Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea Triennale in Matematica

A dive into the inverse Galois problem

Tesi di Laurea in Algebra

Relatore:
Chiar.ma Prof.ssa
NICOLETTA CANTARINI

Presentata da:
FILIPPO BELFIORI

Sessione Estiva
Anno Accademico 2021/2022

Un matematico è una macchina,
che trasforma caffè in teoremi ...

Introduction

Galois theory was born at the beginning of the 19th century with the studies of Evariste Galois. One of the most important result of this theory is the *Fundamental Theorem of Galois Theory*, which gives a connection between fields and groups. Indeed, given a field extension $\mathbb{F} \subseteq \mathbb{L}$, there exists a group linked to it, which is the Galois group of the extension. It is therefore natural to ask whether it is possible to go through this connection in the opposite direction: given a finite group G, does there exist a Galois extension of $\mathbb{F}$ with Galois group G? Hence the name *Inverse Galois problem*. If we have an affirmative answer, we will say that the group G occurs as a Galois group over a certain field $\mathbb{F}$. In fact, it turns out that the answer to this problem heavily depends on the base field. For example, over finite fields only cyclic groups occur as Galois groups; while over p-adic fields only solvable groups occur as Galois groups. The classical inverse problem takes $\mathbb{Q}$ as the base field, thus the question is: which finite groups can occur as the Galois groups of finite field extensions of $\mathbb{Q}$? Moreover, if there is an affirmative answer for a certain group G, one can go deeper in the problem and find polynomials with coefficients in $\mathbb{Q}$ whose splitting field realizes the desired extension.

Despite the problem is still unsolved, important achievements have been reached so far. One of the first results, dated to the late 1800s, is the realization of all abelian groups, due to Kronecker and Weber. Hilbert made significant progress in the problem, mainly through his *Irreducibility Theorem* ([8]), by which he proved the realization of S_n and A_n as Galois group of field extensions of $\mathbb{Q}$. In 1937 Scholz and Reichardt ([17],[14]) proved that the classical inverse problem has an affirmative answer for any p-group; in 1954 Šafarevič ([16]) proved it for any solvable group. In order to find these realizations the problem has been attacked using the Rigidity Method: since every finite group appears as the Galois group of a polynomial in $\mathbb{C}[t]$ (*Riemann's Existence Theorem* [7]), one imposes condition in order to ensure that the polynomial can be defined in $\mathbb{Q}[t]$; if this process can be done for a certain group G, one can conclude that there exists a Galois extension of $\mathbb{Q}$ with G as Galois group, by Hilbert's Irreducibility Theorem. Other significant methods have been used through the years, such as geometric methods involving elliptic curves (see, for example, [15],[20]). The problem is still unsolved, for example, for simple groups. Most of them have been realized as Galois group over $\mathbb{Q}$, such as M_{11}, M_{12}, M_{22} and M_{24} ([10]); also for the monster group the answer is affirmative ([21]). However it

is unknown whether groups of type Lie and the Mathieu group M_{23} can occur as Galois group of an extension of $\mathbb{Q}$.

This thesis is focused on the realization of some classes of groups, and is organized as follows:

- In Chapter 1 we collect some important results in Galois theory.
- In Chapter 2 we show how to realize every group as the Galois group of some Galois extension, without requiring $\mathbb{Q}$ as the base field, i.e., we face the so-called "weak" problem.
- Chapter 3 is dedicated to the realization of the groups $(\mathbb{Z}_n)^*$, the cyclic groups and the abelian groups as Galois group of an extension of $\mathbb{Q}$.
- In Chapter 4 we collect some results in group theory and using Dedekind's Theorem we show that the symmetric group S_n occurs as a Galois group over $\mathbb{Q}$.
- Finally in Chapter 5 we collect some explicit examples of realization of Galois groups over $\mathbb{Q}$. In particular we show how to realize every group of order at most 8 and also the general affine group $\mathrm{AGL}(1, \mathbb{F}_p)$.

Notation

Throughout these notes, p will be a prime number. Given a set S, we shall denote by $|S|$ its cardinality. We shall use the following standard (Bourbaki) notation:

- S_n = Symmetric group,
- A_n = Alternating group,
- $\mathbb{Z}$ = Ring of integers,
- $\mathbb{Z}^+$ = Positive integers,
- $\mathbb{Q}$ = Field of rational numbers,
- $\mathbb{R}$ = Field of real numbers,
- $\mathbb{C}$ = Field of complex numbers,
- $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = C_n$ = Cyclic group of n elements,
- $(\mathbb{Z}/n\mathbb{Z})^*$ = multiplicative group of $\mathbb{Z}_n$,
- $V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$ = Klein group,
- Q_8 = Quaternion group,
- $[a]_n$ = Residue class modulo n of a,
- $X \subseteq Y$: X is a subset of Y,
- $X \subset Y$: X is a proper subset of Y,
- $X \cong Y$: group isomorphism between X and Y,
- $H \leq G$: H is a subgroup of G,
- $H \trianglelefteq G$: H is a normal subgroup of G,
- $[G : H]$: the index of H in G,
- $A \oplus B$: direct sum.

Contents

Introduction **I**

1 Galois theory **1**
1.1 Preliminaries 1

2 Weak problem **5**
2.1 Cayley's Theorem 5
2.2 Universal extension 6
2.3 Universal realization of a finite group 8

3 Classical inverse problem **9**
3.1 Cyclotomic polynomials 9
3.2 Cyclic groups 10
3.3 Abelian groups 13

4 Symmetric groups **19**
4.1 Class Equation 19
4.2 Transitive group action 23
4.3 Dedekind's Theorem 26
4.4 Realization of S_n 29
4.5 Consideration 30

5 Examples **33**
5.1 The groups A_3 and S_3 33
5.2 Ordered Examples 37
5.2.1 Order 1 38
5.2.2 Order 2 38
5.2.3 Order 3 38
5.2.4 Order 4 40
5.2.5 Order 5 42
5.2.6 Order 6 42

5.2.7 Order 7 42
5.2.8 Order 8 43
5.3 The group $\mathrm{AGL}(1, \mathbb{F}_p)$ 46

Bibliography **50**

Chapter 1

Galois theory

"Il passato è sale e si scioglie,
ma dà sapore al futuro"

In this chapter we collect some preliminary fundamental results in Galois theory that we will use in the sequel. For all details we refer to [1] and [12].

1.1 Preliminaries

Let $\mathbb{F}$ be a field.

Definition 1.1. A polynomial $f(x) \in \mathbb{F}[x]$ is said to be *separable* if it has no multiple roots in a splitting field over $\mathbb{F}$.

Example 1.2. The polynomial $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ is separable, indeed $f(x)$ splits in $\mathbb{C}[x]$ and its roots are $\sqrt[3]{2}$, $\xi_3\sqrt[3]{2}$ and $\xi_3^2\sqrt[3]{2}$, where ξ_3 is a primitive 3-th root of unity.

Example 1.3. If $\mathbb{K}$ is a field of characteristic p, then $\mathbb{F} := \mathbb{K}(t)$ is an infinite field of characteristic p. The polynomial $f(x) = x^p - t \in \mathbb{F}[x]$ is not separable, since if α is a root of f in a splitting field over $\mathbb{F}$, we have

$$x^p - t = x^p - \alpha^p = (x - \alpha)^p$$

hence α is a multiple root.

Definition 1.4. A field $\mathbb{F}$ is said to be *perfect* if every irreducible polynomial $f(x) \in \mathbb{F}[x]$ is separable.

Proposition 1.5. *Fields of characteristic* 0 *are perfect, in particular* $\mathbb{Q}$ *is a perfect field. Moreover, finite fields are perfect.*

Definition 1.6. (**Galois Group**)
For a field extension $\mathbb{F} \subseteq \mathbb{K}$ we consider the following subset of $\mathrm{Aut}(\mathbb{K})$:

$$\mathrm{Gal}(\mathbb{K}/\mathbb{F}) = \{\varphi \in \mathrm{Aut}(\mathbb{K}) \mid \varphi(a) = a,\ \forall\ a \in \mathbb{F}\}$$

i.e., the set of $\mathbb{K}$-automorphisms that fix the field $\mathbb{F}$.

Remark 1.7. $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ *is a subgroup of* $(\mathrm{Aut}(\mathbb{K}), \circ)$.

Given a subgroup $H \leq \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ we will denote the set of its fixed points by

$$\mathbb{K}^H = \{a \in \mathbb{K} \mid \varphi(a) = a,\ \forall\ \varphi \in H\}\,.$$

Given a field $\mathbb{F}$, for a polynomial $f \in \mathbb{F}[x]$ we define

$$\mathrm{Gal}_{\mathbb{F}}(f) := \mathrm{Gal}(\mathbb{K}/\mathbb{F}), \tag{1.1}$$

where $\mathbb{K}$ is the splitting field of f. We will often use $\mathrm{Gal}(f)$ instead of $\mathrm{Gal}_{\mathbb{F}}(f)$ when the base field is clear.

Proposition 1.8. *Let $\mathbb{F} \subseteq \mathbb{K}$ be a finite and simple field extension. If $[\mathbb{K} : \mathbb{F}] = n$ then $|\,\mathrm{Gal}(\mathbb{K}/\mathbb{F})| \leq n$.*

Proposition 1.9. *Let f be a polynomial of degree n, then $\mathrm{Gal}(f)$ is isomorphic to a subgroup of S_n.*

We know that any automorphism $\sigma \in \mathrm{Gal}(f)$ maps a root of an irreducible factor of f to another root of the same irreducible factor, and σ is uniquely determined by its action on these roots. In general, if f factorizes as $f(x) = f_1(x)f_2(x)\dots f_k(x)$, where $f_i(x)$ has degree n_i, $i = 1, 2, \dots, k$, then since the Galois group permutes the roots of the irreducible factors, we have

$$\mathrm{Gal}(f) \leq S_{n_1} \times \ldots \times S_{n_k}.$$

Theorem 1.10. *Let $\mathbb{F} \subseteq \mathbb{K}$ be a finite field extension, then the following conditions are equivalent:*

a) $\mathbb{K}$ *is the splitting field of a separable polynomial with coefficients in* $\mathbb{F}$*;*

b) $\mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{F})} = \mathbb{F}$*;*

c) the extension is normal and separable;

d) $|\,\mathrm{Gal}(\mathbb{K}/\mathbb{F})| = [\mathbb{K} : \mathbb{F}]$.

If any of the above conditions occurs we will say that $\mathbb{F} \subseteq \mathbb{K}$ is a *Galois extension.*

Proposition 1.11. *Suppose that $\mathbb{F} \subset \mathbb{L}$ is a Galois extension and that we have an intermediate field $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$. Then $\mathbb{K} \subset \mathbb{L}$ is a Galois extension.*

Proposition 1.12. *Let $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ be finite field extensions and $\mathbb{F} \subseteq \mathbb{L}$ be a Galois extension. Then $\mathbb{F} \subseteq \mathbb{K}$ is a Galois extension if and only if $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is a normal subgroup of $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$.*

Theorem 1.13. *Let $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ be finite field Galois extensions. Then*

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \trianglelefteq \mathrm{Gal}(\mathbb{L}/\mathbb{F}) \quad \textit{and} \quad \mathrm{Gal}(\mathbb{K}/\mathbb{F}) \cong \frac{\mathrm{Gal}(\mathbb{L}/\mathbb{F})}{\mathrm{Gal}(\mathbb{L}/\mathbb{K})}.$$

Theorem 1.14 (**Fundamental Theorem of Galois theory**). *Let $\mathbb{F} \subseteq \mathbb{L}$ be a finite field Galois extension. Then there is a bijection between the set of intermediate fields $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ and the set of subgroups of $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ given by he maps*

$$\varphi : \mathbb{K} \longrightarrow \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \qquad \psi : H \longrightarrow \mathbb{L}^H$$

which are one the inverse of the other. Furthermore, if $\mathbb{K}$ is an intermediate field and H is a subgroup of $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ the following hold:

$$\begin{aligned}
&|\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}];\\
&[\mathrm{Gal}(\mathbb{L}/\mathbb{F}) : \mathrm{Gal}(\mathbb{L}/\mathbb{K})] = [\mathbb{K} : \mathbb{F}];\\
&[\mathbb{L} : \mathbb{L}^H] = |H|;\\
&[\mathbb{L}^H : \mathbb{F}] = [\mathrm{Gal}(\mathbb{L}/\mathbb{F}) : H].
\end{aligned}$$

Theorem 1.15 (**Homomorphism extension**). *Let $\varphi : \mathbb{F} \to \overline{\mathbb{F}}$ be a field isomorphism and let $\mathbb{F} \subseteq \mathbb{E}$, $\overline{\mathbb{F}} \subseteq \overline{\mathbb{E}}$ be field extensions. Then φ extends to a homomorphism:*

$$\begin{aligned}
\overline{\varphi} :\ \mathbb{F}[x] &\longrightarrow \overline{\mathbb{F}}[x]\\
a &\longmapsto \varphi(a) \qquad \forall \quad a \in \mathbb{F},\\
x &\longmapsto x.
\end{aligned}$$

Moreover, if $\alpha \in \mathbb{E}$ is a root of the irreducible polynomial $f(x) \in \mathbb{F}[x]$ and $\beta \in \overline{\mathbb{E}}$ is a root of $\overline{\varphi}(f(x))$, then there exists one and only one isomorphism $\Psi : \mathbb{F}[\alpha] \to \overline{\mathbb{F}}[\beta]$ such that $\Psi_{|_{\mathbb{F}}} = \varphi$ and $\Psi(\alpha) = \beta$.

Corollary 1.16. *Let $\mathbb{F} \subseteq \mathbb{E}$ be a field extension and let $\alpha, \beta \in \mathbb{E}$ be 2 different roots of the same irreducible polynomial $f(x) \in \mathbb{F}[x]$. Then $\mathbb{F}[\alpha]$ and $\mathbb{F}[\beta]$ are isomorphic.*

Definition 1.17. A polynomial with integer coefficients is *primitive* if it has 1 as a greatest common divisor of its coefficients.

Lemma 1.18 (**Gauss Lemma**). *A non constant polynomial in $\mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ if and only if it is both irreducible in $\mathbb{Q}[x]$ and primitive in $\mathbb{Z}[x]$.*

Lemma 1.19 (**Tower Lemma**). *Let $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ be finite field extensions. Then*

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{F}].$$

Chapter 2

Weak problem

In this section we will study the realization of a given group G as a Galois group of a generic field extension. The fact we do not ask $\mathbb{Q}$ to be the base field greatly simplifies the problem, hence the name "weak problem".

2.1 Cayley's Theorem

Definition 2.1. For a fixed field $\mathbb{F}$ we define $\mathbb{F}(x_1, \ldots, x_n)$ as the field of rational functions with coefficients in $\mathbb{F}$ and with n indeterminates.

Definition 2.2 (**Group action**). Let G be a group with identity element e and let X be a set. A group action of G on X is a map

$$\begin{array}{rcl} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g \cdot x \end{array}$$

that satisfies the following properties:

(i) $e \cdot x = x \quad$ for all $x \in X$

(ii) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) \quad$ for all $g_1, g_2 \in G$, $x \in X$.

Example 2.3. For a fixed field $\mathbb{F}$, the symmetric group S_n acts on $\mathbb{F}(x_1, \ldots, x_n)$ by permuting the n indeterminates.

Definition 2.4. A rational function $f(x_1, \ldots, x_n) \in \mathbb{F}(x_1, \ldots, x_n)$ is called *symmetric* if it is not changed by any permutation of the variables $x_1, \ldots, x_n$.

Example 2.5. The function

$$f(x_1, x_2, x_3) = \frac{x_1 x_2 x_3 - 4(x_1 x_2 + x_1 x_3 + x_2 x_3)}{(x_1 + x_2 + x_3)^2}$$

is symmetric in x_1, x_2, x_3.

Example 2.6. The function

$$g(x_1, x_2, x_3) = \frac{x_1 + x_3}{x_1 x_2 x_3}$$

is not symmetric, indeed the transposition $(1\ 2)$ switches the variables x_1, x_2.

We will denote by $S(x_1, \ldots, x_n)$ the field of symmetric rational functions.

