Universidad Complutense de Madrid

Characterization and computation of the Galois group of polynomials of degree 7

Degree Final Project

Doble Grado en Ingeniería Informática y Matemáticas

Facultad de Informática y Facultad de Ciencias Matemáticas

July 2016

Author:

David Martínez Rubio

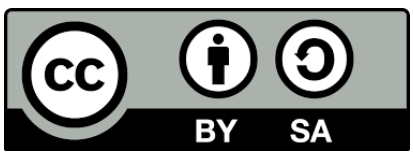
Supervised by the professors:

Juan Ramón Delgado Pérez

José Francisco Fernando Galván

José Manuel Gamboa Mutuberría

Paradoxically, I have found that one of the best ways to avoid repetition is the study of mathematics, the science that is about (abstract) patterns.



Resumen

El objetivo de este trabajo es estudiar métodos generales para el cálculo de grupos de Galois de polinomios irreducibles y concretar dichos métodos para caracterizar y calcular los grupos de Galois de los polinomios irreducibles de grado 7 con coeficientes en $\mathbb{Q}$ concluyendo con una implementación en sage que realiza esta tarea. Primero presentamos dos métodos generales para calcular grupos de Galois y añadimos algunos resultados más que dan información acerca del grupo de Galois. En la segunda parte clasificamos los subgrupos transitivos de $\mathcal{S}_7$, proponemos una resolvente junto con la demostración de las propiedades necesarias que ha de cumplir para poder usar los métodos anteriores y se da un método para calcularla eficientemente. Finalmente se da la implementación en sage del algoritmo y para cada subgrupo transitivo $G \leq \mathcal{S}_7$ se da un polinomio cuyo grupo de Galois es G.

Palabras clave: cálculo de grupos de Galois, algoritmo, polinomios de grado 7, método de la resolvente, factorización de resolventes, clasificación de los grupos transitivos de $\mathcal{S}_7$.

Abstract

The aim of the present project is studying general methods to compute Galois groups of irreducible polynomials and limiting these methods to characterize and to compute the Galois Groups of the irreducible polynomials of degree 7 with coefficients in $\mathbb{Q}$. We also give a sage implementation that computes the Galois groups of these polynomials. Firstly, we give two general methods to compute Galois groups along with some results that give information about them. Secondly, we classify the transitive subgroups of $\mathcal{S}_7$, we propose a resolvent along with proofs of the necessary properties that have to be fulfilled in order to apply the aforementioned methods and we give a method to compute it efficiently. Finally, we give the sage implementation of the algorithm and for each transitive subgroup $G \leq \mathcal{S}_7$ we give a polynomial whose Galois group is G.

Keywords: computation of Galois Groups, algorithm, polynomials of degree 7, resolvent method, factorization of resolvents, classification of the transitive groups of $\mathcal{S}_7$.

Contents

1 Introduction

From the contributions about the cubic and quartic of, among others, del Ferro, Tartaglia, Cardano, and Ferrari (in the 16^{th} century) and of Vieta, Descartes, and Tschirnhaus [29] (in the 18^{th} century) the problem of the solvability by radicals of the polynomial equations of arbitrary degree is proposed.

After the pioneer work of De Moivre about the roots of unity, dense monographs are published during the century of lights, about this topic by Euler, Bezout, Lagrange [22] and Vandermonde [30]. At the end of the century the situation is summarized by Lagrange: the known methods are inapplicable to polynomials of degree greater than 4 and the possibility of the expression of its roots by radicals is still an open problem.

As in other branches of modern mathematics, Gauss marked a turning point with his "Disquisitiones" [13] after the study of the cyclotomic equations, where he "clearly" established an equivalence between the problem of the constructibility of the regular n-agon with ruler and compass and the possibility of expressing the n^{th} roots of unity by quadratic radicals. Gauss intuited that one was the right path, an evidence of it is his comment about the impossibility of the solvability by radicals of the quintic. Finally Ruffini [24] and Abel [1] proved this impossibility.

Almost at the same time, Galois developed his theory [12]: he associated each polynomial f (whose roots are in general unknown) with a group, named the "Galois group of f" after him, whose elements are the permutations that "symmetrize" f and that encode the relevant information about the polynomial equation $f = 0$. From this point of view, the solvability by radicals appears to be equivalent to the solvability of the Galois group of f. The big contribution of Galois was to reduce the problem of the solvability by radicals to the more general question of the computation of the Galois group of a polynomial and, conversely, the computation of a polynomial with a given Galois group.

This degree final project is written within this context. During the 19^{th} century the study of the quintic was a problem that we could consider popular: It interested Ruffini, Abel, Galois, Jacobi, Cayley [5], Harley [16], Cockle [6], McClintock [23], Weber [31], ... Maybe it is less known that a lot of papers were published about the polynomial equation of degree 7: Kronecker in 1858 [21], Klein in 1879 [20], and Weber in its "Lessons" [31], among others. Klein for example writes a 30 pages monograph about it; he obtains a polynomial of degree 7 over the field $\mathbb{Q}(\sqrt{7})$ whose Galois group is the simple group of order 168. The lessons 131 to 147 of the previously mentioned Weber's work are about this group (more than 50 pages). The difficulty of the problems that arise in this context is such that it is not until 1968 that W. Trinks shows the first polynomial (it was $x^7 - 7x + 3$)

whose Galois group over $\mathbb{Q}$ is isomorphic to the simple group of order 168 [28].

In this degree final project we present several general methods to compute Galois groups of irreducible polynomials and then, we use them to develop the theoretical framework that is necessary to characterize and to compute the Galois group of any irreducible polynomial f of degree 7 with coefficients in $\mathbb{Q}$. Finally, we develop an algorithm and give a sage implementation that outputs the Galois group of f.

In the first section, dedicated to general methods for computing Galois groups, we give the notion of the resolvents of a polynomial, which is a very useful tool for computing Galois groups. We show two different uses of resolvents that are used to compute Galois groups: The Resolvent Method and the Factorization of Resolvents Method. The exposition of the first method is mostly based on [7], with some help of [26], [19], [2], [14], [11] and own work to add details and to adapt some proofs to our context. Most authors assert the theorems included here about Tschirnhaus transformations without a proof. To give the proofs we have adapted some ideas found in [15]. The second method is based on [27] although the proofs have been slightly modified. Then we show a general algorithm for computing the Galois group of any polynomial [26]. The computations are impractical for modestly high degree, but it has the virtue of showing that the problem has a solution. Finally we state Dedekind's Theorem and Chebotarev Density Theorem and we prove the former [7], [25].

The second section is about computing Galois groups of irreducible polynomials of degree 7. In order to use the methods in the first section, it is necessary to have the classification and the inclusion diagram of the transitive subgroups of the symmetric group $\mathcal{S}_n$, where n is the degree of the polynomial whose Galois group we aim to compute. Therefore, we begin with a deep study of the transitive subgroups of $\mathcal{S}_7$. We prove that there are just 7 transitive subgroups of $\mathcal{S}_7$ up to conjugacy. The proof is based on one given by W. Burnside [3] pp. 229-231 in 1897. His proof is mostly a sequence of claims, with no explanation nor detail at all, from which he derives the result. The most challenging part of this project has been the development of proofs for each of his claims and to provide a full detailed deep study of the transitive subgroups of $\mathcal{S}_7$. The approach we have chosen to compute Galois groups is the Factoring Resolvents Method. For it, we give a specific resolvent, we prove it is always separable (needed in order to apply a theorem from the first section) and compute we the orbits of some group actions. Putting all together, we find what is needed to determine the Galois group of an irreducible polynomial of degree 7 with coefficients in $\mathbb{Q}$. Then we develop some theoretical results to obtain an efficient algorithm that computes the Galois group. The key idea about how to efficiently compute a linear resolvent can be found in [27]. To conclude, for each transitive subgroup $G \leq \mathcal{S}_7$ we show a polynomial whose Galois group is G. We use the algorithm to prove that its Galois group is actually G.

2 Computing Galois groups

In this section we present general methods to compute the Galois groups of irreducible polynomials. We do not impose restrictions on the degree of the polynomial. We will work over an arbitrary field and, when needed, we will impose some restrictions on its characteristic.

Let's fix some notations. In the whole section K will be an arbitrary field, $f \in K[\mathtt{x}]$ an irreducible polynomial of degree n, $\alpha_1, \ldots, \alpha_n$ will be the roots of f in its splitting field Σ_f over K. Gal_f will stand for the Galois group of f over K, unless we need to express the field extension explicitly, in which case we will use $\Gamma(L : K)$ for the group of all the K-automorphisms of L. We may assume that Gal_f is a subgroup of the permutation group $\mathcal{S}_n$. Recall that a subgroup G of $\mathcal{S}_n$ is transitive (see Definition 3.5 below) if given indices $i, j \in \{1, \ldots, n\}$ there exists $\sigma \in G$ such that $\sigma(i) = j$. As f is irreducible in $K[\mathtt{x}]$ the group Gal_f is transitive. Indeed, given two roots α_i and α_j of f in Σ_f there exist isomorphisms

$$K(\alpha_i) \longrightarrow \frac{K[\mathtt{x}]}{\langle f \rangle} \longrightarrow K(\alpha_j) \quad ; \quad \alpha_i \mapsto \mathtt{x} * \langle f \rangle \mapsto \alpha_j$$

whose composition lifts to an isomorphism $\phi_{ij} \in \Gamma(\Sigma_f : K)$ and satisfies $\phi_{ij}(\alpha_i) = \alpha_j$.

We will use the notation $F^\sigma(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ for $F(\mathtt{x}_{\sigma(1)}, \ldots, \mathtt{x}_{\sigma(n)})$.

If M is an intermediate field between K and Σ_f, M^* will stand for $\Gamma(\Sigma_f : M)$ and if H is a subgroup of Gal_f, $H^\dagger$ will stand for the fixed field of H.

We first remember the Fundamental Theorem of Galois Theory.

Theorem 2.1. *If $L : K$ is a finite Galois extension, this is a finite normal and separable extension, with Galois Group G and if the maps $*$ and $\dagger$ are defined as above, then:*

1. *The Galois Group G has order $[L : K]$.*
2. *The maps $*$ and $\dagger$ are mutual inverses, and set up an order-reversing one-to-one correspondence between the set of subfields M such that $K \subseteq M \subseteq L$ and the set of all subgroups H of G.*
3. *If M is an intermediate field, then the extension $L : M$ is always normal (hence Galois) and*
$$[L : M] = |M^*| \qquad [M : K] = |G|/|M^*|$$
4. *Let M be an intermediate field. Then $M : K$ is a normal extension if and only if M^* is a normal subgroup of G. In this case the Galois group of the extension $M : K$ is isomorphic to the quotient group G/M^*.*

A proof can be found in [26] chapter 12.

Several of the methods that will be exposed in this section use multivariate symmetric polynomials evaluated at the roots of f. In general, we will not know the roots $\alpha_1, \ldots, \alpha_n$ so we will need to reformulate these polynomials with respect to the coefficients of f. The next theorem states this can always be done. In addition, there is a recursive algorithm to perform this transformation that can be derived from most of the proofs. Really, those methods use symmetric polynomials evaluated at the roots of f to work with polynomials that can be expressed in terms of the coefficients of f.

Definition 2.2. Let A be a ring and let $g \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ be a polynomial. We say that g is a *symmetric polynomial* if $g^\sigma = g$, for all $\sigma \in \mathcal{S}_n$.

Definition 2.3. We call *elementary symmetric polynomials in n variables* to the homogeneous polynomials

$$\mathtt{s}_k := \sum_{1 \leq i_1 < \cdots < i_k \leq n} \mathtt{x}_{i_1} \cdots \mathtt{x}_{i_k}$$

The evaluation of $\mathtt{s}_i$ at the roots of a polynomial f with roots $\alpha_1, \ldots, \alpha_n$ will be denoted by s_i, that is, $s_i := \mathtt{s}_i(\alpha_1, \ldots, \alpha_n)$.

Theorem 2.4. *Let A be a ring and let $g \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ be a symmetric polynomial. Then there exists a unique polynomial $h \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ such that $g = h(\mathtt{s}_1, \ldots, \mathtt{s}_n)$.*

A proof can be found in [8] pp. 136-139.

Resolvents are the main algebraic objects that are used to compute Galois groups of polynomials. Here we give the general definition of G-relative H-invariant resolvent. For simplicity we denote G/H a complete system of left cosets representatives of G with respect to H, that is, cosets of the form σH.

Definition 2.5. Let $F \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ and let G be a subgroup of $\mathcal{S}_n$. The *stabilizer of F with respect to G* is the subgroup

$$\mathrm{Stab}_G(F) := \{\sigma \in G \mid F^\sigma = F\}.$$

Definition 2.6. Let $H \leq G \leq \mathcal{S}_n$ and let $F \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ be a polynomial such that $H := \mathrm{Stab}_G(F)$.

In this case, if $\alpha_1, \ldots, \alpha_n \in \Sigma_f$ are the roots of f, the polynomial

$$R_{G,F}(\mathtt{y}) := \prod_{\sigma \in G/H} (\mathtt{y} - F^\sigma(\alpha_1, \ldots, \alpha_n))$$

is called a *G-relative H-invariant resolvent*. If $G = \mathcal{S}_n$ we call it a *universal resolvent*. In that case, we will denote it with R_F.

Theorem 2.7. *Assume $Gal_f \leq G$. Then*

$$R_{G,F}(\mathtt{y}) := \prod_{\sigma \in G/H} (\mathtt{y} - F^{\sigma}(\alpha_1, \ldots, \alpha_n)) \in K[\mathtt{y}]$$

Proof. The polynomial $R_{G,F}(\mathtt{y})$ is invariant under the action of G and, since $Gal_f \leq G$, it is also invariant under the action of Gal_f. Therefore every coefficient of $R_{G,F}(\mathtt{y})$ is in K. □

Let's also define the classical notion of discriminant and how we can use it to obtain information about the Galois group of a polynomial.

Definition 2.8. Suppose that $f \in K[\mathtt{x}]$ and let $\alpha_1, \ldots, \alpha_n$ be its roots in a splitting field Σ_f over K. Let

$$\delta := \prod_{i<j} (\alpha_i - \alpha_j)$$

Then we define the discriminant $\Delta(f)$ of f as δ^2.

Theorem 2.9. *Let $f \in K[\mathtt{x}]$, where $char(K) \neq 2$. Then*

1. *$\Delta(f) \in K$.*
2. *$\Delta(f) = 0$ if and only if f has a multiple root in Σ_f.*
3. *$\Delta(f)$ is a perfect square in K if and only if Gal_f is contained in the alternating group $\mathcal{A}_n$.*

Proof. For the first part, let $\sigma \in \mathcal{S}_n$, acting on the set $\{\alpha_1, \ldots, \alpha_n\}$ of roots of f in Σ_f. It is easy to check that $\sigma(\delta) = \pm\delta$, the sign being $+$ if σ is an even permutation and $-$ if σ is odd. Indeed in many algebra texts the sign of a permutation is defined in this manner. Therefore, $\delta \in \mathcal{A}_n^{\dagger}$. Further, $\Delta(f) = \delta^2$ is unchanged by any permutation in $\mathcal{S}_n$, hence lies in K by theorem 2.4.

Part 2 follows from the definition of δ.

If $\Delta(f)$ is a perfect square in K, then $\delta \in K$, so δ is fixed by Gal_f. As odd permutations change δ to $-\delta$ and since $char(K) \neq 2$ we have $\delta \neq -\delta$. Therefore, all permutations in Gal_f are even, that is, $Gal_f \leq \mathcal{A}_n$. Conversely, if $Gal_f \leq \mathcal{A}_n$, then $\delta \in Gal_f^{\dagger} = K$. Therefore, $\Delta(f)$ is a perfect square in K. □

Using these tools we will describe and prove several methods to successfully compute Gal_f all along the rest of this section.

2.1 The Resolvent Method

The so-called resolvent method computes Gal_f once a classification of the transitive subgroups of $\mathcal{S}_n$ is known.

Step 1: Find invariant polynomials. For each transitive subgroup H of $\mathcal{S}_n$, we look for a polynomial φ in $\mathtt{x}_1, \ldots, \mathtt{x}_n$ such that $\mathrm{Stab}_{\mathcal{S}_n}(\varphi) = H$. The following proposition assures that this is always possible.

Proposition 2.10. *Let F be the monomial $\mathtt{x}_1\mathtt{x}_2^2 \ldots \mathtt{x}_{n-1}^{n-1}$. Then, the stabilizer of the polynomial*

$$\varphi := \sum_{h \in H} F^h \tag{1}$$

is H.

Proof. The polynomial φ is invariant under H by construction, so $H \leq \mathrm{Stab}_{\mathcal{S}_n}(\varphi)$. On the other hand, if $\sigma \in \mathrm{Stab}_{\mathcal{S}_n}(\varphi)$ then F^σ appears in the right side of (1) as one of the summands. But, there are only $|H|$ monomials in the sum, and the map which maps $\sigma \in \mathrm{Stab}_{\mathcal{S}_n}(\varphi)$ to F^σ is a bijection. In particular it is injective. Therefore $|\mathrm{Stab}_{\mathcal{S}_n}(\varphi)| \leq |H|$ and thus $H = \mathrm{Stab}_{\mathcal{S}_n}(\varphi)$. □

An algorithm to compute Galois groups based on the polynomial introduced above will be very slow in general, so we will want to find polynomials φ of small degree, such that $H = \mathrm{Stab}_{\mathcal{S}_n}(\varphi)$. Unfortunately there are some cases where the previous proposition offers an invariant polynomial with minimal degree, for example for $H = \mathcal{A}_n$ (see [11] p. 8).

