UNIVERSITAT DE BARCELONA

Treball final de màster

MÀSTER DE MATEMÀTICA AVANÇADA

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

The Inverse Problem of Galois Theory: The Rigidity Method

Autor: Josep Miquel Martínez Marín

Directora: Dr. Núria Vila
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 10 de setembre de 2019

Contents

Introduction

The development of Galois theory was a key turning point in the history of mathematics. It began the study of fields that are still active and solved one of the most important problems in mathematics at the time.

The Inverse Galois Problem asks whether given a finite group G and a field K, if it is possible to find a Galois extension L/K such that $G \cong \mathrm{Gal}(L/K)$. The answer to this problem depends, of course, on the properties of the group G and on the properties of the field K. For instance, the solution to this problem is positive only for cyclic groups when K is a finite field, whereas the solution is always positive when $K = \mathbb{C}(t)$. It remains an open problem to show whether all groups are Galois groups over $K = \mathbb{Q}$, although some partial solutions have been given. For example, in 1937 Scholz [Sch37] and Reichardt [Rei37] simultaneously but independently proved that p-groups can be realised as Galois groups over $\mathbb{Q}$ for any odd prime p. Taking this as a starting point, later on Šafarevič proved that all solvable groups are Galois groups over $\mathbb{Q}$ in [Š54].

This work will study one of the main methods developed to partially solve the problem, the Rigidity Method. These techniques first appeared in the work of Belyi [Bel79], Matzat [Mat84] and Thompson [Tho84c]. The Rigidity Method takes as starting point the solution in $\mathbb{C}(t)$. What we attempt is to bring down the solution to $\mathbb{Q}$, ideally achieving the following descent:

$$\begin{array}{c} \mathbb{C}(t) \\ | \\ \overline{\mathbb{Q}}(t) \\ | \\ \mathbb{Q}(t) \\ | \\ \mathbb{Q} \end{array}$$

In §1 we explain how the problem is solved over $\mathbb{C}(t)$ and how this solution is also valid with no restrictions at all in $\overline{\mathbb{Q}}(t)$, using a result by Grothendieck. In 1892, Hilbert showed that any Galois group over $K(t)$ is also a Galois group over K whenever K is a number field. This result is called Hilbert's irreducibility theorem, and was first proved in [Hil92]. The only descent remaining to make is from $\overline{\mathbb{Q}}(t)$ to $\mathbb{Q}(t)$. The Rigidity Method achieves precisely this descent, but this descent comes with a price: we have to ask for some restrictive conditions on the group. On the other hand, these conditions turn out to be satisfied by many simple groups, which, in a way, are the complete opposite to solvable groups, so this solution and the one given by Šafarevič somewhat complement each other.

We devote §2 to the introduction of one of the key concepts of this work, the concept of characters of finite groups. Characters are the map defined as the trace of an homomorphism of a finite group G into a general linear group over the complex numbers.

A connection between characters and Galois theory arises from the existence of an action of $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ on the set of characters of a finite group G whenever $(n, |G|) = 1$. It is precisely in the nature of this action that we find one of the conditions we will impose on G to apply the Rigidity Method: the rationality of conjugacy classes. This is explained in §3 along with the second condition: rigidity condition, which gives name to the method. We finish §3 by proving character-theoretic criterion for rigidity due to John Thompson.

In §4 we prove the main result of the work: the Basic Rigidity Theorem. We show that whenever these rationality and rigidity conditions are met in a group with trivial center, we are able to find a Galois extension $L/\mathbb{Q}(t)$ such that

$$G \cong \mathrm{Gal}(L/\mathbb{Q}(t)).$$

However, it is sometimes the case that the rationality condition is too strict for some groups. To solve this problem, we explain a generalization of the Basic Rigidity Theorem which gets rid of the rationality condition on a finite group G and finds an abelian extension $K/\mathbb{Q}$ of finite degree such that G occurs as Galois group of a Galois extension of $K(t)$.

Finally in §5 we see applications of the Basic Rigidity Theorem and some generalizations to some relevant groups. We apply the result to the symmetric and alternating groups, for which a Galois realization had already been done in [Hil92]. We also apply our findings to some of the projective special linear groups of dimension 2 over odd-characteristic fields. After the applications of the method to families of groups, we work with particular examples, which are the special linear group $\mathrm{SL}_2(\mathbb{F}_8)$, the Tits group ${}^2\mathrm{F}_4(2)'$ and the sporadic groups M_{11}, M_{22} and J_2.

The main reference of this work is [MM99], which constitutes an encyclopedic book on the topic. Moreover, a series of lectures given by J. P. Serre and written down by H. Darmon in [Ser92] were found particularly useful by the student as a complementary resource to Malle and Matzat's book.

Acknowledgements

I wish to thank my supervisor Núria Vila for her valuable help and her constructive suggestions during the planning and development of this work. It has been a great experience to work and learn under the supervision of someone with such vast knowledge and experience on the topic of this thesis.

§1 The Inverse Galois Problem over $\overline{\mathbb{Q}}(t)$

We begin by showing that the problem always has positive solution over $\overline{\mathbb{Q}}(t)$. With this goal in mind we begin by working on $\mathbb{C}(t)$ and finding that its solution here is always positive as well, and the descent to $\overline{\mathbb{Q}}(t)$ will not be restricting at all so the same result will be valid. We do not go into details during this section and rather explain the results more superficially.

1.1 Solving the problem over $\mathbb{C}(t)$

The Riemann sphere is a model of the extended complex plane. A point at infinity is added to $\mathbb{C}$ and what we get is in fact the projective line $\mathbb{P}_1(\mathbb{C})$. From $\mathbb{P}_1(\mathbb{C})$ we remove a set of points, $S = \{P_1, \ldots, P_s\}$. For any $P_0 \in \mathbb{P}_1(\mathbb{C}) \setminus S$, let $\{\gamma_1, \ldots, \gamma_s\}$ be a collection of homotopy classes of nonintersecting loops from P_0 counterclockwise around P_i.

We have that the fundamental group $\pi_1(\mathbb{P}_1(\mathbb{C}) \setminus S; P_0)$ can be presented as

$$\pi_1(\mathbb{P}_1(\mathbb{C}) \setminus S, P_0) = \langle \gamma_1, \ldots, \gamma_s \mid \gamma_1 \cdots \gamma_s = 1 \rangle \tag{1}$$

(see [ST80], §47).

The function field of $\mathbb{P}_1(\mathbb{C})$ is isomorphic to the field of rational functions $\mathbb{C}(t)$. The set $S \subset \mathbb{P}_1(\mathbb{C})$ is bijective to the subset of primes $\mathbb{S}$ of $\mathbb{C}[t]$ with valuation ideal having common zero at one of the points P_i.

Let $\hat{\pi}_1(\mathbb{P}_1(\mathbb{C}) \setminus S, P_0)$ be the profinite completion of the fundamental group $\pi_1(\mathbb{P}_1(\mathbb{C}) \setminus S, P_0)$. Let $\mathfrak{N}_{\mathbb{S}}$ be the set of all finite Galois extensions of $\mathbb{C}(t)$ unramified outside of $\mathbb{S}$. Then the maximal extension of $\mathbb{C}(t)$ unramified outside of $\mathbb{S}$ is exactly

$$\mathbb{C}(t)^{\mathbb{S}} = \bigcup_{N \in \mathfrak{N}_{\mathbb{S}}} N$$

and we have

$$\mathrm{Gal}(\mathbb{C}(t)^{\mathbb{S}}/\mathbb{C}(t)) = \varprojlim \mathrm{Gal}(N/\mathbb{C}(t))_{N \in \mathfrak{N}_{\mathbb{S}}}.$$

Now the key result here is the famous Riemann Existence Theorem. It involves elements of complex analysis, topology, algebraic geometry and number theory in its statement and multiple proofs. It is in fact in the *intersectional* nature of the result where its strength is.

Theorem 1.1 (Profinite Riemann Existence Theorem)**.** *There is an isomorphism*

$$\mathrm{Gal}(\mathbb{C}(t)^{\mathbb{S}}/\mathbb{C}(t)) \cong \hat{\pi}_1(\mathbb{P}_1(\mathbb{C}) \setminus S, P_0).$$

Proof. This result is Theorem 1.3 of Chapter I of [MM99]. Chapter 6 of [Ser92] also proves this result. □

Let G be any finite group, and consider a set of generators $g_1, \ldots, g_{s-1}$. For this particular s we can make the construction of $\mathbb{S}$ as before and consider the following homomorphism

$$\psi : \mathrm{Gal}(\mathbb{C}(t)^{\mathbb{S}}/\mathbb{C}(t)) \to G$$

mapping

$$\psi(\gamma_i) = \begin{cases} g_i & 1 \leq i \leq s-1 \\ g_{s-1}^{-1} \cdots g_1^{-1} & i = s \end{cases}$$

Observe that we have given a presentation of G in the same way as the presentation we gave for $\pi_1(\mathbb{P}_1(\mathbb{C}) \setminus S, P_0)$. The fixed field $N = (\mathbb{C}(t)^{\mathbb{S}})^{\ker \psi}$ is a Galois extension of $\mathbb{C}(t)$ and we have

$$\mathrm{Gal}(N/\mathbb{C}(t)) \cong \mathrm{Gal}(\mathbb{C}(t)^{\mathbb{S}}/\mathbb{C}(t))/\ker \psi \cong G.$$

This proves the following result.

Theorem 1.2. *Every finite group occurs as Galois group over* $\mathbb{C}(t)$.

In section 1.3 of Chapter I of [MM99] it is shown that in fact all finite groups occur as Galois groups over $\mathbb{R}(t)$, however we omit the explanation since this is not necessary for the solution over $\overline{\mathbb{Q}}(t)$.

1.2 Descending to $\overline{\mathbb{Q}}(t)$

As can be seen in [Gro61], page 290, Corollary 2.12, we have that the result explained above can be extended to any algebraically closed subfield $K \subset \mathbb{C}$. Repeating the same argument as before, if we remove a set of points $S = \{P_1, \ldots, P_s\}$ from $\mathbb{P}_1(K)$ then it turns out that identically, there is a set $\mathbb{S} = \{\mathfrak{P}_1, \ldots, \mathfrak{P}_s\}$ of valuation ideals of the function field of $\mathbb{P}_1(K) \cong K(t)$ are in correspondence with the points in S.

Now with this set $\mathbb{S}$ we construct the maximal algebraic extension $M_{\mathbb{S}}/K(t)$ unramified outside $\mathbb{S}$ as we did earlier in $\mathbb{C}(t)$. What Grothendieck's result shows is that

$$\hat{\pi}_1(\mathbb{P}_1(K) \setminus S, P_0) = \mathrm{Gal}(M_{\mathbb{S}}/K(t)).$$

Again by §47 of [ST80], given a base point $P_0 \notin S$, this fundamental group can be presented as

$$\pi(\mathbb{P}_1(K) \setminus S, P_0) = \langle \gamma_1, \ldots, \gamma_s \mid \gamma_1 \cdots \gamma_s = 1 \rangle.$$

Hence we have the following result.

Theorem 1.3. *With the notation used in the previous paragraphs, we have*

$$\mathrm{Gal}(M_{\mathbb{S}}/K(t)) \cong \langle \gamma_1, \ldots, \gamma_s \mid \gamma_1 \cdots \gamma_s = 1 \rangle\hat{}.$$

And identically as in the previous section, for any finite group G which can be presented with $s-1$ generators we have that the map

$$\phi : \mathrm{Gal}(M_{\mathbb{S}}/K(t)) \to G$$

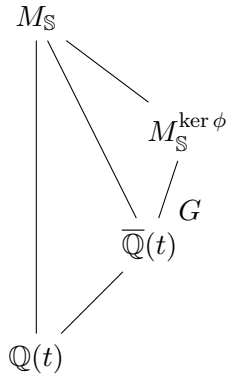
defined by

$$\phi(\gamma_i) = \begin{cases} g_i & 1 \leq i \leq s-1 \\ g_{s-1}^{-1} \cdots g_1^{-1} & i = s \end{cases} \tag{2}$$

is a surjective homomorphism and then the fixed field $M_{\mathbb{S}}^{\ker \phi}$ has Galois group isomorphic to G. This proves the following result.

Theorem 1.4. *Every finite group occurs as Galois group over* $\overline{\mathbb{Q}}(t)$.

During the rest of the work we denote by $M_{\mathbb{S}}$ the maximal extension of $\overline{\mathbb{Q}}(t)$ unramified outside a certain set $\mathbb{S}$ constructed as before. We have constructed the following field diagram



To understand the descent to $\mathbb{Q}(t)$ it is key to study some of the other Galois groups involved in the above diagram. We now display a key result on the structure of the Galois group $\mathrm{Gal}(M_{\mathbb{S}}/\mathbb{Q}(t))$. Let

$$\Gamma_s = \mathrm{Gal}(M_{\mathbb{S}}/\overline{\mathbb{Q}}(t)) = \langle \gamma_1, \ldots, \gamma_s \mid \gamma_1 \cdots \gamma_s = 1 \rangle\hat{}\,.$$

We have

Theorem 1.5 (Splitting theorem)**.** *If the set* $\mathbb{S}$ *is invariant under the absolute Galois group* $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*, then* $M_{\mathbb{S}}$ *is Galois over* $\mathbb{Q}(t)$ *and in fact*

$$\Gamma = \mathrm{Gal}(M_{\mathbb{S}}/\mathbb{Q}(t)) \cong \Gamma_s \rtimes G_{\mathbb{Q}}.$$

In particular $\Gamma_s \trianglelefteq \Gamma$.

Proof. See [MM99], Theorem 2.4 of Chapter I. □

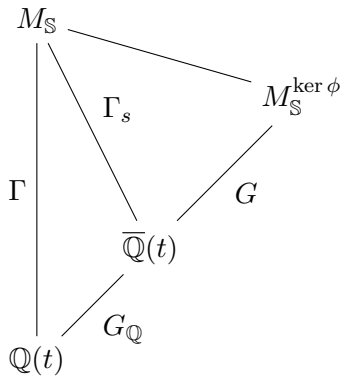
From now on we assume the set of ideals $\mathbb{S}$ is invariant under the action of $G_{\mathbb{Q}}$.