Theorem 2.7 (**Cayley's Theorem**). *Let G be a finite group with n elements. Then G is isomorphic to a subgroup of S_n.*

Proof. The group G acts on itself by multiplication. Let us denote by $*$ the group operation. Then for every $g \in G$ the map

$$\begin{aligned} \Phi_g : G &\to G \\ h &\mapsto g * h \end{aligned}$$

is a bijection. Moreover we can identify the set of bijective maps from G to itself with S_n because G is in particular a set with n elements. One can prove that the map

$$\begin{aligned} \Phi : G &\to S_n \\ g &\mapsto \Phi_g \end{aligned}$$

is a group homomorphism. Furthermore Φ is an injective map, hence G is isomorphic to a subgroup of S_n. □

2.2 Universal extension

Theorem 2.8. *Let $x_1, \ldots, x_n$ be indeterminates. The elementary symmetric functions defined by*

$$\begin{aligned} \sigma_1 &= x_1 + \ldots + x_n; \\ \sigma_2 &= x_1x_2 + x_1x_3 + \ldots + x_2x_3 + x_2x_4 + \ldots + x_{n-1}x_n; \\ &\vdots \\ \sigma_i &= \sum_{1 \le j_1 < j_2 < \ldots < j_i \le n} x_{j_1} x_{j_2} \cdots x_{j_i}; \\ &\vdots \\ \sigma_n &= x_1 x_2 \ldots x_n \end{aligned}$$

are symmetric, and any symmetric rational function in the variables $x_1, \ldots, x_n$ is a rational function in the elementary symmetric functions $\sigma_1, \ldots, \sigma_n$.

Proof. See, for example, [4] for a complete proof. □

Example 2.9. $(x_1 - x_2)^2$ is symmetric in x_1, x_2 and

$$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = \sigma_1^2 - 4\sigma_2.$$

Example 2.10. $x_1^2 + x_2^2 + x_3^2$ is symmetric in x_1, x_2, x_3 and

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) = \\ &= \sigma_1^2 - 2\sigma_2. \end{aligned}$$

Example 2.11. The polynomial $x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2$ is symmetric in x_1, x_2, x_3 and an easy computation shows that

$$x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 = \sigma_2^2 - 2\sigma_1\sigma_3.$$

Theorem 2.12. *The field extension $S(x_1, \ldots, x_n) \subset \mathbb{F}(x_1, \ldots, x_n)$ is a Galois extension with Galois group isomorphic to S_n.*

Proof. The extension $S(x_1, \ldots, x_n) \subset \mathbb{F}(x_1, \ldots, x_n)$ has finite degree, indeed $\mathbb{F}(x_1, \ldots, x_n)$ is the splitting field of the following polynomial

$$q(t) = \prod_{i=1}^{n}(t - x_i) = t^n - (\sum_{i=1}^{n} x_i)t^{n-1} + \ldots + (-1)^n \prod_{i=1}^{n} x_i \in S(x_1, \ldots, x_n)[t] \qquad (2.1)$$

and the extension has degree at most $n!$. Moreover $q(t)$ is trivially a separable polynomial, then $S(x_1, \ldots, x_n) \subset \mathbb{F}(x_1, \ldots, x_n)$ is a Galois extension and from Theorem 1.10 it follows that

$$|\operatorname{Gal}(\mathbb{F}(x_1, \ldots, x_n)/S(x_1, \ldots, x_n))| = [\mathbb{F}(x_1, \ldots, x_n) : S(x_1, \ldots, x_n)] \leq n!\,. \qquad (2.2)$$

On the other hand, if σ is a permutation in S_n, it can be seen as an automorphism of $\mathbb{F}(x_1, \ldots, x_n)$ permuting the indeterminates; besides σ fixes the subfield $S(x_1, \ldots, x_n)$, so it is an element of the Galois group. It follows that $\operatorname{Gal}(\mathbb{F}(x_1, \ldots, x_n)/S(x_1, \ldots, x_n))$ has at least $n!$ elements, and from Equation 2.2 we conclude that $\operatorname{Gal}(\mathbb{F}(x_1, \ldots, x_n)/S(x_1, \ldots, x_n)) \cong S_n$. □

The field extension in Theorem 2.12 is known as the *universal extension with Galois group S_n*.

2.3 Universal realization of a finite group

Theorem 2.13. *Given a finite group G, there exists a Galois extension whose Galois group is isomorphic to G.*

Proof. Let G be a finite group of order n, and let $\mathbb{F}$ be an arbitrary field. We know that the universal extension of degree n,

$$\mathbb{K} = S(x_1, \ldots, x_n) \subset \mathbb{F}(x_1, \ldots, x_n) = \mathbb{L}$$

is a Galois extension with Galois group S_n. Since G is isomorphic to a subgroup of S_n by Theorem 2.7, it follows that G is also isomorphic to a subgroup $H \subset \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Using the maps φ and ψ of Theorem 1.14, we obtain the Galois extension $\mathbb{L}^H \subset \mathbb{L}$ with Galois group

$$\mathrm{Gal}(\mathbb{L}/\mathbb{L}^H) = H \cong G.$$

This shows that $\mathbb{L}^H \subset \mathbb{L}$ is the desired extension. □

Example 2.14. Let $C = \{e, a, a^2\}$ be the cyclic group of order 3. We know it is isomorphic to a subgroup of S_3, which is

$$C \cong A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\} \qquad \text{(in cyclic notation);}$$

and if we take the field extension

$$\mathbb{K} = S(x_1, x_2, x_3) \subset \mathbb{F}(x_1, x_2, x_3) = \mathbb{L}$$

we have $C \cong A_3 \subset S_3 \cong \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Following the steps of the proof of Theorem 2.13 we obtain an intermediate field

$$\mathbb{K} \subset \mathbb{L}^{A_3} \subset \mathbb{L}.$$

For example, the polynomial

$$f(x_1, x_2, x_3) = x_1x_1x_2 + x_2x_2x_3 + x_3x_3x_1$$

is fixed by A_3 but it is not fixed by all the permutations of S_3, since the transposition $(1\ 2)$ sends f to the polynomial

$$g(x_1, x_2, x_3) = x_2x_2x_1 + x_1x_1x_3 + x_3x_3x_2.$$

We now use the functions of Theorem 1.14 to obtain

$$A_3 \xrightarrow{\psi} \mathbb{L}^{A_3} \xrightarrow{\varphi} \mathrm{Gal}(\mathbb{L}/\mathbb{L}^{A_3}).$$

And we conclude that

$$\mathrm{Gal}(\mathbb{L}/\mathbb{L}^{A_3}) = A_3 \cong C.$$

However, in explicit examples, one is often interested in Galois group of polynomials over $\mathbb{Q}$. Thus the question is: which finite groups can occur as the Galois groups of finite field extensions of $\mathbb{Q}$? This is known as the inverse Galois problem (over $\mathbb{Q}$).

Chapter 3

Classical inverse problem

The classical inverse Galois problem consists in determining whether a fixed group G occurs as a Galois group over $\mathbb{Q}$, in other words, determining whether there exists a Galois extension $\mathbb{Q} \subseteq \mathbb{L}$ such that the Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ is isomorphic to G.

3.1 Cyclotomic polynomials

Definition 3.1. For a positive integer n we define the n-th cyclotomic polynomial as the monic polynomial that is the minimal polynomial over $\mathbb{Q}$ of any primitive n-th root of unity. Explicitly it is equal to

$$\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - x_i), \tag{3.1}$$

where φ is Euler's function, and the x_i's are the $\varphi(n)$ different primitive n-th roots of unity. Equivalently,

$$\Phi_n(x) = \prod_{x_i \in \mu_n, o(x_i)=n} (x - x_i),$$

where μ_n is the set of all the n-th roots of unity and $o(x_i)$ is the order of x_i.

Definition 3.2. We also define the following polynomial

$$\Psi_n(x) = \prod_{x_i \in \mu_n, o(x_i)\neq n} (x - x_i).$$

Remark 3.3. $\Phi_n(x) \cdot \Psi_n(x) = x^n - 1$.

Remark 3.4. *We have* $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Remark 3.5. *The polynomial* $\Phi_n(x)$ *has integer coefficients and, if* $n \neq 1$*, it has constant term equal to* 1.

3.2 Cyclic groups

Theorem 3.6. *Let n be a positive integer and let ξ_n be a primitive n-th root of unity. Then $\mathbb{Q} \subseteq \mathbb{Q}(\xi_n)$ is a Galois extension, and the following properties hold:*

(i) $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$;

(ii) $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Proof. If we choose $\xi_n = e^{\frac{2\pi i}{n}}$ we can obtain all other primitive n-th roots of unity by raising ξ_n to the power of positive integers coprime with n and smaller than n. It follows that $\mathbb{Q}(\xi_n)$ is the splitting field over $\mathbb{Q}$ of $\Phi_n(x)$ (see Definition 3.1), which is separable, so we have a Galois extension. We obtain $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$, hence the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) =: G$ has $\varphi(n)$ elements. We can explicitly determine the $\varphi(n)$ elements in G, since for every integer $k < n$ coprime with n, by Theorem 1.15, there exists the following automorphism:

$$\begin{aligned} \gamma_k : \mathbb{Q}(\xi_n) &\to \mathbb{Q}(\xi_n) \\ \xi_n &\mapsto (\xi_n)^k, \end{aligned}$$

which is an element of G. Moreover we can consider the following map

$$\eta : \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^* \tag{3.2}$$

$$\gamma_k \mapsto [k]_n \tag{3.3}$$

which is bijective and a homomorphism of groups since

$$\eta(\gamma_k \circ \gamma_{k'}) = [k \cdot k']_n = [k]_n \cdot [k']_n = \eta_{\gamma(k)} \cdot \eta_{\gamma(k')}.$$

It follows that $G \cong (\mathbb{Z}/n\mathbb{Z})^*$. □

Example 3.7. Let $\xi = e^{\frac{2\pi i}{5}}$ be a primitive 5-th root of unity and set $\mathbb{E} = \mathbb{Q}[\xi]$. The minimal polynomial of ξ is $\varphi(x) = x^4 + x^3 + x^2 + x + 1$ and by Theorem 3.6 we have

$$\mathrm{Gal}(\mathbb{E}/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/4\mathbb{Z}.$$

The elements of the Galois group, in the notation above, are $\{\mathrm{id}, \gamma_2, \gamma_3, \gamma_4\}$, and a generator for this cyclic group is γ_2 since 2 has order 4 in $(\mathbb{Z}/5\mathbb{Z})^*$.

From Theorem 3.6 we know that for all n, $(\mathbb{Z}/n\mathbb{Z})^*$ occurs as a Galois group over $\mathbb{Q}$, but this is not always a cyclic group.

Theorem 3.8. *$(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic if and only if $n = 2$, $n = 4$, $n = p^\alpha$ or $n = 2 \cdot p^\alpha$ where p is an odd prime and $\alpha \in \mathbb{Z}^+$.*

Proof. This was first proved by Gauss. The reader can find a complete proof in [19]. □

In particular we know how to realize every cyclic group with $p-1$ elements where p is an odd prime number. We want to extend this result to every positive integer. To this aim, we will use a theorem due to Dirichlet.

Lemma 3.9. *Let a, n be positive integers and let p be a prime such that $p \mid \Phi_a(n)$ and $p \nmid \Phi_d(n)$ for every d proper divisor of a. Then $p \equiv 1$ mod a.*

Proof. We first observe that p, n are coprime numbers. Indeed $p \mid \Phi_a(n)$ and since the polynomial $\Phi_a(x)$ divides $x^a - 1$ we have that $p \mid n^a - 1$. It follows that $p \nmid n$ otherwise we obtain the absurd $p \mid n^a - 1$ and $p \mid n^a$. We will now show that $[n]_p$ has order a in $\mathbb{Z}_p$. The order of $[n]_p$ divides a because in $\mathbb{Z}_p$ the following holds:

$$[n]_p^a - [1]_p = \prod_{d|a} \Phi_d([n]_p) = [0]_p$$

where the second equality follows from the hypothesis $p \mid \Phi_a(n)$, so $\Phi_a([n]_p) = [0]_p$. On the other hand the order of $[n]_p$ is at least a since if $d < a$, $d \mid a$ we have

$$[n]_p^d - [1]_p = \prod_{d'|d} \Phi_{d'}([n]_p)$$

with $\Phi_{d'}([n]_p) \neq [0]_p$ because by hypothesis $p \nmid \Phi_{d'}(n)$ for every d' proper divisor of a. So the order of $[n]_p$ is exactly a, but since the order of an element divides the order of the group, we obtain $a \mid (p-1)$. □

Theorem 3.10 (**Weak form of Dirichlet's Theorem on arithmetic progressions**)**.** *For every integer $a \neq 0$ there are infinite primes of the form $an+1$, where n is a positive integer.*

Proof. For $a = 1$ the statement is trivial, and without loss of generality we can prove it for $a > 0$. We observe that if $a > 1$ we have to prove that there exist infinite primes p such that $p \equiv 1$ modulo a. Let $a > 1$ and assume by contradiction that there is only a finite number of primes p such that $p \equiv 1 \bmod a$, say $p_1, \ldots, p_q$. For a fixed a, if there exist a prime p and an integer n which satisfy the hypotheses of Lemma 3.9, we have $p \equiv 1 \pmod{a}$, but this is not enough because p could be one of the p_i above. Let us consider instead of a the integer $A = a \cdot p_1 \ldots p_q$. Now, if there exist a prime p and an integer n such that A, n, p satisfy the hypotheses of Lemma 3.9, we can conclude $p \equiv 1 \pmod{A}$ and in particular $p \equiv 1 \pmod{a}$, but in this way we are sure $p \neq p_i$ for every $i = 1, \ldots, q$. The polynomials $\Phi_A(x)$ and $Q(x) := \prod_{d|A, d \neq A} \Phi_d(x)$ are coprime in $\mathbb{C}[x]$ because they have no common roots, so they are coprime also in $\mathbb{Q}[x]$ and from Bezout's Theorem it follows that there exist $U(x)$ and $V(x)$ in $\mathbb{Q}[x]$ such that

$$1 = U(x) \cdot \Phi_A(x) + V(x) \cdot Q(x).$$

We can now choose $n \in \mathbb{Z}$ such that the polynomials $n\Phi_A(x)$ and $nQ(x)$ have integer coefficients. Moreover we can choose n such that $\Phi_A(n) \neq 0$ and $\Phi_A(n) \neq \pm 1$ because on one side we have infinite n such that $n\Phi_A(x), nQ(x) \in \mathbb{Z}[x]$, while $\Phi_A(n)$ and $\Phi_A(n) \mp 1$ only have a finite number of roots. For such a number n we have

$$n = nU(x) \cdot \Phi_A(x) + nV(x) \cdot Q(x)$$

and in particular

$$n = nU(n) \cdot \Phi_A(n) + nV(n) \cdot Q(n). \tag{3.4}$$

Since $\Phi_A(n) \neq 0$ e $\Phi_A(n) \neq \pm 1$, there exists a prime p which divides $\Phi_A(n)$. By the same argument used in Lemma 3.9, it follows that p and n are coprime numbers. Arguing by contradiction, if p divides $Q(n)$ we would have from Equation (3.4) that $p \mid n$ which is an absurd. It follows that $p \nmid Q(n)$ and in particular it does not divide $\Phi_d(n)$ for any $d \mid A$, $d \neq A$, hence the triple A, n, p satisfies the hypotheses of Lemma 3.9. Observe that there is no need to prove that there exists at least one of the prime p such that $p \equiv 1 \bmod a$, because the argument above still works with $A = a$. □

Theorem 3.11. *Let $n \geq 2$ be a positive integer, then there exists a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to the cyclic group $\mathbb{Z}_n$.*

Proof. If $n = 2$ we can choose the splitting field of the polynomial $x^2 - 2$, so that the Galois group consists of $\tau : \sqrt{2} \mapsto -\sqrt{2}$ and id. Let us now assume $n > 2$. We can choose a prime p such that $p \equiv 1 \pmod{n}$ by Theorem 3.10. Let ξ_p be a primitive p-th root of unity. We already know by Theorem 3.6 that $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$. Since $p \equiv 1 \pmod{n}$ it follows that $n \mid (p-1)$, therefore $p - 1 = kn$ for some integer k. The Galois group $G := \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}_{p-1}$ contains a subgroup H isomorphic to $\mathbb{Z}_k$ (the one generated by $[n]_{p-1}$) and by fundamental Theorem of Galois theory we have $H \cong \mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}(\xi_p)^H)$. Since cyclic groups are abelian, H is a normal subgroup of G and by Theorems 1.13 and 1.14 we have that $\mathbb{Q} \subseteq \mathbb{Q}(\xi_p)^H =: \mathbb{E}$ is a Galois extension. Moreover we have:

$$\mathrm{Gal}(\mathbb{E}/\mathbb{Q}) \cong \frac{\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{E})} \cong \frac{\mathbb{Z}_{p-1}}{\mathbb{Z}_k} \cong \mathbb{Z}_n.$$

□

Example 3.12. We can realize $\mathbb{Z}_6$ as a Galois group over $\mathbb{Q}$ using $p = 13$. Indeed, if ξ_{13} is a primitive 13th root of unity, we have $\mathrm{Gal}(\mathbb{Q}(\xi_{13})/\mathbb{Q}) \cong \mathbb{Z}_{12}$ and since $12 = 6 \cdot 2$ it follows that

$$\mathrm{Gal}(\mathbb{E}/\mathbb{Q}) \cong \mathbb{Z}_6$$

where $\mathbb{E} = \mathbb{Q}(\xi_{13})^{\mathbb{Z}_2}$.