Step 2: Compute resolvents. For every subgroup $H \in \mathcal{S}_n$ we try to compute the universal resolvent associated with the polynomial φ introduced in **Step 1** for H. We do not know the roots of f, so in practice we would have to write the universal resolvent with respect to the coefficients of f. (We can do this by theorem 2.4; this is why we use universal resolvents). This is in general very time consuming because the universal resolvent might be huge. Fortunately if $K = \mathbb{Q}$ we can avoid (part of) this difficulty.

Suppose that $g \in \mathbb{Z}[\mathtt{x}]$ is an irreducible polynomial of degree n. Then we can compute accurate enough numerical approximations $\alpha_1^*, \ldots \alpha_n^*$ of the roots of g and multiply out the approximate resolvent:

$$R_\varphi^*(\mathtt{y}) = \prod_{\sigma \in \mathcal{S}_n/H} (\mathtt{y} - \varphi^\sigma(\alpha_1^*, \ldots, \alpha_n^*))$$

By approximating each coefficient of R_φ^* to the nearest integer we will obtain the actual

resolvent, since $R_\varphi(\mathtt{y}) \in \mathbb{Z}[\mathtt{y}]$ because of theorem 2.7. This is the basis of the so-called Stauduhar's method.

When dealing with the computation of Galois groups of irreducible polynomials in $\mathbb{Q}[\mathtt{x}]$ we can restrict to polynomials in $\mathbb{Z}[\mathtt{x}]$ because of the following.

Proposition 2.11. *Let c be the* gcd *of the coefficients' denominators of $f \in \mathbb{Q}[\mathtt{x}]$ and let*

$$g(\mathtt{x}) := c^n f(\frac{\mathtt{x}}{c}).$$

Then $g \in \mathbb{Z}[\mathtt{x}]$ and $Gal_f \simeq Gal_g$.

Proof. It is a straightforward computation to see that $g \in \mathbb{Z}[\mathtt{x}]$ and if $\alpha_1, \ldots, \alpha_n$ are the roots of f, the roots of g are $c\alpha_1, \ldots, c\alpha_n$. Thus $\Sigma_f = \Sigma_g$. □

Step 3: Use resolvents. Resolvents can provide a lot of information about Gal_f. The following theorem is the key of the resolvent method.

Theorem 2.12. *Suppose that f is separable, irreducible and $Gal_f \leq G$. Let H be a subgroup of G.*

(a) If Gal_f is conjugate to a subgroup of H, then $R_{G,F}(\mathtt{y})$ has a root in K. In fact, if Gal_f is contained in $\sigma H \sigma^{-1}$, then $F^\sigma(\alpha_1, \ldots, \alpha_n) \in K$.

(b) If $R_{G,F}(\mathtt{y})$ has a simple root in K, then Gal_f is conjugate to a subgroup of H. In fact, if $F^\sigma(\alpha_1, \ldots, \alpha_n) \in K$ and $F^\sigma(\alpha_1, \ldots, \alpha_n)$ is a simple root of $R_{G,F}(\mathtt{y})$, then $Gal_f \leq \sigma H \sigma^{-1}$.

Proof. (a) If Gal_f is conjugate to a subgroup of H, there exists $\sigma \in \mathcal{S}_n$ such that $Gal_f \leq \sigma H \sigma^{-1}$. This easily implies that $F^\sigma(\alpha_1, \ldots, \alpha_n)$ is invariant under Gal_f and hence it lies in K.

(b) Let $\beta = F^\sigma(\alpha_1, \ldots, \alpha_n) \in K$ be a simple root of $R_{G,F}(\mathtt{y})$. If $Gal_f \not\leq \sigma H \sigma^{-1} = \mathrm{Stab}_{\mathcal{S}_n}(F^\sigma)$, then there exists $\tau \in Gal_f$ such that $\tau \notin \sigma H \sigma^{-1} = \mathrm{Stab}_{\mathcal{S}_n}(F^\sigma)$. Then $(F^\sigma)^\tau \neq F^\sigma$ so the resolvent may be written

$$R_{G,F}(\mathtt{y}) = (\mathtt{y} - F^\sigma(\alpha_1, \ldots, \alpha_n))(\mathtt{y} - (F^\sigma)^\tau(\alpha_1, \ldots, \alpha_n))) \cdots$$

But $\beta \in K$ and K is the fixed field of Gal_f so $F^\sigma(\alpha_1, \ldots, \alpha_n) = \beta = \tau\beta = (F^\sigma)^\tau(\alpha_1, \ldots, \alpha_n)$ which is impossible because β is a simple root of $R_{G,F}(\mathtt{y})$ by hypothesis.

□

Example 1. Let $n = 4$ and

$$F := (\mathtt{x}_1 + \mathtt{x}_2 - \mathtt{x}_3 - \mathtt{x}_4) \cdot \prod_{1 \le i < j \le 4} (\mathtt{x}_i - \mathtt{x}_j)$$

Let $G := \mathrm{Stab}_{S_n}(F)$, which is $\langle (1324) \rangle \le \mathcal{S}_4$ when $char(K) \neq 2$. Thus the corresponding universal resolvent has degree $24/4 = 6$. Consider the polynomial $f = \mathtt{x}^4 + b\mathtt{x}^2 + d$. After a long computation (see [7]) it can be obtained that:

$$R_F(\mathtt{y}) = \mathtt{y}^2 \left((\mathtt{y}^2 + 4b\Delta(f))^2 - 2^6 d \Delta(f)^2 \right)$$

This has the rational multiple root $0 \in K$ but $Gal_f \not\leq \langle (1324) \rangle$ when d is not a square in K. So $R_F(\mathtt{y})$ fails to give accurate information about the Galois group because 0 is not a simple root.

Thus, as long as the resolvent is separable, we can use the previous theorem to decide if Gal_f is conjugate to a subgroup of one of the transitive subgroups of $\mathcal{S}_n$ and we can traverse the diagram of inclusions of these transitive subgroups of $\mathcal{S}_n$ and then find Gal_f up to conjugacy. On the other hand, if the resolvent has a multiple root in K, the resolvent does not give us useful information. The next step avoids this problem.

Step 4: Repair Resolvents.

After a few more computations we can get a new polynomial with the same Galois group as f and with a separable resolvent.

Definition 2.13. Consider the rational function $h(\mathtt{x}) := \frac{h_1(\mathtt{x})}{h_2(\mathtt{x})}$ where $h_1(\mathtt{x}), h_2(\mathtt{x}) \in K[\mathtt{x}]$ and none of the roots $\alpha_1, \ldots, \alpha_n$ of f is a root of h_2. We define the Tschirnhaus transformation of the polynomial f by h as:

$${}^h f := \prod_{i=1}^{n} (\mathtt{x} - h(\alpha_i))$$

Theorem 2.14. *Let $R \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n, \mathtt{z}]$ be a polynomial such that $R(\mathtt{x}_1, \ldots, \mathtt{x}_n, \mathtt{z})$ splits into distinct monic $\mathtt{z}-$linear factors in $K[\mathtt{x}_1, \ldots, \mathtt{x}_n, \mathtt{z}]$, that is, $R = \prod_{i=1}^{m} (\mathtt{z} - P_i(\mathtt{x}_1, \ldots, \mathtt{x}_n))$ where $P_i \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ and $P_i = P_j \Leftrightarrow i = j$. Then there exists a finite set $\mathcal{H} \subset K[\mathtt{z}]$ with the following property:*

For every monic and separable polynomial f of degree n there exists a $h \in \mathcal{H}$ such that both ${}^h f$ and $R(h(\alpha_1), \ldots, h(\alpha_n), \mathtt{z}) \in K[\mathtt{z}]$ are separable.

Proof. Let $d > \deg(D)$ where

$$D := \prod_{i<j} (P_i(\mathtt{x}_1, \ldots, \mathtt{x}_n) - P_j(\mathtt{x}_1, \ldots, \mathtt{x}_n)) \prod_{i<j} (\mathtt{x}_i - \mathtt{x}_j) \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$$

and let $\mathcal{U} \subset K$ such that $|\mathcal{U}| = d$ and let

$$\mathcal{H} := \left\{ \sum_{j=0}^{n-1} u_j \mathtt{z}^j \ ; \ u_0, \ldots, u_{n-1} \in \mathcal{U} \right\}.$$

We show that $\mathcal{H}$ has the desired properties. Indeed, let f be a monic and separable polynomial of degree n and let $\alpha_1, \ldots, \alpha_n$ be its roots in a splitting field Σ_f of f over K. Put

$$\mathtt{y}_i := \sum_{j=1}^{n} \alpha_i^{j-1} \mathtt{t}_j \in \Sigma_f[\mathtt{t}_1, \ldots, \mathtt{t}_n], \quad i = 1, \ldots, n$$

or equivalently

$$\begin{pmatrix} \mathtt{y}_1 \\ \mathtt{y}_2 \\ \vdots \\ \mathtt{y}_n \end{pmatrix} := \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{pmatrix} \begin{pmatrix} \mathtt{t}_1 \\ \mathtt{t}_2 \\ \vdots \\ \mathtt{t}_n \end{pmatrix}$$

The set $\{y_1, \ldots, y_n\}$ is algebraically independent over K because $\{\mathtt{t}_1, \ldots, \mathtt{t}_n\}$ is algebraically independent over K and the determinant of the Vandermonde matrix is not zero. The last is due to the separability of f, its roots are pairwise distinct. Therefore the evaluation of D at $\mathtt{y}_1, \ldots, \mathtt{y}_n$ is not zero. Let's define

$$Q(\mathtt{t}_1, \ldots, \mathtt{t}_n) := D(\mathtt{y}_1, \ldots, \mathtt{y}_n) \in \Sigma_f[\mathtt{t}_1, \ldots, \mathtt{t}_n].$$

As each y_j is a linear combination of $\mathtt{t}_1, \ldots, \mathtt{t}_n$ and $\deg(D) < d$, the degree of Q in each variable $\mathtt{t}_i$, $i = 1, \ldots, n$ is less than d, hence there are elements $u_0, \ldots, u_{n-1} \in \mathcal{U}$ such that $Q(u_0, \ldots, u_{n-1}) \neq 0$. The polynomial $h(\mathtt{z}) = \sum_{i=0}^{n-1} u_i \mathtt{z}^i$ is in $\mathcal{H}$ and as $Q(u_0, \ldots, u_{n-1}) = D(h(\alpha_1), \ldots, h(\alpha_n))$ we have that ${}^h f$ and $R(h(\alpha_1), \ldots, h(\alpha_n), \mathtt{z})$ are separable. □

Corollary 2.15. *Given a monic and separable polynomial f of degree n, a polynomial $F \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$, a group $G \leq \mathcal{S}_n$ and the resolvent $R_{G,F}$ associated to f, there exists a Tschirnhaus transformation g of f by a rational function $h \in K(\mathtt{x})$, that is $g := {}^h f$, such that the resolvent $R'_{G,F}$ associated to g is separable, $Gal_f \simeq Gal_g$ and g is irreducible.*

Proof. If the resolvent R is already separable we can take $h(\mathtt{x}) = \mathtt{x}$. If this is not the case, as R satisfies the conditions of the previous theorem 2.14, there exists $h(\mathtt{x}) = \sum_{i=0}^{n-1} u_i \mathtt{x}^i \in K[\mathtt{x}]$ such that the Tschirnhaus transformation ${}^h f = g \in K[\mathtt{x}]$ satisfies that the resolvent R^* associated to g is separable.

To prove that $Gal_f \simeq Gal_g$ it is enough to prove that $\Sigma_f = \Sigma_g$. The inclusion $\Sigma_g \subset \Sigma_f$ holds because if $\alpha_1, \ldots, \alpha_n$ are the roots of f, the roots of g are $h(\alpha_1), \ldots, h(\alpha_n) \in \Sigma_f$.

To prove the converse inclusion it is enough to show that $[\Sigma_f : K] \leq [\Sigma_g : K]$. As $\Sigma_f : K$ and $\Sigma_g : K$ are Galois extensions we have $|Gal_f| = [\Sigma_f : K]$ and $|Gal_g| = [\Sigma_g : K]$. Thus, all we need to prove is the inequality $|Gal_f| \leq |Gal_g|$. To that end, it suffices to define an injective map

$$Gal_f \to Gal_g \ ; \ \sigma \mapsto \tilde{\sigma}.$$

Let $\sigma \in Gal_f$. Then $\tilde{\sigma}$ is defined as $\tilde{\sigma} : h(\alpha_i) \mapsto h(\alpha_j)$ if $\sigma(\alpha_i) = \alpha_j$.

Finally, the orbit of any root of g under the action of Gal_f is the set of all the roots of g and using the proposition 2.17, which is stated and proved later, we obtain that g is irreducible. □

2.2 Relative Resolvents

Theorem 2.12 is even more useful than it could seem at first sight, since if we find a simple root of $R_{G,F}(\mathtt{y})$ which is in K and we know $\sigma \in G/H$ such that $F^\sigma(\alpha_1, \ldots, \alpha_n) \in K$ we can fix some order in the set of roots and we will know that $Gal_f \leq \sigma H \sigma^{-1}$, that is, we will know a subgroup of $\mathcal{S}_n$ containing Gal_f (exactly, not up to conjugacy). This is useful because we will not have to compute the entire next resolvent to make the next decision step. The following example shows how this can be done.

Example 2. Let $n = 4$ and as in example 1, let

$$F := (\mathtt{x}_1 + \mathtt{x}_2 - \mathtt{x}_3 - \mathtt{x}_4) \cdot \prod_{1 \leq i < j \leq 4} (\mathtt{x}_i - \mathtt{x}_j).$$

As it was previously quoted, $G := \mathrm{Stab}_{\mathcal{S}_n}(F) = \langle (1324) \rangle \leq \mathcal{S}_4$ in characteristic distinct from 2. If $f = \mathtt{x}^4 + a_3\mathtt{x}^3 + a_2\mathtt{x}^2 + a_1\mathtt{x} + a_0 \in K[\mathtt{x}]$, the universal resolvent $R_F(\mathtt{y})$, that was expressed in example 1 in expanded form, has also the form

$$R_F(\mathtt{y}) = \prod_{i=1}^{3} \left(\mathtt{y}^2 - \Delta(f)(4\beta_i + a_1 - 4a_2)\right)$$

where $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$ and $\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$. Note that β_i for $i = 1, 2, 3$ are the roots of another resolvent R_φ where $\varphi = \mathtt{x}_1\mathtt{x}_2 + \mathtt{x}_3\mathtt{x}_4$. In the literature, this is known as the Ferrari resolvent. Suppose that we have already computed the Ferrari resolvent and found that it has a root in K. We may assume that it is β_1 so that $Gal_f \leq \langle (1324), (12) \rangle = \mathrm{Stab}_{S_n}(\varphi)$. To decide if Gal_f lies in the subgroup $\langle (1324) \rangle$, we could use the above resolvent R_F. But since we already know one of the β_i and we have assumed that it is β_1, we have imposed some order on the roots and then we could just use the factor

$$\mathtt{y}^2 - \Delta(f)(4\beta_1 + a_1 - 4a_2) \in K[\mathtt{y}]$$

When we impose some order on the roots, or equivalently we know that $Gal_f \leq \sigma H \sigma^{-1}$ for some $\sigma \in \mathcal{S}_n$ and $H \leq \mathcal{S}_n$ we restrict the factors of the resolvent that are candidates to provide roots in K so we just have to compute a factor of the resolvent instead of the whole resolvent. We called that factor a relative resolvent. The so-called Stauduhar's method that is used when $K = \mathbb{Q}$, as previously mentioned, approximates the roots of f to efficiently compute the resolvent. But, as we know the approximations of the roots, we can order them and therefore we can always work with relative resolvents and save time in computations.

2.3 Factorization of Resolvents

So far we have asked whether resolvents have a root in K. But the resolvents can give us more information. Given a polynomial $F(\mathtt{x}_1, \cdots, \mathtt{x}_n)$ with stabilizer H, the factorization of the resolvent $R_F(\mathtt{y})$ gives information about the orbit lengths under Gal_f of the natural action of $\mathcal{S}_n$ over $F(\alpha_1, \ldots, \alpha_n)$. Let's see how.

First we show that the orbit of each element of Σ_f under the action of Gal_f consists precisely of the roots of a monic irreducible polynomial in $K[\mathtt{x}]$.

Lemma 2.16. *Let $W := \{w_1, \ldots, w_k\} \subset \Sigma_f$ and let $g(\mathtt{x}) := \prod_{i=1}^{k}(\mathtt{x} - w_i)$. Then $g(\mathtt{x}) \in K[\mathtt{x}]$ if and only if Gal_f maps W onto W, that is, for each $\sigma \in Gal_f$ the restriction $\sigma|_W : W \to W$ is a bijection.*

Proof. Let $g(\mathtt{x}) = \sum_{i=0}^{k} a_i \mathtt{x}^i$, $w \in W$ and $\sigma \in Gal_f$. Suppose $g(\mathtt{x}) \in K[\mathtt{x}]$. Then

$$0 = g(w) = \sigma(g(w)) = \sigma\left(\sum_{i=0}^{k} a_i w^i\right) = \sum_{i=0}^{k} a_i (\sigma(w))^i = g(\sigma(w))$$

Thus $\sigma(W) \subset W$. Now $\sigma|_W$ is injective because σ is so, and, as W is finite, $\sigma|_W : W \to W$ is a bijection.