Remark 1.1. *We consider the Galois group* $\mathrm{Gal}(\overline{\mathbb{Q}}(t)/\mathbb{Q}(t))$*. Since* $t^n \in \mathbb{Q}(t)$ *for any* $n \in \mathbb{N}$ *we have that the automorphisms in* $\mathrm{Gal}(\overline{\mathbb{Q}}(t)/\mathbb{Q}(t))$ *only move coefficients. Clearly the coefficients in* $\mathbb{Q}$ *must remain fixed since* $\mathbb{Q} \subset \mathbb{Q}(t)$*. In fact one has that*

$$G_{\mathbb{Q}} \cong \mathrm{Gal}(\overline{\mathbb{Q}}(t)/\mathbb{Q}(t)) = G_{\mathbb{Q}(t)}.$$

In this work we identify $G_{\mathbb{Q}} = G_{\mathbb{Q}(t)}$.

Now that we have named the important groups involved, our current situation is the following.



1.3 The group Γ_s

Although there is no complete description of the absolute Galois group $G_{\mathbb{Q}}$ we can find some information by exploring its actions on certain sets. For instance, if we let $\zeta_n = e^{\frac{2\pi i}{n}}$ then it is clear that an element $\sigma \in G_{\mathbb{Q}}$ sends ζ_n to another primitive root of unity, ζ_n^k for any integer k with $(n,k) = 1$. This defines the homomorphism

$$\begin{aligned} c : G_{\mathbb{Q}} &\to \hat{\mathbb{Z}}^{\times} = \varprojlim(\mathbb{Z}/n\mathbb{Z})^{\times} \\ \sigma &\to c(\sigma) = (c_n(\sigma)) \end{aligned}$$

where $\sigma(\zeta_n) = \zeta_n^{c_n(\sigma)}$.

Definition 1.1. *The homomorphism $c : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}^{\times}$ described above is called the* ***cyclotomic character*** *of $G_{\mathbb{Q}}$.*

By the Kronecker-Weber theorem (see pages 324-325 of [Neu13]) we have that the maximal abelian extension field $\mathbb{Q}^{\text{ab}}$ is generated by the roots of unity. This has as Galois group the abelianization of $G_{\mathbb{Q}}$, and we have that the cyclotomic character induces an isomorphism

$$G_{\mathbb{Q}}^{\text{ab}} = \text{Gal}(\mathbb{Q}^{\text{ab}}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^{\times}.$$

The following is a result due to Abhyankar.

Proposition 1.1. *Each generator γ_i of Γ_s generates a procyclic inertia group $\langle\gamma_i\rangle\hat{}$ at a valuation ideal in $M_{\mathbb{S}}$ above $P_i \in S$.*

Proof. This is Theorem 1.4 of Chapter I of [MM99]. □

Since we are considering $\mathbb{S} = \{\mathfrak{P}_1, \ldots, \mathfrak{P}_s\}$ to be invariant under $G_{\mathbb{Q}}$ then each $\sigma \in G_{\mathbb{Q}}$ permutes the $\mathfrak{P}_i$'s in $\mathbb{S}$ so we may view σ as a permutation of the indices $\{1, 2, ..., s\}$. Let $\tilde{\sigma}$ denote a lifting of σ to Γ. Then, conjugation by $\tilde{\sigma} \in \Gamma$ works as displayed in the following result.

Proposition 1.2. *In Γ_s the element $(\gamma_i)^{\tilde{\sigma}}$ is conjugate to $\gamma_{\sigma(i)}^{c(\sigma)}$.*

Proof. This is theorem 2.6 of Chapter I of [MM99]. □

§2 Character theory

For certain algebraic objects, a classical way of having a better understanding of their behavior is to *represent* these objects *inside* better understood objects, with hopes of using structural information of the latter to understand the former. In the case of groups, we work with homomorphisms into linear groups, which turn out to have very nice properties for finite groups. However, a nonlinear object arises from these homomorphisms, which has even nicer properties and eases computations. These objects are called characters. This section will explain the properties of characters which will be necessary for our work. The usefulness (and necessity) of these characters will appear in §3 and §4.

2.1 Group representations and characters

Definition 2.1. *Let G be a finite group. A **representation** of G is an homomorphism*

$$\Phi : G \to \mathrm{GL}_n(\mathbb{C}).$$

Definition 2.2. *Let G be a finite group and Φ be a representation of G. We say the **character** χ **afforded by** Φ is the map defined as the trace of the image of Φ, i.e.*

$$\begin{aligned} \chi : G &\to \mathbb{C} \\ g &\mapsto tr(\Phi(g)). \end{aligned}$$

Representations and characters can be defined over any arbitrary field K and will have all the following desired properties as long as $char(K)$ does not divide $|G|$. We limit ourselves to representations over $\mathbb{C}$.

Lemma 2.1. *Let G be a group. The characters of G are constant on the conjugacy classes of G.*

Proof. Recall that for square matrices A and B of the same dimension, one has that $tr(AB) = tr(BA)$. For a representation Φ and $g, h \in G$ one has

$$\Phi(h^{-1}gh) = \Phi(h)^{-1}\Phi(g)\Phi(h)$$

and hence

$$tr(\Phi(h^{-1}gh)) = tr(\Phi(h)^{-1}\Phi(g)\Phi(h)) = tr(\Phi(g)\Phi(h)\Phi(h)^{-1}) = tr(\Phi(g))$$

and we are done. □

Definition 2.3. *We say two representations Φ and Ψ are **similar** if there is a regular matrix A such that $\Phi(g) = A^{-1}\Psi(g)A$ for all $g \in G$.*

Lemma 2.2. *Similar representations afford equal characters.*

Proof. For regular matrices A and B, one has that $tr(A^{-1}BA) = tr(BAA^{-1}) = tr(B)$. □

Observe that for two representations Φ, Ψ of a group G one can define

$$\Theta(g) = \begin{pmatrix} \Phi(g) & 0 \\ 0 & \Psi(g) \end{pmatrix}$$

and Θ is also a representation of G. Since $tr(\Theta(g)) = tr(\Phi(g)) + tr(\Psi(g))$ we have that characters are closed under addition. The set of characters that cannot be written as sum of other characters is the set of **irreducible characters**, and will be denoted by $\mathrm{Irr}(G)$.

2.2 Some properties of characters

We now state some properties of characters that we will need.

Proposition 2.1. *Let G be a group. Then the number of irreducible characters of G equals the number of conjugacy classes of G and in fact one has*

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = |G|.$$

Proof. See [Isa94], Corollary 2.7. □

Since there are exactly the same number of irreducible characters as there are conjugacy classes, we display the values of irreducible characters of a group in character tables, having conjugacy classes in the columns and the values of irreducible characters in the rows.

Lemma 2.3. *Let Φ be a representation of G affording the character χ. Let $g \in G$ and let n be the order of g. Then*

1. *$\Phi(g)$ is similar to a diagonal matrix $\mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_j)$.*
2. *$\varepsilon_i^n = 1$ for all $1 \leq i \leq j$.*
3. *$\chi(g) = \sum_{i=1}^{j} \varepsilon_i$.*
4. *$\chi(g^{-1}) = \overline{\chi(g)}$.*

Proof. See [Isa94], Lemma 2.15. □

Corollary 2.1. *Let ζ_n denote a primitive nth root of unity. The values of all irreducible characters of a finite group G are in $\mathbb{Z}[\zeta_{|G|}] \subset \mathbb{Q}(\zeta_{|G|}) \subset \mathbb{Q}^{ab}$.*

Theorem 2.1 (Second orthogonality relation)**.** *Let $g, h \in G$. Then*

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = 0$$

if g is not conjugate to h in G. Otherwise, the sum equals $|C_G(g)|$ (this denotes the size of the centralizer of g in G).

Proof. See [Isa94], Theorem 2.18. □

As the name of the previous theorem suggests, there is a first orthogonality relation. In fact using these relations one can define an inner product on the set of functions that are constant on conjugacy classes of G, and this endows the set with the structure of a finite dimensional complex Hilbert space, having $\mathrm{Irr}(G)$ as orthonormal basis. This inner product is defined as follows.

Definition 2.4. *Let θ_1, θ_2 be two class functions of G (functions that are constant on the conjugacy classes of G). The **inner product** of θ_1 and θ_2 is*

$$[\theta_1, \theta_2] = \frac{1}{|G|} \sum_{g \in G} \theta_1(g)\overline{\theta_2(g)}.$$

Remark 2.1. *Observe that the dimension of $\Phi(g)$ is exactly $\chi(1)$ (in particular $\chi(1)$ is always an integer). Let $I_{\chi(1)}$ denote the identity matrix of dimension $\chi(1)$.*

Proposition 2.2. *Let Φ be an irreducible representation of G affording the character χ. Let $g \in G$. Then*

$$\frac{1}{|G|} \sum_{h \in G} \Phi(h^{-1}gh) = \frac{\chi(g)}{\chi(1)} I_{\chi(1)}.$$

Proof. This is a particular case of Corollary 1 of §2.2 of [Ser71] by observing that the matrix $\Phi(g)$ defines a linear map $\mathbb{C}^{\chi(1)} \to \mathbb{C}^{\chi(1)}$. □

§3 Rationality and rigidity

3.1 Rationality of conjugacy classes

Definition 3.1. *Let G be a finite group and $Cl(G)$ be the set of its conjugacy classes. We say a class $\mathscr{C} \in Cl(G)$ is **rational** if any irreducible character of G takes rational (and hence integer) values on $\mathscr{C}$ i.e. $\chi(\mathscr{C}) \in \mathbb{Z}$ for all $\chi \in \mathrm{Irr}(G)$.*

Example 3.1. As displyed by [GAP19], the character table of the symmetric group S_5 is

	1A	2A	2B	3A	6A	4A	5A
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	-1	1
χ_3	4	-2	0	1	1	0	-1
χ_4	5	-1	1	-1	-1	1	0
χ_5	6	0	-2	0	0	0	-1
χ_6	5	1	1	-1	1	-1	0
χ_7	4	2	0	1	-1	0	-1

It is very easy now to check visually that S_5 has all conjugacy classes rational. This is in fact true for all symmetric groups S_n (see Proposition 5.3).

Remark 3.1. *Let ζ_m be a primitive mth root of unity. For any element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ we have that, if Φ is an irreducible representation of G then $\sigma \circ \Phi$ is too an irreducible representation, and if the irreducible character afforded by Φ is χ, then $\sigma \circ \Phi$ affords $\sigma \circ \chi$ and this is also an irreducible character of G. This defines an action of $(\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ on the set* Irr(G).

Proposition 3.1. *Let m be the order of G. A conjugacy class $\mathscr{C} \in Cl(G)$ is rational if and only if $\mathscr{C}^n = \mathscr{C}$ whenever $(n, m) = 1$.*

Proof. Let ζ_m be a primitive mth root of unity. Let $n \in (\mathbb{Z}/m\mathbb{Z})^\times$. Then $g \mapsto g^n$ is a group action of $(\mathbb{Z}/m\mathbb{Z})^\times$ on G. Let $\sigma_n \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ be the field automorphism defined by $\sigma_n(\zeta_m) = \zeta_m^n$.

Now by Lemma 2.3 we have that if Φ is an irreducible representation affording the character χ, then for any $g \in G$, $\Phi(g)$ is similar to a diagonal matrix. This matrix is of the form $\mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_j)$ where j is the size of $\Phi(g)$. Moreover, if k is the order of g in G, then the ε's are kth roots of unity. Since Φ is an homomorphism we have $\Phi(g^n) = \Phi(g)^n$, and $\Phi(g)^n$ is similar to $\mathrm{diag}(\varepsilon_1^n, \ldots, \varepsilon_j^n)$. Hence

$$\chi(g^n) = \varepsilon_1^n + \cdots + \varepsilon_j^n$$

and since k divides $m = |G|$ we find that for any conjugacy class $\mathscr{C} \in Cl(G)$ we have

$$\sigma_n \circ \chi(\mathscr{C}) = \chi(\mathscr{C}^n).$$

Now suppose that $\mathscr{C} = \mathscr{C}^n$. Then $\sigma_n \circ \chi(\mathscr{C}) = \chi(\mathscr{C})$. Since all automorphisms in $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ are of the form σ_n for $(n, m) = 1$ we have that $\chi(\mathscr{C})$ remains fixed for all Galois automorphisms, and then $\chi(\mathscr{C}) \in \mathbb{Q}$.

Now suppose that $\mathscr{C}$ is rational. Then we have

$$\chi(\mathscr{C}) = \sigma_n \circ \chi(\mathscr{C}) = \chi(\mathscr{C}^n) \tag{3}$$

for all characters $\chi \in$ Irr(G). By Theorem 2.1 and equality 3 we have that for $g \in \mathscr{C}$

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(g^n)} = \sum_{\chi \in \mathrm{Irr(G)}} |\chi(g)|^2 \neq 0$$

and then g and g^n are conjugate, so $\mathscr{C} = \mathscr{C}^n$. □

3.2 The rigidity condition

Let $v = (\mathscr{C}_1, \ldots, \mathscr{C}_s)$ be a s-tuple of conjugacy classes of a finite group G, with $s \geq 3$. We denote

$$\overline{A}(v) = \overline{A}(\mathscr{C}_1, \ldots, \mathscr{C}_s) = \{(g_1, \ldots, g_s) \in \mathscr{C}_1 \times \cdots \times \mathscr{C}_s \mid g_1 \cdots g_s = 1\}.$$

We define

$$A(v) = \{(g_1, \ldots, g_s) \in \overline{A}(v) \mid \langle g_1, \ldots, g_s \rangle = G\}.$$

We have that G acts by component-wise conjugation on both A and $\overline{A}$.

Definition 3.2. *The family $(\mathscr{C}_1, \ldots, \mathscr{C}_s)$ is called **rigid** if $|A(v)| = |G|$. It is **strictly rigid** if it is rigid and $|\overline{A}(v)| = |A(v)|$.*

Proposition 3.2. *If $\mathbb{Z}(G) = \{1\}$ then the action by conjugation of G on $A(v)$ is free.*

Proof. Suppose that for some $h \in G$ and $(g_1, \ldots, g_s) \in A(v)$ that $hg_ih^{-1} = g_i$ for all $1 \leq i \leq s$. Since the g_i's generate G then h commutes with a set of generators of G and then it must commute with all of G, so $h \in Z(G) = \{1\}$ so the action is free. □

Corollary 3.1. *If $A(v)$ is nonempty and $Z(G) = \{1\}$ then $(\mathscr{C}_1, \ldots, \mathscr{C}_s)$ is rigid if and only if G acts on $A(v)$ transitively.*

Proof. For any $(g_1, \ldots, g_s) \in A(v)$ we have that if $h \neq g \in G$ then g and h move $(g_1, \ldots, g_s)$ to different elements in $A(v)$. Then $|A(v)| = |G|$ if and only if $A(v)$ is the only orbit under this action. □

3.3 Checking rigidity with characters

The goal of this section finding a formula for $|\overline{A}(v)|$, where $v = (\mathscr{C}_1, \ldots, \mathscr{C}_s)$. This formula was originally found by Thompson in [Tho84c], and is considered one of his great contributions to the Rigidity Method. We follow section 7.2 of [Ser92].