Example 3.13. The Galois group of the polynomial $f = x^4 + 5x^2 + 5$ over $\mathbb{Q}$ is cyclic of order 4. First we note that f is irreducible by Eisenstein criterion with $p = 5$. One can prove that its roots are:

$$\alpha_{1,2} = \left(\frac{-5 \pm \sqrt{5}}{2}\right)^{\frac{1}{2}} \qquad \alpha_{3,4} = -\alpha_{1,2}\,;$$

moreover we have:

$$\alpha_1 \cdot \alpha_2 = \sqrt{5} = 2\alpha_1^2 + 5,$$

so it follows that:

$$\begin{aligned}
&\alpha_2 = 2\alpha_1 + 5 \cdot (\alpha_1)^{-1} \in \mathbb{Q}[\alpha_1],\\
&\alpha_3 = -\alpha_1 \in \mathbb{Q}[\alpha_1],\\
&\alpha_4 = -\alpha_2 \in \mathbb{Q}[\alpha_1]
\end{aligned}$$

and we deduce that $\mathbb{Q}[\alpha_1]$ is the splitting field of f, which is a separable polynomial of degree 4. Hence $\mathrm{Gal}(f)$ is isomorphic to a subgroup of S_4 of order 4, since $\mathbb{Q} \subset \mathbb{Q}[\alpha_1]$ is a Galois extension, so it is either the Klein group or the cyclic group $\mathbb{Z}_4$. By Theorem 1.15 there exists $s \in \mathrm{Gal}(f)$ such that $s(\alpha_1) = \alpha_2$. Then we have

$$s(\sqrt{5}) = s(2\alpha_1^2 + 5) = 2 \cdot s(\alpha_1)^2 + 5 = 2\alpha_2^2 + 5 = -\sqrt{5}$$

then

$$\begin{aligned}
&s(\alpha_2) = s\left(\frac{\sqrt{5}}{\alpha_1}\right) = \frac{-\sqrt{5}}{\alpha_2} = -\alpha_1 = \alpha_3\\
&s(\alpha_3) = s(-\alpha_1) = -\alpha_2 = \alpha_4.
\end{aligned}$$

Hence the order of s is 4 and $\mathrm{Gal}(f) \cong \mathbb{Z}_4$.

3.3 Abelian groups

Theorem 3.14 (**Chinese remainder Theorem**). *Let $n_1, \ldots, n_k$ be positive integer, $n_i > 1\ \forall\, i$, such that $(n_i, n_j) = 1\ \forall\, i \neq j$ and let $a_1, \ldots, a_k \in \mathbb{Z}$. Then the following system of congruence*

$$\begin{cases} x \equiv a_1 \ (mod\ n_1) \\ \vdots \\ x \equiv a_k \ (mod\ n_k) \end{cases} \tag{3.5}$$

has one and only one solution S modulo $N = n_1 \cdot \ldots \cdot n_k$.

Proof. We set $N = n_1 \cdot \ldots \cdot n_k$ and for all $i = 1, \ldots, k$ we denote $N_i = \frac{N}{n_i}$. Then we have a solution of system (3.5) given by $S = a_1 N_1 N_1^{-1} + \ldots + a_k N_k N_k^{-1}$, where N_i^{-1} is the inverse of N_i modulo n_i (we know it exists because N_i and n_i are coprime numbers by construction). Moreover S is the only solution modulo N, because if S' is another solution of system (3.5) we have $S' \equiv S \pmod{n_1}, \ldots, S' \equiv S \pmod{n_k}$ and since n_i are coprime numbers, we obtain $S' \equiv S \pmod{N}$. □

Corollary 3.15. *In the notation of Theorem 3.14, $\mathbb{Z}_N$ is in one-to-one correspondence with $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$:*

$$\begin{aligned} \eta : \mathbb{Z}_N &\to \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k} \\ [a]_N &\mapsto ([a]_{n_1}, \ldots, [a]_{n_k}) \end{aligned}$$

Moreover, the restriction of the map η from $\mathbb{Z}_N^*$ to $\mathbb{Z}_{n_1}^* \times \ldots \times \mathbb{Z}_{n_k}^*$ is also bijective.

Proof. The map η is bijective thanks to Theorem 3.14. We will now prove the second part of the corollary for $k = 2$, and $N = nm$. Consider $[a]_N \in \mathbb{Z}_N^*$, thus $(a, nm) = 1$ and in particular $(a, n) = 1 = (a, m)$. It follows that $([a]_n, [a]_m) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$, hence the restriction of the map η is well defined. On the other hand, since η is bijective, taken $([a]_n, [b]_m) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$, there exists $[c]_N \in \mathbb{Z}_N$ such that $[c]_n = [a]_n$ and $[c]_m = [b]_m$, but we have to show that $[c]_N \in \mathbb{Z}_N^*$. Indeed, since $c = kn + a$ for some $k \in \mathbb{Z}$, it follows that $(c, n) = (a, n) = 1$ and for the same reason $(c, m) = 1$. Hence $(c, nm) = (c, N) = 1$ and $[c]_N \in \mathbb{Z}_N^*$. The general case is analogous. □

Definition 3.16 (**Finitely generated group**)**.** An abelian group G is said to be *finitely generated* if there exist $g_1, \ldots, g_n \in G$ such that every element $g \in G$ can be written as a linear combination of them

$$g = a_1 g_1 + \ldots + a_n g_n$$

with a_i integer coefficients.

Theorem 3.17 (**Classification of finitely generated groups**)**.** *Let M be a finitely generated abelian group. Then either*

$$M \cong \mathbb{Z}^k \ , \ k \geq 0$$

or

$$M \cong \mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}$$

with $k \geq 0$, for some integers d_i such that if $i < j$, $d_i \mid d_j$.

Note that $\mathbb{Z}_{d_i}$ stands for $\mathbb{Z}/d_i\mathbb{Z}$.

Proof. The reader can find a complete proof of the statement in [5]. □

Corollary 3.18. *In the notation of Theorem 3.17, if M is a finite abelian group, it follows that*

$$M \cong \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}$$

for some integers d_i such that if $i < j$, $d_i \mid d_j$.

Proof. M is finite, hence $k = 0$. □

Theorem 3.19 (**Kronecker-Weber**). *Let A be a finite abelian group. Then $A \cong \mathrm{Gal}(\mathbb{E}/\mathbb{Q})$ where $\mathbb{E}$ is a subfield of $\mathbb{Q}(\omega)$ for some s-th primitive root of unity ω.*

Proof. If $A = \{\mathrm{id}\}$ we can take $\mathbb{E} = \mathbb{Q}$. Otherwise, since A is an abelian finite group, by Corollary 3.18 we have

$$A \cong \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_t}$$

for some $d_i \geq 2$ where $d_i \mid d_j$ if $i < j$. From Dirichlet's Theorem 3.10 we can take $p_1, \ldots, p_t$ different primes such that $p_i \equiv 1 \pmod{d_i}$ for all $i = 1, \ldots, t$. Indeed, even if some of the d_i's can be the same, the Theorem guarantees infinitely many primes with that property. Then for all $i = 1, \ldots, t$ there exists an integer m_i such that $p_i - 1 = m_i \cdot d_i$. We define $s = p_1 \cdot \ldots \cdot p_t$. Now, we notice that

$$\begin{aligned} \phi : \mathbb{Z}_{p_i-1} &\to \mathbb{Z}_{d_i} \\ [a]_{p_i-1} &\mapsto [a]_{d_i} \end{aligned}$$

is a surjective homomorphism, indeed:

- For $[a]_{p_i-1}$, $[b]_{p_i-1} \in \mathbb{Z}_{p_i-1}$ we have:

  $$\phi([a]_{p_i-1} + [b]_{p_i-1}) = \phi([a+b]_{p_i-1}) = [a+b]_{d_i} = [a]_{d_i} + [b]_{d_i} = \phi([a]_{p_i-1}) + \phi([b]_{p_i-1}).$$

- For every $[c]_{d_i} \in \mathbb{Z}_{d_i}$ we can pick $[d]_{p_i-1} \in \mathbb{Z}_{p_i-1}$ such that $\phi([d]_{p_i-1}) = [c]_{d_i}$ since $p_i - 1 \equiv 0 \pmod{d_i}$.

Taking products, we obtain a surjective homomorphism:

$$\prod_{i=1}^{t} \mathbb{Z}_{p_i-1} \to A.$$

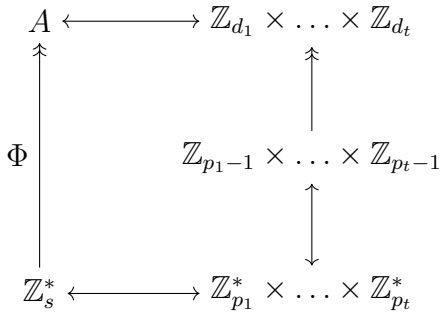
Moreover, since the primes p_i's are all different, by the Chinese remainder Theorem and Corollary 3.15 we have that

$$\mathbb{Z}_s^* \cong \mathbb{Z}_{p_1}^* \times \ldots \times \mathbb{Z}_{p_t}^* \cong \mathbb{Z}_{p_1-1} \times \ldots \times \mathbb{Z}_{p_t-1}$$

and thus we have the surjective homomorphism:

$$\Phi : \mathbb{Z}_s^* \to A.$$

We can display this first part of the proof as follows:



Let us denote by H the kernel of Φ, then we know from group theory that:

$$A \cong \mathbb{Z}_s^*/H.$$

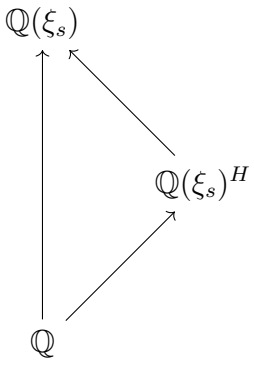
Hence we only need to find a Galois extension with Galois group isomorphic to $\mathbb{Z}_s^*/H$. We already know from Theorem 3.6 that if ξ_s is a primitive s-th root of unity, then $\mathbb{Q} \subseteq \mathbb{Q}(\xi_s)$ is a Galois extension with Galois group isomorphic to $\mathbb{Z}_s^*$. By the fundamental Theorem of Galois theory, since H is a subgroup of $\mathbb{Z}_s^*$, we can deduce that it corresponds to the field subextension $\mathbb{Q}(\xi_s)^H$ such that:

$$\mathrm{Gal}(\mathbb{Q}(\xi_s)/\mathbb{Q}(\xi_s)^H) = H.$$

Since $\mathbb{Z}_s^*$ is abelian, H is a normal subgroup and by Proposition 1.12 we have the Galois extension $\mathbb{Q} \subseteq \mathbb{Q}(\xi_s)^H$ with Galois group:

$$\mathrm{Gal}(\mathbb{Q}(\xi_s)^H/\mathbb{Q}) \cong \frac{\mathrm{Gal}(\mathbb{Q}(\xi_s)/\mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\xi_s)/\mathbb{Q}(\xi_s)^H)} \cong \frac{\mathbb{Z}_s^*}{H} \cong A \quad \text{(see Theorem 1.13)}.$$

We can display this last part of the proof as follows:



Another way to find the subgroup H is to consider for all $i = 1, \ldots, t$ the cyclic subgroup of $\mathbb{Z}_{p_i-1}$ generated by $[d_i]_{p_i-1}$:

$$H_i =< [d_i]_{p_i-1} > \subseteq \mathbb{Z}_{p_i-1}$$

which has order m_i. We now consider the subgroup $H = H_1 \times \ldots \times H_t$ of the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_s)/\mathbb{Q})$. H is a normal subgroup because we are in an abelian context. Let $\mathbb{E}$ be the field of elements fixed by H, then by Theorem 1.14 it follows that $\mathbb{Q} \subseteq \mathbb{E}$ is a Galois extension such that

$$\mathrm{Gal}(\mathbb{E}/\mathbb{Q}) \cong \frac{\mathbb{Z}_{p_1-1} \times \ldots \times \mathbb{Z}_{p_t-1}}{H_1 \times \ldots \times H_t} \cong \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_t} \cong A.$$

□

Chapter 4

Symmetric groups

4.1 Class Equation

Definition 4.1. For a group G we define the *center* of the group G as the set of elements that commute with all of the elements of G:

$$Z(G) = \{z \in G : gz = zg \ \ \forall g \in G\}$$

and for $x \in G$ the *centralizer of x in G*:

$$C_G(x) = \{g \in G : gx = xg\}.$$

One can define the following equivalence relation on G:

$$x \sim y \iff \exists\ g \in G \quad s.t. \quad x = g^{-1}yg.$$

Proposition 4.2 (**Class Equation**). *For a finite group G we have:*

$$|G| = |Z(G)| + \sum_{j=1}^{k} [G : C_G(x_j)]$$

where the sum is extended to elements that are not in the center of G and belong to different equivalence classes.

Proof. Since conjugacy is an equivalence relation on G, we have that G is partitioned by the set of conjugacy classes. Thus:

$$|G| = \sum_i |\mathcal{O}_{x_i}|$$

where $\mathcal{O}_{x_i}$ is the conjugacy class of an element x_i and the sum runs over different conjugacy classes. Moreover, $|\mathcal{O}_{x_i}| = |G|/|C_G(x_i)|$. In particular, $|\mathcal{O}_{x_i}| = 1$ if and only if $x_i \in Z(G)$. The result follows. □

We will first study the realization of S_p as a Galois group over $\mathbb{Q}$ for a prime p. In order to do this, we will use the following result due to Cauchy.