Conversely, suppose Gal_f maps W onto W. Then each element $\sigma \in Gal_f$ induces a permutation of W. Thus $\sigma(a_i) = a_i$ because a_i is a symmetric function of $w_1, \ldots, w_k$. This implies that $a_i \in K$ and therefore $g(\mathtt{x}) \in K[\mathtt{x}]$.

□

Proposition 2.17. *Let $w \in W := \{w_1, \ldots, w_k\} \subset \Sigma_f$. Denote by $Gal_f w$ the orbit $\{\sigma(w) \mid \sigma \in Gal_f\}$. Then $W = Gal_f w$ if and only if $g(\mathtt{x}) = \prod_{i=1}^{k}(\mathtt{x} - w_i)$ is an irreducible polynomial in $K[\mathtt{x}]$.*

Proof. If $Gal_f w = W$, then by lemma 2.16, $g(\mathtt{x}) \in K[\mathtt{x}]$. If $g(\mathtt{x})$ is reducible, then $g(\mathtt{x})$ has a factor $h(\mathtt{x}) \in K[\mathtt{x}]$ where $h(\mathtt{x}) = \prod_{i \in I}(\mathtt{x} - w_i)$ for some $I \subsetneq \{1, \ldots, k\}$ and $h(w) = 0$.

Then again by lemma 2.16, Gal_f maps $\{w_i \mid i \in I\}$ onto itself, which contradicts the fact that $W = Gal_f w$.

Conversely, suppose that $g(\mathtt{x})$ is an irreducible polynomial in $K[\mathtt{x}]$. By lemma 2.16 we know that Gal_f maps W onto itself, so $Gal_f w \subset W$. Suppose $Gal_f w = \{w_i \mid i \in I\}$ with $I \subsetneq \{1, \ldots, k\}$. Then by the same lemma, $\prod_{i \in I}(\mathtt{x} - w_i) \in K[\mathtt{x}]$ is a proper divisor of $g(\mathtt{x})$ in $K[\mathtt{x}]$ which contradicts the irreducibility of $g(\mathtt{x})$. □

Corollary 2.18. *Let $F \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ be a polynomial such that $H = Stab_{\mathcal{S}_n}(F)$, suppose the resolvent R_F is separable and let $R_F = \prod_{i=1}^{k}(\mathtt{x} - F_i(\alpha_1, \ldots, \alpha_n))$ where $F_i(\alpha_1, \ldots, \alpha_n) = F^{\sigma}(\alpha_1, \ldots, \alpha_n)$ for some $\sigma \in \mathcal{S}_n/H$. Let also $t \in I \subsetneq \{1, \ldots, k\}$.*

1. *If $Gal_f F_t(\alpha_1, \ldots, \alpha_n) = \{F_i(\alpha_1, \ldots, \alpha_n) | i \in I\}$, then*

$$g(\mathtt{x}) := \prod_{i \in I}(\mathtt{x} - F_i(\alpha_1, \ldots, \alpha_n))$$

   is an irreducible polynomial in $K[\mathtt{x}]$.

2. *If $g(\mathtt{x}) = \prod_{i \in I}(\mathtt{x} - F_i(\alpha_1, \ldots, \alpha_n))$ is an irreducible factor of R_F then we have $Gal_f F_t = \{F_i | i \in I\}$.*

Proof. It is a consequence of proposition 2.17 □

Corollary 2.19. *Let R_F be the universal resolvent associated to F and suppose it is separable. Then the orbit length partition under Gal_f of the action of F over $\mathcal{S}_n$ is the same as the partition of $\deg(R_F)$ induced by the degrees of the irreducible factors of R_F over K.*

Thus given the polynomial F, if for every transitive subgroup of $G \leq \mathcal{S}_n$ we compute the orbit length partition under G of the action of F over $\mathcal{S}_n$ and we factorize R_F, we will discard those subgroups whose orbit length partition is different to the partition of $\deg(R_F)$ induced by the degrees of the irreducible factors of R_F over K. Sometimes, fixing n, the Galois group of irreducible polynomials of degree n can be characterized using a few resolvents and the corresponding orbit length partitions of the transitive subgroups of $\mathcal{S}_n$.

2.4 A general algorithm

We now describe a method to compute the Galois group of any polynomial. The computations are impractical for modestly high degree, but it has the virtue of showing that the problem of computing Gal_f has a solution which is independent on the degree and that it does not need a classification of the transitive subgroups of $\mathcal{S}_n$.

The idea is to consider not just how an element σ of Gal_f acts on $\alpha_1, \ldots, \alpha_n$, but how σ acts on arbitrary linear combinations

$$\beta = \mathtt{y}_1\alpha_1 + \cdots + \mathtt{y}_n\alpha_n$$

To make this action computable we perform polynomials having roots $\sigma(\beta)$ as σ runs through G. To do so, define

$$\sigma_{\mathtt{y}}(\beta) := \mathtt{y}_{\sigma(1)}\alpha_1 + \cdots + \mathtt{y}_{\sigma(n)}\alpha_n, \quad \sigma_\alpha(\beta) := \mathtt{y}_1\alpha_{\sigma(1)} + \cdots + \mathtt{y}_n\alpha_{\sigma(n)}$$

By rearranging terms we see that $\sigma_\alpha(\beta) = \sigma_{\mathtt{y}}^{-1}(\beta)$.

Since the roots $\alpha_1, \ldots, \alpha_n$ of f are pairwise distinct $\sigma_{\mathtt{y}}(\beta) \neq \tau_{\mathtt{y}}(\beta)$ if $\sigma \neq \tau$. Define the polynomial

$$Q := \prod_{\sigma \in \mathcal{S}_n} (\mathtt{t} - \sigma_{\mathtt{y}}(\beta)) = \prod_{\sigma \in \mathcal{S}_n} (\mathtt{t} - \sigma_\alpha(\beta))$$

If we expand into powers of $\mathtt{t}$ the second expression of Q, collect like terms, and write all symmetric polynomials in the α_j as polynomials in the s_k we find that

$$Q = \sum_{j=0}^{n!} \left(\sum_i g_i(s_1, \ldots, s_n) \mathtt{y}_1^{i_1} \ldots \mathtt{y}_n^{i_n} \right) \mathtt{t}^j$$

where the g_i are explicitly computable functions of $s_1, \ldots, s_n$. In particular $Q \in K[\mathtt{t}, \mathtt{y}_1, \ldots, \mathtt{y}_n]$.

We next split Q into a product of irreducible factors, $Q = Q_1 \cdots Q_k$ in $K[\mathtt{t}, \mathtt{y}_1, \ldots, \mathtt{y}_n]$. In the ring $\Sigma_f[\mathtt{t}, \mathtt{y}_1, \ldots, \mathtt{y}_n]$ we can write

$$Q_j = \prod_{\sigma \in A_j} (\mathtt{t} - \sigma_{\mathtt{y}}(\beta))$$

where $\{A_j\}$ is a partition of $\mathcal{S}_n$. We choose the labels so that the identity in $\mathcal{S}_n$ is contained in A_1, so $(\mathtt{t} - \beta)$ divides Q_1 in $\Sigma_f[\mathtt{t}, \mathtt{y}_1, \ldots, \mathtt{y}_n]$.

If $\sigma \in \mathcal{S}_n$, then

$$Q = \sigma_{\mathtt{y}}(Q) = (\sigma_{\mathtt{y}}(Q_1)) \cdots (\sigma_{\mathtt{y}}(Q_k)).$$

Hence $\sigma_{\mathtt{y}}$ permutes the irreducible factors Q_j of Q. Define

$$G = \{\sigma \in \mathcal{S}_n | \sigma_{\mathtt{y}}(Q_1) = Q_1\}$$

as a subgroup of $\mathcal{S}_n$. Then we have the following characterization of Gal_f:

Theorem 2.20. *Gal_f is isomorphic to the group G.*

Proof. The subset A_1 of $\mathcal{S}_n$ is, in fact, equal to G, because

$$\begin{aligned} A_1 &= \{\sigma \mid \mathtt{t} - \sigma_{\mathtt{y}}(\beta) \text{ divides } Q_1 \text{ in } \Sigma_f[\mathtt{t}, \mathtt{y}_1, \ldots, \mathtt{y}_n]\} \\ &= \{\sigma \mid \mathtt{t} - \beta \text{ divides } \sigma_{\mathtt{y}}^{-1}(Q_1) \text{ in } \Sigma_f[\mathtt{t}, \mathtt{y}_1, \ldots, \mathtt{y}_n]\} \\ &= \{\sigma \mid \sigma_{\mathtt{y}}^{-1}(Q_1) = Q_1\} = G. \end{aligned}$$

Define

$$H = \prod_{\sigma \in G} (\mathtt{t} - \sigma_\alpha(\beta)) = \prod_{\sigma \in G} (\mathtt{t} - \sigma_{\mathtt{y}}(\beta)).$$

Clearly, $H \in K[\mathtt{t}, \mathtt{y}_1, \ldots, \mathtt{y}_n]$ and H divides Q in $\Sigma_f[\mathtt{t}, \mathtt{y}_1, \ldots, \mathtt{y}_n]$. Hence H divides Q in $\Sigma_f(\mathtt{y}_1, \ldots, \mathtt{y}_n)[\mathtt{t}]$. Therefore H divides Q in $K(\mathtt{y}_1, \ldots, \mathtt{y}_n)[\mathtt{t}]$. Thus H divides Q in $K[t, \mathtt{y}_1, \ldots, \mathtt{y}_n]$ so $G \leq Gal_f$.

Conversely, if $\tau \in Gal_f$ then

$$\begin{aligned}\tau(Q_1) &= \prod_{\sigma \in A_1} \big(\mathtt{t} - \tau_{\mathtt{y}}(\sigma_{\mathtt{y}}(\beta))\big() = \prod_{\sigma \in A_1} \big(\mathtt{t} - \tau_\alpha^{-1}(\sigma_{\mathtt{y}}(\beta))\big) \\ &= \tau_\alpha^{-1}\left(\prod_{\sigma \in A_1} \big(\mathtt{t} - \sigma_{\mathtt{y}}(\beta)\big)\right) = \tau_\alpha^{-1}(Q_1).\end{aligned}$$

But $Q_1 \in K[\mathtt{t}, \mathtt{y}_1, \ldots, \mathtt{y}_n]$, so $\tau_\alpha^{-1}(Q_1) = Q_1$. Hence $\tau \in G$, and therefore $Gal_f \leq G$. □

2.5 Dedekind's Theorem and Chebotarev Density Theorem

In this section $K = \mathbb{Q}$. Besides, after a transformation as described in proposition 2.11 we can assume that $f \in \mathbb{Z}[\mathtt{x}]$. Let p be a prime and let $\bar{f} \in \mathbb{F}_p[\mathtt{x}]$ be the polynomial obtained by reducing the coefficients of f modulo p. Then the following theorem of Dedekind shows how $\bar{f}$ can give information about the Galois group of f over $\mathbb{Q}$.

Theorem 2.21. (Dedekind) *Let $f \in \mathbb{Z}[\mathtt{x}]$ be monic and separable of degree n. Given a prime p such that $p \nmid \Delta(f)$, let*

$$\bar{f} = \bar{f}_1 \bar{f}_2 \ldots \bar{f}_r,$$

where $\bar{f}_1, \ldots, \bar{f}_r \in \mathbb{F}_p[\mathtt{x}]$ are monic and irreducible. Also set $d_i = \deg(\bar{f}_i)$. Then:

(a) The Galois group of $\bar{f}$ over $\mathbb{F}_p$ is cyclic of order $lcm(d_1, d_2, \ldots, d_r)$.

(b) The Galois group of f over $\mathbb{Q}$ contains an element that acts on the roots of f according to a product of disjoint cycles of the form

$$\underbrace{(\ldots)}_{d_1-cycle}\ \underbrace{(\ldots)}_{d_2-cycle}\ \cdots\ \underbrace{(\ldots)}_{d_r-cycle}$$

Hence Gal_f contains an element of order $lcm(d_1, d_2, \ldots, d_r)$.

Proof. Observe first that $\bar{f}$ is separable, since $p \nmid \Delta(f)$ and $\Delta(\bar{f})$ is the reduction of $\Delta(f)$ modulo p.

Let $m \in \mathbb{Z}^+$. Since

$$\mathtt{x}^{p^m} - \mathtt{x} = \prod_{\alpha \in \mathbb{F}_{p^m}} (\mathtt{x} - \alpha)$$

a separable polynomial in $\mathbb{F}_p[\mathtt{x}]$ splits completely over $\mathbb{F}_{p^m}$ if and only if it divides $\mathtt{x}^{p^m} - \mathtt{x}$. Thus:

$$\begin{aligned}\bar{f} \text{ splits completely over } \mathbb{F}_{p^m} &\Leftrightarrow \bar{f}_i \text{ splits completely over } \mathbb{F}_{p^m} \text{ for all } i \\ &\Leftrightarrow \bar{f}_i \text{ divides } \mathtt{x}^{p^m} - \mathtt{x} \text{ for all } i \\ &\Leftrightarrow d_i = \deg(\bar{f}_i) \text{ divides } m \\ &\Leftrightarrow lcm(d_1, d_2, \ldots, d_r) \text{ divides } m.\end{aligned}$$

This implies that the splitting field of $\bar{f}$ over $\mathbb{F}_p$ is $\mathbb{F}_{p^d}$, where $d = lcm(d_1, d_2, \ldots, d_r)$. Since the group $\Gamma(\mathbb{F}_{p^d} : \mathbb{F}_p)$ is cyclic of order d, part (a) follows.

For part (b), let $\mathtt{u} := (\mathtt{u}_1, \ldots, \mathtt{u}_n)$ and consider

$$Q_{\mathtt{u}}(\mathtt{y}) := \prod_{\sigma \in \mathcal{S}_n} \left(\mathtt{y} - (\mathtt{u}_1\alpha_{\sigma(1)} + \cdots + \mathtt{u}_n\alpha_{\sigma(n)})\right)$$

$$\bar{Q}_{\mathtt{u}}(\mathtt{y}) := \prod_{\sigma \in \mathcal{S}_n} \left(\mathtt{y} - (\mathtt{u}_1\bar{\alpha}_{\sigma(1)} + \cdots + \mathtt{u}_n\bar{\alpha}_{\sigma(n)})\right)$$

where $\bar{s}_i$ is the reduction of s_i modulo p and $\bar{\alpha_1}, \ldots, \bar{\alpha_n}$ are the roots of $\bar{f}$. Note that $s_i \in \mathbb{Z}$ and $\bar{s}_i \in \mathbb{F}_p$ and therefore $Q_{\mathtt{u}} \in \mathbb{Z}[\mathtt{u}_1, \ldots, \mathtt{u}_n, \mathtt{y}]$ and $\bar{Q}_{\mathtt{u}} \in \mathbb{F}_p[\mathtt{u}_1, \ldots, \mathtt{u}_n, \mathtt{y}]$. Given an irreducible factor Q_1 of $Q_{\mathtt{u}}$ theorem 2.20 implies that Gal_f is conjugate to

$$G = \{\sigma \in \mathcal{S}_n \mid \sigma(Q_1) = Q_1\}.$$

We may assume that Q_1 is an irreducible factor of $Q_{\mathtt{u}}(\mathtt{y})$ in the ring $\mathbb{Z}[\mathtt{u}_1, \ldots, \mathtt{u}_n, \mathtt{y}]$. Reducing it modulo p gives $\bar{Q}_1 \in \mathbb{F}_p[\mathtt{u}_1, \ldots, \mathtt{u}_n, \mathtt{y}]$. If $\bar{g}$ is an irreducible factor of $\bar{Q}_1$, then it is also an irreducible factor of $\bar{Q}_{\mathtt{u}}(\mathtt{y})$, so by theorem 2.20, the Galois group $Gal_{\bar{f}}$ of $\bar{f}$ over $\mathbb{F}_p$ is conjugate in $\mathcal{S}_n$ to the subgroup

$$\bar{G} = \{\sigma \in \mathcal{S}_n \mid \sigma(\bar{g}) = \bar{g}\}.$$

We claim that $\bar{G} \leq G$. To prove this, suppose that $\sigma(\bar{g}) = \bar{g}$ but $\sigma(Q_1) =: Q_2 \neq Q_1$. The equality $\sigma(Q_{\mathtt{u}}(\mathtt{y})) = Q_{\mathtt{u}}(\mathtt{y})$ implies that Q_2 is also an irreducible factor of $Q_{\mathtt{u}}(\mathtt{y})$. Since $\mathbb{Z}[\mathtt{u}_1, \ldots, \mathtt{u}_n, \mathtt{y}]$ is a UFD, there exists $q \in \mathbb{Z}[\mathtt{u}_1, \ldots, \mathtt{u}_n, \mathtt{y}]$ such that

$$Q_{\mathtt{u}}(\mathtt{y}) = Q_1 Q_2 q.$$

Reducing this equality modulo p we get

$$\bar{Q}_{\mathtt{u}}(\mathtt{y}) = \bar{Q}_1\bar{Q}_2\bar{q} \in \mathbb{F}_p[\mathtt{u}_1, \ldots, \mathtt{u}_n, \mathtt{y}]. \tag{2}$$

Furthermore the $\mathcal{S}_n$-action is compatible with reduction modulo p, so $\bar{Q}_2 = \sigma(\bar{Q}_1)$. Since $\bar{g}$ divides $\bar{Q}_1$, we see that $\bar{g} = \sigma(\bar{g})$ divides $\sigma(\bar{Q}_1) = \bar{Q}_2$. By the above equation

(2), this implies that $\bar{g}^2$ divides $\bar{Q}_{\mathtt{u}}(\mathtt{y})$, and this is false because, by its definition $\bar{Q}_{\mathtt{u}}$ is a product of distinct irreducible factors in $\Sigma_{\bar{f}}(\mathtt{y})$. This implies that the same is true over $\mathbb{F}_p$. Hence we have a contradiction, which proves that $\sigma(Q_1) = Q_1$ whenever $\sigma(\bar{g}) = \bar{g}$. Thus $\bar{G} \leq G$.

