4^2x_7^2 + x_4x_7x_1^2x_5^2 + x_1x_6x_4^2x_5^2 + x_4x_5x_1^2x_6^2 \\
&\quad + x_1x_6x_3^2x_7^2 + x_3x_7x_1^2x_6^2 + x_1x_7x_3^2x_5^2 + x_3x_5x_1^2x_7^2 + x_1x_5x_3^2x_6^2 + x_3x_6x_1^2x_5^2 \qquad .
\end{aligned}$$

Some closed formulas for the multi-resolvent of (h_4, h_3) are the following:

$$\begin{aligned}
\mathcal{L}_{\Theta_9,(h_4,h_3)} &= (x^2 - \Delta(h_3)\Delta(h_4)) \\
\mathcal{L}_{\Theta_{39},(h_4,h_3)} &= x^4 - 2x^2\Delta(h_3)\Delta(h_4) + (\Delta(h_3) - \Delta(h_4))^2 \\
\mathcal{L}_{x_1\delta_{5,7},(h_4,h_3)} &= \mathrm{Res}_z(h_4(z), x^2 - z^2\Delta(h_3)) \\
\mathcal{L}_{x_5 b_4,(h_4,h_3)} &= \mathrm{Res}_z(h_3(z), z^3\mathcal{L}_{b_4,h_4}(x/z)) \qquad .
\end{aligned}$$

For the computation of the T_{18}-relative T_{14}-resolvent see Section 5 of Chapter 9.

Case $f = h_5h_2$ and $\Omega_f = (\Omega_{h_5}, \Omega_{h_2})$.

Two groups can be identified only by the type of the factorization of f: $T_{32} = \mathcal{A}_5 \times \mathfrak{S}_2$ and $T_{33} = C_5 \times \mathfrak{S}_2$.

After we take the testing groups of index less than 20 in $T_{26} = \mathfrak{S}_5 \times \mathfrak{S}_2$ and we avoid the groups which do not give any useful information. In the following table, we process as the previous section: the three last columns are associated with T_{26}-relative resolvents (which are multi-resolvents).

Remark 48. The groups $\mathfrak{S}_2 \times T_7^{(5)}$ and $T_7^{(5)} \times \mathfrak{S}_2$ are conjugate subgroups in $\mathfrak{S}_7$ but not in T_{26}. As testing group we chose the conjugate $\mathfrak{S}_2 \times T_7^{(5)}$ because $T_7^{(5)} \times \mathfrak{S}_2$ gives no useful information.

H:	$\mathfrak{S}_1 \times \mathfrak{S}_6$	T_{27}	T_{29}	$\mathfrak{S}_2 \times T_7^{(5)}$
Θ :	x_1	$\delta_5\delta_{6,7}$	$\sqrt{m_5}\delta_{6,7}$	$\delta_{3,5}\delta_{6,7}$
T_{26}	$\mathfrak{S}_5 \times \mathfrak{S}_2$	2	12	20
T_{27}^+	$\mathfrak{S}_5, \mathfrak{S}_2$	1^2	6^2	20
T_{28}	$M_5 \times \mathfrak{S}_2$	2	2, 10	20
T_{29}^+	$M_5, \mathfrak{S}_2$	1^2	$1^2, 5^2$	20
T_{30}	$D_5 \times \mathfrak{S}_2$	2	2, 10	10^2
T_{31}	$D_5, \mathfrak{S}_2$	2	2, 10	5^4

where $\sqrt{m_5}$ is deduced from the Cayley-invariant given in degree 5 :

$$\sqrt{m_5} = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - (x_1x_3 + x_3x_5 + x_5x_2 + x_2x_4 + x_4x_1) \qquad .$$

Remark 49. In order to determine the group T_{27} it is preferable to compute the product of the determinant of h_5 and h_2 instead of the determinant of f.

We can use factorizations in extensions. For example, if h_5 is irreducible in Q_{h_2} then $G_{\Omega_f} \in \{T_{26}, T_{28}, T_{30}, T_{31}, T_{32}\}$. Now suppose that h_5 is reducible in K_{h_2}. If $G_{\Omega_f}(h_5) = \mathfrak{S}_5$ then $G_{\Omega_f}(f) = T_{27}^+$, if $G_{\Omega_f}(h_5) = M_5$ then $G_{\Omega_f} = T_{29}^+$ and if $G_{\Omega_f} = D_5$ then $G_{\Omega_f} = T_{31}$.