Theorem 4.3 (**Cauchy**). *Let G be a finite group of order $n > 1$ and let p be a prime that divides n. Then there exists an element $a \in G$ of order p.*

Proof. Let G be a group with identity element e. If $n = p$ is a prime, every element $a \in G$, $a \neq e$ has order p since the order of an element divides the order of the group. We will prove the general case by induction on $|G|$, the base case being $n = p$.
Let us first suppose that G is abelian. Fix $a \in G$, $a \neq e$, and let $H =< a >$ be the cyclic group generated by a. If $p \mid |H|$ the element $a^{\frac{|H|}{p}}$ has order p. Otherwise, if $p \nmid |H|$ it must be $p \mid |G/H|$ since $|G| = |H| \cdot |G/H|$ and by hypothesis $p \mid |G|$. Since $|G/H| < |G|$ we know by the induction argument that there exists $xH \in G/H$ of order p:

$$(xH)^p = H \Rightarrow x^pH = H \Rightarrow x^p \in H.$$

If the order of x is m we have $(xH)^m = H$. It follows that $p \mid m$ and thus the element $x^{\frac{m}{p}}$ has order p.
Now suppose that G is not abelian. Then $G \neq Z(G)$ and by the Class Equation:

$$|G| = |Z(G)| + \sum_j [G : C_G(x_j)].$$

If $p \mid |Z(G)|$ we conclude using the previous case since $Z(G)$ is an abelian subgroup of G. If $p \nmid |Z(G)|$ then there exists j such that $p \nmid [G : C_G(x_j)]$. Indeed, arguing by contradiction, if p divides all of this terms, we would have that p divides $|Z(G)|$ which is an absurd. For such a fixed j, since $|G| = [G : C_G(x_j)] \cdot |C_G(x_j)|$ and $p \mid |G|$ we have $p \mid |C_G(x_j)|$. On the other hand, $|C_G(x_j)| < |G|$ and we conclude by the inductive hypothesis. □

Theorem 4.4. *Let $f \in \mathbb{Q}[t]$ be an irreducible polynomial of degree a prime p. Suppose f splits in $\mathbb{C}$ with exactly 2 non real roots z, w. Then $z = \overline{w}$ and $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_p$.*

Proof. Since the polynomial f is irreducible on $\mathbb{Q}$, which is a perfect field, we know that f is separable. It follows by Theorem 1.10 that $|\mathrm{Gal}_{\mathbb{Q}}(f)| = [\mathbb{L} : \mathbb{Q}]$, where $\mathbb{L}$ is the splitting field of f over $\mathbb{Q}$. Let α be a root of f, then $[\mathbb{Q}[\alpha] : \mathbb{Q}] = p$. On the other hand $\mathbb{Q} \subseteq \mathbb{Q}[\alpha] \subseteq \mathbb{L}$ and from the Tower Lemma it follows that $p \mid [\mathbb{L} : \mathbb{Q}] = |\mathrm{Gal}_{\mathbb{Q}}(f)|$. We know from Cauchy's Theorem 4.3 that there exists an element with order p in $\mathrm{Gal}_{\mathbb{Q}}(f)$. Moreover the group $\mathrm{Gal}_{\mathbb{Q}}(f)$ can be seen as a subgroup of S_p by Proposition 1.9, and without loss of generality we can take the cycle $(1\ 2\ 3\ \ldots\ p)$ as the element of order p. The complex conjugation

$$\begin{aligned} \tau : \mathbb{L} &\to \mathbb{L} \\ z &\mapsto \overline{z} \end{aligned}$$

is an element of $\mathrm{Gal}_{\mathbb{Q}}(f)$. The map τ exchanges the two non real roots of f, hence it corresponds to a transposition $(i\ j)$ in the identification with a subgroup of S_p. We can now consider the p-cycle starting from the i element, obtaining $(i\ k_1\ k_2\ \dots k_{p-1})$. Renumbering the roots of f in a way such that $i = 1$ we have the cycle $c = (1\ \tilde{k}_1\ \dots \tilde{k}_{p-1})$ and the transposition $(1\ j) = (1\ \tilde{k}_l)$ for some l. On the other hand there exists a power raise of c of the form $(1\ \tilde{k}_l\ \dots \tilde{k}_d)$, indeed the length of the cycle is a prime p, hence its power raises can only be either the identity, either a cycle of length p. Renumbering the roots, we obtain that the following elements

$$(1\ 2)\ \ (1\ 2\ \dots\ p)$$

are in $\mathrm{Gal}_{\mathbb{Q}}(f)$. We know that these two cycles generate S_p. □

Example 4.5. The polynomial $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$ is irreducible and it has exactly 2 non real roots. Indeed we compute

$$f'(x) = 5x^4 - 6,$$

and the real roots of $f'(x) = 0$ are $x_{1,2} = \pm\sqrt[4]{\frac{6}{5}}$. Moreover we have

$$\begin{aligned} f'(x) > 0 &\iff 5x^4 - 6 > 0 \iff x^2 < -\sqrt{\frac{6}{5}} \quad \vee \quad x^2 > \sqrt{\frac{6}{5}} \\ &\iff x < -\sqrt[4]{\frac{6}{5}} \quad \vee \quad x > \sqrt[4]{\frac{6}{5}}. \end{aligned}$$

Since

$$\lim_{x\to-\infty} f(x) = -\infty \qquad \text{and} \qquad \lim_{x\to+\infty} f(x) = +\infty,$$

f has local maximum and local minimum respectively in $-\sqrt[4]{\frac{6}{5}}$ and $+\sqrt[4]{\frac{6}{5}}$, with relative values

$$\begin{aligned} f\left(-\sqrt[4]{\frac{6}{5}}\right) &= \left(-\sqrt[4]{\frac{6}{5}}\right)^5 - 6\left(-\sqrt[4]{\frac{6}{5}}\right) + 3 = -\frac{6}{5}\sqrt[4]{\frac{6}{5}} + 6\sqrt[4]{\frac{6}{5}} + 3 > 0 \\ f\left(\sqrt[4]{\frac{6}{5}}\right) &= \left(\sqrt[4]{\frac{6}{5}}\right)^5 - 6\left(\sqrt[4]{\frac{6}{5}}\right) + 3 = -\frac{24}{5}\sqrt[4]{\frac{6}{5}} + 3 < 0. \end{aligned}$$

Hence the polynomial has plot as in Figure 4.1 and $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_5$.

Example 4.6. The reader shouldn't think that in order to have Galois group S_p, a polynomial must have exactly two non real roots. For example, the polynomial x^3-4x+1 has Galois group S_3 (see Example 5.9) but it has all real roots: computing its first derivative one can see that f has graph on $\mathbb{R}$ as in Figure 4.2.

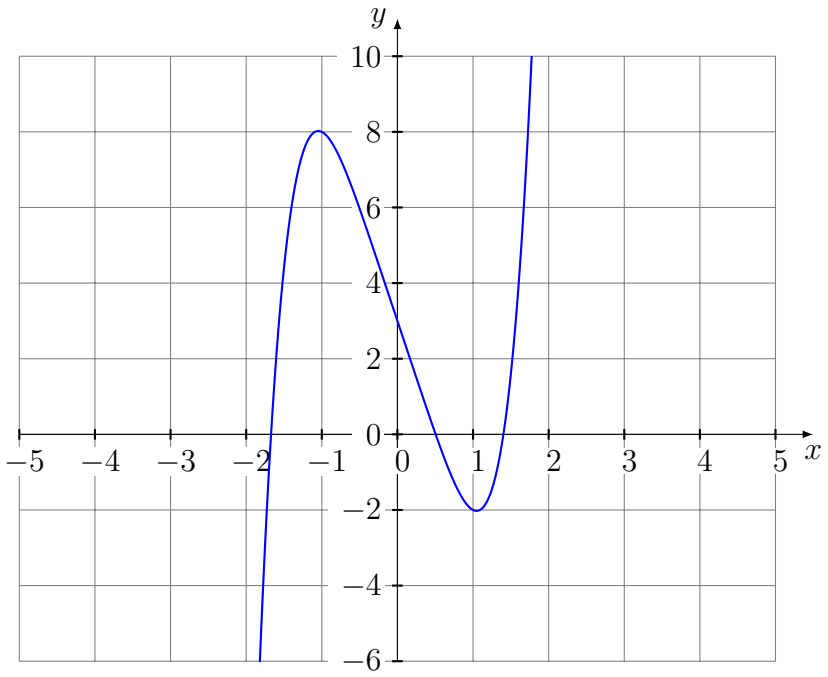


Figure 4.1: $x^5 - 6x + 3$

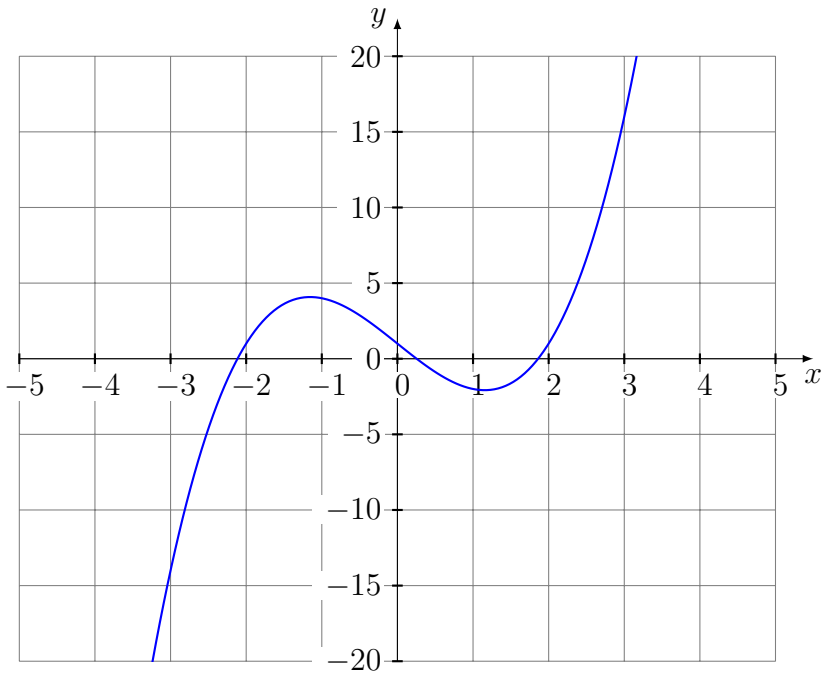


Figure 4.2: $x^3 - 4x + 1$

4.2 Transitive group action

Definition 4.7 (**Transitive group action**). Let G be a group with an action on a non trivial set X. The action is said to be *transitive* if

$$\forall\ x, y \in X\ \ \exists\ g \in G \text{ s.t. } g \cdot x = y.$$

We will say that the group G is transitive on X.

Definition 4.8. A subgroup G of S_n is said to be *transitive* if for every couple of indices $i, j \in \{1, 2, \ldots, n\}$ there exists an element $\sigma \in G$ such that $\sigma(i) = j$; in other words, the action of G on $\{1, 2, \ldots, n\}$

$$\begin{array}{ccc} G \times \{1, 2, \ldots, n\} & \longrightarrow & \{1, 2, \ldots, n\} \\ (\sigma, i) & \longmapsto & \sigma(i) \end{array}$$

is transitive.

Proposition 4.9. *Let $\mathbb{K}$ be a field and let $f \in \mathbb{K}[x]$ be a separable polynomial and $G = \mathrm{Gal}_{\mathbb{K}}(f)$. G acts transitively on the roots of f if and only if f is irreducible in $\mathbb{K}[x]$.*

Proof. If f has degree n, $f = \sum_{i=0}^{n} a_i x^i$, we already know that G can be viewed as a subgroup of S_n. That is because the Galois group G permutes the roots of f. Indeed, if α is a root of f in a splitting field $\mathbb{L}$ of f and $\sigma \in G$ we have:

$$f(\sigma(\alpha)) = \sum_{i=0}^{n} a_i \sigma(\alpha)^i = \sum_{i=0}^{n} \sigma(a_i \alpha^i) = \sigma(f(\alpha)) = 0$$

since σ is a field automorphism of $\mathbb{L}$ and fixes the elements in $\mathbb{K}$. So the elements of G map roots of f to roots of f. Suppose f is an irreducible polynomial and take α, $\alpha' \in \mathbb{L}$ different roots of f. In this case using Theorem 1.15 we know that there exists a field automorphism of $\mathbb{L}$ that fixes $\mathbb{K}$ and maps $\alpha \mapsto \alpha'$, hence G is transitive. On the other hand, suppose G is transitive and suppose by contradiction that f is a reducible polynomial, $f = f_1 \cdot \ldots \cdot f_k$, where each f_i is irreducible of degree at least 1 and $k > 1$. Here we obtain the absurd that the action can not be transitive because each root of f_i can only map to another root of f_i. In other words, let the roots of f be $\alpha_1, \ldots, \alpha_n$. Since f_1 is a non constant factor of f, we can find i such that $f_1(\alpha_i) = 0$. Now pick any $j \in \{1, \ldots, n\}$. By our transitivity assumption, there exists $\sigma \in \mathrm{Gal}_{\mathbb{K}}(f)$ such that $\sigma(\alpha_i) = \alpha_j$. Since f_1 has coefficients in $\mathbb{K}$, we know that σ sends roots of f_1 in roots of f_1, hence $f_1(\alpha_j) = 0$. Since j was arbitrary and $\alpha_1, \ldots, \alpha_n$ are distinct, it follows that f_1 has at least n roots, which implies that $deg(f_1) \geq n$, hence $f = f_1$. □

Definition 4.10 (**Double transitive action**)**.** Let G be a group with an action on a non trivial set X. The action is said to be *double transitive* if

$$\forall\ x, x, y, y' \in X \text{ with } x \neq x' \text{ and } y \neq y'\ \exists\ g \in G \text{ s.t. } gx = y \text{ and } gx' = y'.$$

If the action is clear, we will simply say that the group G is double transitive.

Definition 4.11 (**Stabilizer**)**.** Given an action of a group G on a set X, for every element $x \in X$ the *stabilizer subgroup* of x (also called the isotropy group of x) is the set of all elements in G that fix x:

$$\mathrm{Stab}_G(x) = \{g \in G \mid gx = x\}.$$

Lemma 4.12. *Let G be a group with transitive action on a non trivial set X. Taken $x, y \in X$ we have*

$$\mathrm{Stab}_G(y) = g \cdot \mathrm{Stab}_G(x) \cdot g^{-1}$$

where $g \in G$ verifies $gx = y$.

Proof. If $h \in \mathrm{Stab}_G(y)$ we have $hy = y$. Since $h = gg^{-1}hgg^{-1}$ we have to show that $g^{-1}hg$ is an element of $\mathrm{Stab}_G(x)$:

$$(g^{-1}hg)x = (g^{-1}h)y = g^{-1}y = x.$$

Viceversa, let $z \in \mathrm{Stab}_G(x)$ so that $zx = x$ and gzg^{-1} is an element of $g \cdot \mathrm{Stab}_G(x) \cdot g^{-1}$. We have to show that this element fixes y. Indeed, we have:

$$(gzg^{-1})y = (gz)x = gx = y.$$

□

Proposition 4.13. *Let G be a group acting on a non trivial set X and let $x \in X$. The action is double transitive on X if and only if the action is transitive on X and $\mathrm{Stab}_G(x)$ is transitive on $X \setminus \{x\}$.*

Proof. The case $|X| = 2$ is trivially true since transitivity and double transitivity are the same conditions. Suppose $|X| > 2$. If G is double transitive on X, then for every $x, y, y' \in X$, with $x \neq y$, $x \neq y'$ there exists $g \in G$ such that

$$gx = x \text{ and } gy = y'$$

hence G is transitive on X and $\mathrm{Stab}_G(x)$ is double transitive on $X \setminus \{x\}$.
Suppose now that G is transitive on X and $\mathrm{Stab}_G(x)$ is transitive on $X \setminus \{x\}$, where x is an arbitrary element of X. We will first prove that for every element $y \in X$ it also holds that $\mathrm{Stab}_G(y)$ is transitive on $X \setminus \{y\}$. Let $y \in X$. By hypothesis there exists an

element $g \in G$ such that $y = gx$. By Lemma 4.12 we have $\mathrm{Stab}_G(y) = g\,\mathrm{Stab}_G(x)g^{-1}$. Take $z_1, z_2 \in X \setminus \{y\}$; then we have that $g^{-1}z_1, g^{-1}z_2 \neq g^{-1}y = x$. By hypothesis there exists $h \in \mathrm{Stab}_G(x)$ such that $hg^{-1}z_1 = g^{-1}z_2$, hence

$$ghg^{-1}z_1 = z_2.$$

Since $ghg^{-1} \in \mathrm{Stab}_G(y)$, we deduce that $\mathrm{Stab}_G(y)$ is transitive on $X \setminus \{y\}$ for every $y \in X$. Consider now $x_1, x_2, y_1, y_2 \in X$ with $x_1 \neq x_2$ and $y_1 \neq y_2$. As above, there exist $g \in \mathrm{Stab}_G(x_1)$ and $g' \in \mathrm{Stab}_G(y_2)$ such that $gx_2 = y_2$ and $g'x_1 = y_1$. Then

$$(g' \circ g)x_1 = g'x_1 = y_1 \qquad \text{and} \qquad (g' \circ g)x_2 = g'y_2 = y_2.$$

This proves the thesis if $x_1 \neq y_2$. On the other hand, if $x_1 = y_2$, one can take $z \in X, z \neq x_1, y_1$ and $k \in \mathrm{Stab}_G(x_1)$, $k' \in \mathrm{Stab}_G(z)$ and $k'' \in \mathrm{Stab}_G(y_1)$ such that $kx_2 = z$, $k'x_1 = y_1$ e $k''z = y_2$. We have:

$$k''k'k(x_1) = k''k'(x_1) = k''(y_1) = y_1 \text{ and } k''k'k(x_2) = k''k'(z) = k''(z) = y_2.$$