Theorem 3.1. *Let $g_i \in \mathscr{C}_i$. We have*

$$|\overline{A}(\mathscr{C}_1, \ldots, \mathscr{C}_s)| = \frac{|\mathscr{C}_1| \cdots |\mathscr{C}_s|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1) \cdots \chi(g_s)}{\chi(1)^{s-2}}.$$

Proof. Let Φ be an irreducible representation of G, affording the character χ. By Proposition 2.2 we have

$$\frac{1}{|G|} \sum_{h \in G} \Phi(h^{-1}gh) = \frac{\chi(g)}{\chi(1)} I_{\chi(1)}.$$

Multiplying both sides by $\Phi(x)$ for any $x \in G$ we get

$$\frac{1}{|G|} \sum_{h \in G} \Phi(h^{-1}ghx) = \frac{\chi(g)}{\chi(1)} \Phi(x)$$

and taking traces we have

$$\frac{1}{|G|} \sum_{h \in G} \chi(h^{-1}ghx) = \frac{\chi(g)\chi(x)}{\chi(1)}.$$

With an inductive argument we get that for any $g_1, \ldots, g_k \in G$,

$$\frac{1}{|G|^s} \sum_{h_1, \ldots, h_s \in G} \chi(h_1^{-1} g_1 h_1 \cdots h_s^{-1} g_s h_s x) = \frac{\chi(g_1) \cdots \chi(g_s)\chi(x)}{\chi(1)^s}.$$

We consider now the class function defined by

$$\theta(g) = \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi(g).$$

This is indeed a class function since it is a linear combination of irreducible characters, and in fact by Proposition 2.1

$$\theta(1) = \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = 1$$

and by Theorem 2.1 and the fact that 1 is only conjugate to itself we have that whenever $g \neq 1$,

$$\theta(g) = \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi(g) = \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(1)} = 0$$

So θ is in fact the characteristic function of the element $1 \in G$. If we denote by $\mathcal{A}$ the set of s-tuples $(h_1, \ldots, h_s)$ such that $h_1^{-1} g_1 h_1 \cdots h_s^{-1} g_s h_s x = 1$ we have that

$$\sum_{h_1, \ldots, h_s \in G} \theta(h_1^{-1} g_1 h_1 \cdots h_s^{-1} g_s h_s x) = |\mathcal{A}|. \tag{4}$$

On the other hand

$$\frac{1}{|G|^s} \sum_{h_1, \ldots, h_s \in G} \theta(h_1^{-1} g_1 h_1 \cdots h_s^{-1} g_s h_s x) =$$

$$= \frac{1}{|G|^s} \sum_{h_1, \ldots, h_s \in G} \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi(h_1^{-1} g_1 h_1 \cdots h_s^{-1} g_s h_s x) =$$

$$= \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(1)}{|G|} \left(\frac{1}{|G|^s} \sum_{h_1, \ldots, h_s \in G} \chi(h_1^{-1} g_1 h_1 \cdots h_s^{-1} g_s h_s x) \right) =$$

$$= \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1) \cdots \chi(g_s)\chi(x)}{\chi(1)^{s-1}}$$

and now applying equality 4 we finally have

$$|\mathcal{A}| = |G|^{s-1} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1) \cdots \chi(g_s)\chi(x)}{\chi(1)^{s-1}}. \tag{5}$$

Now given the class vector $v = (\mathscr{C}_1, \ldots, \mathscr{C}_s)$ we have that $\overline{A}(v)$ denotes the set of s-tuples $(x_1, \ldots, x_s)$ such that $x_1 \cdots x_s = 1$ and $x_i \in \mathscr{C}_i$, $1 \leq i \leq s$.

Consider $(x_1, \ldots, x_s) \in \overline{A}(v)$. Let $y \in C_G(x_i)$ for some $1 \leq i \leq s$. This means $yx_i = x_i y$. Since $(x_1, \ldots, x_s) \in \overline{A}(v)$ we have

$$x_1 \cdots x_i \cdots x_s = 1$$

and then

$$x_1 \cdots x_i y y^{-1} \cdots x_s = 1$$

and since y centralizes x we have

$$x_1 \cdots y x_i y^{-1} \cdots x_s = 1$$

and then $(1, \ldots, 1, y^{-1}, 1, \ldots, 1) \in \mathcal{A}$. Since this can be done for any $y \in C_G(x_i)$ and for any $1 \leq i \leq s$ we have that for any s-tuple in $\overline{A}(v)$ we have $|C_G(x_1)| \cdots |C_G(x_s)|$ tuples in $\mathcal{A}$, and given that two conjugate elements have identical centralizers

$$|\overline{A}(v)| = \frac{|\mathcal{A}|}{|C_G(g_1)| \cdots |C_G(g_s)|}$$

and now applying equality 5 with $x = 1$ we get

$$|\overline{A}(v)| = \frac{|G|^{s-1}}{|C_G(g_1)| \cdots |C_G(g_s)|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1) \cdots \chi(g_s)}{\chi(1)^{s-2}}$$

and since

$$|\mathscr{C}_i| = \frac{|G|}{|C_G(g_i)|}$$

we finally get

$$|\overline{A}(v)| = \frac{|\mathscr{C}_1| \cdots |\mathscr{C}_s|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1) \cdots \chi(g_s)}{\chi(1)^{s-2}}.$$

□

With this last theorem, we may proceed to prove rigidity as the following result shows.

Proposition 3.3. *Let G be a group with $Z(G) = \{1\}$. A class vector $v = (\mathscr{C}_1, \ldots, \mathscr{C}_s)$ of G is strictly rigid if $A(v)$ is nonempty and*

$$|G| = \frac{|\mathscr{C}_1| \cdots |\mathscr{C}_s|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1) \cdots \chi(g_s)}{\chi(1)^{s-2}}.$$

Proof. Let $(g_1, \ldots, g_s) \in A(v) \neq \emptyset$. We define the map

$$\begin{aligned} f : G &\to A(v) \\ g &\mapsto (g^{-1} g_1 g, \ldots, g^{-1} g_s g). \end{aligned}$$

Since $Z(G) = \{1\}$ we have that the action by conjugation of G on $A(v)$ is free, and then f is injective, showing $|G| \leq A(v)$. Now by hypothesis we have $|G| = |\overline{A}(v)|$ and since $A(v) \subseteq \overline{A}(v)$ we have

$$|G| \leq |A(v)| \leq |\overline{A}(v)| \leq |G|$$

so all inequalities above must be equalities and v si strictly rigid. □

§4 The main result

In §1 we managed to descend from $\mathbb{C}(t)$ to $\overline{\mathbb{Q}}(t)$ with no restrictions on the properties of the group G. What the following results will achieve is the descent from $\overline{\mathbb{Q}}(t)$ to $\mathbb{Q}(t)$, and then the rationality and rigidity conditions will play a key role.

4.1 The Basic Rigidity Theorem

From now on $S = \{P_1, \dots, P_s\} \subset \mathbb{P}_1(\overline{\mathbb{Q}})$ will denote a set of points which have associated valuation ideal set $\mathbb{S}$ invariant invariant under $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \cong \mathrm{Gal}(\overline{\mathbb{Q}}(t)/\mathbb{Q}(t))$. Recall that $\Gamma = \mathrm{Gal}(M_{\mathbb{S}}/\mathbb{Q}(t))$ and

$$\Gamma_s = \mathrm{Gal}(M_{\mathbb{S}}/\overline{\mathbb{Q}}(t)) \cong \langle \gamma_1, \dots, \gamma_i \mid \gamma_1 \cdots \gamma_s = 1 \rangle^{\wedge}$$

and we had

$$\Gamma = \Gamma_s \rtimes G_{\mathbb{Q}}.$$

Consider $v = (\mathscr{C}_1, \dots, \mathscr{C}_s)$ a vector of conjugacy classes of G. Let $\mathcal{H} \subset \mathrm{Hom}(\Gamma_s, G)$ be the subset of surjective maps ϕ that map γ_i inside $\mathscr{C}_i$ for all $1 \leq i \leq s$. Recall that we denoted by $A(v)$ the set of s-tuples $(g_1 \dots g_s)$ in $\mathscr{C}_1 \times \cdots \times \mathscr{C}_s$ that generated G and with the relation $g_1 \cdots g_s = 1$. We have the following result.

Theorem 4.1. *The sets $\mathcal{H}$ and $A(v)$ are bijective.*

Proof. For a s-tuple $(g_1, \dots, g_s) \in A(v)$ consider the homomorphism

$$\begin{aligned} \varphi : \Gamma_s &\to G \\ \gamma_i &\mapsto g_i. \end{aligned}$$

Since $\langle g_1, \dots, g_s \rangle = G$ then φ is clearly surjective and then $\varphi \in \mathcal{H}$.

Conversely let $\varphi \in \mathcal{H}$ and consider the s-tuple $(g_1, \dots, g_s) = (\varphi(\gamma_1), \dots, \varphi(\gamma_s))$. By surjectivity of φ we have $\langle g_1, \dots, g_s \rangle = G$ and

$$g_1 \cdots g_s = \varphi(\gamma_1) \cdots \varphi(\gamma_s) = \varphi(\gamma_1 \cdots \gamma_s) = 1$$

so $(g_1, \dots, g_s) \in A(v)$. □

This is a particular case of the much more general Hurwitz classification (Theorem 4.1 of [MM99]).

We define an action of G on $\mathcal{H}$ as follows. Let $g \in G, \varphi \in \mathcal{H}, \gamma \in \Gamma_s$, then

$$(g \cdot \varphi)(\gamma) = g^{-1} \varphi(\gamma) g.$$

Since the action of G on $A(v)$ is also by conjugation then we have

Corollary 4.1. *$\mathcal{H}$ and $A(v)$ are isomorphic as G-sets.*

Remark 4.1. *Recall that when $\mathbb{S}$ was invariant (as a set) under the action of $G_{\mathbb{Q}}$ we could view automorphisms in $G_{\mathbb{Q}}$ as a permutation on the indices $\{1,\dots,s\}$ of elements in $\mathbb{S}$. Since we have chosen each ideal to be invariant under $G_{\mathbb{Q}}$ it turns out that this permutation is trivial. The set $\mathbb{S}$ is a set of valuation ideals of the ring $\overline{\mathbb{Q}}[t]$ so it suffices to choose the points P_i such that the corresponding ideals $\mathfrak{P}_i$ are in $\mathbb{Q}[t]$.*

Remark 4.2. *The cyclotomic character appears in the statement of Proposition 1.2 because of the profinite nature of the group Γ_s. As explained in §7.3 of [Ser92], when we construct the surjective homomorphism $\Gamma_s \to G$, we can interpret Proposition 1.2 as the existence of an element $n \in (\mathbb{Z}/|G|\mathbb{Z})^\times$ such that each $g_i \in \mathscr{C}_i$ is conjugate to g_i^n for all $1 \leq i \leq s$.*

We now state and prove the main result of this work.

Theorem 4.2 (Basic Rigidity Theorem)**.** *Let G be a finite group with $Z(G) = \{1\}$. If there exists a class vector $v = (\mathscr{C}_1,\dots,\mathscr{C}_s)$ which is rigid and rational then there is a Galois extension of $\mathbb{Q}(t)$ with Galois group isomorphic to G.*

Proof. We define a Γ-action on $\mathrm{Hom}(\Gamma_s, G)$. Let $\gamma \in \Gamma$, $\psi \in \mathrm{Hom}(\Gamma_s, G)$ and define

$$(\psi \star \gamma)(x) = \psi(\gamma^{-1} x \gamma).$$

This is a well defined action since $\Gamma_s \trianglelefteq \Gamma$ by Theorem 1.5. Moreover, we can extend the G-action defined just before Corollary 4.1 to $\mathrm{Hom}(\Gamma_s, G)$ by

$$g \cdot \psi(x) = g^{-1}\psi(x)g$$

and it turns out that both actions commute. Indeed let $\gamma \in \Gamma, g \in G$ and $\psi \in \mathrm{Hom}(\Gamma_s, G)$, we have that for all $x \in \Gamma_s$

$$((g \cdot \psi) \star \gamma)(x) = (g \cdot \psi)(\gamma^{-1} x \gamma) = g^{-1}\psi(\gamma^{-1} x \gamma)g = (g \cdot (\psi \star \gamma))(x).$$

By hypothesis there exists a rigid class vector v, so by Proposition 3.2 and Corollary 3.1 we have that the action of G on $A(v)$ is free and transitive. It follows from Corollary 4.1 that we have that the action of G on $\mathcal{H}$ is also free and transitive.

Our next goal is to prove that $\mathcal{H}$ is stable under the action of Γ on $\mathrm{Hom}(\Gamma_s, G)$. Let $\gamma \in \Gamma$ and $\varphi \in \mathcal{H}$. Then

$$\varphi \star \gamma(\gamma_i) = \varphi(\gamma^{-1}\gamma_i\gamma)$$

and by Proposition 1.2 and Remark 4.1 we have that

$$\varphi \star \gamma(\gamma_i) = \varphi(\gamma_i^{c(\sigma)})$$

for some $\sigma \in G_{\mathbb{Q}}$. By Remark 4.2 we have

$$\varphi(\gamma_i^{c(\sigma)}) = g_i^n$$

for some n coprime to $|G|$. By the equivalent definition of rationality given by Proposition 3.1 we have that $g_i^n \in \mathscr{C}_i^n = \mathscr{C}_i$ and then

$$\varphi(\gamma_i^{c(\sigma)}) \in \mathscr{C}_i$$

or equivalently

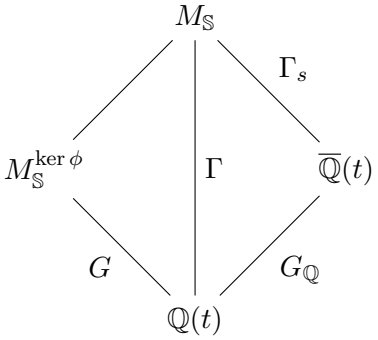
$$\varphi \star \gamma \in \mathcal{H}$$

and our claim is proved.