6.1. Case $f = h_2^1 h_2^2 h_3$ and $\Omega_f = (\Omega_{h_2^1}, \Omega_{h_2^2}, \Omega_{h_3})$.

The Galois group of f is one of those in first column of the next table. The last column contains a submatrix of the partition matrix relative to T_{34}.

H:	$I_1 \times \mathfrak{S}_6$	T_{35}	T_{36}	T_{37}	T_{38}
Θ:	x_1	$\delta_3\delta_{4,5}\delta_{6,7}$	$\delta_{4,5}\delta_{6,7}$	$\delta_3\delta_{4,5}$	δ_3
T_{34}	$\mathfrak{S}_3 \times \mathfrak{S}_2 \times \mathfrak{S}_2$	2	2	2	2
T_{35}^+	$\mathfrak{S}_3, \mathfrak{S}_2, \mathfrak{S}_2$	1^2	2	2	2
T_{36}	$\mathfrak{S}_3 \times T_9^{(4)}$	2	1^2	2	2
T_{37}	$T_7^{(5)} \times \mathfrak{S}_2$	2	2	1^2	2
T_{38}	$\mathcal{A}_3 \times \mathfrak{S}_2 \times \mathfrak{S}_2$	2	2	2	1^2
T_{39}	$\mathfrak{S}_3 \times T_9^{(4)}$	2	1^2	1^2	2
T_{40}^+	$\mathcal{A}_3 \times T_9^{(4)}$	1^2	1^2	2	1^2

We have $T_{35} = [(1,2,3), (1,2)(4,5), (1,2)(6,7)]$.

Bibliography

[1] Abdeljaouad, Ines., (1996), Calcul d'invariants primitifs de groupes finis, LIP6 Report 1997-020.

[2] H. Anai, M. Noro and K. Yokoyama *Computation of the splitting field and the Galois groups of polynomials* Progress in Mathematics, 143 (conference MEGA'94), Birkhaüser Verlag, 29–50.

[3] Ampère, M. , (1826), *Fonctions interpolaires* Annales de M.Gergonne

[4] J.M. Arnaudiès, *Sur la rèsolution explicite des équations de degré 5 quand elles sont résolubles par radicaux*, Bull. Sc. Math. 2^e série, vol. 100, 1976, 241–254.

[5] J.M. Arnaudiès, J. Bertin **Groupes, Algèbres et Géométrie**, Tome I, Ellypses, 1993

[6] J.M.Arnaudiès , A. Valibouze, (1993) *Résolvantes de Lagrange*, LITP Report 93.61

[7] J.M.Arnaudiès , A. Valibouze, (1996) *Lagrange resolvents*, special issue of MEGA'96 (A. Cohen and M-F- Roy Eds), Journ. of Pure and Appl. Algeb. **117&118** (1997), 23-40.

[8] J.M.Arnaudiès , A. Valibouze, (1994) *Calculs de résolvantes*, LITP Report 94.46, July 1994

[9] J.M.Arnaudiès , A. Valibouze (1994), Calculs de groupes de Galois jusqu'au degré 11, LITP Reports 94-25 94-30 94-48 94-49 94-50.

[10] Artin, E., **Galois Theory**, Notre Dame Mathematical Lectures No. 2, Notre Dame, IN: Notre Dame University Press 1959.

[11] Artin, M., **Algebra**,

[12] P. Aubry, A. Valibouze, 1997, *Computing characteristic polynomials associated with some quotient ring*, preprint.

[13] E.H. Berwick, (1915), *The Condition That A Quintic Equation Should Be Soluble By Radicals* Proc. London Math. Soc. (2) **14**. 301-307.

[14] E.H. Berwick, (1929) *On Soluble Sextic equations* Proc. London Math. Soc. (2) **29**, 1-28.

[15] Buchberger, B., "Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal" Phd-Thesis, University of Innsbruck, 1965.