□

Lemma 4.14. *Let $(i_1 \quad i_2 \ \ldots \ i_k)$ be a k-cycle of S_n and $\sigma \in S_n$. Then*

$$\sigma(i_1 \quad i_2 \ \ldots \ i_k)\sigma^{-1} = (\sigma(i_1) \quad \sigma(i_2) \ \ldots \ \sigma(i_k)).$$

Proof. Let us set $\tau = \sigma(i_1 \quad i_2 \ \ldots \ i_k)\sigma^{-1}$ and $\mu = (\sigma(i_1) \quad \sigma(i_2) \ \ldots \ \sigma(i_k))$. We prove that τ and μ have the same image for all indices. Let $j \in 1, \ldots, n$ be an index. Then if $j = \sigma(i_r)$ for some r, $1 \leq r \leq k-1$, then:

$$\tau(j) = \sigma(i_{r+1}) \qquad \mu(j) = \sigma(i_{r+1});$$

if $j = \sigma(i_k)$ then:

$$\tau(j) = \sigma(i_1) \qquad \mu(j) = \sigma(i_1);$$

if $j \notin \{\sigma(i_1) \quad \sigma(i_2) \ \ldots \ \sigma(i_k)\}$ then:

$$\tau(j) = j \qquad \mu(j) = j.$$

□

Proposition 4.15. *Let p be a prime and G a transitive subgroup of S_p with a transposition. Then $G = S_p$.*

Proof. Let $i, j \in \{1, 2, \ldots, p\}$.
We define the following equivalence relation on $\{1, 2, \ldots, p\}$:

$$i \sim j \Leftrightarrow i = j \quad or \quad (i \ \ j) \in G.$$

Due to the transitivity of G we have that if $i \sim j$ and $j \sim k$ with $i \neq j \neq k \neq i$ then

$$(i\ \ j)(j\ \ k)(i\ \ j) = (i\ \ k) \in G$$

hence $i \sim k$. We will denote by $[i]$ the equivalence class of i. Taken $(i\ \ j) \in G$ and $\sigma \in G$ we have by Lemma 4.14 that

$$(\sigma(i)\ \ \sigma(j)) = \sigma(i\ \ j)\sigma^{-1} \in G$$

hence $\sigma([i]) = [\sigma(i)]$. Since G is transitive, every equivalence class has the same cardinality. Indeed for every $i, j \in \{1, 2, \ldots, p\}$ such that $[i] \neq [j]$ there exists $\sigma \in G$ such that $\sigma(i) = j$, so $\sigma([i]) = [\sigma(i)] = [j]$ and it follows that $|[i]| = |\sigma([i])| = |[j]|$. On the other hand $|([i])| \mid p$ and $|([i])| \neq 1$ because G has at least one transposition by hypothesis. It follows that there is only one equivalence class and so all the transpositions are in G. Since transpositions generate S_p we have $G = S_p$. □

Proposition 4.16. *Let $n > 1$ be a positive integer and $G \leq S_n$ a double transitive subgroup with a transposition. Then $G = S_n$.*

Proof. By hypothesis there exist $i, j \in \{1, 2, \ldots, n\}$ such that the transposition $(i\ \ j) \in G$. Since G is double transitive, it follows that for every couple of elements $k, l \in \{1, 2, \ldots, n\}$ there exists $g \in G$ such that $g(i) = k$ and $g(j) = l$. Then

$$g(i\ \ j)g^{-1} = (g(i)\ \ g(j)) = (k\ \ l) \in G$$

hence G contains all the transpositions, which generate S_n. □

In the next paragraphs we will use the reduction of a polynomial modulo a prime p, formally described by the following map:

$$\begin{aligned} \mathbb{Z}[x] &\to \mathbb{Z}_p[x] \\ f(x) &\mapsto \overline{f}(x) \end{aligned}$$

where $\overline{f}(x)$ is the polynomial $f(x)$ whose coefficients have been reduced modulo p. We will denote the finite field $\mathbb{Z}_p$ by $\mathbb{F}_p$.

Example 4.17. The reduction modulo 5 of $f(x) = 7x^6 + 2x^4 + 13x^2 + 9x + 1$ is $\overline{f}(x) = 2x^6 + 2x^4 + 3x^2 + 4x + 1$.

4.3 Dedekind's Theorem

Lemma 4.18. *For every p prime and n positive integer, there is a unique field of cardinality p^n, up to isomorphism.*

Proof. Let us set $q = p^n$. We define the polynomial $f = x^q - x$ in $\mathbb{F}_p[x]$ and let $\mathbb{K}$ be its splitting field, where f has different roots because $f' = -1 \neq 0$. Let $A = \{\alpha_1, \ldots, \alpha_q\}$ be the set of roots of f. It holds that $\beta \in A \Leftrightarrow \beta^q = \beta$. Moreover we observe that $0, 1 \in A$ and for all $\beta, \gamma \in A$

$$\begin{cases} \beta \cdot \gamma \in A \\ \gamma^{-1} \in A \ \ (\gamma \neq 0) \\ \gamma + \beta \in A \end{cases}$$

where the last property follows from Frobenius endomorphism. Thus A is a field and $A = \mathbb{K}$. Moreover it is unique (up to isomorphism) because the splitting field is so. □

Corollary 4.19. *For every prime p and positive integer n there exists an irreducible polynomial of degree n in $\mathbb{F}_p[x]$.*

Proof. If we denote by $\mathrm{GF}(p^n)$ the only field of cardinality p^n, we have $\mathrm{GF}(p^n) = \mathbb{Z}_p[\alpha]$ for some $\alpha \in \mathrm{GF}(p^n)$. The minimal polynomial of α meets the requirements. □

Lemma 4.20. *Let p be a prime and $n \in \mathbb{Z}^+$. Set $q = p^n$ and let $\mathbb{L} = \mathrm{GF}(q)$ be the finite field with q elements. Then $\mathrm{Gal}(\mathbb{L}/\mathbb{F}_p)$ is cyclic.*

Proof. We know that $\mathbb{L} = \mathbb{F}_p(\alpha)$ for some $\alpha \in \mathbb{L}$ with minimal polynomial $f(x) \in \mathbb{F}_p(x)$ of degree n. Since finite fields are perfect, $\mathbb{F}_p \subset \mathbb{L}$ is a Galois extension, hence $|\mathrm{Gal}(\mathbb{L}/\mathbb{F}_p)| = n$. Let us set $G = \mathrm{Gal}(\mathbb{L}/\mathbb{F}_p)$ and consider the Frobenius endomorphism

$$\begin{aligned} \Psi : \mathbb{L} &\to \mathbb{L} \\ a &\mapsto a^p. \end{aligned}$$

Since Ψ fixes $\mathbb{F}_p$ it follows that $\Psi \in G$. Moreover, ψ^k for $0 < k < n$ are all different non trivial elements of G. We conclude

$$G =< \Psi > .$$

□

Lemma 4.21. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n. Let p be a prime. Let $\overline{f}(x) \in \mathbb{F}_p(x)$ be the polynomial obtained by reducing the coefficients modulo p. Assume that both f, $\overline{f}$ have no multiple roots. Then both $\mathrm{Gal}_{\mathbb{Q}}(f)$ and $\mathrm{Gal}_{\mathbb{F}_p}(\overline{f})$ are isomorphic to subgroups of S_n. Moreover, denote these subgroups as respectively G and G_p, then $G_p \subseteq G$.*

Proof. For the proof we refer to [9]. □

Theorem 4.22 (**Dedekind**). *Let $f \in \mathbb{Z}[x]$, $deg(f) = n$, be a polynomial without multiple roots. Let p be a prime such that the reduction*

$$\overline{f}(x) = g_1(x) \ldots g_h(x) \in \mathbb{F}_p[x],$$

does not have multiple roots and every g_i is an irreducible factor of $\overline{f}$ in $\mathbb{F}_p[x]$. Then the subgroup of S_n isomorphic to $\mathrm{Gal}_{\mathbb{Q}}(f)$ contains a permutation σ whose cycle decomposition

$$\sigma = \gamma_1 \dots \gamma_h$$

is such that $l(\gamma_i) = deg(g_i)$, where $l(\gamma_i)$ is the length of the cycle.

Proof. We know by Lemma 4.20 that $G_p = \mathrm{Gal}_{\mathbb{F}_p}(\overline{f})$ is cyclic and therefore also the subgroup of S_n isomorphic to it is cyclic. Hence there exists a permutation σ that generates G_p. Let us consider σ as product of disjoint cycles

$$\sigma = (i_{1,1} \;\; i_{1,2} \dots i_{1,m_1})(i_{2,1} \;\; i_{2,2} \dots i_{2,m_2}) \cdots (i_{k,1} \;\; i_{k,2} \dots i_{k,m_k}).$$

Since G_p maps roots of an irreducible polynomial in $\mathbb{F}_p[x]$ in roots of the same polynomial, it follows that the numbers m_1, $m_2, \dots$, m_k are the numbers of roots of respectively $g_1, \dots$, g_h, so $k = h$. Moreover, since g_i does not have multiple roots for all i, we have that m_1, $m_2, \dots$, m_k are the degrees of $g_1, \dots$, g_h. By Lemma 4.21 it follows that

$$\sigma \in G_p \subseteq \mathrm{Gal}_{\mathbb{Q}}(f).$$

□

Example 4.23. Our goal is to prove that the polynomial $f = x^4+12x^3+14x^2+14x+34 \in \mathbb{Z}[x]$ has Galois group S_4. The polynomial f is irreducible by Eisenstein's criterion with $p = 2$, hence it is separable because $\mathbb{Q}$ is a perfect field. Moreover we compute

$$\overline{f} = x^4 + 2x^2 + 2x + 1 \pmod 3 = (x-1)(x^3 + x^2 + 2) \pmod 3,$$
$$\overline{f} = x^4 + 2x^3 + 4x^2 + 4x + 4 \pmod 5 = (x-1)(x-2)(x^2 + 2) \pmod 5$$

where the factors are irreducible respectively in $\mathbb{F}_3$ and $\mathbb{F}_5$ which are perfect fields, hence they have no multiple roots. By Dedekind's Theorem 4.22, $\mathrm{Gal}_{\mathbb{Q}}(f)$ has a cycle of length 2 and a cycle of length 3 (indeed the factors of degree 1 correspond to cycles of length 1, hence the identity permutation). We define $G = \mathrm{Gal}_{\mathbb{Q}}(f)$ and we number the roots of f with $\{1, 2, 3, 4\}$. Without loss of generality, we consider the 3-cycle to be (1 2 3). The subgroup $\mathrm{Stab}_G(4)$ acts transitively on $\{1, 2, 3\}$ because (1 2 3) $\in \mathrm{Stab}_G(4)$ and this cycle and its powers acts transitively. We already know from Proposition 4.9 that G is transitive; then G is double transitive because of Proposition 4.13. Since G is double transitive and contains a transposition (the 2-cycle), it follows from Proposition 4.16 that $G \cong S_4$.

Lemma 4.24. *Let $f \in \mathbb{Z}[x]$ be a primitive polynomial. If there exists a prime p such that p does not divide the leading coefficient of f and the reduction of f modulo p is irreducible in $\mathbb{Z}_p[x]$ then f is also irreducible in $\mathbb{Z}[x]$.*

Proof. Let $\Phi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ the map of reduction modulo p. Arguing by contradiction, if f is (non trivially) reducible in $\mathbb{Z}[x]$ we have:

$$f = g \cdot h \quad \text{with} \quad 0 < deg(g) < deg(f) \quad \text{and} \quad 0 < deg(h) < deg(f)$$

and since p does not divide the leading coefficient of f, it follows that p does not divide the leading coefficients of g and h neither. Since Φ_p is an homomorphism, we have:

$$\Phi_p(f) = \Phi_p(g) \cdot \Phi_p(h)$$

where

$$0 < deg(\Phi_p(g)) < deg(\Phi_p(f)) \quad \text{and} \quad 0 < deg(\Phi_p(h)) < deg(\Phi_p(f)),$$

indeed the degrees of the reduced polynomials are the same as the original ones because p does not divide their leading coefficients. We obtain an absurd, since $\Phi_p(f)$ is irreducible in $\mathbb{Z}_p[x]$. □

Example 4.25. Consider the polynomial $f(x) = 4x^4 + 6x^3 + x^2 - 3x - 4$ and take $p = 3$. We have that $3 \nmid 4$ and the reduction of f modulo 3 is

$$\overline{f}(x) = x^4 + x^2 + 2 \in \mathbb{Z}_3[x],$$

which has no roots in $\mathbb{Z}_3$. Moreover, it can not be factorized as 2 polynomials of degree 2, since the only irreducible polynomials of degree 2 in $\mathbb{Z}_3[x]$ are $x^2 + 1$, $x^2 + x + 2$ and $x^2 + 2x + 2$. Hence, $\overline{f}$ is irreducible in $\mathbb{Z}_3[x]$ and by Lemma 4.24 it follows that f is irreducible in $\mathbb{Z}[x]$.

4.4 Realization of S_n

We are now ready for the following general result:

Theorem 4.26. *For every $n \in \mathbb{Z}$, $n > 2$, there exists a polynomial $f(x) \in \mathbb{Q}[x]$ such that $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_n$.*

Proof. Let n be a positive integer greater than 2. We know from Corollary 4.19 that for every prime p and for every positive integer m there exists an irreducible polynomial of degree m in $\mathbb{F}_p[x]$. Hence we are able to choose 3 polynomials of degree n having the following properties:

- $f_1(x) \in \mathbb{F}_2[x]$ irreducible,
- $f_2(x) \in \mathbb{F}_3[x]$ with an irreducible factor of degree $n - 1$ and a factor of degree 1,

- $f_3(x) \in \mathbb{F}_5[x]$ with an irreducible factor of degree 2 and, if n is even, two factors of degree $n-3$ and 1 respectively, else if n is odd, one other factor of degree $n-2$.

Let $f \in \mathbb{Z}[x]$ such that $\overline{f} \equiv f_1 \pmod 2$, $\overline{f} \equiv f_2 \pmod 3$ and $\overline{f} \equiv f_3 \pmod 5$. This choice is always possible because if we denote by f_1', f_2', f_3' the polynomials obtained by the change of coefficients $[\alpha_i]$ of f_1, f_2, f_3 with coefficients $\alpha_i \in \mathbb{Z}$, we can take $f = 15f_1' + 10f_2' + 6f_3'$ as our polynomial. We observe that f is irreducible by Lemma 4.24 with $p = 2$, since the leading coefficient of f is odd and the reduction of f modulo 2 corresponds to f_1 which is irreducible in $\mathbb{F}_2[x]$ by construction. It follows that f is also irreducible in $\mathbb{Q}[x]$ by Gauss Lemma, hence its splitting field is a Galois extension of $\mathbb{Q}$ and its Galois group acts transitively on the set of roots of f by Proposition 4.9. We notice that f_2 and f_3 have no multiple roots since finite fields are perfect (see Proposition 1.5). By Dedekind's Theorem, if n is even, $\mathrm{Gal}_{\mathbb{Q}}(f)$ contains an $(n-1)$-cycle and a permutation σ whose cycle decomposition has a 2-cycle and an $(n-3)$-cycle; on the other hand, if n is odd, $\mathrm{Gal}_{\mathbb{Q}}(f)$ contains an $(n-1)$-cycle and a permutation τ whose cycle decomposition has a 2-cycle and an $(n-2)$-cycle. Both cases have an $(n-1)$-cycle, thus $\mathrm{Gal}_{\mathbb{Q}}(f)$ is double transitive (same reason as in Example 4.23) because it is transitive and we consider $\mathrm{Stab}_G(x)$ where x is the only element missing in the $(n-1)$-cycle. Furthermore, if n is even, σ^{n-3} is a transposition, and if n is odd, τ^{n-2} is also a transposition. In both cases $\mathrm{Gal}_{\mathbb{Q}}(f)$ is double transitive and contains a transposition, hence $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_n$ by Proposition 4.16. □

Example 4.27. Take the polynomial $f(t) = t^4 + 16t^3 - 4t^2 + 3t - 11 \in \mathbb{Z}[t]$. We have:

- $f(t) \equiv t^4 + t + 1 \pmod 2$
- $f(t) \equiv t^4 + t^3 - t^2 + 1 \equiv (t^3 - t + 1)(t + 1) \pmod 3$
- $f(t) \equiv t^4 + t^3 + t^2 - 2t - 1 \equiv (t^2 - 2)(t + 2)(t - 1) \pmod 5$

These factors satisfy the properties required in the proof of Theorem 4.26, hence we conclude $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_4$.