The surjective homomorphisms $\phi \in \mathrm{Hom}(\Gamma, G)$ define extensions $M_S^{\ker\phi}/\mathbb{Q}(t)$ with Galois group

$$\mathrm{Gal}(M_S^{\ker\phi}/\mathbb{Q}(t)) \cong \Gamma/\ker\phi \cong G$$

having the following situation:



so what is left is to prove that at least one of such homomorphisms exist. What we will show is that any $\psi \in \mathcal{H} \subset \mathrm{Hom}(\Gamma_s, G)$ can be extended to an homomorphism $\phi \in \mathrm{Hom}(\Gamma, G)$, and since homomorphisms in $\mathcal{H}$ are surjective, ϕ will be one of the homomorphisms we wish to find. Recall that by hypothesis v is rigid and then $A(v) \neq \emptyset$ and by Theorem 4.1 we have $\mathcal{H} \neq \emptyset$ so this will conclude the proof.

Recall that $\mathcal{H}$ is stable under the action of Γ. Let $\psi \in \mathcal{H}$. For any $\gamma \in \Gamma$ we have that $\psi \cdot \gamma \in \mathcal{H}$. Now since the action of G on $\mathcal{H}$ is transitive we have that there exists $g_\gamma \in G$ such that

$$g_\gamma \cdot \psi = \psi \star \gamma.$$

Since the G-action on Γ is also free we have that g_γ is unique. Hence we can define

$$\begin{aligned} \phi : \Gamma &\to G \\ \gamma &\mapsto g_\gamma \end{aligned}$$

and, since the G-action and the Γ-action commute, we have

$$\phi(\alpha\beta) \cdot \psi = \psi \star (\alpha\beta) = (\phi(\alpha) \cdot \psi) \star \beta = \phi(\alpha) \cdot (\psi \star \beta) = \phi(\alpha)\phi(\beta) \cdot \psi,$$

so ϕ is multiplicative and since $\phi(1) = 1$ then ϕ is an homomorphism. Now let $\alpha \in \Gamma_s$. For all $\beta \in \Gamma_s$ we have

$$(\phi(\alpha) \cdot \psi)(\beta) = (\psi \star \alpha)(\beta) = \psi(\alpha^{-1}\beta\alpha) = \psi(\alpha^{-1})\psi(\beta)\psi(\alpha) = (\psi(\alpha) \cdot \psi)(\beta).$$

In other words $\phi(\alpha) \in G$ acts on ψ identically as $\psi(\alpha)$ does. Since the G-action on $\mathcal{H}$ is free we have $\psi(\alpha) = \phi(\alpha)$ for all $\alpha \in \Gamma_s$ and ϕ extends ψ. This concludes the proof. □

Remark 4.3. *Although the result has been proven for class vectors of arbitrary length, the vast majority of applications of the Rigidity Theorem involve class vectors of length 3. In fact, in general for any non cyclic group, a vector of conjugacy classes v must have size at least 3 and it must not include the conjugacy class of 1 in order to have $A(v) \neq \emptyset$.*

4.2 Generalizations of the Rigidity Theorem

Even though the Basic Rigidity Theorem allows us to realize some groups as Galois groups over $\mathbb{Q}$ (as we will do in some cases in section 5), there are some generalizations.

The rationality condition is what allows us to guarantee that our group can is a Galois group with base field $\mathbb{Q}(t)$. However, many interesting groups do not verify the rationality condition for any rigid tuple of conjugacy classes.

Example 4.1. The character table of the alternating group A_5 as displayed by [GAP19] is

	1A	2A	3A	5A	5B
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_3	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

We can see that the conjugacy classes denoted by $5A$ and $5B$ are not rational. The number denoting the conjugacy class is the order of any of its representatives, so we have that no element of order 5 in A_5 is in a rational conjugacy class. Since any vector of conjugacy classes v for which we might have $|A(v)| = |A_n|$ must include either $5A$ or $5B$ we have that our Basic Rigidity Theorem can not be applied here.

After the previous example we can now ask ourselves whether we can find a generalization of the Rigidity Method which allows us to realize groups as Galois groups over number fields even if we can not find a rational and rigid class vector.

Consider now the same stage as the one from Theorem 4.2 but without the rationality condition. We go back again to using the cyclotomic character. Recall that all elements of any conjugacy class have the exact same order. Let $\mathscr{C}$ be a conjugacy class of a finite group G. By Remark 4.2, we have that for any $\sigma \in G_{\mathbb{Q}}$, there is some n coprime to $|G|$ such that

$$\mathscr{C}^{c(\sigma)} = \mathscr{C}^n.$$

Consider a class vector $v = (\mathscr{C}_1, \ldots, \mathscr{C}_s)$. We define the subgroup $\Delta_v \leq G_{\mathbb{Q}}$ as

$$\Delta_v = \{\sigma \in G_{\mathbb{Q}} \mid \mathscr{C}_i^{c(\sigma)} = \mathscr{C}_i, 1 \leq i \leq s\}.$$

It turns out that Δ_v is a normal subgroup of G. Indeed, $G_{\mathbb{Q}}$ acts on the set

$$\{v^n = (\mathscr{C}_1^n, \ldots, \mathscr{C}_s^n) \mid (n, |G|) = 1\},$$

and this action defines a permutation representation of $G_{\mathbb{Q}}$ which has Δ_v as its kernel. Hence we can define the fixed field of a class vector.

Definition 4.1. *Let $v = (\mathscr{C}_1, \ldots, \mathscr{C}_s)$ be a class vector of G. The **fixed field of** v is defined as $\mathbb{Q}_v = \overline{\mathbb{Q}}^{\Delta_v}$.*

It turns out that the quotient $G_{\mathbb{Q}}/\Delta_v$ is an abelian group. By the fundamental theorem of Galois theory we have that

$$G_{\mathbb{Q}}/\Delta_v \cong \mathrm{Gal}(\mathbb{Q}_v/\mathbb{Q})$$

and hence $\mathbb{Q}_v$ is an abelian extension of $\mathbb{Q}$.

Now let $\chi \in \mathrm{Irr}(G)$ and let $\sigma \in \Delta_v$. Then By [Hup67] Section V.13.1 (c), we have that $\sigma(\chi(\mathscr{C})) = \chi(\mathscr{C}^{c(\sigma)})$. Thus, we have that

$$\sigma(\chi(\mathscr{C}_i)) = \chi(\mathscr{C}_i^{c(\sigma)}) = \chi(\mathscr{C}_i)$$

for all $1 \leq i \leq s$. This proves that

$$\mathbb{Q}(\{\chi(\mathscr{C}_i) \mid \chi \in \mathrm{Irr}(G), 1 \leq i \leq s\}) \subseteq \mathbb{Q}_v.$$

In fact we have

Proposition 4.1. *Let $v = (\mathscr{C}_1, \ldots \mathscr{C}_s)$ be a class vector of a finite group G. Then*

$$\mathbb{Q}_v = \mathbb{Q}(\{\chi(\mathscr{C}_i) \mid \chi \in \mathrm{Irr}(G), 1 \leq i \leq s\}).$$

Proof. For the proof of the result and some details omitted above, see Chapter I, Proposition 4.4 of [MM99]. □

With this concept of fixed field of a class vector, we can state a more general Rigidity Theorem.

Theorem 4.3. *Let G be a finite group with $Z(G) = \{1\}$. If G has a rigid class vector v then there is a Galois extension of $\mathbb{Q}_v(t)$ with Galois group isomorphic to G.*

Proof. This is Theorem 4.8 of [MM99]. □

Observe that if $v = (\mathscr{C}_1, \ldots, \mathscr{C}_s)$ is a rational vector of conjugacy classes, then $\Delta_v = G_{\mathbb{Q}}$ and then the fixed field $\mathbb{Q}_v$ is exactly $\mathbb{Q}$. However in the case that the vector is rational we can take advantage of Proposition 3.1. Otherwise, Theorem 4.3 can be proved similarly to our Theorem 4.2.

Moreover, since Hilbert's irreducibilty theorem is also valid for every number field (see [Hil92]) we have that the previous result is sufficient to realize G as Galois group over $\mathbb{Q}_v$.

Remark 4.4. *The result mentioned above has an even more general statement. It asks for $Z(G)$ to have a complement in G, i.e., a subgroup $H \leq G$ such that $H \cap Z(G) = \{1\}$ and $HZ(G) = G$. However, by Chapter IV, Corollary 1.7 of [MM99], this can be replaced without loss of generality by the assumption that $Z(G) = \{1\}$.*

Indeed, if $Z(G)$ has a complement H in G we have that $HZ(G) = G$ and $H \cap Z(G) = 1$, so we have

$$G \cong Z(G) \times H.$$

Let $h \in Z(H)$, then h commutes with all elements in H and since $h \in G$ then h commutes with all elements in $Z(G)$. Now since $G \cong Z(G) \times H$ we have that $h \in Z(G)$ but $H \cap Z(G) = \{1\}$, proving that $Z(H) = \{1\}$. By the mentioned result, if $Z(G)$ and H are Galois groups over any number field K then so is G. Now $Z(G)$ is abelian so it is Galois group over any number field (this is a classic result, but could very well be thought of as a trivial consequence of [Šč54]). Since $Z(H) = \{1\}$ we can finally see how realization of G as Galois group over K has been reduced to the realization of a group with trivial center.

§5 Applications of the Rigidity Method

In this section we study notable families of groups and attempt to apply the strongest possible version of the Rigidity Method.

5.1 Auxiliary results

We display some general results which greatly help us in the application of the method in some particular cases.

Recall that the commutator subgroup $[G, G]$ of a group G is defined by

$$[G, G] = \langle a^{-1}b^{-1}ab \mid a, b \in G \rangle.$$

This group is also known as the derived subgroup of G, and sometimes denoted by G'. It is not true in general that all elements of $[G, G]$ are commutators. It is straightforward to check that $[G, G]$ is a normal subgroup of G. A group is said to be perfect if $G = [G, G]$.

Proposition 5.1. *Let $G = \langle g_1, g_2, g_3 \rangle$ with $g_1 g_2 g_3 = 1$ and the orders of all g_i are pairwise coprime. Then G is perfect.*

Proof. Suppose G has proper commutator subgroup. The commutator subgroup G' is then a proper normal subgroup of G and G/G' is a nontrivial abelian group. By the decomposition theorem of abelian groups we have that

$$G/G' \cong C_{q_1} \times \cdots \times C_{q_n}$$

where the q_j's are prime powers and C_q denotes the cyclic group of order q. Denote by φ the isomorphism above. We have that $\varphi = (\varphi_1, \ldots, \varphi_n)$ where

$$\varphi_j : G/G' \to C_{q_j}.$$

Then for example

$$(G/G')/\ker\varphi_1 \cong C_{q_1} \tag{6}$$

and since $\ker\varphi_1 \trianglelefteq G/G'$ there exists a normal subgroup $G' \subseteq N \trianglelefteq G$ such that $N/G' \cong \ker\varphi_1$ and by equality 6 and the third isomorphism theorem we have

$$G/N \cong (G/G')/(N/G') \cong C_{q_1}$$

so we have found a quotient G/N which is cyclic of prime power order.

Suppose $q_1 = p^k$ for p a prime. We have that $\langle g_1N, g_2N, g_3N\rangle = G/N$ and then either $g_iN = N$ or p divides the order of g_iN in G/N. Since these orders must divide the orders of g_i in G and these are pairwise coprime by assumption then p divides at most one of the orders of g_iN and the rest are trivial elements. Now the condition that $g_1g_2g_3 = 1$ forces all g_iN to be trivial in G/N, which contradicts the fact that these elements should generate G/N. □

Recall that from basic group theory, a subgroup H of a group G whose has index is the smallest prime dividing $|G|$ is always normal. In particular any subgroup of index 2 is a normal subgroup. We have the following result.

Proposition 5.2. . *Let G be a finite group with trivial center and H a subgroup of index 2. If there is a rationally rigid triple of conjugacy classes in G then both G and H occur as Galois groups over $\mathbb{Q}$.*

Proof. See Theorem 3.20 of [Vol96]. □

This result first appears in J. Thompson's paper [Tho84a], pages 249-250. He thanks J. P. Serre for the key idea, which uses concepts from [Tho84c]. Thompson mentions the argument using it for a particular group, and Volklein's proof seems more straightforward to the author.

5.2 The symmetric and alternating groups

The symmetric group S_n is the group of permutations of the set $\{1, \dots, n\}$. A famous result of group theory is that any group is isomorphic to a subgroup of some symmetric group. It has a notable subgroup, the alternating group A_n, which is a normal subgroup of index 2 and constitutes the first family of finite simple groups for $n \geq 5$.

It is a well known fact on the symmetric group S_n that every element is conjugate to all the elements of S_n of the same order.

Proposition 5.3. *All conjugacy classes of S_n are rational.*

Proof. By Proposition 3.1 it suffices to show that for any $g \in S_n$ and any $k \in \mathbb{Z}$ such that $(k, |S_n|) = 1$, g is conjugate to g^k. By basic group theory one has that since k is coprime to the order of g, g^k has the same order as g and then g and g^k are conjugate by the previous comment. We are done. □

Proposition 5.4. *Let kA denote the conjugacy class of elements of order k in S_n. Then $v = (2A, nA, (n-1)A)$ is a strictly rigid vector of conjugacy classes.*

Proof. First of all, if we have a triple $(x, y, z) \in \overline{A}(v)$, we have that $xy = z^{-1}$ and then xy must have order $n - 1$. Observe that for any permutation $(ij) \in 2A$, having that $(ij)y \in (n-1)A$ for $y \in nA$ means that i and j occur consecutively in y, otherwise the resulting permutation has order $n-2$. Since we can write permutations beginning with any element in their expression, the resulting permutations in nA that give elements in $(n-1)A$ are of the form

$$(ij...) \text{ or } (ji...).$$

Since they have order n, there are exactly $(n-2)!$ different ways of *filling the dots*, and for any such way, the resulting permutations are clearly different. Since we have $\binom{n}{2}$ trasposition in S_n, we have $2(n-2)!\binom{n}{2} = n!$ elements in $\overline{A}(v)$, so $|\overline{A}(v)| = |S_n|$.