[16] Gregory Butler and John McKay, (1983), *The transitive groups of degree up to 11*, Comm. Algebra **11**, 863-911.

[17] Cauchy, A. *Usage des fonctions interpolaires dans la détermination des fonctions symétriques des racines d'une équation algébrique donnée.* Oeuvre Volume **5** p.473 extrait 108.

[18] D. Casperson, J. McKay, (1994) *Symmetric functions, m-sets, and Galois groups*, Math. Comp.

[19] A. Cayley, (1861), *On a new auxiliary equation in the theory of equation of the fifth order*, Philosophical Transactions of the Royal Society of London, **CLL**

[20] Clifton J. Williamson (1994) *On Algebraic Construction Of Tri-Diagonal Matrices*, Submitted to Proceedings of CNTA-4 (Canadian Number Theory Association)

[21] Colin, A. Théorie de Galois effective, Mémoire de DEA, Ecole Polytechnique, 1994.

[22] Colin, A. *Formal computation of Galois groups with relative resolvents* Conference AAECC'10,(Paris, July 1995), LNCS **948**, 169-182

[23] Colin, A. (1996) *An efficient symbolic algorithm to compute Lagrange resolvents for computational Galois theory*, preprint

[24] Colin, A. *Identification of the Galois group thanks to symbolic computation of relative resolvents and tables of partitions*, ISSAC'97 Conference (Haway, July 1997).

[25] Colin, A. **theorie des invariants effective. Application à la théorie de Galois et à la résolution de systèmes algébriques. Implantation en AXIOM.** Thèse de l'École Polytechnique. Palaiseau. 1997.

[26] L. Ducos and C. Quitté, (1996), *Algèbre de décomposition universelle, Implémentation et applications à la théorie de Galois*, Rapport interne du Département de Mathématiques de l'université de Poitier, **98**.

[27] Y. Eichenlaub **Problèmes effectifs de Galois en degrés 8 à 11**. PhD thesis, Bordeaux 1 University, 1996.

[28] Faugère, J.C., Gianni, P., Lazard, D. and Mora, T., Efficient Computation of Zero–dimensional Gröbner Bases by Change of Ordering. J. Symb. Comp.,vol. **16**, (1993), 329-344.

[29] Faugère, J.C., **Résolution des systèmes d'équations algébriques**, PhD thesis, Université Paris 6, 1994

[30] Faugère, J.C., (1997) *A new efficient algorithm for computing Gröbner Basis (F4)*, Task 3.3.2.1 Frisco report, preprint.

[31] Foulkes, H.O., (1931), *The resolvents of an equation of seventh degree*, Quart. J. Math. Oxford Ser. (2), 9-19.

[32] Galois, E., **Oeuvres Mathématiques**, publiées sous les auspices de la SMF, Gauthier-Villars, 1897

[33] K. Girstmair, (1987) *On invariant Polynomials and Their Application in Field Theory* Maths of Comp., vol. **48**, no 178, 781-797

[34] I. Gil-Delessalle, A. Valibouze, (1996), *Galois inverse problem for some subgroups of degree 12*, preprint

[35] M.Giusti, D.Lazard, A.Valibouze, (1988). *Algebraic transformations of polynomial equations, symmetric polynomials and elimination. Symbolic and Algebraic Computation, International Symposium ISSAC '88* (P. Gianni, ed.), Lect. Notes in Comp. Sc. **358**, 309-314.

[36] GAP `Groups, Algorithms and Programming, GAP 3.3` Martin Schönert and others, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, **93**

[37] GAP, A. Valibouze, (1994) *Calculs de matrices de partitions*, (manuscrit)

[38] Kemper, G., (1996), *Calculating invariant rings of finite groups over arbitrary fields*, JSC **21** 351-366

[39] G. Kemper, The *Invar* package for calculating rings of invariants, IWR Preprint **93-34**, Heidelberg, 1994

[40] Lamb J., *A 15-ic resolvent of the binary sectic*, Proc. Leeds Phil. Soc., **1** (1927), 149-151

[41] Lagrange, J.L., (1770), *Reflexions sur la résolution algébrique des équations*, **Mémoires de l'Académie de Berlin**, 205-421, (**Oeuvres de Lagrange**, tome IV, 205-421)

[42] Lagrange, J.L., *Traité de la résolution des équations numériques : Notes sur la théorie des équations algébriques*, **Oeuvres de Lagrange** , Tome VIII, 133-367

[43] A. Lascoux, P.Pragaz (1988) *S-function series*, J. Phys.A : Math. Gen. **21**, 4105-4114.