4.5 Consideration

Since S_n occurs as a Galois group over $\mathbb{Q}$, and every finite group occurs as a subgroup of some S_n (see Cayley's Theorem 2.7), it follows that every finite group occurs as a Galois group over some finite extension of $\mathbb{Q}$, but does every finite group occur as a Galois group over $\mathbb{Q}$ itself? This problem is still unsolved.

Example 4.28. Most specializations of the universal polynomial of degree n over $\mathbb{Q}$ have S_n as their Galois group. This follows from the *Hilbert Irreducibility Theorem*, which is discussed in [6]. For example, one can prove that the Galois group of $x^n - x - 1 \in \mathbb{Q}[x]$ is S_n for all $n \geq 2$ (see [18]).

Example 4.29. Consider the polynomial $p_n(x) = 1+x+\frac{1}{2}x^2+\ldots+\frac{1}{n!}x^n$. In 1930 Schur proved that p_n has Galois group A_n if $n \equiv 0 \bmod 4$, otherwise its Galois group is S_n.

If a finite group G occurs as a Galois group over $\mathbb{Q}$, then for all normal subgroups H of G, the quotient group G/H occurs as a Galois group over $\mathbb{Q}$. Indeed, if we set $G = \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ for some finite Galois extension $\mathbb{L} \subset \mathbb{Q}$, using the functions φ and ψ of the fundamental Theorem of Galois theory, we have

$$H \xrightarrow{\psi} \mathbb{L}^H \xrightarrow{\varphi} \mathrm{Gal}(\mathbb{L}/\mathbb{L}^H).$$

Since $H \cong \mathrm{Gal}(\mathbb{L}/\mathbb{L}^H)$ is a normal subgroup of G, we have

$$\mathrm{Gal}(\mathbb{L}^H/\mathbb{Q}) \cong \frac{\mathrm{Gal}(\mathbb{L}/\mathbb{Q})}{\mathrm{Gal}(\mathbb{L}/\mathbb{L}^H)} \cong G/H,$$

hence $\mathbb{Q} \subset \mathbb{L}^H$ is the desired extension. Since we know we can realize cyclic groups, abelian groups, $(\mathbb{Z}/n\mathbb{Z})^*$ and S_n, then we know we can realize every quotient group of these groups.

Unfortunately, the only normal subgroup of S_n for $n \geq 5$ is A_n and the quotient group S_n/A_n is the group of order 2. If we consider the case $n = 4$, also the Klein group is a normal subgroup of S_4, hence we can realize $S_4/V_4 \cong S_3$ as a Galois group, but we already knew it.

Chapter 5

Examples

We want now to go a bit further in the realization of some groups as Galois groups. In order to understand the vastity of the inverse Galois problem, we will first remind a very important result in group theory.

Definition 5.1. A nontrivial group G is said to be *simple* if its only normal subgroups are the trivial group and the group itself.

Theorem 5.2 (**Classification of the finite simple groups**)**.** *Every finite simple group belongs to one of the following classes:*

- *cyclic groups of prime order;*
- *alternating groups of degree at least* 5*;*
- *Lie groups;*
- *sporadic groups;*
- *the Tits group;*

where the first three classes have infinite elements.

Proof. After years of studies from many authors, the proof was completed and announced in 2004 by Aschbacher in [11]. □

5.1 The groups A_3 and S_3

Definition 5.3. In $\mathbb{Q}[x_1, \ldots, x_n]$ we define:

$$\sqrt{\Delta} = \prod_{i<j}(x_i - x_j).$$

Definition 5.4. For a polynomial f with roots $\{\alpha_1, \ldots, \alpha_n\}$ we define:

$$\sqrt{\Delta(f)} = \prod_{i<j}(\alpha_i - \alpha_j).$$

Lemma 5.5. *For a permutation $\sigma \in S_n$ it holds that*

$$\sigma(\sqrt{\Delta}) = sgn(\sigma) \cdot \sqrt{\Delta}.$$

Proof. Since every permutation is product of transpositions, we prove that if $\tau = (i\ \ j)$ is a transposition, then

$$\tau(\sqrt{\Delta}) = -\sqrt{\Delta}.$$

Assume $i < j$ and observe that there is $\epsilon \in \{+1, -1\}$ such that

$$\sqrt{\Delta} = \epsilon(x_i - x_j) \prod_{k \neq i,j} (x_i - x_k)(x_j - x_k) \prod_{l,m \neq i,j\ \ l<m} (x_l - x_m). \tag{5.1}$$

Indeed the factors appearing in the right-hand side are, up to sign, the factors of $\sqrt{\Delta}$. For example, when $k \neq i, j$, then

$$x_i - x_k = \begin{cases} x_i - x_k, & i < k, \\ -(x_k - x_i), & k < i. \end{cases}$$

Combining all of these signs gives $\epsilon = \pm 1$. Since the transposition τ takes $(x_i - x_k)(x_j - x_k)$ to $(x_j - x_k)(x_i - x_k)$ and does not affect $(x_l - x_m)$ for $l, m \neq i, j$, it follows by Equation (5.1) that $\tau(\sqrt{\Delta}) = -\sqrt{\Delta}$. Let us write $\sigma \in S_n$ as product of transpositions $\sigma = \tau_1 \cdots \tau_s$. Then

$$\sigma(\sqrt{\Delta}) = (\tau_1 \cdots \tau_s)(\sqrt{\Delta}) = (-1)^s\sqrt{\Delta} = sgn(\sigma) \cdot \sqrt{\Delta}.$$

□

Proposition 5.6. *Let $f(x) \in \mathbb{Q}[x]$ be a separable polynomial of degree n and let $\alpha_1, \ldots, \alpha_n$ be its different roots in the splitting field of f.*

a) If $\sigma \in \mathrm{Gal}(f)$ corresponds to $\overline{\sigma} \in S_n$ in the identification of $\mathrm{Gal}(f)$ with a subgroup of S_n, then

$$\sigma(\sqrt{\Delta(f)}) = sgn(\overline{\sigma}) \cdot \sqrt{\Delta(f)}.$$

b) The subgroup of S_n isomorphic to $\mathrm{Gal}(f)$ is contained in A_n if and only if $\sqrt{\Delta(f)} \in \mathbb{Q}$.

Proof. Let $\mathbb{L}$ be the splitting field of f and consider ϕ the evaluation homomorphism

$$\begin{aligned} \phi : \mathbb{Q}[x_1, \ldots, x_n] &\to \mathbb{L} \\ a &\mapsto a \qquad \forall a \in \mathbb{Q}, \\ x_i &\mapsto \alpha_i. \end{aligned}$$

Clearly $\sqrt{\Delta(f)} = \phi(\sqrt{\Delta})$. Then

$$\begin{aligned} \sigma(\sqrt{\Delta(f)}) &= \sigma\left(\prod_{i<j}(\alpha_i - \alpha_j)\right) = \prod_{i<j}(\sigma(\alpha_i) - \sigma(\alpha_j)) = \prod_{i<j}(\alpha_{\overline{\sigma}(i)} - \alpha_{\overline{\sigma}(j)}) = \\ &= \phi\left(\prod_{i<j}(x_{\overline{\sigma}(i)} - x_{\overline{\sigma}(j)})\right) = \phi(\overline{\sigma}(\prod_{i<j}(x_i - x_j))) = \phi(sgn(\overline{\sigma}))(\sqrt{\Delta}) = \\ &= sgn(\overline{\sigma})\phi(\sqrt{\Delta}) = sgn(\overline{\sigma})\sqrt{\Delta(f)}, \end{aligned}$$

This proves the first part of the Proposition. We now observe that

$$\sqrt{\Delta(f)} \in \mathbb{Q} \iff \sigma(\sqrt{\Delta(f)}) = \sqrt{\Delta(f)} \qquad \forall\ \sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q}).$$

Using the first part of the Proposition we get

$$\sigma(\sqrt{\Delta(f)}) = sgn(\overline{\sigma}) \cdot \sqrt{\Delta(f)}.$$

Hence

$$\sqrt{\Delta(f)} \in \mathbb{Q} \iff sgn(\overline{\sigma}) \cdot \sqrt{\Delta(f)} = \sqrt{\Delta(f)} \qquad \forall\ \sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q}).$$

Since f is separable, $\sqrt{\Delta(f)} \neq 0$ and if we simplify it we get

$$\sqrt{\Delta(f)} \in \mathbb{Q} \iff sgn(\overline{\sigma}) = 1 \quad \forall\ \sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q}) \iff \mathrm{Gal}(\mathbb{L}/\mathbb{Q}) \subseteq A_n.$$

□

Example 5.7. Consider the following cubic polynomial

$$f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$$

and set $x = y - a/3$ so that it becomes

$$g(y) = y^3 + py + q$$

where

$$p = \frac{1}{3}(3b - a^2) \qquad q = \frac{1}{27}(2a^3 - 9ab + 27c).$$

The splitting field for these two polynomials, $f(x)$ and $g(y)$, is the same since their roots differ by the constant term $a/3 \in \mathbb{Q}$. Moreover f and g have the same discriminant since it only depends on the differences of roots. Let α, β, γ be the roots of $g(y)$. We compute its discriminant in terms of p and q. In order to do this we observe that

$$g(y) = (y-\alpha)(y-\beta)(y-\gamma)$$

and if we differentiate

$$g'(y) = (y-\alpha)(y-\beta) + (y-\alpha)(y-\gamma) + (y-\beta)(y-\gamma).$$

Then

$$\begin{aligned} g'(\alpha) &= (\alpha-\beta)(\alpha-\gamma), \\ g'(\beta) &= (\beta-\alpha)(\beta-\gamma), \\ g'(\gamma) &= (\gamma-\alpha)(\gamma-\beta). \end{aligned}$$

Therefore

$$\Delta(g) = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 = -g'(\alpha)g'(\beta)g'(\gamma).$$

On the other hand, it results that $g'(y) = 3y^2 + p$, hence we get

$$\begin{aligned} -\Delta(g) &= (3\alpha^2+p)(3\beta^2+p)(3\gamma^2+p) = \\ &= 27\alpha^2\beta^2\gamma^2 + 9p(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) + 3p^2(\alpha^2+\beta^2+\gamma^2) + p^3. \end{aligned}$$

Note that if we consider the elementary symmetric functions in α, β, γ we obtain $\sigma_1 = 0$, $\sigma_2 = p$, $\sigma_3 = -q$. The expression above for $-\Delta$ is symmetric in α, β, γ and as we did in Examples 2.9, 2.10, 2.11, we obtain

$$-\Delta = 27(-q)^2 + 9p(p^2) + 3p^2(-2p) + p^3$$

hence

$$\Delta = -4p^3 - 27q^2$$

and expressing it in terms of a, b, c we get

$$\Delta = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc,$$

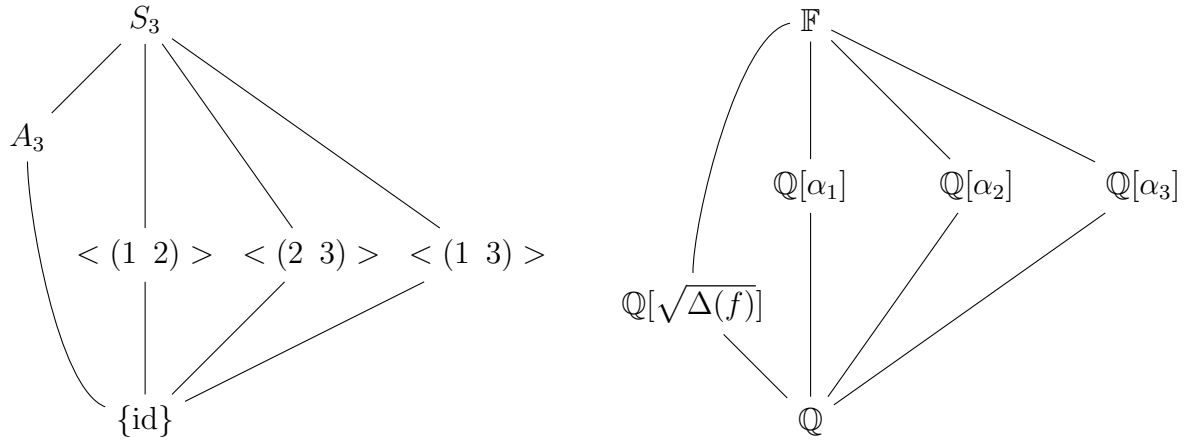
in other words we have an expression to determine Δ through the coefficients of the polynomial.

We analyze the Galois group of a cubic polynomial and it turns out that we can determine it by computing Δ with the expression above.

If the cubic f is reducible and splits in 3 linear factors, then its Galois group is trivial; while if f is reducible but only splits into a linear factor and an irreducible quadratic,

then we obtain a Galois group of order 2. Consider now the case f irreducible. Let us denote by α_1, α_2, α_3 the different roots of f and by $\mathbb{L}$ its splitting field. The Galois group of f is a normal subgroup of S_3, hence there are only 2 possibilities, namely, either A_3 or S_3 (the subgroup generated by a transposition is not normal, since two transpositions are always conjugate). Thanks to Proposition 5.6 we know that the Galois group is A_3 if and only if the discriminant Δ is a square.

$$\begin{aligned} \mathrm{Gal}(f) &\cong A_3 \qquad if \quad \sqrt{\Delta(f)} \in \mathbb{Q}, \\ \mathrm{Gal}(f) &\cong S_3 \qquad if \quad \sqrt{\Delta(f)} \notin \mathbb{Q}. \end{aligned}$$



Example 5.8. The polynomial $f = x^3 - 3x + 1$ is irreducible in $\mathbb{Q}[x]$, since its possible rational roots are only ± 1 (recall that if f is a monic polynomial, a root of f in $\mathbb{Q}$ must be an integer and must divide the constant term), but $f(1) \neq 0 \neq f(-1)$. Its discriminant is

$$(-4) \cdot (-3)^3 - 27 = 81 = 9^2$$

hence its Galois group is A_3.

Example 5.9. On the other hand, $g = x^3 - 4x + 1 \in \mathbb{Q}[x]$ is also irreducible for the same reason as in Example 5.8, but its discriminant is 229, which is not a square in $\mathbb{Q}$, hence its Galois group is isomorphic to S_3.

5.2 Ordered Examples

We will now show how to realize every group of order at most 8. Moreover, we will show how to realize $\mathrm{AGL}(1, \mathbb{F}_p)$. The reader can find many other group realizations in [3].

5.2.1 Order 1

The only group with 1 element is the trivial group $G = \{e\}$. Taken a polynomial $f(x) \in \mathbb{Q}[x]$ all roots lie in $\mathbb{Q}$, we have that $\mathrm{Gal}_{\mathbb{Q}}(f) = G$.

5.2.2 Order 2

The only group of order 2 is the cyclic group $\mathbb{Z}_2$. We already know by Theorem 3.11 that every cyclic group occurs as a Galois group over $\mathbb{Q}$. Now we want to give an explicit example of a polynomial with Galois group $\mathbb{Z}_2$. For a fixed element $a \in \mathbb{Q}$ which is not a square in $\mathbb{Q}$, the polynomial $f = x^2 - a$ has Galois group over $\mathbb{Q}$ isomorphic to $\mathbb{Z}_2$. Indeed the splitting field of f is clearly $\mathbb{Q}[\sqrt{a}]$, which is a field extension of $\mathbb{Q}$ of degree 2, and it follows that the Galois group has at most 2 elements. The identity map and the field automorphism

$$\begin{aligned} \mathbb{Q}[\sqrt{a}] &\to \mathbb{Q}[\sqrt{a}] \\ b &\mapsto b \qquad \forall\, b \in \mathbb{Q} \\ \sqrt{a} &\mapsto -\sqrt{a} \end{aligned}$$

are two different elements of the Galois group, then $\mathrm{Gal}(\mathbb{Q}[\sqrt{a}]/\mathbb{Q}) \cong \mathbb{Z}_2$.
Observe that if we take f as above with a a square in $\mathbb{Q}$, it follows that the splitting field of f is $\mathbb{Q}$, hence its Galois group is the trivial one because only the identity map belongs to it.