It is well known that (12) and $(12...n)$ generate S_n. Consider a triple $((ij), y, z) \in \overline{A}(v)$. Viewing S_n as the set of permutations fo n elements, it is clear that we can relabel the elements $\{1, ..., n\}$ by setting $k \mapsto y(k)$ $1 \leq k \leq n$. This transforms (12) into (ij) and $(12...n)$ into y. Hence $(ij), y, z$ generates the group of symmetries of these new relabeled n elements which of course is isomorphic to S_n. □

Proposition 5.5. *The groups S_n have trivial center for $n \geq 3$.*

Proof. Suppose $1 \neq x \in Z(S_n)$. Then there exist $i \neq j \in \{1, \dots, n\}$ such that $x(i) = j$. Now since $n \geq 3$ there is $k \in \{1, \dots, n\} \setminus \{i, j\}$. Consider the permutation (ik). Recall that permutations are injective so $x(i) \neq x(k)$ and then

$$((ik) \circ x)(i) = j \neq x(k) = (x \circ (ik))(i)$$

so x does not commute with (ik), contradicting the assumption that it is a central element. □

Theorem 5.1. *The group S_n occurs as Galois group over $\mathbb{Q}$.*

Proof. For the case $n = 2$ we have $S_2 \cong C_2$ so this case is trivial. For the remaining cases, Propositions 5.3 and 5.4 together with the fact that S_n has trivial center, the hypothesis of the Basic Rigiditiy Theorem (Theorem 4.2) are verified. □

Corollary 5.1. *The group A_n occurs as Galois group over $\mathbb{Q}$.*

Proof. The alternating group has index 2 in S_n so the result follows by Proposition 5.2. □

It is worth mentioning that these results was proved by Hilbert in [Hil92], long before the Rigidity Method was developed.

5.3 The projective special linear groups $\mathrm{PSL}_2(\mathbb{F}_p)$

The special linear groups $\mathrm{SL}_2(\mathbb{F}_p)$ are the groups of 2×2 matrices of determinant 1 over the finite field $\mathbb{F}_p$. Its center is formed by the matrices $I_2, -I_2$. The projective special linear group is defined by

$$\mathrm{PSL}_2(\mathbb{F}_p) = \mathrm{SL}_2(\mathbb{F}_p)/\langle -I_2 \rangle.$$

The groups $\mathrm{PSL}_2(\mathbb{F}_p)$ are all simple for $p \geq 5$. The order of the groups $\mathrm{PSL}_2(\mathbb{F}_p)$ is exactly $\frac{1}{2}p(p-1)(p+1)$. A complete study of these groups, their conjugacy classes and their character tables was the object of my Bachelor thesis [MM18]. A more concise version of this exploration and computations is done in section 3.9 of [Ree08].

As can be seen in both works, $\mathrm{PSL}_2(\mathbb{F}_p)$ always includes a unique conjugacy class $2A$ of order 2. It is denoted by ω in [Ree08] and depends on the residue of p modulo 4. These groups also include two different conjugacy classes of order p, denoted by pA, pB (which are denoted by $c\langle z\rangle, d\langle z\rangle$ in [MM18] and by u, u' in [Ree08]).

It is easy to check that

$$X = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}, Y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$$

verify

$$XYZ = 1$$

in $\mathrm{PSL}_2(\mathbb{F}_p)$. We have that $X^2 = -I_2$ so X has order 2 in $\mathrm{PSL}_2(\mathbb{F}_p)$. Moreover Y has order p in $\mathrm{PSL}_2(\mathbb{F}_p)$ and it belongs to the class we have denoted by pA.

Finally, by basic number theory we have that 2 is not a quadratic residue modulo p if and only if $p \equiv \pm 3 (\mathrm{mod}\, 8)$. In this case, -2 generates $\mathbb{F}_p^\times$ and then by checking the description of the conjugacy class pB in any of the referenced works one sees that $Z \in pB$.

The subgroup generated by X, Y, Z must have order divisible by both 2 and p. Dickson's famous study of the projective linear groups included the description of its maximal subgroups, and this is explained in modern terms in [Kin05].

By Corollary 2.2 of [Kin05] we have that the only maximal subgroups of $\mathrm{PSL}_2(\mathbb{F}_p)$ which can have order dividing 2 and p are groups of order $\frac{p(p-1)}{2}$, which stabilize a point in the

projective plane $\mathbb{P}_1(\mathbb{F}_p)$. These groups are in fact called Frobenius groups and are denoted by G_p and in fact we have

$$G_p \cong C_p \rtimes (\mathbb{F}_p^\times)^2$$

where C_p denotes a cyclic group of order p (see [Nac14]). Now let (a, b) be coordinates of a point in $\mathbb{P}^1(\mathbb{F}_p)$. We have that a and b can not be 0 simultaneously and that (a, b) is identified with the pairs $(\lambda a, \lambda b)$, $\lambda \in \mathbb{F}_p^\times$. Now

$$X\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a-b \\ 2a-b \end{pmatrix}, Y\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a+b \\ b \end{pmatrix}, Z\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ -2a+b \end{pmatrix}$$

so if X, Y, Z were to stabilize the point of the projective plane represented by (a, b) we would have that either

$$2a - b = 0 = -2a + b$$

and then the second coordinate of all images is 0 so $b = 0$ but since $2a - b = 0$ we have $a = 0$, or $2a - b \neq 0$ and then

$$X\begin{pmatrix} a \\ b \end{pmatrix} = (-1)Z\begin{pmatrix} a \\ b \end{pmatrix}$$

so looking at the first coordinates we have $a - b = -a$ so $2a = b$ and then $2a - b = 0$, contradicting our previous assumption. This shows that X, Y, Z can not stabilize the same point in the projective plane $\mathbb{P}^1(\mathbb{F}_p)$. By the previous comments we have that X, Y, Z can not all be in any maximal subgroup of $\mathrm{PSL}_2(\mathbb{F}_p)$ and then $\langle X, Y, Z\rangle = \mathrm{PSL}_2(\mathbb{F}_p)$. This shows

$$(X, Y, Z) \in A(2A, pA, pB)$$

and in particular $A(2A, pA, pB)$ is nonempty.

Proposition 5.6. *If $p \equiv -3 (\mathrm{mod}\, 8)$, the class vector $(2A, pA, pB)$ is strictly rigid.*

Proof. In this case, the class $2A$ is what we denote in [MM18] by $a^{\frac{p-1}{4}}\langle z\rangle$. The relevant part of the character table of $\mathrm{PSL}_2(\mathbb{F}_p)$ in this case is

	$1A$	pA	pB	$2A$
1_G	1	1	1	1
ξ_1	$\frac{1}{2}(p+1)$	$\frac{1}{2}(1+\sqrt{p})$	$\frac{1}{2}(1-\sqrt{p})$	-1
ξ_2	$\frac{1}{2}(p+1)$	$\frac{1}{2}(1-\sqrt{p})$	$\frac{1}{2}(1+\sqrt{p})$	-1
χ_i	$p+1$	1	1	$2\cdot(-1)^i$

for $1 \leq i \leq \frac{p-5}{4}$. Moreover as seen in [Ree08] we have

$$|2A| = \frac{1}{2}p(p+1), |pA| = \frac{1}{2}(p-1)(p+1) = |pB|.$$

We compute

$$|\overline{A}(2A,pA,pB)| = \frac{p(p-1)^2(p+1)^3}{4p(p-1)(p+1)}\left(1+\frac{p-1}{p+1}+\frac{2}{p+1}\sum_{i=1}^{\frac{p-5}{4}}(-1)^i\right) =$$
$$= \frac{(p-1)(p+1)^2}{4}\left(1+\frac{p-1}{p+1}+\frac{-1-(-1)^{\frac{p-1}{4}}}{p+1}\right) =$$
$$= \frac{(p-1)(p+1)^2}{4}\cdot\frac{2p}{p+1} = \frac{1}{2}p(p-1)(p+1) =$$
$$= |\mathrm{PSL}_2(\mathbb{F}_p)|.$$

□

Example 5.1. In Appendix A.2 we can the character table of one of these groups, the group $\mathrm{PSL}_2(\mathbb{F}_{13})$. The reader can find that the characters included in our character table from Proposition 5.6 are in this case denoted by `X.1`, `X.2`, `X.3`, `X.8` and `X.9` in the GAP table.

Proposition 5.7. *If $p \equiv 3 (\mathrm{mod}\, 8)$, the class vector $(2A, pA, pB)$ is strictly rigid.*

Proof. In this case, the class $2A$ is what we deonte by $b^{\frac{p+1}{4}}$ in [MM18]. The relevant part of the character table of $\mathrm{PSL}_2(\mathbb{F}_p)$ in this case is

	$1A$	pA	pB	$2A$
1_G	1	1	1	1
η_1	$\frac{1}{2}(p-1)$	$\frac{1}{2}(-1+\sqrt{-p})$	$\frac{1}{2}(-1-\sqrt{-p})$	1
η_2	$\frac{1}{2}(p-1)$	$\frac{1}{2}(-1-\sqrt{-p})$	$\frac{1}{2}(-1+\sqrt{-p})$	1
χ_i	$p-1$	-1	-1	$2\cdot(-1)^{i+1}$

for $1 \leq i \leq \frac{p-3}{4}$. Moreover as seen in [Ree08] we have

$$|2A| = \frac{1}{2}p(p-1), |pA| = \frac{1}{2}(p-1)(p+1) = |pB|,$$

and we have that

$$\overline{A}(2A,pA,pB) = \frac{p(p-1)^3(p+1)^2}{4p(p-1)(p+1)}\left(1+\frac{p+1}{p-1}-\frac{2}{p-1}\sum_{i=1}^{\frac{p-3}{4}}(-1)^i\right) =$$
$$= \frac{(p-1)^2(p+1)}{4}\left(1+\frac{p+1}{p-1}-\frac{(-1)-(-1)^{\frac{p+1}{4}}}{p-1}\right) =$$
$$= \frac{(p-1)^2(p+1)}{4}\left(1+\frac{p+1}{p-1}\right) = \frac{(p-1)^2(p+1)}{4}\cdot\frac{2p}{p-1} =$$
$$= \frac{1}{2}p(p-1)(p+1) = |\mathrm{PSL}_2(\mathbb{F}_p)|.$$

□

Example 5.2. In Appendix A.1 we can the character table of one of these groups, the group $\mathrm{PSL}_2(\mathbb{F}_{11})$. It is easy to see that the characters we displayed in Proposition 5.7 are denoted by `X.1`, `X.2`, `X.3`, `X.4` and `X.5` in the GAP table.

Theorem 5.2. *If $p \equiv 3 (\mathrm{mod}\, 8)$, the groups $\mathrm{PSL}_2(\mathbb{F}_p)$ occur as Galois groups over $\mathbb{Q}(\sqrt{-p})$. If $p \equiv -3 (\mathrm{mod}\, 8)$, the groups $\mathrm{PSL}_2(\mathbb{F}_p)$ occur as Galois groups over $\mathbb{Q}(\sqrt{p})$.*

Proof. We have shown that $A(2A, pA, pB)$ is nonempty. Now Propositions 5.6, 5.7 guarantee that the hypothesis of Proposition 3.3 are met. Now the result follows by Theorem 4.3. □

With stronger refinements of the Rigidity Method, Matzat was able to prove the following result in [Mat84].

Theorem 5.3. *If $p \not\equiv \pm 1 (\mathrm{mod}\, 24)$ then the groups $\mathrm{PSL}_2(\mathbb{F}_p)$ occur as Galois groups over $\mathbb{Q}$.*

As we mentioned some pages ago, it was Thompson who introduced the character theoretic criterion we proved in §3. Matzat's proof used stronger results on the structure of the groups $\mathrm{PSL}_2(\mathbb{F}_p)$. However it did allow him to show a more general statement than us. The reader may observe that our result follows from Matzat's. Before Matzat, Shih proved a series of results involving linear groups as Galois groups, including Theorem 5.3. His work is explained in Chapter 5 of [Ser92].

5.4 The group $\mathrm{SL}_2(\mathbb{F}_8)$

The group $\mathrm{SL}_2(\mathbb{F}_8)$ is the group of 2×2 matrices over the field $\mathbb{F}_8$ with determinant 1. It has exactly 504 elements. The center of any matrix group is exactly its subgroup of scalar matrices. An element

$$A = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \in Z(\mathrm{SL}_2(\mathbb{F}_8))$$

must verify $\alpha^2 = 1$, and in characteristic 2 we know that this means $\alpha = 1$. This proves the following result

Proposition 5.8. $Z(\mathrm{SL}_2(\mathbb{F}_8)) = \{1\}$.

In particular $\mathrm{SL}_2(\mathbb{F}_8) \cong \mathrm{PSL}(\mathbb{F}_8)$, and since these are simple then so is $\mathrm{SL}_2(\mathbb{F}_8)$. This group is denoted by $\mathrm{L}_2(8)$ in the ATLAS [CCN+85] and can be found in page 6.

The character table of $\mathrm{SL}_2(\mathbb{F}_8)$ as displayed by [GAP19] can be seen at Appendix A.3. We denote by $9A, 9B, 9C$ the conjugacy classes denoted by `9a`, `9b`, `9c` in the GAP table. These conjugacy classes have all representatives of order 9 and in fact we have the following result.