[44] Susan Landau and Gary Lee Miller, (1983), *Solvability by radicals is Polynomial time*, 15^th ACM Symp. on Theory of Computing , ACM, 140-151.

[45] Susan Landau, (1984), *Polynomial time algorithms for Galois groups*, EUROSAM-84 (Cambridge, England), L.N.C.S, Springer-Verlag, 225-236.

[46] D.Lazard, A.Valibouze, (1991) *Computing subfields: Reverse of the primitive element problem*, proc. de Mega'92 (Nice, april 1992). Progress in Mathematics **109**, 163-176.

[47] Lehobey, F., *Algorithmiques Methods and Practical Issues in the Computation of Galois Groupe of Polynomials*, Mémoire de DEA option algorithmique, Algèbre et Géométrie, Université de Rennes I, (1994)

[48] Lehobey, F., (1997), *Resolvent Computations by Resultants Without Extraneous Powers* , ISSAC'97 Conference (Haway, July 1997).

[49] Luther, (1848), *Ueber die Factoren des algebraisch lösbaren irreducible Gleichungen vom sechsten Grade und ihren Resolvanten*, Journal für Math., **37** , 193-220.

[50] A. Machï, A. Valibouze, (1991), *L'idéal des relations symétriques et l'idéal des relations*, preprint.

[51] J. McKay et E. Regener, (1985), *Actions of permutation groups on r-sets* Communications in Algebra, **13** (3), 619-630

[52] J. McKay and L. Soicher, (1985), *Computing Galois Groups over the rationals*, Journal of number theory **20**, 273-281.

[53] `Maxima DOE` maintened by William SCHELTER

[54] N. Rennert, Calculs de résolvantes en AXIOM. Mémoire de DEA , 1996.

[55] Rennert, N. , Valibouze, A., (1997) *Modules de Cauchy, polynômes caractéristiques et résolvantes*, submitted to Exp. Math (extract to LITP Report 95-62, (1995))

[56] F. Rouiller, **Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux**, Thèse de l'Université de Rennes I, 1996.

[57] Samuel, P., Zariski, O., **Commutative Algebra**, Van Nostrand company, INC., 1958

[58] J.A. Serret, (1850), *Mémoire sur les fonctions de quatre, cinq et six lettres, Journal de Math.* **15**, 45-70

[59] Leonard Soicher, The computation of the Galois groups, Thesis in departement of computer science, Concordia University, Montreal, Quebec, Canada, (1981).

[60] R.P. Stauduhar, (1973), *The determination of Galois groups*, Math. Comp. **27**, 981-996.

[61] N. Tchebotarev **Grundzüge des Galois'shen Theorie** P. Noordhoff, 1950

[62] A. Valibouze, (1988), Manipulations de fonctions symétriques, Thesis in University Paris VI.

[63] A. Valibouze, (1989) *Résolvantes et fonctions symétriques*, *Proceedings of the ACM-SIGSAM 1989 International Symposium on Symbolic and Algebraic Computation, ISSAC'89 (Portland, Oregon)*. ACM Press, 390-399.

[64] Valibouze A. (1994) `Extension SYM de MACSYMA, manuel de l'utilisateur`, (manuscrit)

[65] A. Valibouze, (1995) *Computation of the Galois group of the Resolvent Factors for the Direct and Inverse Galois Problems*, AAECC'10 conference (Paris, July 1995), LNCS **948**, 456-468 (LITP Report 94-58 (1994))

[66] K. Yokoyama, (1996), *A modular method for computing the Galois Groups of Polynomials* MEGA'96 conference (Eindoven, june 1996).

[67] K. Yokoyama, M. Noro, T. Takeshima , (1992) *Solution of systems of algebraic equations and linear maps on Residue Class ring*, Journal of Symbolic Computation **14**, 399-417 .

Index