By part (a) the Galois group of $\bar{f}$ over $\mathbb{F}_p$ contains an element whose action on the roots of $\bar{f}$ is given by a product of disjoint cycles of lengths $d_1, \ldots, d_r$. Since the conjugate of a product of disjoint cycles of lengths $d_1, \ldots, d_r$ is a permutation of the same cyclic type, we see that $\bar{G}$, and hence G, contain a permutation of the desired cyclic type. Since G is conjugate to Gal_f, the Galois group of f must contain an automorphism whose action on the roots is as described in part (b) of the theorem. □

Using Dedekind's theorem, one can significantly restrict the possible candidates to be Gal_f and in some cases Gal_f can be found this way. Chebotarev Density Theorem, stated below says that the proportions of elements that we obtain with Dedekind's Theorem with several primes less than a natural N tend to the actual proportions of the elements in Gal_f when N tends to infinity. This property can be used to implement a probabilistic method that guess Gal_f with a very high probability.

Theorem 2.22. (Chebotarev) *For each partition $[r_1, \ldots, r_m]$ of n, the proportion of primes $p \leq k$ such that $p \nmid \Delta(f)$ and such that the degrees of the factorization of $\bar{f} \in \mathbb{F}_p[\mathtt{x}]$ in irreducible factors form the partition $[r_1, \ldots, r_m]$ of n tends, when $k \to \infty$, to $l_{[r_1,\ldots,r_m]}/|Gal_f|$ where $l_{[r_1,\ldots,r_m]}$ is the number of elements in Gal_f whose decomposition in disjoint cycles induces the partition $[r_1, \ldots, r_m]$ of n.*

3 The case of degree 7

In this section we will apply the general ideas of the previous one to the particular case of irreducible polynomials of degree 7 with coefficients in $\mathbb{Q}$. Thus in this section $K = \mathbb{Q}$. We will try to show the power of the tools we have at hand. Although there are some methods that are degree independent (see [11]), the ones explained in the previous section require a classification of the transitive subgroups of $\mathcal{S}_n$. We will prove that up to conjugacy there exist exactly 7 transitive subgroups in $\mathcal{S}_7$, we will develop a general method to compute Gal_f when $n = 7$ and we will prove that for every transitive subgroup $G \leq \mathcal{S}_7$ there exists a polynomial in $\mathbb{Q}[\mathtt{x}]$ whose Galois group is G.

3.1 Transitive subgroups of $\mathcal{S}_7$

Before we prove that there are exactly 7 transitive subgroups of $\mathcal{S}_7$ up to conjugacy, we need some previous results. We will use some results about primitive groups to bound the order of the transitive subgroups of $\mathcal{S}_7$ other than $\mathcal{A}_7$ and $\mathcal{S}_7$. The regularity of the transitive subgroups that contain just one Sylow 7-subgroup will be essential.

Let's first remember the third Sylow Theorem.

Theorem 3.1. *Let p be a prime number and let G be a finite group whose order is $|G| = p^n m$ where m and n are positive integers and p does not divide m. Then, the number n_p of Sylow p-subgroups of G satisfies the following:*

1. *$n_p = [G : N_G(H)]$ for every Sylow p-subgroup H of G.*
2. *n_p divides m and $n_p - 1$ is a multiple of p.*

We will introduce now some notions, as the primitivity of a group, that will appear in the next results which are needed to prove later the main theorem at the end of this section.

Definition 3.2. Let G be a subgroup of $\mathcal{S}_n$. Then:

1. G is *imprimitive* if the set $\{1, \dots, n\}$ is a disjoint union

$$\{1, \dots, n\} = R_1 \sqcup \cdots \sqcup R_k, \quad R_i \neq \varnothing \text{ for all } i,$$

   such that for every $\tau \in G$ and every $1 \leq i \leq k$ there exists an index j with $1 \leq j \leq k$ that depends on τ and i such that $\tau(R_i) = R_j$. We also require that $k > 1$ and $|R_i| > 1$ for some i. We call each R_i an *imprimitive system.*

2. G is *primitive* if it is not imprimitive.

Example 3. The cyclic subgroup of $\mathcal{S}_n$ generated by a cycle is primitive.

Definition 3.3. We will say that a group G is of *degree* n if there is a $G' \cong G$ such that $G' \leq \mathcal{S}_n$ but there is no $G' \cong G$ such that $G' \leq \mathcal{S}_{n-1}$.

Definition 3.4. Let $\sigma \in G \leq \mathcal{S}_n$ be an element of a subgroup of $\mathcal{S}_n$. We define the *support of* σ as

$$\operatorname{supp}(\sigma) = \{1 \leq i \leq n : \sigma(i) \neq i\} = \{1, 2, \dots, n\} \backslash \operatorname{Fix}(\sigma).$$

Definition 3.5. A group $G \in \mathcal{S}_n$ is said to be *k-transitive* if for any k symbols $a_1, \dots, a_k$ pairwise distinct and any other k symbols $b_1, \dots, b_k$ pairwise distinct, there exists $\sigma \in G$ such that for all $i \in \{1, \dots, k\}$ we have $\sigma(a_i) = b_i$. If $k = 1$ we usually say that G is transitive instead of 1-transitive.

Proposition 3.6. *Let p be a prime and $G \leq \mathcal{S}_p$ a subgroup. Then the following are equivalent:*

(a) G is transitive.

(b) The order of G is divisible by p.

(c) G contains a p-cycle.

Proof. For $(a) \Rightarrow (b)$, by the Fundamental Theorem of Group Actions, the size of an orbit divides the order of the group. Then we are done, since transitivity implies that $\{1, 2, \ldots, p\}$ is an orbit of the action of G, in fact the unique one.

$(b) \Rightarrow (c)$. By Cauchy Theorem there is a p-subgroup in G, which in this case it is a cyclic group of order p. Therefore G contains a p-cycle.

$(c) \Rightarrow (a)$. If G contains a p-cycle, G is clearly transitive. □

Proposition 3.7. *Let G be a group of degree n. If G is primitive then it is transitive. In addition, if n is prime and G is transitive then G is primitive.*

Proof. If G is not transitive let a and b be two symbols such that there is no permutation in G that transforms a into b. Then the symbols a_i such that some permutation of G transforms a into a_i and the remaining symbols form two imprimitive systems and therefore G is imprimitive.

Suppose now the degree of G is a prime number and assume G is transitive. If it were imprimitive, the size of all the imprimitive systems would be pairwise equal and therefore it has to be a divisor of p. However, the size of all the imprimitive systems cannot be 1 and on the other hand it cannot be p because the number of imprimitive systems must be greater than 1.

□

Proposition 3.8. *A 2-transitive group is primitive.*

Proof. Suppose it is imprimitive. We take two elements i, j that belong to the same imprimitive system R and as the group is 2-transitive there must be a permutation that transforms i into i and j into an element that belongs to an imprimitive system distinct to R. But that is impossible for the assumption of imprimitivity, therefore the group must be primitive. □

Lemma 3.9. *Let G be a primitive group of degree n and let $H \leq G$ be a primitive subgroup that keeps $n-m$ elements fixed and is transitive in the remaining m elements. Then there exists a subgroup $H' \leq G$ conjugated to H such that $supp(H) \cap supp(H') \neq \varnothing$.*

Proof. Suppose the statement is false. Then, the supports of the conjugate subgroups to H are pairwise disjoint by the transitivity of G. Every symbol $a \in \{1, 2, \ldots, n\}$ must be in the support of a conjugate subgroup to H. Indeed, if $\sigma \in G$ is an element that transforms $b \in \text{supp}(H)$ into a, then $a \in \text{supp}(\sigma^{-1}H\sigma)$.

Now, as G is primitive, there must exist conjugate subgroups H_1, H_2 and H_3 to H and $\tau \in G$ such that there are $i, j \in \text{supp}(H_1)$ with $\tau(i) \in \text{supp}(H_2)$ and a $\tau(j) \in \text{supp}(H_3)$. But then $H_2' := \tau H_2 \tau^{-1}$ is a conjugate subgroup to H such that $i \in \text{supp}(H_2')$ but $j \notin \text{supp}(H_2')$. This is a contradiction with the fact that the supports of the conjugate subgroups to H are pairwise disjoint. □

Now we will obtain an upper bound of the order of a primitive group of degree n, other than $\mathcal{A}_n$ and $\mathcal{S}_n$. The result will follow by the two next theorems.

Theorem 3.10. *Let G be a group of degree n that does not contain $\mathcal{A}_n$. If G is k-transitive then $k \leq \frac{1}{3}n + 1$.*

Proof. Let G be k-transitive. Let us prove that G contains a permutation whose support has, at most, k elements. Pick $\sigma \in G$ and suppose that $|\text{supp}(\sigma)| = s > k$. We represent σ as

$$\sigma = (a_1, a_2, \ldots, a_i) \cdots (\ldots, a_{j-1}, a_j)(a_{j+1}, \ldots, a_{k-1}, a_k, \ldots) \cdots$$

If $j + 1 < k$, take τ such that $\tau(a_i) = a_i$ for $i \in \{1, 2, \ldots, k-1\}$ and $\tau(a_k) = b_k$ where $b_k \in \text{supp}(\sigma) \backslash \{a_1, \ldots, a_k\}$. There must be a permutation like τ because G is k-transitive. Now we have

$$\tau^{-1}\sigma\tau = (a_1, a_2, \ldots, a_i) \ldots (\ldots, a_{j-1}, a_j)(a_{j+1}, \ldots, a_{k-1}, b_k, \ldots) \ldots$$

and $\sigma \neq \tau^{-1}\sigma\tau$, so $\tau^{-1}\sigma\tau\sigma^{-1}$ is not the identity and it keeps $a_1, \ldots, a_{k-2}$ fixed. We claim that $|\text{supp}(\tau^{-1}\sigma\tau\sigma^{-1})| \leq 2s - 2k + 2$. Indeed, $|\text{supp}(\tau^{-1}\sigma\tau)| = |\text{supp}(\sigma^{-1})| = s$, but $|\text{supp}(\tau^{-1}\sigma\tau) \cap \text{supp}(\sigma^{-1})| \geq k$, hence the support size of the product $(\tau^{-1})(\sigma\tau\sigma^{-1})$ is at most $2s - k$. But, in addition, we have already proved that $a_1, \ldots, a_{k-2} \notin \text{supp}(\tau^{-1}\sigma\tau\sigma^{-1})$ and therefore $|\text{supp}(\tau^{-1}\sigma\tau\sigma^{-1})| \leq 2s - 2k + 2$.

If $j = k - 1$ we take τ such that $\tau(a_i) = a_i$ for $i \in \{1, 2, \ldots, k-1\}$ and $\tau(a_k) = c_k$ where c_k is an element that does not occur in $\text{supp}(\sigma)$. We do the same as before and now we obtain that the permutation $\tau^{-1}\sigma\tau\sigma^{-1}$ is not trivial, fixes the elements $a_1, \ldots, a_{k-1}$ and $|\text{supp}(\tau^{-1}\sigma\tau\sigma^{-1})| \leq 2s - 2k + 2$.

We have proved that if $2s - 2k + 2 < s$ or, equivalently, $s < 2k - 2$ then G contains a permutation whose support has less than s elements. This process may be repeated until we arrive at a non trivial permutation whose support has $k' \leq k$ elements:

$$\sigma' = (a_1, a_2, \ldots, a_i) \ldots (a_{j+1}, \ldots, a_{k'})$$

and considering τ such that $\tau(a_i) = a_i$ for $i \in \{1, 2, \ldots, k' - 1\}$ and $\tau(a_{k'}) = b_{k'}$, with $b_{k'}$ not occurring in $\text{supp}(\sigma')$, we have

$$\tau^{-1}\sigma'\tau = (a_1, a_2, \ldots, a_i) \ldots (a_{j+1}, \ldots, b_{k'})$$

$$\rho := \sigma'^{-1}\tau^{-1}\sigma'\tau = (a_{j+1}, a_{k'}, b_{k'})$$

Now as $b_{k'}$ was any symbol not occurring in σ', if $k = 2$, then k' must be 2 and we can obtain the cycles (a_1, a_2, j), for $j \in \{3, 4, \ldots, n\}$, and these generate $\mathcal{A}_n$, which was not the case by hypothesis.

If $k \geq 3$ then we can do what we have just done with σ' but using ρ and we would obtain the 3-cycles $(a_{j+1}, a_{k'}, j)$ for $j \in \{1, 2, \ldots, n\} \backslash \{a_{j+1}, a_{k'}\}$. If we consider τ' such that $\tau'(a_{j+1}) = a_{j+1}$, $\tau'(a_{k'}) = a_{k'}$ and $\tau(b_{k'}) = j$, then $\tau^{-1}\rho\tau = (a_{j+1}, a_{k'}, j)$. These also generate $\mathcal{A}_n$, which was not the case.

So $|\text{supp}(\sigma)| \geq 2k - 2$ for all $\sigma \in G \backslash \{\text{id}\}$. But G is k-transitive and therefore it has non trivial permutations whose support has $n - (k - 1)$ or less symbols. Hence, the following inequality must hold

$$n - k + 1 \geq 2k - 2$$

or equivalently

$$k \leq \frac{1}{3}n + 1$$

□

Theorem 3.11. *Let G be a primitive group of degree n such that $\mathcal{A}_n \not\leq G$, which has a primitive subgroup H that keeps exactly $n - m$ elements fixed and is transitive in the remaining m elements. Then $m \geq \frac{2}{3}n$ and G is $(n - m + 1)$-transitive.*

Proof. By lemma 3.9, there exists a conjugate subgroup H' of H such that $\text{supp}(H) \cap \text{supp}(H') \neq \varnothing$. Suppose we choose H' so that the size of the intersection of these two sets of m elements is as great as possible, say s. We denote by $\alpha_1, \alpha_2, \ldots, \alpha_{m-s}, \gamma_1, \gamma_2, \ldots, \gamma_s$ and by $\beta_1, \beta_2, \ldots, \beta_{m-s}, \gamma_1, \gamma_2, \ldots, \gamma_s$, respectively, the supports of H and H'. Then $\langle H, H' \rangle$ is a transitive subgroup in the $2m - s$ elements α, β and γ which keeps fixed the remaining elements of $\{1, 2, \ldots, n\}$.

H is primitive, so if $s \leq m - 2$ we can take a permutation $\rho \in H$ such that $\rho(\alpha_i) = \alpha_j$ for some i, j and at the same time ρ does not change all the α's into the α's. Now

$|\mathrm{supp}(H) \cap \mathrm{supp}(\rho^{-1}H'\rho)| > s$. Indeed, both operate on the β's and they have at least $s-(m-s-1)$ γ's in common (or zero if $s-(m-s-1)<0$) because ρ can at most transform $m-s-1$ γ's into α's. This contradiction proves that s must be equal to $m-1$.

Now $\langle H, H'\rangle$ is 2-transitive. This is so because H and H' were transitive, so for $j \neq k$, given $x := \gamma_j$ or α_1 and $y := \gamma_k$ or β_1, there exists $\sigma \in H$ and $\sigma' \in H'$ such that $\sigma(\alpha_1) = x$ and $\sigma'(\beta_1) = \sigma^{-1}(y)$, so $\sigma'\sigma$ transforms α_1 and β_1 into x and y respectively, that is, $\sigma(\sigma'(\alpha_1)) = x$ and $\sigma(\sigma'(\beta_1)) = y$. If we want to transform α_1 and β_1 into β_1 and α_1 respectively, we can apply first a permutation $\sigma \in H$ that transforms α into γ_j for some j, then a permutation $\sigma' \in H'$ that transforms γ_j into β_1 and finally a permutation in H that transforms $\sigma'(\sigma(\beta_1))$ into α_1.