Proposition 5.9. *The class vector $v = (9A, 9B, 9C)$ is strictly rigid.*

Proof. As shown in Appendix A.3, all these conjugacy classes have centralizers of size 9. This means the size of each conjugacy class is $\frac{504}{9} = 56$. Thus we have all the information we need to compute the size of $\overline{A}(v)$ using the expression of Proposition 3.1. Let $\zeta_9 = e^{\frac{2\pi i}{9}}$. The elements denoted by `A, B, C` in the character table (which we will denote by a, b, c) have values

$$a = -\zeta_9^4 - \zeta_9^5, b = -\zeta_9^2 - \zeta_9^7, c = \zeta_9^2 + \zeta_9^4 + \zeta_9^5 + \zeta_9^7.$$

In the expression we need to compute, the product abc appears, so we need to find its value. We have

$$\begin{aligned} abc &= (-\zeta_9^4 - \zeta_9^5)(-\zeta_9^2 - \zeta_9^7)(\zeta_9^2 + \zeta_9^4 + \zeta_9^5 + \zeta_9^7) = \\ &= 2 + 2\zeta_9 + 2\zeta_9^2 + \zeta_9^3 + 2\zeta_9^4 + 2\zeta_9^5 + \zeta_9^6 + 2\zeta_9^7 + 2\zeta_9^8 \end{aligned}$$

and since ζ_9 is a primitive root of unity, we have that $1 + \zeta_9 + \cdots + \zeta_9^8 = 0$ and then we can simplify the above expression to

$$abc = -\zeta_9^3 - \zeta_9^6.$$

However, ζ_9 is a root of the cyclotomic polynomial $\Phi_9(x) = x^6 + x^3 + 1$ proving that

$$abc = 1.$$

With this value known we may proceed with our computation. We have

$$|\overline{A}(v)| = \frac{56^3}{504}\left(1 + \frac{1}{7} + \frac{1}{7} + \frac{1}{7} + \frac{1}{7} - \frac{1}{8} + 0 + 0 + 0\right) = 504 = |\mathrm{SL}_2(\mathbb{F}_8)|.$$

What is left is to show that any triple $(x, y, z) \in \overline{A}(v)$ generates $\mathrm{SL}_2(\mathbb{F}_8)$. Suppose this is false, then there is a triple $x, y, z \in \mathrm{SL}_2(\mathbb{F}_8)$ which generates a proper subgroup of $\mathrm{SL}_2(\mathbb{F}_8)$. As displayed in page 6 of the ATLAS [CCN+85], we have that the only maximal subgroups of $\mathrm{SL}_2(\mathbb{F}_8)$ which contain elements of order 9 are isomorphic to the dihedral group of 9 elements D_{18} (this groups are sometimes written as $D_{2\cdot 9}$). Thus necessarily the subgroup generated by x, y, z must be isomorphic to a subgroup of D_{18}.

We abuse notation by writing $D_{18} \leq \mathrm{SL}_2(\mathbb{F}_8)$ and then $x, y, z \in D_{18}$. Since x is of order 9 we have $\langle x \rangle$ is a subgroup of index 2 in D_{18} and by the structure of the dihedral groups (see for example Chapter I, Section 6 of [Hun74]), all elements of order 9 belong to $\langle x \rangle$. This proves $y, z \in \langle x \rangle$. In other words, $y = x^k, z = x^m$ and since their order is 9 we have $m, k \neq 3, 6$ and given that $y \neq x \neq z$ we have

$$y, z \in \{x^2, x^{-2}, x^4, x^{-4}\}$$

and since y, z belong to distinct conjugacy classes, clearly $y \neq z$. In any of the possible cases we have

$$xyz = x^{1+m+k} \neq 1,$$

contradicting the fact that $(x, y, z) \in \overline{A}(v)$. This shows that all 3-tuples in $\overline{A}(v)$ generate $\mathrm{SL}_2(\mathbb{F}_8)$ and then $|A(v)| = \overline{A}(v) = |\mathrm{SL}_2(\mathbb{F}_8)|$ and v is strictly rigid. □

Theorem 5.4. *The group* $\mathrm{SL}_2(\mathbb{F}_8)$ *occurs as Galois group over the cyclotomic field* $\mathbb{Q}(\zeta_9)$.

Proof. Propositions 5.8 and 5.9 ensure that $\mathrm{SL}_2(\mathbb{F}_8)$ verifies the hypothesis of Theorem 4.3. The base field $\mathbb{Q}_v$ for the class vector $v = (9A, 9B, 9C)$ is exactly $\mathbb{Q}(\zeta_9)$, as can be seen from the character table in Appendix A.3. □

5.5 The Tits group ${}^2\mathrm{F}_4(2)'$

The Tits group is a simple group of order

$$2^{11} \cdot 3^3 \cdot 5^2 \cdot 13 = 17971200.$$

In general, the Ree groups ${}^2\mathrm{F}_4(2^{2n+1})$ were constructed by Ree (see [Ree61]). Jacques Tits proved that ${}^2\mathrm{F}_4(2)$ is almost simple and that its derived subgroup, ${}^2\mathrm{F}_4(2)'$ is simple (see [Tit64]). It is sometimes considered the 27th sporadic group and it is included in pages 74-75 of the ATLAS [CCN+85]. A common presentation of ${}^2\mathrm{F}_4(2)'$ is

$${}^2\mathrm{F}_4(2)' \cong \langle a, b \mid a^2 = b^3 = (ab)^{13} = [a,b]^5 = [a, bab]^4 = ((ab)^4 ab^{-1})^6 = 1 \rangle.$$

Its character table can be seen in Appendix A.4. We denote by $2A, 5A, 13A$ the conjugacy classes denoted by `2a, 5a, 13a` in the table.

Proposition 5.10. *The class vector* $v = (2A, 5A, 13A)$ *is rigid.*

Proof. In its character table we have the size of the centralizers of each conjugacy class, so we find the sizes of the classes

$$|2A| = \frac{17971200}{10240} = 1755, |5A| = \frac{17971200}{50} = 359424, |13A| = \frac{17971200}{13} = 1382400.$$

We compute the expression from Proposition 3.1. We have

$$\overline{A}(v) = \frac{1755 \cdot 359424 \cdot 1382400}{17971200} \left(1 + \frac{-10}{27} + \frac{-10}{27} + \frac{192}{1728}\right) = 17971200 = |{}^2\mathrm{F}_4(2)'|.$$

Now since $2, 5, 13$ are pairwise coprime, by Proposition 5.1 we have that any triple in $\overline{A}(v)$ generates a perfect subgroup $H \leq {}^2\mathrm{F}_4(2)'$. The maximal subgroup structure of ${}^2\mathrm{F}_4(2)'$ is also shown in page 74 of the ATLAS. From all of the maximal subgroups shown, only onehas order dividing $2, 5$ and 13, which is $\mathrm{PSL}_2(\mathbb{F}_{25})$, denoted by $\mathrm{L}_2(25)$ in ATLAS notation. We have that either $H \leq \mathrm{PSL}_2(\mathbb{F}_{25})$ or $H = {}^2\mathrm{F}_4(2)'$ (we abuse the notation and view $\mathrm{PSL}_2(\mathbb{F}_{25})$ as a subgroup of ${}^2\mathrm{F}_4(2)'$).

By Corollary 2.2 of [Kin05] we have that there is no proper subgroup of $\mathrm{PSL}_2(\mathbb{F}_{25})$ with order divisible by $2, 5$ and 13 that is perfect, leaving $H = \mathrm{PSL}_2(\mathbb{F}_{25})$ and $H = {}^2\mathrm{F}_4(2)'$ as the only options left.

The group $\mathrm{PSL}_2(\mathbb{F}_{25})$ is included in page 16 of the ATLAS, and we can see that it has only one conjugacy class of order 2. Its centralizer has order 24. Let $g \in 2A$. We have that

if $H = \mathrm{PSL}_2(\mathbb{F}_{25})$ then $g \in \mathrm{PSL}_2(\mathbb{F}_{25})$ and then g belongs to the only conjugacy class of $\mathrm{PSL}_2(\mathbb{F}_{25})$ of elements of order 2. Then

$$|C_{\mathrm{PSL}_2(\mathbb{F}_{25})}(g)| = 24$$

and we have that

$$|C_{^2\mathrm{F}_4(2)'}(g)| = 10240.$$

Now, if an element of $\mathrm{PSL}_2(\mathbb{F}_{25})$ centralizes g in $\mathrm{PSL}_2(\mathbb{F}_{25})$ then it must also centralize g in ${}^2\mathrm{F}_4(2)'$. Hence

$$C_{\mathrm{PSL}_2(\mathbb{F}_{25})}(g) \leq C_{^2\mathrm{F}_4(2)'}(g).$$

However 24 does not divide 10240, which is a contradiction. This shows that necessarily $H = {}^2\mathrm{F}_4(2)'$ and then $A(v) \neq \emptyset$ so by Proposition 3.3 we are done. □

Now from the character table of ${}^2\mathrm{F}_4(2)'$ we see that $2A$ and $5A$ are rational and $13A$ has two characters with values in $\mathbb{Q}(\sqrt{13})$. This proves the following result

Theorem 5.5. *The Tits group ${}^2\mathrm{F}_4(2)'$ occurs as Galois group over $\mathbb{Q}(\sqrt{13})$.*

5.6 Some sporadic groups

The sporadic groups are the 26 simple groups which appeared in the Classification of Finite Simple Groups which were not alternating groups or groups of Lie type. Six of these are called the Pariahs, given that they do not occur as subquotients (quotients of subgroups) of the most notable sporadic group: the Monster group. The remaining 20 sporadic groups were called the Happy Family by Robert Griess.

The *modus operandi* for these groups will be as in the previous sections. We compute the expression given by Proposition 3.1. After checking that it coincides with the order of the group, we try to prove that no triples in $\overline{A}(v)$ generate a proper subgroup by looking at the structure of the maximal subgroups given by the ATLAS [CCN+85].

5.6.1 The Mathieu group M_{11}

The sporadic group M_{11} is the smallest sporadic group. It has order

$$7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11.$$

Mathieu studied the group M_{11} as a stabilizer of a point of the second Mathieu group, M_{12}. A straightforward presentation of M_{11} is

$$\mathrm{M}_{11} \cong \langle a, b, c, \mid a^{11} = b^5 = c^4 = (ac)^3 = 1, b^{-1}ab = a^4, c^{-1}bc = b^2 \rangle.$$

It is a subquotient of the Griess-Fischer Monster group.

Its character table can be found in Appendix A.5. We see that M_{11} has conjugacy classes of orders 2, 4 and 11, denoted by `2a, 4a, 11a`, which we denote by $2A, 4A, 11A$. Given

the relatively small size of the table of M_{11}, the sum of the expression of $|\overline{A}(2A, 4A, 11A)|$ given by Theorem 3.1 is easy to compute. Since we have the values of the centralizers, we conclude

$$|2A| = 165, |4A| = 990, |11A| = 720$$

and then

$$|\overline{A}(2A, 4A, 11A)| = \frac{165 \cdot 990 \cdot 720}{7920}\left(1 - \frac{2}{5} - \frac{3}{45}\right) = 7920 = |\mathrm{M}_{11}|.$$

This group is included in page 18 of the ATLAS [CCN+85]. Its maximal subgroups are displayed there, and given their orders, the only one which can include an element of order 11 is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_{11})$ (which the ATLAS denotes as $\mathrm{L}_2(11)$).

However the code `Exponent(PSL(2, 11))` in [GAP19] returns 330 as the exponent of this group, that is, the lowest common multiple of the orders of all its elements. Since 4 does not divide 330 we conclude that the elements of $4A$ can not belong in any maximal subgroup of M_{11} that is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_{11})$, thus proving that any triple in $\overline{A}(2A, 4A, 11A)$ generates M_{11}.

Furthermore observe that the values of the irreducible characters of M_{11} for these conjugacy classes all live in $\mathbb{Q}(\sqrt{-11})$. We have proved the following result.

Theorem 5.6 (Matzat, 1979)**.** *The group* M_{11} *occurs as Galois group over the field* $\mathbb{Q}(\sqrt{-11})$.

For Matzat's proof see [Mat79]. The will to realize it as Galois group over $\mathbb{Q}$ led him to find stronger versions of the Rigidity Theorem which would allow for these realizations even if the values of the characters were not necessarily rational. It was not until 8 years later that he would publish a realization over $\mathbb{Q}$ (see [MZM87]). The stronger techniques used here are explained in [Mat87] and later sections of [MM99].

5.6.2 The Mathieu group M_{22}

The automorphism group $\mathrm{Aut}(G)$ of any finite group G includes a notable normal subgroup, the subgroup of inner automorphisms, i.e. automorphisms that can be written as conjugation by an element of G, denoted by $\mathrm{Inn}(G)$. This group is particularly interesting as it is isomorphic to $G/Z(G)$ (we map any element g to the inner automorphism defined as conjugation by g and the kernel turns out to be $Z(G)$). For simple groups we have $G \cong \mathrm{Inn}(G)$. The group

$$\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$$

is called the group of outer automorphisms of G.

The group M_{22} is the third Mathieu group. It is a group of order

$$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 443520$$

and it was introduced by Mathieu as a permutation group on 22 objects. It is a subquotient of the Monster group. It is included in pages 39-41 of the ATLAS [CCN+85], where it is

shown that $|\operatorname{Out}(\mathrm{M}_{22})| = 2$. In other words, $\operatorname{Aut}(\mathrm{M}_{22})/\operatorname{Inn}(\mathrm{M}_{22})$ is a cyclic group of order 2, so $\operatorname{Aut}(\mathrm{M}_{22})$ is an extension of degree 2 of $\operatorname{Inn}(\mathrm{M}_{22}) \cong \mathrm{M}_{22}$. We write $\operatorname{Aut}(\mathrm{M}_{22}) = \mathrm{M}_{22}.2$ to denote this. We view M_{22} as a subgroup of $\mathrm{M}_{22}.2$ and of course M_{22} has index 2 in $\mathrm{M}_{22}.2$ and in particular $\mathrm{M}_{22} \trianglelefteq \mathrm{M}_{22}.2$.

It is also seen in the atlas that all conjugacy classes of M_{22} are conjugacy classes of $\mathrm{M}_{22}.2$ except the one denoted by $11B$. We display the character table of $\operatorname{Aut}(\mathrm{M}_{22}) = \mathrm{M}_{22}.2$ in Appendix A.6. In here, the first 11 columns correspond to the conjugacy classes of $\mathrm{M}_{22}.2$ which are also conjugacy classes of M_{22} (see [CCN+85]). We denote by $2B, 4C, 11A$ the conjugacy classes denoted by `2b`, `4c` and `11a` in the table and we see that only $11A$ is also a conjugacy class of M_{22}.