5.2.3 Order 3

The only group of order 3 is the cyclic group $G = \mathbb{Z}_3$. Hence, we look for a Galois extension over $\mathbb{Q}$ of order 3, so that its Galois group has exactly order 3. In order to get a Galois extension of degree 3, we need a polynomial of degree 3 with all real roots, since otherwise complex conjugation is an automorphism of order 2. We consider the cyclotomic polynomial $\Phi_7(x) = x^6 + x^5 + \ldots + x + 1$ which is irreducible and generates a Galois extension over $\mathbb{Q}$ of degree 6 with Galois group $\mathbb{Z}_6$, and if ξ_7 is a primitive 7th root of unity, $L = \mathbb{Q}(\xi_7)$ is the extension. The element $\xi_7 + \xi_7^{-1} = 2cos(\frac{2\pi}{7})$ is fixed by complex conjugation (an element of order 2) and no other element of $\mathrm{Gal}(\mathbb{Q}(\xi_7)/\mathbb{Q})$ fixes it. But then $\mathbb{Q} \subset \mathbb{Q}(\xi_7 + \xi_7^{-1}) = \mathbb{K}$ is a Galois extension of degree 3, because that is the index of the Galois group over the group generated by complex conjugation, and we can use the fundamental Theorem of Galois theory. Note that the extension is a Galois extension, since $\mathbb{Z}_6$ is abelian, hence all its subgroups are normal. Hence $\mathbb{Q} \subset \mathbb{K}$ is the desired extension. We can explicitly determine the minimal polynomial of $2cos(\frac{2\pi}{7})$, indeed the polynomial

$$p(x) = x^3 + x^2 - 2x - 1$$

is irreducible by Lemma 4.24 with $p = 2$, it is monic, and an easy computation shows that

$$p(\xi_7 + \xi_7^{-1}) = 0$$

by using the fact that $\xi_7^7 = 1$. Note that in Example 5.8, we have another example of a polynomial with Galois group $\mathbb{Z}_3 \cong A_3$. However, the method we have just used, can be generalized. Take p a prime, and consider the cyclotomic polynomial $\Phi_p(x)$, which is irreducible and if $\mathbb{L}$ is its splitting field, we have

$$\mathbb{L} = \mathbb{Q}(\xi_p) \qquad G = \mathrm{Gal}(\mathbb{L}/\mathbb{Q}) = \mathbb{Z}_{p-1}.$$

Observe that the element $\xi_p + \xi_p^{-1}$ is fixed by complex conjugation and no other element of G fixes it. Then we can use the fundamental Theorem of Galois theory:

$$\begin{array}{ccc} G & & \mathbb{L} \\ \uparrow & & \uparrow \\ \frac{p-1}{2} & & 2 \\ | & & | \\ H =< \tau > & & \mathbb{Q}(\xi_p + \xi_p^{-1}) \\ \uparrow & & \uparrow \\ 2 & & \frac{p-1}{2} \\ | & & | \\ \{\mathrm{id}\} & & \mathbb{Q} \end{array}$$

Indeed, if we set $\mathbb{K} = \mathbb{Q}(\xi_p + \xi_p^{-1})$, this is an intermediate field and

$$H = \mathrm{Gal}(\mathbb{L}/\mathbb{K}) =< \tau >,$$

where τ is the complex conjugation. Then we have that $\mathbb{Q} \subset \mathbb{K}$ is a Galois extension since $\mathbb{Z}_{p-1}$ is abelian and

$$[\mathbb{K} : \mathbb{Q}] = [\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) : H] = \frac{p-1}{2}.$$

Hence its Galois group is the cyclic group $\mathbb{Z}_{\frac{p-1}{2}}$. Using this argument, we can realize every cyclic group of order $\frac{p-1}{2}$ with p prime. The polynomial that realizes this extension is the minimal polynomial of $\xi_p + \xi_p^{-1}$ over $\mathbb{Q}$. We will refer to this method as Method I, and we can use it, for example, to realize the groups $\mathbb{Z}_5$, $\mathbb{Z}_8$, $\mathbb{Z}_9$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{14}$ and $\mathbb{Z}_{15}$.

5.2.4 Order 4

There are 2 groups of order 4, which are the cyclic group $\mathbb{Z}_4$ and the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$. We have already seen in Example 3.13 that the polynomial x^4+5x^2+5 has Galois group $\mathbb{Z}_4$. On the other hand, if we want to find a polynomial whose Galois group is the Klein group V_4, we can use the following proposition.

Proposition 5.10. *Let $\mathbb{Q} \subset \mathbb{L}$ be a finite field extension. Then the following are equivalent:*

a) $\mathbb{L} = \mathbb{Q}(\sqrt{\alpha}, \sqrt{\beta})$ for some $\alpha, \beta \in \mathbb{Q}$ such that none of α, β or $\alpha\beta$ is a square in $\mathbb{Q}$.

b) $\mathbb{L}$ is a Galois extension of $\mathbb{Q}$ with Galois group V_4.

Proof. Suppose first that condition a holds. Then

$$[\mathbb{Q}(\sqrt{\alpha}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{\beta}) : \mathbb{Q}] = 2$$

since neither α or β is a square in $\mathbb{Q}$. Now from Tower Lemma we get

$$[\mathbb{L} : \mathbb{Q}] = [\mathbb{Q}(\sqrt{\alpha}, \sqrt{\beta}) : \mathbb{Q}(\sqrt{\alpha})] \cdot [\mathbb{Q}(\sqrt{\alpha}) : \mathbb{Q}] \leq 4$$

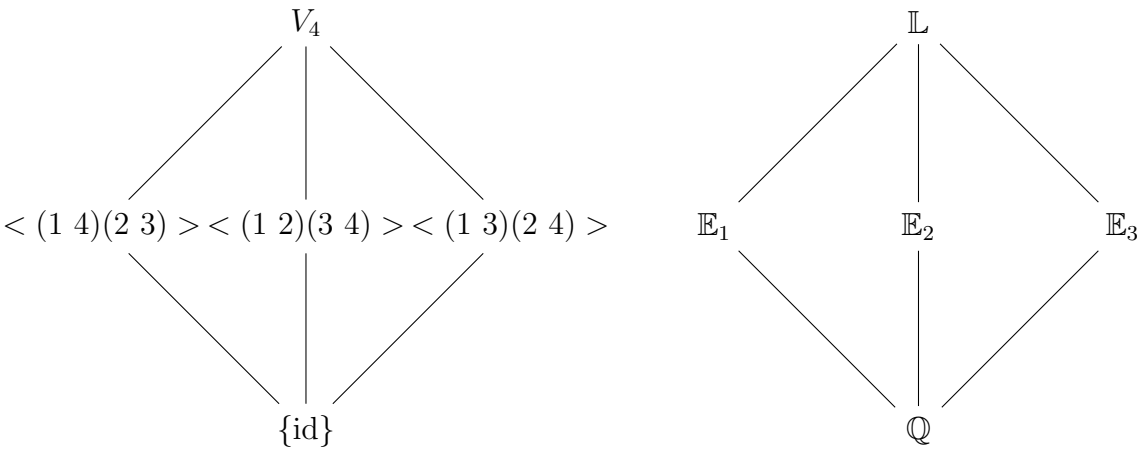
hence $[\mathbb{L} : \mathbb{Q}(\sqrt{\alpha})] \leq 2$. Assume that $\mathbb{L} = \mathbb{Q}(\sqrt{\alpha})$, then $\sqrt{\beta} \in \mathbb{Q}(\sqrt{\alpha})$, so that $\sqrt{\beta} = a + b\sqrt{\alpha}$ for some $a, b \in \mathbb{Q}$ and $\beta = a^2 + b^2\alpha + 2ab\sqrt{\alpha}$. Thus $a = 0$ or $b = 0$, indeed $\beta \in \mathbb{Q}$. If $b = 0$, then β is a square. If $a = 0$, then $\alpha\beta = b^2\alpha^2$ is a square. In any case, this is a contradiction, hence $\mathbb{L}$ is a quadratic extension of $\mathbb{Q}(\sqrt{\alpha})$. This way we conclude that $[\mathbb{L} : \mathbb{Q}] = 4$. But $\mathbb{L}$ is clearly the splitting field for the polynomial

$$(x^2 - \alpha) \cdot (x^2 - \beta)$$

which is a separable polynomial and it follows that we have a Galois extension. Then $G = \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ has 4 elements:

$$\mathrm{id} \qquad \tau : \begin{cases} \sqrt{\alpha} \mapsto -\sqrt{\alpha} \\ \sqrt{\beta} \mapsto \sqrt{\beta} \end{cases} \qquad \sigma : \begin{cases} \sqrt{\alpha} \mapsto \sqrt{\alpha} \\ \sqrt{\beta} \mapsto -\sqrt{\beta} \end{cases} \qquad \sigma\tau : \begin{cases} \sqrt{\alpha} \mapsto -\sqrt{\alpha} \\ \sqrt{\beta} \mapsto -\sqrt{\beta} \end{cases}$$

and thus is isomorphic to V_4.
Now assume that condition b holds. Since $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) \cong V_4$, there exist three intermediate subfields $\mathbb{E}_1$, $\mathbb{E}_2$, $\mathbb{E}_3$ between $\mathbb{Q}$ and $\mathbb{L}$ which are extensions of degree 2 over $\mathbb{Q}$, corresponding to the three subgroups of V_4 of order 2.



Thus each of these is a quadratic extension. Suppose $\mathbb{E}_1 = \mathbb{Q}(\sqrt{\alpha})$ and $\mathbb{E}_2 = \mathbb{Q}(\sqrt{\beta})$, where neither α or β is a square in $\mathbb{Q}$. The fact $\mathbb{E}_1 \neq \mathbb{E}_2$ implies that $\alpha\beta$ is also not a square in $\mathbb{Q}$. Indeed, $\sqrt{\beta} \notin \mathbb{Q}(\sqrt{\alpha})$, so

$$\sqrt{\beta} \neq a + b\sqrt{\alpha} \qquad \forall\ a, b \in \mathbb{Q}$$

hence

$$\beta \neq a^2 + b^2\alpha + 2ab\sqrt{\alpha} \qquad \forall\ a, b \in \mathbb{Q}.$$

In particular, it is true for $a = 0$:

$$\beta \neq b^2\alpha \qquad \forall\ b \in \mathbb{Q}.$$

Arguing by contradiction, if there exists $c \in \mathbb{Q}$ such that $\alpha\beta = c^2$, we could take $b = \frac{c}{\alpha}$ and we would have the contradiction

$$\beta = b^2\alpha.$$

Moreover $\mathbb{Q}(\sqrt{\alpha}, \sqrt{\beta})$ is an extension of degree 4 over $\mathbb{Q}$ and it is a subfield of $\mathbb{L}$, hence

$$\mathbb{L} = \mathbb{Q}(\sqrt{\alpha}, \sqrt{\beta}).$$

□

Now, if we consider the polynomial

$$x^4 - 7x^2 + 10 = (x^2 - 2) \cdot (x^2 - 5)$$

we have that its splitting field is $\mathbb{L} = \mathbb{Q}(\sqrt{2}, \sqrt{5})$, and since none of $2, 5, 10$ is a square in $\mathbb{Q}$, we have that

$$\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) = V_4.$$

5.2.5 Order 5

The only group of order 5 is the cyclic group $G = \mathbb{Z}_5$. We can realize this group using Method I with $p = 11$, and the minimal polynomial of $\xi_{11} + \xi_{11}^{-1}$ results

$$p(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1.$$

5.2.6 Order 6

There are 2 groups of order 6, which are the cyclic group $\mathbb{Z}_6$ and the dihedral group $D_6 = S_3$. We can realize $\mathbb{Z}_6$ using the 7th cyclotomic polynomial. Set $\mathbb{L}$ as the splitting field of $\Phi_7(x)$ we have

$$\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) = \mathbb{Z}_6.$$

On the other hand, in Example 5.9, we found that the polynomial $x^3 - 4x + 1$ has Galois group $S_3 = D_6$.

5.2.7 Order 7

The only group of order 7 is the cyclic group $\mathbb{Z}_7$. To realize this group, we will use a slightly different method from Method I. Let ξ_{29} be a primitive 29th root of unity. Then we know that if we set $\mathbb{L} = \mathbb{Q}(\xi_{29})$ we have

$$G = \mathrm{Gal}(\mathbb{L}/\mathbb{Q}) = \mathbb{Z}_{28}.$$

Since $[2]_{29}$ is a generator of $(\mathbb{Z}/29\mathbb{Z})^*$, the Galois group is generated by the automorphism $\xi_{29} \mapsto \xi_{29}^2$ (see the isomorphism in Equation (3.2)). Furthermore, we can find an element of order 4 by the seventh power of this automorphism, namely $\psi : \xi_{29} \mapsto \xi_{29}^{2^7} = \xi_{29}^{12}$. Let H be the cyclic subgroup of G of order 4 generated by ψ. Then, using the fundamental Theorem of Galois theory, we have that $G/H \cong \mathbb{Z}_7$ is the Galois group of the Galois extension $\mathbb{Q} \subset \mathbb{Q}(\xi_{29})^H = \mathbb{K}$. One can find out that $\mathbb{K} = \mathbb{Q}(\theta)$, where

$$\theta = \xi_{29} + \xi_{29}^{12} + \xi_{29}^{28} + \xi_{29}^{17},$$

and that the minimal polynomial of θ is

$$f(x) = x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1.$$

For details see, for example, [3].

5.2.8 Order 8

There are 5 groups of order 8 (up to isomorphism), namely $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_8 and Q_8 (quaternion group). We can realize the cyclic group Z_8 using Method I with $p = 17$; one can find out that the minimal polynomial of $\xi_{17} + \xi_{17}^{-1} = \xi$ is

$$p(x) = x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 + 10x^3 - 10x^2 - 4x + 1$$

and $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) = \mathbb{Z}_8$. In order to find a Galois extension with Galois group $\mathbb{Z}_2 \times \mathbb{Z}_4$, we observe that by Chinese reminder Theorem

$$(\mathbb{Z}/15\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$

hence we only need to find a Galois extension with Galois group $(\mathbb{Z}/15\mathbb{Z})^*$. We know by Theorem 3.6 that

$$\mathrm{Gal}(\mathbb{Q}(\xi_{15})/\mathbb{Q}) \cong (\mathbb{Z}/15\mathbb{Z})^*$$

hence $\mathbb{Q} \subset \mathbb{Q}(\xi_{15})$ is the desired extension, and the minimal polynomial of ξ_{15} over $\mathbb{Q}$ is the 15th cyclotomic polynomial

$$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.$$

In order to realize $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ we will follow the steps of the proof of Kronecker-Weber Theorem. We know that if ξ_{165} is a primitive 165th root of unity, then

$$\mathrm{Gal}(\mathbb{Q}(\xi_{165})/\mathbb{Q}) \cong (\mathbb{Z}_{165})^* \cong (\mathbb{Z}_3)^* \times (\mathbb{Z}_5)^* \times (\mathbb{Z}_{11})^*.$$

Using $p_1 = 3$, $p_2 = 5$ and $p_3 = 11$ we have three different primes such that $p_i \equiv 1$ modulo 2, and we have the surjective homomorphism

$$\begin{aligned} \phi : \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{10} &\to \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\ ([a]_2, [b]_4, [c]_{10}) &\mapsto ([a]_2, [b]_2, [c]_2). \end{aligned}$$

We now consider the following subgroups:

$$H_1 =< [2]_2 >= \{e\} \leq \mathbb{Z}_2 \qquad H_2 =< [2]_4 > \cong \mathbb{Z}_2 \leq \mathbb{Z}_4 \qquad H_3 =< [2]_{10} > \cong \mathbb{Z}_5 \leq \mathbb{Z}_{10}$$

and $H = H_1 \times H_2 \times H_3$. Set $\mathbb{E}$ the field of elements fixed by H, then

$$\mathrm{Gal}(\mathbb{E}/\mathbb{Q}) \cong \frac{\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{10}}{H_1 \times H_2 \times H_3} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