Therefore by proposition 3.8, $\langle H, H'\rangle$ is a primitive group of degree $2m-(m-1) = m+1$ which fixes $n-m-1$ elements. We may argue about this subgroup as we have done about H. Among the subgroups conjugate to $\langle H, H'\rangle$, there must be at least one which operates on m of the symbols of the support of $\langle H, H'\rangle$. This group and $\langle H, H'\rangle$ generate a 3-transitive group of degree $m+2$, which fixes $n-m-2$ elements. Proceeding this way, we find finally that G itself must be $(n-m+1)$-transitive. Using the previous theorem (3.10) we deduce that $m \geq \frac{2}{3}n$. □

Corollary 3.12. *A primitive group of degree n that contains a cycle of length m, with $m < \frac{2}{3}n$, is either $\mathcal{A}_n$ or $\mathcal{S}_n$.*

Proof. It suffices to apply Theorem 3.11 to the subgroup H generated by the cycle of length m. □

Corollary 3.13. *Let G be a primitive group of degree n such that $\mathcal{A}_n \not\leq G$. Then*

$$|G| \leq \frac{n!}{2 \cdot 3 \cdots p}$$

where $2, 3, \ldots, p$ are the distinct primes which are less than $\frac{2}{3}n$.

Proof. Let q be a prime that divides n. Every subgroup of a group H whose order divides the order of a Sylow q-subgroup is contained in a Sylow q-subgroup of H. Therefore, in $\mathcal{S}_n$, any q-cycle is contained in a Sylow q-subgroup of $\mathcal{S}_n$. The Sylow q-subgroups of the symmetric group form a single conjugate class, thus every Sylow q-subgroup of $\mathcal{S}_n$ contains a q-cycle.

The group generated by a q-cycle is a primitive group that fixes $n-q$ elements and is transitive in the remaining q elements. Hence if $q \leq \frac{2}{3}n$, it follows by theorem 3.11 that no primitive group of degree n, other than $\mathcal{A}_n$ and $\mathcal{S}_n$, can contain a Sylow q-subgroup of

$\mathcal{S}_n$ and therefore if the order of a Sylow q-subgroup of $\mathcal{S}_n$ is q^α, the highest power of q that divides the order of G is less than or equal to $q^{\alpha-1}$.

□

We will use the latter corollary to bound the order of the primitive subgroups of $\mathcal{S}_7$ other than $\mathcal{A}_7$ and $\mathcal{S}_7$. The next proposition is a key step for the main proof. But before, we present a lemma that will be used in the proof of the proposition and in the rest of the section.

Lemma 3.14. *The elements of a transitive group $G \in \mathcal{S}_n$ which fix a given symbol form a subgroup of G and its order is $|G|/n$.*

Proof. It is straightforward to see that the permutations that fix an element form a subgroup, for if σ and σ' fix a given element then also does $\sigma\sigma'^{-1}$. Let H be this subgroup, we can assume the element fixed is the symbol 1, and let also $\sigma_i \in G$ be permutations that transform 1 into i, for $i \in \{2, 3, \ldots, n\}$. Now we decompose the elements of G in the following sets:

$$H,\ H\sigma_2,\ H\sigma_3,\ \ldots,\ H\sigma_n$$

These sets are obviously disjoint because two elements of different sets transform 1 into a different element. On the other hand, if $\rho \in G$ transforms 1 into i, then $\rho\sigma_i^{-1} \in H$ and therefore $\rho \in H\sigma_i$. As $|H\sigma_i| = |H|$ for $2 \leq i \leq n$ we conclude that the order of H is $|G|/n$. □

Proposition 3.15. *Let G be a non-cyclic primitive group of prime degree p. Let $\sigma \in G$ be a permutation of order p. Let $H := \langle\sigma\rangle$ and let $N_G(H)$ be the normalizer of H in G. Then:*

1. *$H \subsetneq N_G(H)$ and $|N_G(H)|$ divides $p(p-1)$.*
2. *If $\frac{1}{2}(p-1)$ is a prime other than 2 (note that in such a case $p \neq 2$), and G contains more than one subgroup of order p, then $\frac{1}{2}(p-1)$ divides the order of G. Besides, in this case $|N_G(H)| \neq 2p$.*

Proof. Such σ exists because by 3.7 G is transitive and then we get the existence of σ by 3.6.

1. To prove that $|N_G(H)|$ divides $p(p-1)$ we just need to prove that $|N_{\mathcal{S}_n}(H)| = p(p-1)$. The only permutations of order p in $\mathcal{S}_n$ are p-cycles. There are $(p-1)!$ different p-cycles. But the subgroups generated by two of these cycles just share the identity,

hence there are $(p-2)!$ Sylow p-subgroups of order p. By the third Sylow theorem,

$$|N_{\mathcal{S}_p}(H)| = |\mathcal{S}_p|/n_p = p!/(p-2)! = p(p-1).$$

Now if $N_G(H) = H$, then there are $|G|/p$ conjugate subgroups to H. Indeed, G acts by conjugation on the family of conjugate groups of H and the size of this family equals the index of the orbit stabilizer, which is $[G : N_G(H)] = |G|/|N_G(H)| = |G|/p$. Then G contains $|G|(p-1)/p$ elements of order p. In this case G would contain exactly $|G|/p$ permutations whose orders are not divisible by p. But this is impossible because $|G|/p$ (> 1) is the order of a subgroup of G such that it fixes a given symbol, none of the permutations in this subgroup has order p and there are p such subgroups, which are not all pairwise equal. This contradiction proves that $H \subsetneq N_G(H)$.

2. Note that $H \leq \mathcal{A}_n$ because H is generated by a p-cycle and p is odd. If $1 + kp$ is the number of Sylow p-subgroups of G then by Theorem 3.1

$$|G| = N_G(H)(1 + kp) = p\left(\frac{p-1}{d}\right)(1 + kp)$$

where d divides $p - 1$. If $\frac{p-1}{2}$ is a prime, and if G contains more than one Sylow p-subgroup and $\frac{p-1}{2}$ does not divide the order of G, then the order of $N_G(H)$ equals $2p$. A permutation of order 2 in $N_G(H)$ must be the product of $\frac{p-1}{2}$ transpositions (this is derived by the remark following this proposition), thus it is an odd permutation because by hypothesis $\frac{p-1}{2}$ is odd. The group G must therefore contain the normal subgroup $K := \mathcal{A}_n \cap G$ in which these permutations of order 2 do not occur. $H \leq \mathcal{A}_n$ and then in such a group we would have that $H = N_K(H)$ and we have just seen that this is impossible unless $K = H$, which is not the case because G has more than one Sylow p-subgroup and thus its order is greater than $2p$.

□

Let's prove the following lemma in order to make an important remark about the previous proposition.

Lemma 3.16. *Let $n \in \mathbb{Z}^+$. Let $C_{\mathcal{S}_n}(\sigma) = \{\rho \in \mathcal{S}_n : \rho\sigma = \sigma\rho\}$ be the centralizer of σ. Then $C_{\mathcal{S}_n}(\sigma) = \langle\sigma\rangle$.*

Proof. The inclusion $\langle\sigma\rangle \leq C_{\mathcal{S}_n}(\sigma)$ is obvious. Hence it suffices to prove that both groups have the same number of elements, that is $|C_{\mathcal{S}_n}(\sigma)| = n$. Let $\mathrm{Bij}(\mathcal{S}_n)$ denote the group of bijections of $\mathcal{S}_n$ and let $\mathcal{S}_n \to \mathrm{Bij}(\mathcal{S}_n), \tau \mapsto \tilde{\tau}$ where $\tilde{\tau} : \mathcal{S}_n \to \mathcal{S}_n$, $\alpha \mapsto \tau^{-1}\alpha\tau$.

The stabilizer of σ with respect to this action is

$$\mathrm{Stab}_{\mathcal{S}_n}(\sigma) = C_{\mathcal{S}_n}(\sigma)$$

and the orbit is $O_\sigma = \{\tau^{-1}\sigma\tau : \tau \in \mathcal{S}_n\}$. The last set is the set of all the n-cycles. Then

$$|C_{\mathcal{S}_n}(\sigma)| = |\mathrm{Stab}_{\mathcal{S}_n}(\sigma)| = \frac{\mathrm{ord}(\mathcal{S}_n)}{|O_\sigma|} = \frac{n!}{(n-1)!} = n = \mathrm{ord}(\langle\sigma\rangle)$$

□

Remark 3.17. Let p be a prime number, and let $G \leq \mathcal{S}_p$ be a group that contains just one subgroup H of order p. Recall that by propositions 3.6 and 3.7 G is primitive. If G is cyclic, then it has order p. Otherwise by the previous proposition 3.15.1, the order of G must divide $p(p-1)$. This is so because H is the only Sylow p-subgroup in G, hence it is normal in G and consequently G is a subgroup of $N_{\mathcal{S}_p}(H)$.

We will give now some properties of $N_{\mathcal{S}_p}(H)$. Let $\alpha \in \{1, 2, \ldots, p-1\}$ be an integer such that the class $\alpha + p\mathbb{Z}$ generates the multiplicative group $\mathbb{Z}_p^*$ of units of the ring $\mathbb{Z}_p$ and let $\sigma \in H$ be a generator of H. As every element in H but the identity is a p-cycle, there exists $\rho \in N_{\mathcal{S}_p}(H)$ such that $\rho^{-1}\sigma\rho = \sigma^\alpha$. Iterating the conjugation by ρ we obtain $\rho^{-k}\sigma\rho^k = \sigma^{\alpha^k}$ for all k. For $k = p-1$ we have $\rho^{-(p-1)}\sigma\rho^{p-1} = \sigma^{\alpha^{p-1}}$ and by lemma 3.16 ρ^{p-1} must be the identity or a p-cycle. The latter is impossible because if ρ^{p-1} is a p-cycle then $\mathrm{ord}(\rho)$ is a multiple of p and then it would be exactly p and $\rho = \sigma^t$ for some t. Otherwise $\rho^{-1}\sigma\rho = \sigma^{-t}\sigma\sigma^t = \sigma \neq \sigma^\alpha$, which is false. Thus the order of ρ is $p-1$.

Besides, every permutation in $N_{\mathcal{S}_p}(H)$ but the identity fixes at most one symbol. Indeed, as the powers of σ distinct to the identity fix no symbol, if there exists $\tau \in N_{\mathcal{S}_p}(H)\backslash\langle\sigma\rangle$ such that for two distinct symbols a, b we have that $\tau(a) = a$ and $\tau(b) = b$, then let t be an integer with $1 \leq t < p$ such that $\sigma^t(a) = b$. Now $\tau^{-1}\sigma^t\tau(a) = \tau(\sigma^t(\tau^{-1}(a))) = b$. But as $\tau \in N_{\mathcal{S}_p}(H)$ then $\tau^{-1}\sigma^t\tau \in \langle\sigma\rangle$ and therefore $\tau^{-1}\sigma^t\tau$ would be σ^t, and this is impossible again by lemma 3.16.

Without loss of generality, we can assume that $\sigma := (1, 2, \ldots, p)$. Suppose that τ is a permutation that fixes one symbol unchanged and $\tau^{-1}\sigma\tau = \sigma^\alpha$. We can suppose $\tau(1) = 1$. We have

$$\sigma^\alpha = (1, \alpha+1, 2\alpha+1, \ldots)$$

But

$$\tau^{-1}\sigma\tau = (\tau(1), \tau(2), \ldots, \tau(p)) = (1, \tau(2), \ldots, \tau(p)),$$

and thus

$$\tau(2) = \alpha+1, \tau(3) = 2\alpha+1, \ldots, \tau(r) = (r-1)\alpha+1 \pmod p.$$

Consequently

$$\tau = (2, \alpha+1, \alpha^2+1, \ldots)\cdots$$

and $\alpha^k + 1 = 2 \pmod p$ if and only if $\alpha^k = 1$. As $\alpha + p\mathbb{Z}$ generates $\mathbb{Z}_p^*$ the smallest value of k such that $\alpha^k + 1 = 2$ is $k := p - 1$, that is,

$$\tau = (2, \alpha + 1, \alpha^2, +1, \ldots, \alpha^{p-2} + 1)$$

and τ is a cycle of length $p - 1$. Hence, σ and τ are cycles of length p and $p - 1$ satisfying $\tau^{-1}\sigma\tau = \sigma^\alpha$. Therefore $\langle \sigma, \tau \rangle$ is a semidirect product $\mathbb{Z}_p \ltimes \mathbb{Z}_{p-q}$ of order $p(p - 1)$.

In addition, for each $0 \leq k < p$, we have $\tau_k := \sigma^{-k}\tau\sigma^k$, which is a cycle of length $p - 1$ and the symbol that is fixed by it is different for each k. Therefore the $p(p - 1)$ elements of $N_{\mathcal{S}_p}(H)$ are the $p(p - 2) + 1$ powers of the τ_k's and the $p - 1$ non trivial powers of σ.

Theorem 3.18. *The symmetric group $\mathcal{S}_7$ contains, up to conjugacy, 7 transitive subgroups.*

Proof. By theorem 3.7, every transitive group of degree 7 is primitive. If it does not contain $\mathcal{A}_7$, its order must be a divisor of $\frac{7!}{2\cdot 3} = 7 \cdot 6 \cdot 5 \cdot 4 = 840$ because of corollary 3.13.

If a primitive group G of degree 7 contains just one Sylow 7-subgroup H then, by the previous remark 3.17 the group must be isomorphic to a subgroup of $N_{\mathcal{S}_7}(H)$ of order 42. As all Sylow 7-subgroups of $\mathcal{S}_7$ are conjugate also their normalizers are conjugate in $\mathcal{S}_7$. The same occurs for the subgroups of $N_{\mathcal{S}_7}(H)$ that contain the 7-cycle and all the groups of the same order in $\mathcal{S}_7$. If $\sigma := (1, 2, 3, 4, 5, 6, 7)$ and $\tau := (2, 4, 3, 7, 5, 6)$ are given by the construction of the previous remark with $\alpha = 3$, then the primitive groups that contain just one Sylow 7-subgroup are conjugate to one of the following: $\langle \sigma, \tau \rangle, \langle \sigma, \tau^2 \rangle, \langle \sigma, \tau^3 \rangle, \langle \sigma \rangle$ which have orders 42, 21, 14, and 7 respectively.

If a primitive group G of degree 7 contains more than one Sylow 7-subgroup and if $\mathcal{A}_n \not\leq G$, then by theorem 3.15, as 7 and $(7 - 1)/2 = 3$ are primes, we have that 3 divides the order of G. Let $H \leq G$ be a Sylow 7-subgroup. Again by theorem 3.15, $|N_G(H)|$ must be a divisor of $7 \cdot (7 - 1) = 42$ different from 7 and 14, so it must be 21 or 42. The number of Sylow 7-subgroups in G must be $[G : N_G(H)]$ and it has to be congruent to 1 modulo 7. We know that the order of G must divide 840 so n_7 must be a divisor of $840/21 = 40$ or $840/42 = 20$, congruent to the unity modulo 7 and greater than 1. The only possible value for n_7 is 8. Hence $|G| = 168$ and $|N_G(H)| = 21$ and G contains 8 Sylow 7-subgroups.

G must be 2-transitive. Indeed, assume that one of the subgroups H of order $168/7 = 24$ defined by the permutations of G that fix a given symbol is not transitive in the six symbols that are permuted by the group. The group G cannot contain a cycle of length 3 because then it would contain $\mathcal{A}_7$ by corollary 3.12. Hence the elements of order 3 in H are the products of two 3-cycles. In that case H is isomorphic to a subgroup of $\mathcal{S}_3 \times \mathcal{S}_3$, otherwise it would be transitive, and it must not contain cycles of length 3. Consequently H contains at most four elements of order 3. In addition, as H cannot contain elements of order 4,

the remaining 20 elements must be either involutions or the identity. But there are just 16 of such elements in $\mathcal{S}_3 \times \mathcal{S}_3$.

This subgroup H of order 24, transitive in 6 symbols, must contain 4 Sylow 3-subgroups. By the third Sylow theorem, n_3 must be equal to 1 or 4. If $n_3 = 1$ then the only Sylow 3-subgroup is normal in H and there would be elements of order 6 in H. These elements must be cycles of length 6. Indeed, none of them can be the product of a 2-cycle and a 3-cycle because the transitivity of H implies that the subgroup of permutations that fix a given symbol, among the six that H permutes, has order $24/6 = 4 < 6$. Now let $\rho \in G$ be a permutation of order 7, let σ be one of the cycles of order 6 in the subgroup of order 24 and let τ be an element of order 2 in the subgroup of order 4 given by the permutations of G that fix the same symbol as σ and another given symbol. We shall show that the order of $K := \langle \rho, \sigma, \tau \rangle$ is 84 and thus K will be a primitive subgroup of G (because its order is a multiple of 7). But we already know that no primitive subgroup of degree 7 has order 84 and we will conclude that the group H of order 24 must contain 4 Sylow 3-subgroups.

Let's see first that $|K| \geq 84$. We prove that for $0 \leq a, a' < 7$; $0 \leq b, b' < 6$; $0 \leq c, c' < 2$ such that $(a, b, c) \neq (a', b', c')$ then $\rho^a \sigma^b \tau^c \neq \rho^{a'} \sigma^{b'} \tau^{c'}$. Assume that $\rho^a \sigma^b \tau^c = \rho^{a'} \sigma^{b'} \tau^{c'}$, or equivalently

$$\rho^{a-a'} \sigma^b \tau^{c-c'} = \sigma^{b'}. \tag{3}$$

If $a = a'$ then $\sigma^{b-b'} = \tau^{c'-c}$. The latter can be satisfied just if either $(b, c) = (b', c')$, which is impossible, or if both $\sigma^{b-b'}$ and $\tau^{c'-c}$ are permutations of order 2. The last case is also impossible because $\sigma^{b-b'}$ must be the disjoint product of three cycles of order 2 and $\tau^{c-c'}$ can permute at most 4 symbols.