Proposition 5.11. *The class vector* $(2B, 4C, 11A)$ *of* $\operatorname{Aut}(\mathrm{M}_{22})$ *is rigid.*

Proof. The sizes of the centralizers of these conjugacy classes are displayed in Appendix A.6, so we can compute the sizes of the conjugacy classes

$$|2B| = \frac{2 \cdot 443520}{1344} = 660, |4C| = \frac{2 \cdot 443520}{48} = 18480, |11A| = \frac{2 \cdot 443520}{22} = 40320.$$

We compute

$$\begin{aligned}\overline{A}(2B, 4C, 11A) &= \frac{660 \cdot 18480 \cdot 40320}{2 \cdot 443520}\left(1 + 1 + \frac{7}{21} + \frac{7}{21} + \frac{9}{45} + \frac{9}{45} + \frac{9}{45} + \frac{9}{45} + \frac{-28}{210}\right) = \\ &= 2 \cdot 443520 = |\operatorname{Aut}(\mathrm{M}_{22})|.\end{aligned}$$

Now the maximal subgroups of $\operatorname{Aut}(\mathrm{M}_{22})$ are listed in the ATLAS as well and we see that the only one with order divisible by 11 is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_{11}).2 \cong \mathrm{PGL}_2(\mathbb{F}_{11})$ (using the same notation for the extensions of order 2). Again we identify $\mathrm{PSL}_2(\mathbb{F}_{11})$ and $\mathrm{PGL}_2(\mathbb{F}_{11})$ as subgroups of $\operatorname{Aut}(\mathrm{M}_{22})$ and it is also specified in the ATLAS that

$$\mathrm{M}_{22} \cap \mathrm{PGL}_2(\mathbb{F}_{11}) = \mathrm{PSL}_2(\mathbb{F}_{11}).$$

Let H be the subgroup generated by a triple in $\overline{A}(2B, 4C, 11A)$. Since the order of H divides 11 we have that either $H \leq \mathrm{PGL}_2(\mathbb{F}_{11})$ or $H = \operatorname{Aut}(\mathrm{M}_{22}) = \mathrm{M}_{22}.2$.

Suppose that $H \leq \mathrm{PGL}_2(\mathbb{F}_{11})$. Let $g \in 2B$. We have that $g \in \mathrm{M}_{22}.2$ but $g \notin \mathrm{M}_{22}$. Hence $g \in \mathrm{PGL}_2(\mathbb{F}_{11})$ but $g \notin \mathrm{PSL}_2(\mathbb{F}_{11})$.

The groups $\mathrm{PSL}_2(\mathbb{F}_{11})$ and $\mathrm{PGL}_2(\mathbb{F}_{11})$ are included in page 7 of the ATLAS and we can see that $\mathrm{PGL}_2(\mathbb{F}_{11})$ only has one conjugacy class of elements of order 2 which is not in $\mathrm{PSL}_2(\mathbb{F}_{11})$, and its centralizer in $\mathrm{PGL}_2(\mathbb{F}_{11})$ has order 10. Now doing the same argument of the centralizers as we did in the proof of Proposition 5.10 we have that 10 would have to divide the order of the centralizer of g in $\operatorname{Aut}(\mathrm{M}_{22})$. However, the order of this centralizer is 1344 (see Appendix A.6). This yields a contradiction, and we have that $H = \operatorname{Aut}(\mathrm{M}_{22})$. By Proposition 3.3 we have that $(2B, 4C, 11A)$ is rigid. □

As a corollary of the previous proposition we have the following result.

Theorem 5.7. *The groups* $\mathrm{Aut}(\mathrm{M}_{22})$ *and* M_{22} *occur as Galois groups over* $\mathbb{Q}$.

Proof. As seen in Appendix A.6 the values of the characters of the conjugacy classes $2B, 4C, 11A$ are all rational, so by Proposition 5.11 we have that the hypothesis of Theorem 4.2 are met and then $\mathrm{Aut}(\mathrm{M}_{22})$ occurs a Galois group over $\mathbb{Q}$.

Now given that we found a rationally rigid triple for $\mathrm{Aut}(\mathrm{M}_{22})$ and that the index of M_{22} in $\mathrm{Aut}(\mathrm{M}_{22})$ is 2, by Proposition 5.2 we have that M_{22} also occurs as Galois group over $\mathbb{Q}$. □

5.6.3 The Hall-Janko group J_2

The group J_2 is the second of the four Janko groups, also called the Hall-Janko group and occasionally denoted HJ. It is a sporadic group of order $604800 = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7$ and it is included in page 42 of the ATLAS [CCN+85]. It is in fact the only one of the Janko groups which also occurs as a subquotient of the Monster group. Its most straightforward presentation is

$$\mathrm{J}_2 \cong \langle a, b, u, v \mid u = ab, v = ab^{-1}, a^2 = b^3 = u^1 5 = (u^4 v^2 u^3 v^3)^2 = (u^3 v (u^2 v^2)^2)^2 = 1 \rangle.$$

As can be seen in its character table in Appendix A.7 it has four conjugacy classes of order 5 and one of order 7. We consider the class vector $(5A, 5B, 7A)$ picking the conjugacy classes denoted by `5a, 5b, 7a` in the character table.

The sum for $|\overline{A}(5A, 5B, 7A)|$ is easy given that a lot of the character values in $7A$ are zero. The sizes of the conjugacy classes are

$$|5A| = |5B| = \frac{604800}{300} = 2016, |7A| = \frac{604800}{7} = 86400.$$

Then we have that

$$|\overline{A}(5A, 5B, 7A)| = \frac{2016^2 \cdot 86400}{604800} \left(1 + \frac{16}{36} + \frac{-25}{90} + \frac{-25}{160} + \frac{9}{225}\right) = 604800 = |\mathrm{J}_2|.$$

Since H contains elements of orders 5 and 7 (for instance g and k) we have that both 5 and 7 must divide the order of H. However we check the maximal subgroups of J_2 in the ATLAS and find that there is no maximal subgroup of order divisible by 5 and 7 at the same time. This proves $H = \mathrm{J}_2$ and then $(5A, 5B, 7A)$ is rigid. Since the values of the irreducible characters in these conjugacy classes values in $\mathbb{Q}(\zeta_5)$, so we have proved that

Theorem 5.8. *The group* J_2 *occurs as Galois group over* $\mathbb{Q}(\zeta_5)$.

§6 Final comments

The Rigidity Method has proved to be a very successful solution to the inverse problem. In fact, it attacked the problem from the perspective of a type of groups for which the problem was far from solved: simple groups and groups with trivial center.

When the first results came to light thanks to the work of number theorists such as Matzat, a wide number of group theorists jumped on the problem as it had somewhat turned into a group theoretic *game*. As mentioned during this work, John Thompson published in 1984 the character-theoretic criterion we explained. But that was not his only great achievement. As a proof of the power of the method and his criterion, he realized the Fischer-Griess Monster group, the biggest of the sporadic groups, as Galois group over the rationals. Even more surprising is the fact that this was before any other sporadic group had been realized as sporadic group over the rationals.

After the publication of Thompson's paper [Tho84c], a great amount of simple groups were proven to be Galois groups over $\mathbb{Q}$. For instance, W. Feit, P. Fong and Thompson himself used this results for Lie type groups (see for example [FFS84] and [Tho84b]). However, possibly one of the greatest achievements of the method was the realization of most sporadic groups as Galois groups over $\mathbb{Q}$, completed by David Hunt (see [Hun86]). He achieved a realization for all sporadic groups except the Mathieu group M_{23}.

And even though the method has proved greatly successful, it still has an enormous failure: the absence of a realization of M_{23} over the rationals. It has been realized over $\mathbb{Q}(\sqrt{-23})$ but that is as far down as it has been possible (Chapter II, Theorem 9.9 of [MM99]). No other method has been able to find a Galois extension of $\mathbb{Q}$ with Galois group M_{23}. Right now, the Inverse Problem of Galois Theory is in need of a great idea to be pushed forward. Perhaps M_{23} is in fact the group that proves that the Inverse Problem has a negative solution. But what is so special about M_{23}?

The solutions given by the Rigidity Method have been used in an attempt to realize central extensions $\tilde{G}$ of simple groups G. Relevant results include the realization of $\tilde{A}_n$ as Galois group over $\mathbb{Q}$ (see [Vil85]) and $\tilde{\mathrm{M}}_{12}$ (see [BLV86]). Some of these techniques are explained in the final chapters of [Ser92].

Finally, it is worth mentioning that another recent method towards the solution of the Inverse Galois Problem over $\mathbb{Q}$ include the use of points of finite order of elliptic curves an their automorphism groups, which can be naturally viewed inside Galois groups over the field of definition of the curve.

§A Character Tables

The character tables are too big to be included in the middle of the text and are included in this appendix. The tables in this section are taken from [GAP19].

GAP notation

In general, GAP displays character tables very similarly to the ATLAS [CCN+85]. The elements marked by `X.k` denote irreducible characters, and the columns denoted by `1a, 3a, 9a, 9b`... denote conjugacy classes (the number denoting the order of any element of the conjugacy class). Right above the conjugacy class notation, the size of the centralizer of each conjugacy class may be included as can be seen in the ATLAS. The actual output given by GAP gives much more informaton, some of which was omitted to ease the comprehension of the tables. For complex character values, GAP writes `E(n)` for the primitive nth root of unity $e^{\frac{2\pi i}{n}}$, and by `ER(x)` the square root of x. The dots in the character table denote zeros.

A.1 Characters of $\mathrm{PSL}_2(\mathbb{F}_{11})$

```
      1a 5a 5b 11a 11b 2a 3a 6a

X.1    1  1  1   1   1  1  1  1
X.2    5  .  .   B  /B  1 -1  1
X.3    5  .  .  /B   B  1 -1  1
X.4   10  .  .  -1  -1 -2  1  1
X.5   10  .  .  -1  -1  2  1 -1
X.6   11  1  1   .   . -1 -1 -1
X.7   12  A *A   1   1  .  .  .
X.8   12 *A  A   1   1  .  .  .

A = E(5)^2+E(5)^3
  = (-1-ER(5))/2 = -1-b5
B = E(11)+E(11)^3+E(11)^4+E(11)^5+E(11)^9
  = (-1+ER(-11))/2 = b11
```

A.2 Characters of $\mathrm{PSL}_2(\mathbb{F}_{13})$

```
      1a 2a 3a 6a 7a 7b 7c 13a 13b

X.1    1  1  1  1  1  1  1   1   1
X.2    7 -1  1 -1  .  .  .   D  *D
X.3    7 -1  1 -1  .  .  .  *D   D
X.4   12  .  .  .  A  C  B  -1  -1
X.5   12  .  .  .  B  A  C  -1  -1
X.6   12  .  .  .  C  B  A  -1  -1
X.7   13  1  1  1 -1 -1 -1   .   .
X.8   14  2 -1 -1  .  .  .   1   1
X.9   14 -2 -1  1  .  .  .   1   1

A = -E(7)^3-E(7)^4
B = -E(7)^2-E(7)^5
C = -E(7)-E(7)^6
D = -E(13)-E(13)^3-E(13)^4-E(13)^9-E(13)^10-E(13)^12
  = (1-ER(13))/2 = -b13
```

A.3 Characters of $\mathrm{SL}_2(\mathbb{F}_8)$

```
      504 8  9  9  9  9  7  7  7
      1a 2a 3a 9a 9b 9c 7a 7b 7c

X.1    1  1  1  1  1  1  1  1  1
X.2    7 -1 -2  1  1  1  .  .  .
X.3    7 -1  1  A  C  B  .  .  .
X.4    7 -1  1  B  A  C  .  .  .
X.5    7 -1  1  C  B  A  .  .  .
X.6    8  . -1 -1 -1 -1  1  1  1
X.7    9  1  .  .  .  .  D  F  E
X.8    9  1  .  .  .  .  E  D  F
X.9    9  1  .  .  .  .  F  E  D

A = -E(9)^4-E(9)^5
B = -E(9)^2-E(9)^7
C = E(9)^2+E(9)^4+E(9)^5+E(9)^7
D = E(7)^3+E(7)^4
```

```
E = E(7)^2+E(7)^5
F = E(7)+E(7)^6
```

A.4 Characters of ${}^2\mathrm{F}_4(2)'$

```
              10   1
    17971200 240 536 108 192128 64 50 12 32 32 16 16  10  12  12  13  13  16  16  16  16
          1a  2a  2b  3a  4a 4b 4c 5a 6a 8a 8b 8c 8d 10a 12a 12b 13a 13b 16a 16b 16c 16d

X.1        1   1   1   1   1  1  1  1  1  1  1  1  1   1   1   1   1   1   1   1   1   1
X.2       26  -6   2  -1  -2 -2  2  1 -1  .  .  .  .  -1   1   1   .   .   D  -D  -D   D
X.3       26  -6   2  -1  -2 -2  2  1 -1  .  .  .  .  -1   1   1   .   .  -D   D   D  -D
X.4       27  -5   3   .   3 -1 -1  2  .  A /A -1 -1   .   .   .   1   1   E  -E   E  -E
X.5       27  -5   3   .   3 -1 -1  2  . /A  A -1 -1   .   .   .   1   1  -E   E  -E   E
X.6       78  14  -2  -3   2 -2  2  3  1  2  2  .  .  -1  -1  -1   .   .   .   .   .   .
X.7      300 -20  -4   3  -4  4  4  . -1  .  .  .  .   .  -1  -1   1   1   .   .   .   .
X.8      325   5 -11   1   1  5  1  .  1  1  1 -1 -1   .   1   1   .   .  -1  -1  -1  -1
X.9      351  31  15   .   3 -1  3  1  . -1 -1  1  1   1   .   .   .   .  -1  -1  -1  -1
X.10     351  -1  -9   .   3  3 -1  1  .  A /A  1  1  -1   .   .   .   .  -E   E  -E   E
X.11     351  -1  -9   .   3  3 -1  1  . /A  A  1  1  -1   .   .   .   .   E  -E   E  -E
X.12     624 -16  16   3   .  .  . -1  1  .  .  .  .  -1   B  -B   .   .   .   .   .   .
X.13     624 -16  16   3   .  .  . -1  1  .  .  .  .  -1  -B   B   .   .   .   .   .   .
X.14     650  10  10   2   6  2 -2  . -2  2  2  .  .   .   .   .   .   .   .   .   .   .
X.15     675  35   3   .   3  3  3  .  . -1 -1 -1 -1   .   .   .  -1  -1   1   1   1   1
X.16     702  30   6   .  -6  2 -2  2  .  .  .  .  .   .   .   .   .   .   F   F  -F  -F
X.17     702  30   6   .  -6  2 -2  2  .  .  .  .  .   .   .   .   .   .  -F  -F   F   F
X.18    1300  20 -12   4   . -4  .  .  .  .  .  2 -2   .   .   .   .   .   .   .   .   .
X.19    1300  20 -12   4   . -4  .  .  .  .  . -2  2   .   .   .   .   .   .   .   .   .
X.20    1728 -64   .   .   .  .  .  3  .  .  .  .  .   1   .   .  -1  -1   .   .   .   .
X.21    2048   .   . -4   .  .  . -2  .  .  .  .  .   .   .   .   .   C  *C   .   .   .   .
X.22    2048   .   . -4   .  .  . -2  .  .  .  .  .   .   .   .  *C   C   .   .   .   .
```

```
A = -1+2*E(4)
  = -1+2*ER(-1) = -1+2i
B = -E(12)^7+E(12)^11
  = ER(3) = r3
C = -E(13)-E(13)^3-E(13)^4-E(13)^9-E(13)^10-E(13)^12
  = (1-ER(13))/2 = -b13
D = E(8)+E(8)^3
  = ER(-2) = i2
E = -E(4)
  = -ER(-1) = -i
F = E(8)-E(8)^3
  = ER(2) = r2
```