One can prove (see, for example, [3]) that $\mathbb{E} = \mathbb{Q}(\alpha)$ is the splitting field for

$$p(x) = x^8 + 12x^7 + 68x^6 + 234x^5 + 547x^4 + 906x^3 + 960x^2 + 504x + 144.$$

We want now to show that D_8 occurs as a Galois group over $\mathbb{Q}$. Consider the polynomial $f = x^4 - 2$ which is irreducible in $\mathbb{Q}[x]$ due to Eisenstein's criterion, and set $G = \mathrm{Gal}_{\mathbb{Q}}(f)$ its Galois group isomorphic to a subgroup of S_4. We order the roots of f as $(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2})$, thus the splitting field of f is $\mathbb{L} = \mathbb{Q}(\sqrt[4]{2}, i)$. Let us compute the discriminant of f:

$$\begin{aligned}\sqrt{\Delta(f)} &= (\sqrt[4]{2} + \sqrt[4]{2})(\sqrt[4]{2} - i\sqrt[4]{2})(\sqrt[4]{2} + i\sqrt[4]{2})(-\sqrt[4]{2} - i\sqrt[4]{2})(-\sqrt[4]{2} + i\sqrt[4]{2})(i\sqrt[4]{2} + i\sqrt[4]{2}) \\ &= -2^{11}\end{aligned}$$

which is not a square in $\mathbb{Q}$. By Proposition 5.6 it follows that G is not contained in A_4. By Tower Lemma we have

$$[\mathbb{L} : \mathbb{Q}] = [\mathbb{L} : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8,$$

hence $|G| = 8$. This implies it is a Sylow-2 subgroup of S_4, all of which are isomorphic by the second Sylow theorem. We know that D_8 is such a subgroup, hence

$$G \cong D_8.$$

We want now to find a Galois extension with Galois group the quaternion group Q_8. The candidate extension is $\mathbb{Q} \subset \mathbb{Q}(\alpha) = \mathbb{L}$ where $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$. First we note that we have an intermediate field $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$ given by $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. This is a proper subfield of $\mathbb{L}$ since $\alpha \notin \mathbb{K}$. Indeed, if we consider $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ such that $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{3}) = \sqrt{3}$ we have that

$$\frac{\sigma(\alpha^2)}{\alpha^2} = \frac{2-\sqrt{2}}{2+\sqrt{2}} = 3 - 2\sqrt{2} = (1-\sqrt{2})^2.$$

It follows that $\sigma(\alpha^2) = \alpha^2(1-\sqrt{2})^2$. Arguing by contradiction, if $\alpha \in \mathbb{K}$, we have

$$\sigma(\alpha) = \pm\alpha(1-\sqrt{2}),$$

and so

$$\sigma(\sigma(\alpha)) = \alpha(1-\sqrt{2})(1+\sqrt{2}) = -\alpha,$$

which is an absurd since σ has order 2. Moreover, one can prove that $\sqrt{2}+\sqrt{3} \in \mathbb{L}$, hence $\mathbb{K} \subset \mathbb{L}$. It follows that

$$[\mathbb{L} : \mathbb{Q}] = [\mathbb{L} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{Q}] = 2 \cdot 4 = 8.$$

The minimal polynomial of $(2+\sqrt{2})(3+\sqrt{3})$ over $\mathbb{Q}$ is

$$f(x) = \prod_{\tau \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})} (x - \tau((2+\sqrt{2})(3+\sqrt{3}))) = \prod (x - (2 \pm \sqrt{2})(3 \pm \sqrt{3}))$$

and

$$g(x) = f(x^2) = x^8 - 24x^6 + 144x^4 - 288x^2 + 144$$

is a polynomial of degree 8 and it has α as a root, hence $g(x)$ is the minimal polynomial of α over $\mathbb{Q}$. The polynomial $g(x)$ has 8 different roots:

$$\pm\sqrt{(2 \pm \sqrt{2})(3 \pm \sqrt{3})}$$

and each of these roots is an element of $\mathbb{L}$. Hence $\mathbb{L}$ is the splitting field of a separable polynomial, and so $\mathbb{Q} \subset \mathbb{L}$ is a Galois extension and $G = \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ is a group of order 8. G acts transitively on the roots of $g(x)$ and we know that an element of G is uniquely determined by its image on α. Consider the following roots of $g(x)$:

$$\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})} \qquad \beta = \sqrt{(2-\sqrt{2})(3+\sqrt{3})}$$
$$\gamma = \sqrt{(2+\sqrt{2})(3-\sqrt{3})} \qquad \delta = \sqrt{(2-\sqrt{2})(3-\sqrt{3})}$$

and set σ, τ the elements of G such that

$$\sigma(\alpha) = \beta \qquad \tau(\alpha) = \gamma.$$

We now observe that $\sigma(\alpha^2) = \beta^2$ and so that

$$\sigma(2+\sqrt{2})\sigma(3+\sqrt{3}) = (2-\sqrt{2})(3+\sqrt{3})$$

and $\sigma(\alpha\beta) = \sigma(\sqrt{2}(3+\sqrt{3})) = -\alpha\beta$. It follows that $\sigma(\beta) = -\alpha$ and so σ is an element of order 4 in G. Using the same argument for τ, it follows that $\tau(\gamma) = -\alpha$ and τ is an element of order 4 of G. We observe that

$$\sigma^2(\alpha) = \tau^2(\alpha) = -\alpha.$$

Let us now compute the composition

$$\sigma\tau(\alpha) = \sigma(\gamma) = \sigma\left(\frac{\alpha\gamma}{\alpha}\right) = \frac{\sigma(\sqrt{6}(2+\sqrt{2}))}{\sigma(\alpha)} = \frac{-\sqrt{6}(2-\sqrt{2})}{\beta} = -\frac{\beta\delta}{\beta} = -\delta$$

and

$$\tau\sigma(\alpha) = \tau(\beta) = \tau\left(\frac{\alpha\beta}{\alpha}\right) = \frac{\tau(\sqrt{2}(3+\sqrt{3}))}{\tau(\alpha)} = \frac{\sqrt{2}(3-\sqrt{3})}{\gamma} = \frac{\gamma\delta}{\gamma} = \delta.$$

Moreover we observe that

$$\tau\sigma^3(\alpha) = \tau\sigma(-\alpha) = -\tau\sigma(\alpha) = -\delta = \sigma\tau(\alpha),$$

hence $\sigma\tau = \tau\sigma^3$. We now observe that these elements of G satisfy the relations of elements of Q_8, indeed the map

$$\begin{aligned} G &\to Q_8 \\ \sigma &\mapsto i \\ \tau &\mapsto j \\ \sigma\tau &\mapsto ij = k \end{aligned}$$

is an isomorphism of groups, since it is a surjective homomorphism and both groups have order 8.

5.3 The group $\mathrm{AGL}(1, \mathbb{F}_p)$

Example 5.11. Let $\xi_p = e^{2\pi i/p}$ be a p-th root of unity, where p is prime. We consider the polynomial $x^p - 2$, whose roots are $\xi_p^j \sqrt[p]{2}$ for $0 \leq j \leq p-1$, hence

$$\mathbb{L} = \mathbb{Q}(\xi_p, \sqrt[p]{2})$$

is its splitting field over $\mathbb{Q}$. Since p is prime, the minimal polynomial of ξ_p over $\mathbb{Q}$ is $x^{p-1}+\ldots+1$; while the minimal polynomial of $\sqrt[p]{2}$ over $\mathbb{Q}$ is x^p-2 by Eisenstein criterion. Then we have that $p \mid [\mathbb{L} : \mathbb{Q}]$ and $(p-1) \mid [\mathbb{L} : \mathbb{Q}]$. Since p and $p-1$ are relatively prime and $[\mathbb{L} : \mathbb{Q}] \leq p(p-1)$, we have $[\mathbb{L} : \mathbb{Q}] = p(p-1)$. Hence $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ is a group of order $p(p-1)$. To see what group this is, let $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. We know that σ is uniquely determined by

$$\sigma(\xi_p) \in \left\{\xi_p, \ldots, \xi_p^{p-1}\right\}, \qquad \sigma(\sqrt[p]{2}) \in \left\{\sqrt[p]{2}, \xi_p\sqrt[p]{2}, \xi_p^2\sqrt[p]{2}, \ldots, \xi_p^{p-1}\sqrt[p]{2}\right\}.$$

In other words, there are integers $1 \leq i \leq p-1$ and $0 \leq j \leq p-1$ such that

$$\sigma(\xi_p) = \xi_p^i, \qquad \sigma(\sqrt[p]{2}) = \xi_p^j \sqrt[p]{2}. \tag{5.2}$$

We will denote this σ by $\sigma_{i,j}$. The number of possible pairs (i,j) is $(p-1)\cdot p = p(p-1)$. Since this is also the order of $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$, it follows that all possible pairs

$$(i,j) \in \{1, \ldots, p-1\} \times \{0, \ldots, p-1\} \tag{5.3}$$

must occur in Equation 5.2. In order to determine the group structure, we need to compute the composition of $\sigma_{i,j}$ and $\sigma_{r,s}$. This is done as follows:

$$\begin{aligned} \sigma_{i,j} \circ \sigma_{r,s}(\xi_p) &= \sigma_{i,j}(\xi_p^r) = (\sigma_{i,j}(\xi_p))^r = (\xi_p^i)^r = \\ &= \xi_p^{ir}, \\ \sigma_{i,j} \circ \sigma_{r,s}(\sqrt[p]{2}) &= \sigma_{i,j}(\xi_p^s \sqrt[p]{2}) = (\sigma_{i,j}(\xi_p))^s \sigma_{i,j}(\sqrt[p]{2}) = (\xi_p^i)^s(\xi_p^j \sqrt[p]{2}) = \\ &= \xi_p^{is+j} \sqrt[p]{2}. \end{aligned}$$

The computation suggests that

$$\sigma_{i,j} \circ \sigma_{r,s} = \sigma_{ir,is+j}$$

Unfortunately, the pair $(ir, is + j)$ need not lie in Equation 5.3. We can resolve this difficulty by realizing that for $i \in \mathbb{Z}$, ξ_p^i depends only on the congruence class of i modulo p. If we set $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$, then for

$$(a, b) \in \mathbb{F}_p^* \times \mathbb{F}_p,$$

we can define $\sigma_{a,b}$ to be the element of $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ such that

$$\sigma_{a,b}(\xi_p) = \xi_p^a, \qquad \sigma_{a,b}(\sqrt[p]{2}) = \xi_p^b \sqrt[p]{2}.$$

Then the above computation shows that $\sigma_{a,b} \circ \sigma_{c,d} = \sigma_{ac,ad+b}$. Hence the Galois group is $(\mathbb{F}_p^* \times \mathbb{F}_p, *)$, where the group operation $*$ is such that $(a, b) * (c, d) = (ac, ad + b)$; the identity element is $(1, 0)$ and the inverse element of (a, b) is $(a^{-1}, -ba^{-1})$. The composition formula leads to a geometric description of the Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. Given $a, b \in \mathbb{F}_p$, the function $\gamma_{a,b} : \mathbb{F}_p \to \mathbb{F}_p$ defined by $\gamma_{a,b}(u) = au + b$ is an affine linear transformation, and it is a bijection if and only if $a \neq 0$. All such $\gamma_{a,b}$ form a group of order $p(p-1)$ under composition, and it is called $\mathrm{AGL}(1, \mathbb{F}_p)$, the one-dimensional affine linear group modulo p. An easy computation shows that

$$\gamma_{a,b} \circ \gamma_{c,d} = \gamma_{ac,ad+b}.$$

Thus the map $\sigma_{a,b} \mapsto \gamma_{a,b}$ gives an isomorphism

$$\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) \cong \mathrm{AGL}(1, \mathbb{F}_p).$$

Bibliography

[1] D. A. Cox. *Galois theory*. John Wiley & Sons, Incorporated, 2th edition, 2012.

[2] R. A. Dean. *A Rational Polynomial whose Group is the Quaternions*. Taylor & Francis, Ltd, The American Mathematical Monthly, 1981. URL: `https://www.jstor.org/stable/2320711?seq=1`.

[3] J. W. Duggins and K. M. Pringle. *Polynomials that realize groups of order 16 or less as Galois groups*. Pi Mu Epsilon Journal Vol. 12, No. 6, 2007.

[4] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons Inc, third edition, 2003.

[5] G. Gaiffi. *Dispense del corso di algebra 1*. 2017. URL: `http://people.dm.unipi.it/~gaiffi/Algebra1-2016/Pages/dispense1.pdf`.

[6] C. R. Hadlock. *Field Theory and Its Classical Problems*. Carus Monographs, Volume 19, MMA, Washington, DC, 1978.

[7] D. Harbater. *Riemann's Existence Theorem. In "The Legacy of Bernhard Riemann After 150 Years"*. Higher Education Press and International Press, Beijing-Boston, 2015. URL: `https://www2.math.upenn.edu/~harbater/RETppr.pdf`.

[8] D. Hilbert. *Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten*. J. reine angew. Math. 110 (1892) 104–129, 1892.

[9] N. Jacobson. *Basic Algebra*. W.H. Freeman and company, New York, 1985.

[10] B. H. Matzat and A. Zeh-Marschke. *Realisierung der Mathieugruppen M_{11} und M_{12} als Galoisgruppen über $\mathbb{Q}$*. J. Number Theory 23, 1986.

[11] A. Michael. *The Status of the Classification of the Finite Simple Groups*. Notices of the American Mathematical Society. Vol. 51, no. 7., 2004.

[12] J.S. Milne. *Fields and Galois theory*. John Wiley & Sons, Incorporated, 2th edition, v4.61, 2020. URL: `https://www.jmilne.org/math/CourseNotes/FT461.pdf`.

[13] F. Ranjbar. *Inverse Galois problem and significant methods*. University of Tehran, 2015. URL: `https://arxiv.org/ftp/arxiv/papers/1512/1512.08708.pdf`.

[14] H. Reichardt. *Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung*. J. reine angew. Math. 177, 1937.

[15] A. Reverter and N. Vila. *Polynomials of Galois representations attached to elliptic curves*. Rev. R. Acad. Cienc. Exact. Fis. Nat. (Esp), Vol. 94. 3°, 2000.

[16] I. R. Šafarevič. *Construction of fields of algebraic numbers with given solvable Galois group*. Izv. Akad. Nauk SSSR, Ser. Mat. 18, 1954.

[17] A. Scholz. *Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I*. Math. Z. 42, 1937.

[18] J. P. Serre. *Topics in Galois Theory*. Jones and Barlett, Boston, 1992.

[19] D. Shanks. *Solved and Unsolved problems in Number Theory, 4th ed*. Chelsea publishing company, New York, 1993. URL: `https://mathematicalolympiads.files.wordpress.com/2012/08/solved-and-unsolved-problems-in-number-theory-daniel-shanks.pdf`.

[20] J. Silverman. *The Arithmetic of Elliptic Curves*. New York, Springer, 1986.

[21] J. G. Thompson. *Some finite groups which appear as* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$*, where* $\mathbb{K} \subseteq \mathbb{Q}(\mu_n)$. J. Algebra 89, 1984.

[22] H.G.J. Tiesinga. *The inverse Galois Problem*. Bachelor Project Mathematics, University of Groningen, 2016. URL: `https://fse.studenttheses.ub.rug.nl/14148/1/thesisclassic.pdf`.

[23] N. Vila. *On the inverse problem of Galois theory*. Autonomous University of Barcelona, 1992. URL: `https://www-jstor-org.ezproxy.unibo.it/stable/43737189?seq=1`.

[24] M. B. Villarino, W. Gasarch, and K. W. Regan. *Hilbert's proof of his irreducibility theorem*. Cornell University, 2017. URL: `https://arxiv.org/pdf/1611.06303.pdf`.

[25] B.L. van der Waerden. *Moderne Algebra*. Frederick Ungar Publishing CO, New York, 1949.

[26] D. Yates. *The inverse Galois Problem*. University of Bristol, 2017. URL: `https://www.researchgate.net/profile/Dean-Yates/publication/320835842_The_Inverse_Galois_Problem_4th_year_project`.

Ringraziamenti

Ringrazio tutti coloro che in questi anni mi hanno accompagnato e sostenuto in questo viaggio alla scoperta della matematica.
Ringrazio la mia relatrice, Nicoletta Cantarini, per l'aiuto datomi nella stesura di questo elaborato e per avermi fatto comprendere la bellezza della matematica.
Ringrazio la mia famiglia, in particolare i miei genitori che mi hanno permesso di compiere questo percorso e che hanno sempre creduto in me.
Ringrazio tutti gli amici che mi sono sempre stati vicini, nello svago come nel percorso universitario ciascuno è stato un pilastro fondamentale.