For the case $a \neq a'$, we obtain a contradiction too. The equation (3) is equivalent to $\rho^{a-a'} = \sigma^{b'-b} \tau^{c'-c}$ but $\rho^{a-a'}$ displaces all the symbols and $\sigma^{b'-b} \tau^{c'-c}$ fixes at least one symbol.

Finally, there are by construction two symbols such that the subgroup of K of the permutations that fix those two symbols is $\langle \tau \rangle$, which has order 2. However given any two symbols, the subgroup consisting of the permutations of G that fix those two symbols has always order 4. Hence $K \neq G$.

Using a classification of the groups of order 24 we see that there are just two groups which contain 4 Sylow 3-subgroups, but just one of them does not contain permutations of order 6, the symmetric group acting on four symbols, $\mathcal{S}_4$. Hence H is isomorphic to $\mathcal{S}_4$.

Note that every group of degree 7 and order 168 is simple. If it were not simple, as it is 2-transitive, a normal subgroup of it other than the trivial group and itself would be

transitive and therefore by 3.6 its order would be a multiple of 7 and it would contain a Sylow 7-subgroup. But all the 7-Sylow groups of G are conjugate in G and the normal group must contain all of them and consequently it would be G because we have already proved that the order of a transitive group of degree 7 which contains more than one Sylow 7-subgroup is greater than or equal to 168. This also implies that $G < \mathcal{A}_7$ because otherwise the subgroup of the even permutations of G would be a normal subgroup of G other than the identity and itself.

The actual construction of the group is now reduced to a bounded number of trials. A group of degree 6 isomorphic with $\mathcal{S}_4$ and containing no odd permutations, may always be represented in the form

$$H = \{(2,3,4)(5,6,7),\ (2,7,6,3)(4,5)\},$$

and we have to find a cycle σ of order 7 such that $\langle\sigma\rangle H = H\langle\sigma\rangle$. Without loss of generality we assume that $H \leq G$.

Now we are led to prove that for any element $\rho \in G$ of order 3, there exists a permutation $\sigma \in G$ of order 7, such that ρ transforms σ into its square, this is, $\rho^{-1}\sigma\rho = \sigma^2$. Then, we may assume without loss of generality that σ is of the form $(1,2,...)$ and $\rho = (2,3,4)(5,6,7)$. We will obtain just three permutations satisfying these conditions and just two of them will be permutable with H and we will conclude that there are just two subgroups of order 168 which contain H. The latter will let us finish our argument.

Let $\rho \in G$ be a permutation of order 3, as for any element $a \in G$ we have that $\rho^{-1}a^k\rho = (\rho^{-1}a\rho)^k$, then conjugation by ρ maps every Sylow 7-subgroup to either itself or to another 7-Sylow. In addition, as conjugation by ρ applied three times is the identity, the orbits of conjugation by ρ of Sylow 7-subgroups consist of either 1 or 3 Sylow 7-subgroups. G has 8 Sylow 7-subgroups and as $8 \neq 0 \pmod 3$ there must be a Sylow 7-subgroup K whose orbit under conjugation by ρ is itself. Again, as conjugation by ρ applied three times is the identity, the automorphism induced by conjugation over K must be the exponentiation by a cubic root of the unity in $\mathbb{Z}_7^*$. These roots are 1, 2 and 4, but the automorphism cannot be the identity by lemma 3.16. Then ρ transforms an element $\sigma \in K$ into σ^2 or σ^4. In the second case, note that ρ^2 transforms σ into σ^2. Assume for a while that ρ and ρ^2 are conjugate in G (we will prove it later), and let τ be the element of G such that $\rho^2 = \tau^{-1}\rho\tau$. Then

$$\rho^{-2}\sigma\rho^2 = \sigma^2 \iff \tau^{-1}\rho^{-1}\tau\sigma\tau^{-1}\rho\tau = \sigma^2 \iff \rho^{-1}\tau\sigma\tau^{-1}\rho = \tau\sigma^2\tau^{-1} = (\tau\sigma\tau^{-1})^2$$

and ρ transforms $\tau\sigma\tau^{-1}$, which is an element of order 7, into its square.

Every subgroup of order 3 in G is a Sylow 3-subgroup and therefore they are all conjugate in G. Hence to prove that any element of G of order 3 is conjugate in G to its square

it suffices to prove, without loss of generality, that $\rho := (2,3,4)(5,6,7)$ is conjugate to its square. The permutation $\tau := (3,4)(5,7) = (2,7,6,3)(4,5) \cdot \rho^{-1} \cdot ((2,7,6,3)(4,5))^2 \in H$ satisfies that $\rho^2 = \tau^{-1}\rho\tau$.

Let's compute now the cycles $(1,2,a,b,c,d,e)$ of order 7 that are transformed by $\rho := (2,3,4)(5,6,7)$ into its square. The equation that must be satisfied is

$$\rho^{-1}\sigma\rho = \sigma^2 \iff (5,7,6)(2,4,3) \cdot (1,2,a,b,c,d,e) \cdot (2,3,4)(5,6,7) = (1,a,c,e,2,b,d).$$

Evaluating at 1: $\rho^{-1}\sigma\rho(1) = 3$ and $\sigma^2(1) = a$, so $a = 3$. Now in a: $\rho^{-1}\sigma\rho(a) = \rho^{-1}\sigma\rho(3) = 4$ and $\sigma^2(a) = c$, so $c = 4$. And evaluating at the symbol $\rho(e)$ we have $\rho^{-1}\sigma\rho\,(\rho(e)) = \sigma\rho(e) = 1$ and $\sigma^2(d) = 1$, so $\rho(e) = d$ and consequently $\rho(d) = b$ and $\rho(b) = e$. Now for $e = 5,6,7$ we obtain three possible permutations, namely

$$(1235476), \quad (1236457) \quad \text{and} \quad (1237465).$$

It appears on trial that the group generated by the first one and H has not order 168, whereas the generated by any of the two others and H have order 168. There are therefore just two groups of order 168 that contain H.

Now in $\mathcal{S}_7$, a subgroup G of order 168 must be one among 30 conjugate subgroups. Indeed, $N_{\mathcal{S}_7}(G)$ must be G, $\mathcal{A}_7$ or $\mathcal{S}_7$ because they are the only groups whose order is a multiple of the order of G (we have already proved that the order of a group whose order is a multiple of 7 must be $7, 14, 21, 42, 168, 7!/2$ or $7!$). However, $\mathcal{A}_7$ and $\mathcal{S}_7$ contain more Sylow 7-subgroups than G and as in each group, every pair of Sylow 7-subgroups are conjugate, $N_{\mathcal{S}_7}(G)$ cannot contain $\mathcal{A}_7$. So $N_{\mathcal{S}_7}(G) = G$ and G must be one among $[\mathcal{S}_7 : N_{\mathcal{S}_7}(G)] = 7!/168 = 30$ conjugate subgroups. These all are contained in $\mathcal{A}_7$. Therefore they form two sets in that group, each of them containing 15 conjugate subgroups. Each of these contains exactly 7 conjugate subgroups of the type

$$H := \{(2,3,4)(5,6,7), (2,7,6,3)(4,5)\},$$

they are the subgroups whose permutations fix a given symbol. Let's prove that $N_{\mathcal{A}_7}(H) = H$ so $\mathcal{A}_7$ will contain a conjugate class of $(7 \cdot 6 \cdot 5 \cdot 4 \cdot 3)/24 = 105$ subgroups conjugate to H. As H fixes the symbol 1 and it is transitive in the remaining 6 symbols, the normalizer cannot contain permutations that displace the symbol 1. This reduces the problem to compute the normalizer respect to $\mathcal{A}_6$ acting in the symbols $2, \ldots, 7$. The index $[\mathcal{A}_6 : H] = 15$ and as $\mathcal{A}_6$ is simple the normalizer cannot be $\mathcal{A}_6$. The index respect to the normalizer cannot be 3 nor 5 because $\mathcal{A}_n$ does not have subgroups of index m for $1 < m < n$ for all $n \geq 5$. The latter is a well know property of $\mathcal{A}_n$, for a proof see [9] Cor. VI.1.4.

As each of these 105 conjugate subgroups will enter in two and only two subgroups of $\mathcal{A}_7$ with order 168, there are $105 \cdot 2/7 = 30$ subgroups of order 168, and in $\mathcal{S}_7$ those are all

conjugate. Finally, the subgroups of order 168 form a single conjugate class in $\mathcal{S}_7$. They are defined by

$$\{(1,2,3,6,4,5,7),(2,3,4)(5,6,7),(2,7,6,3)(4,5)\}.$$

□

To sum up, $\mathcal{S}_7$ has the following transitive subgroups up to conjugacy; we will show the diagram of inclusions of these subgroups:

- The full symmetric group $\mathcal{S}_7$.
- The alternating group $\mathcal{A}_7$.
- The group of order 42. It is generated by a cycle σ of length 7 and a cycle τ of length 6. In the literature, it is called the Frobenius group of order 42 or $\mathbb{F}_{42}$. Note that as $\mathbb{F}_{42}$ has a cycle of length 6 it is not contained in $\mathcal{A}_7$.
- The group of order 21, which is a subgroup of $\mathbb{F}_{42}$. This subgroup is usually called $\mathbb{F}_{21}$. Note it is contained in the group G of order 168 because in the previous proof we saw that the normalizer of a 7-cycle in G has order 21.
- The group of order 14. Let $\sigma := (1,2,3,4,5,6,7)$ and $\tau := (2,4,3,7,5,6)$ be defined as the generators of one of the subgroups of $\mathcal{S}_7$ isomorphic to $\mathbb{F}_{42}$ as we did in the previous proof. Then the generators of this group of order 14 are σ and τ^3. A straightforward computation gives us that $\tau^3\sigma\tau^3\sigma$ is the identity and therefore this group is isomorphic to the dihedral group D_7. As τ^3 is the product of three transpositions, this group is not contained in $\mathcal{A}_7$.
- The cyclic group $\mathbb{Z}_7$. Every transitive subgroup of $\mathcal{S}_7$ contains a subgroup isomorphic to $\mathbb{Z}_7$.
- The group of order 168. We proved that it is contained in $\mathcal{A}_7$. The general linear group $GL(3,\mathbb{F}_2)$ of invertible matrices of dimension 3 with entries in $\mathbb{F}_2$ under multiplication, is isomorphic to the transitive subgroup of $\mathcal{S}_7$ of order 168. Indeed, each element induces a permutation over the three dimensional, non-zero vectors in $\mathbb{F}_2$ by multiplication. The following element, which is in $GL(3,\mathbb{F}_2)$,

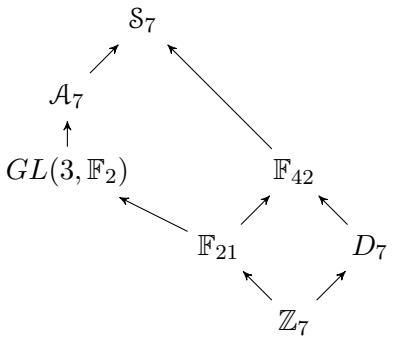
$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

has order 7, hence by lemma 3.6 the group is transitive. This can be checked in the following way. If we denote the vector $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ with the value $a2^2 + b2^1 + c2^0$ we have

that the sequence $\{A^i \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\}_{i=0}^{6} = \{1, 6, 4, 5, 3, 7, 2\}$ iterates over the 7 possible values. There are less than 2^9 invertible matrices in $GL(3, \mathbb{F}_2)$ and therefore, as $2^9 < 7!/2$, the group does not contain $\mathcal{A}_7$. If there is an element of order 4 in $GL(3, \mathbb{F}_2)$ then its order cannot divide 42 and therefore the group must be isomorphic to the transitive group of degree 7 and order 168. The following element of $GL(3, 2)$ has order 4:

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

These groups fit together into the diagram:



3.2 The Galois Group of the irreducible polynomials of degree 7

The Galois group of an irreducible polynomial of degree 7 is a transitive subgroup of $\mathcal{S}_7$. Once we have proved that there are just 7 candidates up to conjugacy to be Gal_f for an irreducible polynomial of degree 7, we will develop the theory explained in the previous section to successfully obtain a characterization of the Galois groups of irreducible polynomials of degree 7. We will use theorem 2.9 and corollary 2.19 with a convenient resolvent. Finally we will provide a computer program that computes the Galois group of irreducible polynomials of degree 7 using this characterization and we will explain the implementation details.

3.2.1 The resolvent P_{35} and its separability

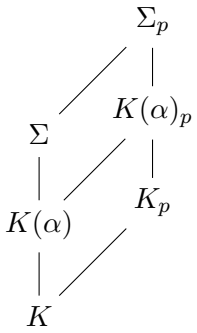
Let $f \in \mathbb{Q}[\mathtt{x}]$ be an irreducible polynomial of degree 7 and let $\alpha_1, \alpha_2, \ldots, \alpha_7$ be its roots in $\mathbb{C}$. Let $F(\mathtt{x}_1, \ldots, \mathtt{x}_n) = \mathtt{x}_1 + \mathtt{x}_2 + \mathtt{x}_3$, we define the linear resolvent P_{35} as the resolvent associated to F. We call it linear because F is a linear polynomial. Let $H := \mathrm{Stab}_{\mathcal{S}_7}(F)$. Recall that the definition of this resolvents is

$$P_{35} := R_F = \prod_{\sigma \in \mathcal{S}_7/H} (\mathtt{y} - (\alpha_1 + \alpha_2 + \alpha_3)^\sigma) \in \mathbb{Q}[\mathtt{y}]$$

In order to use corollary 2.19 to determine the Galois group of f, we need to ensure that P_{35} is always separable. The separability of P_{35} will be derived from the following proposition.

Proposition 3.19. *Let K be a field of zero characteristic and let $f \in K[x]$ be an irreducible polynomial of prime degree p. Let $\sigma \in Gal_f$ be a p-cycle (that exists by 3.6). Let α be a root of f in a splitting field Σ of f over K and let $\alpha_i := \sigma^{i-1}(\alpha)$, $1 \leq i \leq p$ be the roots of f. Let $b_1, b_2, \ldots, b_p \in K$ such that $b_1\alpha_1 + \cdots + b_p\alpha_p \in K$ and such that $\sum_{i=1}^{p} b_i \neq 0$. Then some p^{th} root of the unity is a root of the polynomial $h(\mathtt{x}) = b_1 + b_2\mathtt{x} + \cdots + b_p\mathtt{x}^{p-1}$.*

Proof. Let K_p be the field K extended with a p^{th} root of unity distinct to 1. Analogously, let $K(\alpha)_p$ and Σ_p be the fields $K(\alpha)$ and Σ extended with the same p^{th} root of unity. We have then the following diagram:



Let $\varphi : K(\alpha) \to \Sigma$ defined as

$$\varphi = b_1\mathrm{id} + b_2\sigma + b_3\sigma^2 + \cdots + b_p\sigma^{p-1} \in \mathrm{Hom}_K(K(\alpha), \Sigma)$$

For every $a \in K$ we have $\varphi(a) = (\sum_{i=1}^{p} b_i)\, a \in K$ and by hypothesis $\sum_{i=1}^{p} b_i \neq 0$, so $\varphi|_K : K \to K$ is bijective. On the other hand $\varphi(\alpha) = b_1\alpha_1 + \cdots + b_p\alpha_p \in K$ by hypothesis. Hence there exists $a \in K$ such that $\varphi(\alpha) = \varphi(a)$. Hence $\ker(\varphi) \neq 0$ because $\beta := \alpha - a \in \ker(\varphi)$ and $\beta \neq 0$.

Note that $p \mid [\Sigma_p : K_p]$ and σ lifts to an automorphism $\bar{\sigma} \in \mathrm{Aut}(\Sigma_p : K_p)$. Let $E := \mathrm{Fix}(\langle\bar{\sigma}\rangle)$ and let $\psi : \Sigma_p \to \Sigma_p$ be:

$$\psi := b_1\mathrm{id} + b_2\bar{\sigma} + b_3\bar{\sigma}^2 + \cdots + b_p\bar{\sigma}^{p-1} \in \mathrm{Hom}_E(\Sigma_p, \Sigma_p)$$

We have that $\psi(\beta) = 0$, so $\ker(\psi) \neq 0$. Now, as the extension $\Sigma_p|E$ is cyclic of degree p and E contains a p^{th} root of unity distinct to 1, there exists $c \in E$, and $\gamma \in \Sigma_p$ such

that $\Sigma_p = E(\gamma)$ and $\gamma^p = c$ (see [10] Thm. VII.1.10). Let ω be a p^{th} root of unity, a basis of Σ_p as a vector space over E is $\mathcal{B} := \{1, \gamma, \omega\gamma, \ldots, \omega^{p-1}\gamma\}$. As $\bar{\sigma}^k(\gamma) = \omega^k\gamma$, we have $\psi(\gamma^k) = \gamma^k(b_1 + \omega^k b_2 + \omega^{2k} b_3 + \cdots + \omega^{(p-1)k} b_p) = \gamma^k h(\omega^k)$. That is, the matrix with respect to $\mathcal{B}$ of the linear map ψ is:

$$\begin{pmatrix} h(1) & 0 & \ldots & 0 \\ 0 & h(\omega) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h(\omega^{p-1}) \end{pmatrix}$$

As we proved that $\ker(\psi) \neq 0$ there exists k such that $h(\omega^k) = 0$.