A.5 Characters of M_{11}

```
      7920 48 18  8  5  6  8  8  11  11
        1a 2a 3a 4a 5a 6a 8a 8b 11a 11b

X.1      1  1  1  1  1  1  1  1   1   1
X.2     10  2  1  2  . -1  .  .  -1  -1
X.3     10 -2  1  .  .  1  A -A  -1  -1
X.4     10 -2  1  .  .  1 -A  A  -1  -1
X.5     11  3  2 -1  1  . -1 -1   .   .
X.6     16  . -2  .  1  .  .  .   B  /B
X.7     16  . -2  .  1  .  .  .  /B   B
X.8     44  4 -1  . -1  1  .  .   .   .
X.9     45 -3  .  1  .  . -1 -1   1   1
X.10    55 -1  1 -1  . -1  1  1   .   .

A = E(8)+E(8)^3
  = ER(-2) = i2
B = E(11)+E(11)^3+E(11)^4+E(11)^5+E(11)^9
  = (-1+ER(-11))/2 = b11
```

A.6 Characters of $\mathrm{Aut}(\mathrm{M}_{22})$

Remark A.1. *We only include the relevant centralizer sizes in this case.*

```
                                          22 1344     48
        1a  2a 3a 4a 4b 5a 6a 7a 7b 8a 11a  2b  2c 4c 4d 6b 8b 10a 12a 14a 14b

X.1      1   1  1  1  1  1  1  1  1  1   1   1   1  1  1  1  1   1   1   1   1
X.2      1   1  1  1  1  1  1  1  1  1   1  -1  -1 -1 -1 -1 -1  -1  -1  -1  -1
X.3     21   5  3  1  1  1 -1  .  . -1  -1   7  -1 -1  3  1  1  -1  -1   .   .
X.4     21   5  3  1  1  1 -1  .  . -1  -1  -7   1  1 -3 -1 -1   1   1   .   .
X.5     45  -3  .  1  1  .  .  A /A -1   1   3  -5  3 -1  .  1   .   .   A  /A
X.6     45  -3  .  1  1  .  .  A /A -1   1  -3   5 -3  1  . -1   .   .  -A -/A
X.7     45  -3  .  1  1  .  . /A  A -1   1   3  -5  3 -1  .  1   .   .  /A   A
X.8     45  -3  .  1  1  .  . /A  A -1   1  -3   5 -3  1  . -1   .   . -/A  -A
X.9     55   7  1  3 -1  .  1 -1 -1  1   .  13   5  1  1  1 -1   .   1  -1  -1
X.10    55   7  1  3 -1  .  1 -1 -1  1   . -13  -5 -1 -1 -1  1   .  -1   1   1
X.11    99   3  .  3 -1 -1  .  1  1 -1   .  15  -1  3 -1  . -1  -1   .   1   1
X.12    99   3  .  3 -1 -1  .  1  1 -1   . -15   1 -3  1  .  1   1   .  -1  -1
X.13   154  10  1 -2  2 -1  1  .  .  .   .  14   6  2  2 -1  .   1  -1   .   .
X.14   154  10  1 -2  2 -1  1  .  .  .   . -14  -6 -2 -2  1  .  -1   1   .   .
X.15   210   2  3 -2 -2  . -1  .  .  .   1  14 -10 -2  2 -1  .   .   1   .   .
X.16   210   2  3 -2 -2  . -1  .  .  .   1 -14  10  2 -2  1  .   .  -1   .   .
X.17   231   7 -3 -1 -1  1  1  .  . -1   .   7  -9 -1 -1  1 -1   1  -1   .   .
```

```
X.18    231   7 -3 -1 -1  1  1  .  . -1   .  -7   9  1  1 -1  1 -1   1   .   .
X.19    560 -16  2  .  .  .  2  .  .  .  -1   .   .  .  .  .  .  .   .   .   .
X.20    385   1 -2  1  1  . -2  .  .  1   .  21   5 -3 -3  .  1  .   .   .   .
X.21    385   1 -2  1  1  . -2  .  .  1   . -21  -5  3  3  . -1  .   .   .   .


A = E(7)+E(7)^2+E(7)^4
  = (-1+ER(-7))/2 = b7
```

A.7 Characters of J_2

```
     604800 920 240  80 36 96 300 300  50  50 24 12  7  8  20  20  10  10  12  15  15
        1a  2a  2b  3a 3b 4a  5a  5b  5c  5d 6a 6b 7a 8a 10a 10b 10c 10d 12a 15a 15b

X.1       1   1   1   1  1  1   1   1   1   1  1  1  1  1   1   1   1   1   1   1   1
X.2      14  -2   2   5 -1  2   A  *A   E  *E  1 -1  .  .   G  *G  -G -*G  -1   .   .
X.3      14  -2   2   5 -1  2  *A   A  *E   E  1 -1  .  .  *G   G -*G  -G  -1   .   .
X.4      21   5  -3   3  .  1   B  *B   F  *F -1  .  . -1   G  *G   .   .   1 -*G  -G
X.5      21   5  -3   3  .  1  *B   B  *F   F -1  .  . -1  *G   G   .   .   1  -G -*G
X.6      36   4   .   9  .  4  -4  -4   1   1  1  .  1  .   .   .  -1  -1   1  -1  -1
X.7      63  15  -1   .  3  3   3   3  -2  -2  . -1  .  1  -1  -1   .   .   .   .   .
X.8      70 -10  -2   7  1  2   C  *C   .   . -1  1  .  .  -G -*G   .   .  -1   G  *G
X.9      70 -10  -2   7  1  2  *C   C   .   . -1  1  .  . -*G  -G   .   .  -1  *G   G
X.10     90  10   6   9  . -2   5   5   .   .  1  . -1  .   1   1   .   .   1  -1  -1
X.11    126  14   6  -9  .  2   1   1   1   1 -1  .  .  .   1   1  -1  -1  -1   1   1
X.12    160   .   4  16  1  .  -5  -5   .   .  .  1 -1  .  -1  -1   .   .   .   1   1
X.13    175  15  -5  -5  1 -1   .   .   .   .  3  1  . -1   .   .   .   .  -1   .   .
X.14    189  -3  -3   .  . -3   A  *A   E  *E  .  .  .  1   G  *G   G  *G   .   .   .
X.15    189  -3  -3   .  . -3  *A   A  *E   E  .  .  .  1  *G   G  *G   G   .   .   .
X.16    224   .  -4   8 -1  .   D  *D  -F -*F  . -1  .  .   1   1   .   .   . -*G  -G
X.17    224   .  -4   8 -1  .  *D   D -*F  -F  . -1  .  .   1   1   .   .   .  -G -*G
X.18    225 -15   5   .  3 -3   .   .   .   .  . -1  1 -1   .   .   .   .   .   .   .
X.19    288   .   4   . -3  .   3   3  -2  -2  .  1  1  .  -1  -1   .   .   .   .   .
X.20    300 -20   . -15  .  4   .   .   .   .  1  . -1  .   .   .   .   .   1   .   .
X.21    336  16   .  -6  .  .  -4  -4   1   1 -2  .  .  .   .   .   1   1   .  -1  -1


A = -3*E(5)-3*E(5)^4
  = (3-3*ER(5))/2 = -3b5
B = -3*E(5)-4*E(5)^2-4*E(5)^3-3*E(5)^4
  = (7+ER(5))/2 = 4+b5
C = -5*E(5)-5*E(5)^4
  = (5-5*ER(5))/2 = -5b5
D = 3*E(5)-E(5)^2-E(5)^3+3*E(5)^4
  = -1+2*ER(5) = 1+4b5
  E = -E(5)-2*E(5)^2-2*E(5)^3-E(5)^4
  = (3+ER(5))/2 = 2+b5
F = -2*E(5)-2*E(5)^4
```

```
  = 1-ER(5) = 1-r5
G = E(5)+E(5)^4
  = (-1+ER(5))/2 = b5
```

References

[Bel79] G. V. Belyi. On Galois extensions of a maximal cyclotomic field. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, 43(2):267–276, 1979. 3

[BLV86] P. Bayer, P. Llorente, and N. Vila. $\tilde{M}_1 2$ comme groupe de Galois sur $\mathbb{Q}$. *C. R. Acad. Sc. Paris*, 303:277–280, 1986. 34

[CCN+85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of Finite Groups*. Clarendon Press, Oxford, 1985. 27, 28, 29, 30, 31, 32, 33, 35

[FFS84] W. Feit, P. Fong, and B Srinivasan. Rigidity of $SL_n(q)$ and certain subgroups for $(n, q-1) = 1$ and $n > 2$. *Proceedings of the Rutgers Group Theory Year, 1983-84*, pages 303–308, 1984. 34

[GAP19] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.10.1*, 2019. 11, 19, 27, 31, 35

[Gro61] A. Grothendieck. Revêtements étales et groupe fondamental. *Lecture Notes in Mathematics*, 1961. 6

[Hil92] D Hilbert. Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten. *J. reine angew. Math.*, 110:104–129, 1892. 3, 4, 21, 24

[Hun74] T. W. Hungerford. *Algebra*, volume 73. Springer (Graduate Texts in Mathematics), 1974. 28

[Hun86] D. C. Hunt. Rational rigidity and the sporadic groups. *Journal of Algebra*, 99:577–592, 1986. 34

[Hup67] B. Huppert. *Endliche gruppen I*, volume 134. Springer-verlag, 1967. 20

[Isa94] I. Martin Isaacs. *Character theory of finite groups*, volume 69. Dover Books, 1994. 10, 11

[Kin05] O. King. The subgroup structure of finite classical groups interms of geometric configurations, 2005. Personal Notes. 24, 29

[Mat79] B. H. Matzat. Konstruktion von Zahlkörpern mit der galoisgruppe M_{11} über $\mathbb{Q}(\sqrt{-11})$. *Manuscripta Mathematica - MANUSCR MATH*, 27:103–111, 1979. 31

[Mat84] B. H. Matzat. Konstruktion von Zahl- und Funktionenkörpern mit vorgegebener Galoisgruppe. *J. Reine Agnew. Math.*, 349:179–220, 1984. 3, 27

[Mat87] B. H. Matzat. *Konstruktive Galoistheorie*, volume 1284. Springer, 1987. 31

[MM99] G. Malle and B. H. Matzat. *Inverse Galois Theory*. Springer, 1999. 4, 5, 6, 7, 8, 16, 20, 21, 31, 34

[MM18] J. M. Martínez Marín. Characters of $SL(2,p)$. Bachelor thesis at Universitat de València, 2018. 24, 25, 26

[MZM87] B. H. Matzat and A. Zeh-Marschke. Polynome mit der Galoisgruppe M_{11} über $\mathbb{Q}$. *Journal of symbolic computation*, 4:93–97, 1987. 31

[Nac14] B. Nachman. Generating sequences of $PSL(2,p)$, 2014. `https://arxiv.org/pdf/1210.2073.pdf`. 25

[Neu13] J. Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013. 8

[Ree61] R. Ree. A family of simple groups associated with the simple Lie algebra of type (F_4). *Bull. Amer. Math. Soc.*, 67:115–116, 1961. 29

[Ree08] M. Reeder. Characters of $SL_2(p)$. *Technical report, Boston College*, 2008. 24, 25, 26

[Rei37] H. Reichardt. Konstruktion vol Zahlköpern mit gegebener Galoisgruppe von Primzahlpotenzordnung. *J. Reine Agnew. Math.*, 177:1–5, 1937. 3

[Sch37] A. Scholz. Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung i. *Math. Z.*, 42:161–188, 1937. 3

[Ser71] J. P. Serre. *Linear Representations of Finite Groups*, volume 42. Springer, 1971. 11

[Ser92] J. P. Serre. *Topics in Galois Theory, Volume 1*. Research Notes in Mathematics, 1992. 4, 5, 13, 17, 27, 34

[ST80] H. Seifert and W. Threlfall. *Seifert and Threlfall: A textbook of topology*, volume 89. Academic Press, 1980. 5, 6

[Tho84a] J. G Thompson. Primtive roots and rigidity. *Proceedings of the Rutgers Group Theory Year, 1983-84*, pages 327–350, 1984. 22

[Tho84b] J. G Thompson. PSL_3 and Galois groups over $\mathbb{Q}$. *Proceedings of the Rutgers Group Theory Year, 1983-84*, pages 309–315, 1984. 34

[Tho84c] J. G. Thompson. Some finite groups which appear as $\mathrm{Gal}(L/K)$, where $K \subseteq \mathbb{Q}(\mu_n)$. *Journal of Algebra*, 89 (2):437–499, 1984. 3, 13, 22, 34

[Tit64] J. Tits. Algebraic and abstract simple groups. *Annals of Mathematics*, 80:313?329,, 1964. 29

[Vil85] N. Vila. On central extensions of A_n as Galois group over $\mathbb{Q}$. *Arch. Math.*, 44:424–437, 1985. 34

[Vil92] N. Vila. On the inverse problem of Galois Theory. *Publicacions Matemàtiques*, pages 1053–1073, 1992.

[Vol96] H. Volklein. *Groups as Galois groups: an introduction*. Number 53. Cambridge University Press, 1996. 22

[Š54] I.R. Šafarevič. Construction of fields of algebraic numbers with given solvable Galois group. *Izv. Akad. Nauk SSSR Ser. Mat.*, 18:525–578, 1954. 3, 21