□

Corollary 3.20. *Let p be a prime and let f be an irreducible polynomial of degree p with coefficients in a field K of characteristic zero and such that the polynomial $\sum_{i=0}^{p-1} \mathtt{x}^i$ is irreducible in $K[\mathtt{x}]$. Consider the linear polynomial $F(\mathtt{x}_1, \ldots, \mathtt{x}_p) = \sum_{i=1}^{p} a_i \mathtt{x}_i$. Then the resolvent R_F is separable.*

Proof. Note that if $a_1 = a_2 = \cdots = a_p$, then the resolvent has degree 1 and it is trivially separable.

Let $\alpha_1, \alpha_2, \ldots, \alpha_p$ be the roots of f and suppose R_F is not separable. Then there exists $\sigma \in \mathcal{S}_p \backslash \mathrm{Stab}_{\mathcal{S}_p}(F)$ such that $\sum_{i=1}^{p} a_i\alpha_i = \sum_{i=1}^{p} a_i\alpha_{\sigma(i)}$. Thus if we define $b_i := a_i - a_{\sigma^{-1}(i)} + 1$ for $1 \leq i \leq p$ we have that

$$\sum_{i=1}^{p} b_i\alpha_i = \sum_{i=1}^{p} a_i\alpha_i - \sum_{i=1}^{p} a_i\alpha_{\sigma(i)} + \sum_{i=1}^{p} \alpha_i = \sum_{i=1}^{p} \alpha_i \in K.$$

Now by the previous proposition we have that $\sum_{i=0}^{p-1} b_{i+1}\mathtt{x}^i$ and $\sum_{i=0}^{p-1} \mathtt{x}^i$ share a root and as the latter polynomial is irreducible then $\sum_{i=0}^{p-1} b_{i+1}\mathtt{x}^i = c\sum_{i=0}^{p-1} \mathtt{x}^i$ for $c \in K$. Hence, for all $i \in \{1, \ldots, p\}$ we have that

$$c - 1 = a_i - a_{\sigma^{-1}(i)} = a_{\sigma(i)} - a_i = a_{\sigma^2(i)} - a_{\sigma(i)} = \cdots = a_{\sigma^{-1}(i)} - a_{\sigma^{-2}(i)}$$

Adding all these expressions together but the first one, we obtain $n(c-1) = 0$ for $n := \mathrm{ord}(\sigma)$. Hence $c = 1$ and therefore $b_i = 1$ for $1 \leq i \leq p$. Finally, we obtain that $a_i = a_j$ for all $i, j \in \{1, \ldots, p\}$, but this is a contradiction because we assumed that the resolvent is not separable and therefore not all the a_i can be equal. □

Remark 3.21. Corollary 3.20 proves that P_{35} is separable.

3.2.2 The orbits of the 3-sets

The information of Gal_f we obtain from corollary 2.19 with P_{35} is based on the orbit lengths of $F(\mathtt{x}_1,\ldots,\mathtt{x}_7)=\mathtt{x}_1+\mathtt{x}_2+\mathtt{x}_3$ under the natural action of the transitive subgroups of $\mathcal{S}_7$. They are the same as the orbit lengths of the sets of three elements in $\{1,2,\ldots,7\}$, also called 3-sets. So now we need to compute the orbit length partition of the 3-sets under each transitive subgroup G of $\mathcal{S}_7$.

It is trivial that the action of $\mathcal{S}_7$ over the 3-sets has just one orbit of size 35, this is $|\mathrm{Stab}_{\mathcal{S}_7}(\{1,2,3\})|=7!/35$. As $(1,2)\in\mathrm{Stab}_{\mathcal{S}_7}(\{1,2,3\})$ and $(1,2)$ is an odd permutation, then $\mathrm{Stab}_{\mathcal{A}_7}(\{1,2,3\})=\mathrm{Stab}_{\mathcal{S}_7}(\{1,2,3\})\cap\mathcal{A}_7$ has order $7!/(35\cdot 2)$ and there is an orbit of length $\frac{7!/2}{7!/(35\cdot 2)}=35$. Therefore there is only one orbit.

It is evident that for $i,j,k\in\{1,2,\ldots,7\}$ pairwise distinct, $|\mathrm{Stab}_{\mathbb{Z}_7}(\{i,j,k\})|=1$ and the length of any orbit under $\mathbb{Z}_7$ is $|\mathbb{Z}_7|/|\mathrm{Stab}_{\mathbb{Z}_7}(\{i,j,k\})|=7$.

An easy but important remark is that if $H\leq G$ then an orbit of H is contained in an orbit of G. As $\mathbb{Z}_7$ is contained in every transitive subgroup of $\mathcal{S}_7$, then the size of every orbit is a multiple of 7.

In order to compute the orbit sizes under the action of $GL(3,\mathbb{F}_2)$ we can represent, as we did previously, any symbol from 1 to 7 as a non zero vector in $\mathbb{F}_2^3$. The 3-sets such that the three corresponding vectors are linearly independent form an orbit. Indeed, if $v_1,v_2,v_3\in\mathbb{F}_2^3$ are linearly independent then the matrix whose columns are v_1,v_2 and v_3 can be viewed as an element of $GL(3,\mathbb{F}_2)$. The orbit of that matrix under the natural action over $GL(3,\mathbb{F}_2)$ is formed by all matrices whose columns are linearly independent vectors in $\mathbb{F}_2^3$. There are $|GL(3,\mathbb{F}_2)|/3!=168/6=28$ sets of three linearly independent vectors, because 3! matrices have the same vectors as their columns but in different order. In conclusion, there is an orbit of size 28 and as the orbit sizes must be a multiple of 7, then there is just one more orbit of size 7.

For $\mathbb{F}_{42}$, let's represent it as $AGL(1,\mathbb{F}_7):=\langle(1,2,3,4,5,6,7),(3,2,6,4,5,1)\rangle$, the general affine group over $\mathbb{F}_7$ generated by the operation σ that transforms the element $i\in\mathbb{F}_7$ into $i+1$ and the operation τ that transforms $i\in\mathbb{F}_7$ into $3i$. It is straightforward to check that both groups are isomorphic. Let $i,j,k\in\{1,2,\ldots,7\}$ be pairwise distinct. The copy of $\mathbb{Z}_7\leq\mathbb{F}_{42}$ is generated by σ. Let $A\subset\{1,2,\ldots,7\}$ and let $G\leq\mathcal{S}_7$, we denote the orbit of A under the action of G by $\mathfrak{O}_G(A)$. For any two elements if $a,b\in\mathfrak{O}_{\mathbb{Z}_7}(\{i,j,k\})$ then $\mathfrak{O}_{\mathbb{Z}_7}(\tau\cdot a)=\mathfrak{O}_{\mathbb{Z}_7}(\tau\cdot b)$. Indeed, let $\mathbb{1}=(1,1,1)^t\in\mathbb{F}_7^3$ and let $a,b\in\mathbb{F}_7^3$. a and b are in the same orbit under $\mathbb{Z}_7$ if and only if there is $k\in\mathbb{F}_7$ such that $b=a+k\mathbb{1}$. Now the equality $3(a+k\mathbb{1})=3a+3k\mathbb{1}$ implies that $3a$ and $3(a+k\mathbb{1})$ are in the same orbit under $\mathbb{Z}_7$.

Then applying τ to $\{1,2,3\}$ we obtain

$$\{1,2,3\} \mapsto \{3,6,2\} \mapsto \{2,4,6\} \mapsto \{6,5,4\} \in \mathfrak{O}_{\mathbb{Z}_7}(\{1,2,3\})$$

and as $\{3,6,2\} \notin \mathfrak{O}_{\mathbb{Z}_7}(\{1,2,3\})$ then $|\mathfrak{O}_{\mathbb{F}_{42}}(\{1,2,3\})| = 21$. On the other hand

$$\{1,2,4\} \mapsto \{3,6,5\} \mapsto \{2,4,1\} \in \mathfrak{O}_{\mathbb{Z}_7}(\{1,2,4\})$$

then there is just one more orbit and $|\mathfrak{O}_{\mathbb{F}_{42}}(\{1,2,4\})| = 14$ because $\{3,6,5\} \notin \mathfrak{O}_{\mathbb{Z}_7}(\{1,2,4\})$.

For $\mathbb{F}_{21}$ we have that as $\mathbb{F}_{21} \leq \mathbb{F}_{42}$ and $\mathbb{F}_{21} \leq GL(3,\mathbb{F}_2)$ then the orbit length partition must be either $\{7,14,14\}$ or $\{7,7,21\}$. Note that we are expressing the partition using multisets. Using the previous representation of $\mathbb{F}_{42}$ we can represent $\mathbb{F}_{21}$ as $\langle \sigma, \tau^2 \rangle$. Now $\tau^3 = (3,4)(2,5)(6,1) \in \mathrm{Stab}_{\mathbb{F}_{42}}(\{3,4,7\})$ but $\tau^3 \notin \mathcal{A}_7$ so we have that $|\mathrm{Stab}_{\mathbb{F}_{21}}(\{3,4,7\})| = |\mathrm{Stab}_{\mathbb{F}_{42} \cap \mathcal{A}_7}(\{3,4,7\})| = |\mathrm{Stab}_{\mathbb{F}_{42}}(\{3,4,7\})|/2$. Then

$$|\mathfrak{O}_{\mathbb{F}_{42}}(\{3,4,7\})| = 42/|\mathrm{Stab}_{\mathbb{F}_{42}}(\{3,4,7\})| = 21/|\mathrm{Stab}_{\mathbb{F}_{21}}(\{3,4,7\})| = |\mathfrak{O}_{\mathbb{F}_{21}}(\{3,4,7\})|.$$

In addition, $|\mathfrak{O}_{\mathbb{F}_{42}}(\{3,4,7\})| = 21$ because we saw that $\{3,6,2\}$ is in the orbit of $\mathbb{F}_{42}$ that has order 21 and $\sigma \cdot \{2,3,6\} = \{3,4,7\}$. Hence the orbit length partition of the 3-sets under the action of $\mathbb{F}_{21}$ is $\{7,7,21\}$.

Now for $D_7 \cong \langle \sigma, \tau^3 \rangle$ and $\mathbb{Z}_7 \cong \langle \sigma \rangle \leq D_7$ we have

$$\tau^3 \cdot \{1,2,3\} = \{6,5,4\} \in \mathfrak{O}_{\mathbb{Z}_7}(\{1,2,3\});$$

$$\tau^3 \cdot \{1,2,5\} = \{6,5,2\} \in \mathfrak{O}_{\mathbb{Z}_7}(\{1,2,5\});$$

$$\tau^3 \cdot \{1,3,5\} = \{6,4,2\} \in \mathfrak{O}_{\mathbb{Z}_7}(\{1,3,5\});$$

$$\tau^3 \cdot \{1,2,4\} = \{6,5,3\} \notin \mathfrak{O}_{\mathbb{Z}_7}(\{1,2,4\});$$

Hence the orbit length partition is $\{7,7,7,14\}$.

3.2.3 Determining the Galois group

The orbit length partition of the 35 3-sets is different for every pair of transitive subgroups of $\mathcal{S}_7$ but for $\mathcal{A}_7$ and $\mathcal{S}_7$. Given our irreducible polynomial of degree 7 f, if we compute its associated resolvent P_{35} and we factorize it, then we can decide which is the Galois group of f using corollary 2.19 but for $\mathcal{A}_7$ and $\mathcal{S}_7$. To decide if Gal_f equals $\mathcal{A}_7$ or $\mathcal{S}_7$ it suffices to check if $\Delta(f)$ is a square or not in $\mathbb{Q}$, according to theorem 2.9. The following table summarizes the characterization we have obtained. Again, the orbit length partition is expressed as a multiset.

Degrees of irreducible factors of P_{35}	Is $\Delta(f)$ a square in $\mathbb{Q}$?	Gal_f
$\{35\}$	NO	$\mathcal{S}_7$
$\{35\}$	YES	$\mathcal{A}_7$
$\{7, 28\}$	-	$GL(3, \mathbb{F}_2)$
$\{14, 21\}$	-	$\mathbb{F}_{42}$
$\{7, 7, 21\}$	-	$\mathbb{F}_{21}$
$\{7, 7, 7, 14\}$	-	D_7
$\{7, 7, 7, 7, 7\}$	-	$\mathbb{Z}_7$

3.3 An algorithm

The algorithm is mainly based on the previous table. However, it is not straightforward to compute the resolvent P_{35} in an efficient way and we will need some extra ideas. First of all, we restrict ourselves to polynomials in $\mathbb{Z}[\mathtt{x}]$. We can do so because of proposition 2.11. Note that we do not know the roots of the polynomial f whose Galois group we want to compute. A naive approach would consist of trying to symbolically compute the product

$$\prod_{\sigma \in \mathcal{S}_7/H} (\mathtt{y} - (\mathtt{x}_1 + \mathtt{x}_2 + \mathtt{x}_3)^\sigma) \in \mathbb{Z}[\mathtt{y}, \mathtt{x}_1, \ldots, \mathtt{x}_7]$$

and then, as it is symmetric in the variables $\mathtt{x}_1, \ldots, \mathtt{x}_7$, we would write it as a polynomial in $\mathbb{Z}[\mathtt{y}, \mathtt{s}_1, \ldots, \mathtt{s}_7]$, where $\mathtt{s}_1, \ldots, \mathtt{s}_7$ are the elementary symmetric polynomials. However, just the computation of the product needs more than 4^{35} operations. This makes it unwieldy.

The resolvent P_{35} was very convenient in the characterization because for each transitive subgroup of $\mathcal{S}_7$ the orbits of the 3-sets were different. But that is not the reason why we have chosen this resolvent. The reason is that it is a linear resolvent, and then, as we will see now, we can compute it in a more efficient way. As long as it is possible, it is better to use linear resolvents, although we had to use more than one, instead of a non linear resolvent that could possibly have very different orbits for each of the distinct transitive subgroups of $\mathcal{S}_7$.

The method to efficiently compute a linear resolvent will use three operations. The first one consists of, given two polynomials $g, h \in \mathbb{Q}[\mathtt{x}]$ with roots $\beta_1, \beta_2, \ldots, \beta_r$ and $\gamma_1, \gamma_2, \ldots, \gamma_s$ respectively, computing a polynomial whose roots are the sum of every pair formed by a root of g and a root of h. This can be computed with a resultant. Let a and b be the leading coefficients of g and h respectively. We recall that the resultant of two polynomials

as g and h with respect to the indeterminate $\mathtt{x}$ is defined as

$$\mathrm{res}_{\mathtt{x}}(g,h) := a^s b^r \prod_{i=1}^{r}\prod_{j=1}^{s}(\beta_i - \gamma_j).$$

Then the polynomial we want to compute is

$$SZ(g,h) := \prod_{i=1}^{r}\prod_{j=1}^{s}(\mathtt{x} - (\beta_i + \gamma_j)) = \mathrm{res}_{\mathtt{y}}(g(\mathtt{y}), h(\mathtt{x}-\mathtt{y}))$$

where we have used the notation $SZ(g,h)$ for the polynomial whose zeros are the sum of the zeros of g and h.

The second operation we will need to perform is, given a $c \in \mathbb{Q}\backslash\{0\}$ and a polynomial $g \in \mathbb{Q}[\mathtt{x}]$ with roots $\beta_1, \beta_2, \ldots, \beta_r$, the computation of a polynomial whose zeros are $c\beta_1, c\beta_2, \ldots, c\beta_r$. We can use, for example,

$$MZ(c, g(x)) := c^n g(\mathtt{x}/c).$$

The factor c^n is not necessary but it is convenient if we want to perform all these operations over monic polynomials and we want the result to be a monic polynomial.

Now the third operation we need. Let $g \in \mathbb{Q}[\mathtt{x}]$ monic and let k be a positive integer. We want to compute g from g^k and k, that is, a sort of polynomial root of index k assuming it exists. This can be computed following this pseudocode

```
# Input:  k ∈ ℤ⁺ and a monic polynomial h ∈ ℚ[x], deg(h) > 0 such that
# h = g^k for some monic polynomial g ∈ ℚ[x].
# Output:  g(x)
    if k is 1 then return h. stop
    t(x) <-- h/gcd(h, h') # h' the formal derivative.  t is the separable
    # polynomial whose zeros are the distinct zeros of h
    g(x) <-- t(x) # This will be the solution after the computations
    s(x) <-- h(x) # s(x) will be the part of h we have not processed yet
    while deg(r) < deg(h)/k do
        s(x) <-- s(x)/t(x)
        t(x) <-- gcd(s,t) # In the iteration i the zeros of t(x) are those of
        # h such that they have multiplicity > ki
        g(x) <-- t(x)g(x)
    end while

    return g(x)
```

We will use in the following $PR(k, h(x))$ to denote the polynomial such that $PR(k, h(x))^k = h(x)$. With these tools we can compute any linear resolvent.

Let $M := \{a_1, a_2, \ldots, a_r\}$ be a multiset of elements in $\mathbb{Q}$ and let $f \in \mathbb{Q}[\mathtt{x}]$ be a polynomial of degree n, with $r \leq n$. In the following, it will be useful to use the notation $R(M, f)$ for the universal resolvent of f associated to the linear polynomial $F = \sum_{i=1}^{r} a_i \mathtt{x}_i$.

Theorem 3.22. *Let $M := \{a_1, a_2, \ldots, a_r\}$ be a multiset of elements in $\mathbb{Q}$. Let $f \in \mathbb{Q}[\mathtt{x}]$ be a separable polynomial of degree n and with roots $\alpha_1, \ldots, \alpha_n$ in $\mathbb{C}$. The linear resolvent $R(M, f)$ can be constructed using only the operations SZ, MZ, PR.*

Proof. We proceed by induction on r, the length of M. If $r = 1$ then $R(M, f) = MZ(a_1, f)$.

Now if $r > 1$, let $b_1, b_2, \ldots, b_k$ be the distinct values appearing in $M' := \{a_1, \ldots, a_{r-1}\}$ and let m_i be the multiplicity of b_i in M' for $i = 1, \ldots, k$. By the inductive hypothesis we can compute

$$g := SZ(R(M', f), MZ(a_r, f)).$$

For each zero β of $R(M', f)$, the polynomial g has precisely the zeros $\beta + a_r\alpha_1$, $\beta + a_r\alpha_2$, $\ldots$, $\beta + a_r\alpha_n$. Let M_i be the multiset M' without an element b_i and with an extra $b_i + a_r$, for all $i \in \{1, 2, \ldots, k\}$. Then, among the n values $\beta + a_r\alpha_1$, $\beta + a_r\alpha_2, \ldots, \beta + a_r\alpha_n$ there are m_i roots of the resolvent $R(M_i, f)$ for all $i \in \{1, 2, \ldots, k\}$ and $n - r + 1$ roots of the resolvent $R(M, f)$. Because of the symmetry of g, it is the product of powers of the resolvents $R(M_i, f)$, $1 \leq i \leq k$ and $R(M, f)$. Particularly, counting all the roots that we obtain of each resolvent and dividing by the degree of the corresponding resolvent, we obtain that the multiplicity of the resolvents $R(M_i, f)$ must be $m_i \deg(R(M', f))/\deg(R(M_i, f))$ and the multiplicity of $R(M, f)$ must be $(n - r + 1)\deg(R(M', f))/\deg(R(M, f))$. Hence:

$$g = \left(\prod_{i=1}^{k} R(M_i, f)^{c_i} \right) R(M, f)^c$$

for $c_i := m_i \deg(R(M', f))/\deg(R(M_i, f))$ and $c := (n-r+1)\deg(R(M', f))/\deg(R(M, f))$. By hypothesis we can construct

$$h := \prod_{i=1}^{k} R(M_i, f)^{c_i}$$

hence finally $R(M, f) = PR(c, g/h)$.

□

The previous proof is in fact constructive and gives a recursive algorithm to compute any linear resolvent. In our particular case can compute

$$R_{\mathtt{x}_1+\mathtt{x}_2} = PR(2, SZ(f, f)/MZ(2, f))$$

and

$$R_{x_1+2x_2} = SZ(MZ(2,f),f)/MZ(3,f).$$

With those resolvents we can compute the resolvent $R_{x_1+x_2+x_3}$ as

$$R_{x_1+x_2+x_3} = PR(3, SZ(R_{x_1+x_2}, f)/R_{x_1+2x_2})$$

Putting all together we have written the following code in sage that computes the Galois group of any monic irreducible polynomial of degree 7.

```
from sage.symbolic.expression_conversions import polynomial

def polRoot (pol, index):
    if index == 1:
        return pol;
    else:
        (t, _ ) = pol.quo_rem(pol.gcd(pol.derivative()))
        r = t
        s = pol
        while r.degree() < pol.degree()/index:
            (s, _ ) = s.quo_rem(t^index)
            t = t.gcd(s)
            r = r*t
        return r

def galois7(a6, a5, a4, a3, a2, a1, a0):
    # Computes the Galois Group of the monic polynomial
    # f = x^7 + a6*x^6 + a5*x^5 + a4*x^4 + a3*x^3 + a2*x^2 + a1*x + a0,

    # Definitions of polynomial rings
    mr3.<x,y,z> = ZZ[]
    mry.<y> = ZZ[]

    f = x^7 + a6*x^6 + a5*x^5 + a4*x^4 + a3*x^3 + a2*x^2 + a1*x + a0

    if len(ZZ['x'](f).factor()) != 1:
        print "The polynomial must be irreducible"
        return

    aux = (y-x)^7 + a6*(y-x)^6 + a5*(y-x)^5 + a4*(y-x)^4 + a3*(y-x)^3 + \
        a2*(y-x)^2 + a1*(y-x) + a0
    aux2 = (z-y)^7 + a6*(z-y)^6 + a5*(z-y)^5 + a4*(z-y)^4 + a3*(z-y)^3 + \
        a2*(z-y)^2 + a1*(z-y) + a0

    # Polynomial whose zeros are the sum of each pair of zeros of f
    sz_ff = mry(f.resultant(aux, x))

    # Polynomial whose zeros are the double of the zeros of f
    mz_2f = (2^7)*((y/2)^7 + a6*(y/2)^6 + a5*(y/2)^5 + a4*(y/2)^4 +
        a3*(y/2)^3 + a2*(y/2)^2 + a1*(y/2) +  a0)

    # Linear resolvent R({1,1},f).  It is the square root of sz_ff/mz_2f
    sqrt_sz_ff = polRoot(sz_ff.quo_rem(mz_2f)[0], 2);

    # Polynomial whose zeros are the sum of each pair of zeros of f and
    # zeros of mz_2f
    sz_2f_f = mr3(mz_2f).resultant((z-y)^7 + a6*(z-y)^6 + a5*(z-y)^5 +
        a4*(z-y)^4 + a3*(z-y)^3 + a2*(z-y)^2 + a1*(z-y) + a0, mr3(y))
```

```
49
50      mz3f = (3^7)*((z/3)^7 + a6*(z/3)^6 + a5*(z/3)^5 + a4*(z/3)^4 +
51          a3*(z/3)^3 + a2*(z/3)^2 + a1*(z/3) + a0)
52
53      mrz.<z> = ZZ[]
54
55      # Linear resolvent R({2,1}, f)
56      lr21 = mrz(sz_2f_f.quo_rem(mz3f)[0]);
57
58      h = mrz(mr3(sqrt_sz_ff).resultant(aux2, mr3(y)));
59
60      sol = polRoot(h.quo_rem(lr21)[0], 3)
61
62      factors = sol.factor()
63      factorsNumber = len(factors)
64
65      if factorsNumber == int(5):
66          print "The galois Group is Z_7"
67      elif factorsNumber == int(4):
68          print "The galois Group is D_7"
69      elif factorsNumber == int(3):
70          print "The galois Group is F_21"
71      elif factorsNumber == int(2):
72          if (factors[0][0].degree() == int(7) or
73              factors[1][0].degree() == int(7)):
74              print "The galois Group is GL(3,2)"
75          else:
76              print "The galois Group is F_42"
77      else:
78          if Integer(f.discriminant(x)).is_square():
79              print "The galois Group is A_7"
80          else:
81              print "The galois Group is S_7"
```

3.4 Transitive subgroups of S_7 as Galois groups

We already know that the Galois group of an irreducible polynomial $f \in \mathbb{Q}[x]$ of degree 7 must be a transitive subgroup of $\mathcal{S}_7$ but we have not proved that every transitive subgroup of $\mathcal{S}_7$ is the Galois group of some such polynomial. Now, for each transitive group $G \leq \mathcal{S}_7$, we give an irreducible polynomial whose Galois group is G. We have used the previous program to check the irreducibility of the polynomials and to compute the factorization of P_{35} in irreducible factors over $\mathbb{Q}[x]$ and, if necessary, $\Delta(f)$.

i) The Galois group of $x^7 + x + 1$ is $\mathcal{S}_7$. The factorization of P_{35} is

$$x^{35} + 40x^{29} + 302x^{28} - 1614x^{23} + 2706x^{22} + 3828x^{21} - 5072x^{17} + 2778x^{16} - 18084x^{15} + 36250x^{14} - 5147x^{11} - 1354x^{10} - 21192x^9 - 26326x^8 - 7309x^7 - 1728x^5 - 1728x^4 + 720x^3 + 928x^2 - 64x - 128$$

and $\Delta(f) = -870199$ which is not a square in $\mathbb{Q}$.

ii) The Galois group of $x^7 + 7x^4 + 14x + 3$ is $\mathcal{A}_7$. The factorization of P_{35} is

$x^{35}+14x^{32}+413x^{29}+906x^{28}+13132x^{26}-3024x^{25}-161308x^{23}+245952x^{22}+34452x^{21}+3536330x^{20}+878325x^{19}+979650x^{18}-50662472x^{17}-14462154x^{16}+1139607x^{15}+291322076x^{14}-39053637x^{13}-26860869x^{12}-708606241x^{11}+356062812x^{10}-42630588x^{9}+606902716x^{8}-502461054x^{7}+165734856x^{6}-22994965x^{5}-16661736x^{4}+7516845x^{3}-1610140x^{2}+146013x+120159$

and

$$\Delta(f) = 4202539929 = 64827^2$$

iii) The Galois group of $x^7 - 7x^3 + 14x^2 - 7x + 1$ is $GL(3, \mathbb{F}_2)$. The factorization of P_{35} is

$(x^7 - 14x^4 + 7x^3 + 14x^2 - 56x - 32)(x^{28} + 14x^{25} + 49x^{24} - 154x^{23} - 28x^{22} + 922x^{21} - 2401x^{20} - 4116x^{19} + 1400x^{18} + 14210x^{17} - 120995x^{16} + 148120x^{15} - 94460x^{14} + 133770x^{13} - 612598x^{12} + 1813574x^{11} - 2805152x^{10} - 409682x^{9} - 379624x^{8} - 2173462x^{7} - 8323924x^{6} - 5589528x^{5} - 2982203x^{4} - 1499890x^{3} - 1323140x^{2} - 254184x + 61744)$

iv) The Galois group of $x^7 + 2$ is $\mathbb{F}_{42}$. The factorization of P_{35} is

$(x^{14} + 26x^7 + 512)(x^{21} + 578x^{14} - 228x^7 - 8)$

v) The Galois group of $x^7 - 14x^5 + 56x^3 - 56x + 22$ is $\mathbb{F}_{21}$. The factorization of P_{35} is

$(x^7 - 28x^5 + 224x^3 - 448x + 94)(x^7 - 28x^5 + 224x^3 - 448x + 192)(x^{21} - 84x^{19} + 2436x^{17} - 31136x^{15} + 6358x^{14} + 203840x^{13} - 84392x^{12} - 733824x^{11} + 420728x^{10} + 1480192x^{9} - 988064x^{8} - 1652036x^{7} + 1138368x^{6} + 986496x^{5} - 620928x^{4} - 284032x^{3} + 137984x^{2} + 27104x - 10648)$

vi) The Galois group of $x^7 + 7x^3 + 7x^2 + 7x - 1$ is D_7. The factorization of P_{35} is

$(x^7 - 7x^5 - 7x^4 + 7x^3 - 7x^2 + 7x - 3)(x^7 - 7x^5 + 21x^3 + 28x^2 + 35x + 25)(x^7 + 14x^5 + 7x^4 + 56x^3 + 84x^2 + 126x + 81)(x^{14} + 7x^{10} - 28x^9 + 63x^8 - 62x^7 + 784x^6 - 2156x^5 + 4361x^4 - 6587x^3 + 6748x^2 - 5383x + 2333)$

vii) The Galois group of $x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1$ is $\mathbb{Z}_7$. The factorization of P_{35} is

$(x^7 + 3x^6 - 21x^5 - 73x^4 - 23x^3 + 125x^2 + 138x + 41)(x^7 + 3x^6 - 21x^5 - 73x^4 + 6x^3 + 125x^2 - 7x - 17)(x^7 + 3x^6 - 21x^5 - 44x^4 + 122x^3 + 125x^2 - 210x + 41)(x^7 + 3x^6 - 21x^5 - 44x^4 + 151x^3 + 125x^2 - 413x + 157)(x^7 + 3x^6 - 21x^5 - 15x^4 + 64x^3 + 38x^2 - 36x - 17)$

References

[1] Abel, N-H. *Euvres Complètes*, ed. L. Sylow-S. Lie, Grondahl & Son, Christiana, 1881.

[2] Bright, Curtis *Computing the Galois Group of a Polynomial*, https://cs.uwaterloo.ca/~cbright/reports/computing-galois-group.pdf

[3] Burnside, W. *Theory of Groups of Finite Order*, Cambridge: Dover Publications, 1955

[4] Cangelmi, L. *Resolvents and Galois Groups*. Rend. Sem. Mat. Univ. Poi. Torino Voi. 53, 3 (1995) Number Theor. pp. 207 – 222

[5] Cayley, A. *On a New Auxiliary Equation in the Theory of Equations of the Fifth Order*, Philosophical Transactions of the Royal Society of London, CLI (1861), pp. 210 – 214.

[6] Cockle, J. *On the Resolution of Quintics* , Quarterly Journal of Pure and Applied Mathematics, 4 (1861), pp. 5 – 7.

[7] Cox, David A. *Galois Theory*. 2012, ed. John Wiley and Sons.

[8] Fernando, José F. and Gamboa, J. Manuel *Estructuras Algebraicas: Divisibilidad en Anillos Conmutativos* 1^{st} edition. Sanz y Torres. pp. 127 – 156

[9] Fernando, José F. and Gamboa, J. Manuel *Estructuras Algebraicas: Teoría Elemental de Grupos* 1^{st} edition. Sanz y Torres.

[10] Fernando, José F. and Gamboa, J. Manuel *Ecuaciones Algebraicas: Extensiones de Cuerpos y Teoría de Galois* 1^{st} edition. Sanz y Torres. pp.

[11] Fieker, Claus and Klüners, Jurgen *Computation of Galois Groups of Rational Polynomials*, 2014

[12] Galois, É. *Écrits et Mémoires Mathématiques d'Évariste Galois*, ed. R. Bourgne, J.P. Azra, Gauthier-Villars, Paris, 1962.

[13] Gauss, C. F. *Disquisitiones Arithmeticae*, Apud Gerh. Fleisher Iun. Lipsiae, 1801

[14] Geissler, Katarina and Kluners, Jurgen *Galois Group Computation for Rational Polynomials*, 2000

[15] Girstmair, K. *On the Computation of Resolvents and Galois Groups*, Manuscripta Mathematica 43 pp. 289-307 (1983)

[16] Harley, R. *On the Theory of Quintics*, Quarterly Journal of Pure and Applied Mathematics, 3 (1859), pp. 343 – 359.

[17] Hulpke, A. *Techniques for the Computation of Galois*, http://www.math.colostate.edu/~hulpke/paper/gov.pdf

[18] Hulpke, A. *Galois Groups Through Invariant Relations*, http://www.math.colostate.edu/~hulpke/paper/neugal.pdf

[19] Jones, John *Topics in Fields and Galois Theory*, http://hobbes.la.asu.edu/courses/site/544/Topics-Galois-Theory.pdf

[20] Klein, F. *Über die Auflösung Gewisser Gleichungen vom Siebenten und Achten Grade*, Math Ann. 15 (1879).

[21] Kronecker, L. *Ueber Gleichungen des* 7^{ten} *Grades*, Monatsberichte der Berlin Akademie, April 1858.

[22] Lagrange, J.L.. *Réflexions sur la Résolution Agebraique des Équations*, Nouveaux Mémoires de l'Acad. Royale des sciences et belles-lettres, avec l'histoire pour la même année, 1 (1770), pp. 134 – 215; 2 (1771), pp. 138 – 253 (*Euvres de Lagrange*, vol. 3, Gauthier-Villars (1869), pp. 203 – 421).

[23] McClintock, E. *On the Resolution of Quintic Equations*, Amer. Journal of Math. VI (1884), pp. 301 – 315.

[24] Ruffini, P. *Theoria generale delle equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto*, 1799

[25] Stevenhagen, P. and Lenstra Jr., H. W. *Chebotarev and his density theorem*, Math. Intelligencer 18, no. 2 (1996), pp. 26 – 37.

[26] Stewart, Ian *Galois Theory*, 3^{rd} edition, 2003. Chapman & Hall / CRC Mathematics

[27] Soicher, Leonard *The Computation of Galois Groups*, 1981

[28] Trinks, W. *Ein Beispiel enies Zahlkörpers mit der Galoisgruppen* $PSL(3,2)$ *über* $\mathbb{Q}$, manuscrito, Universität Karlsruhe, 1968.

[29] Tschirnhaus, E.W. *Methodus Anferendi Omnes Terminos intermedios ex data aequationes*, Acta Eruditorum, Leipzig (1683), pp. 204 – 207.

[30] Vandermonde, A. T. *Mémoires sur la résolution des équations*, Histoire de l'Acad. Royale des sciences, avec les mémoires des Math. & de Phys. pour la même année, (1771), pp. 365 – 416.

[31] Weber, H. *Lehrbuch der Algebra*, Chelsea Publishing Company, New York, (1864), 1961.