



Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

REALISING S_n AND A_n
AS GALOIS GROUPS OVER \mathbb{Q}
An Introduction to the
Inverse Galois Problem

Mireia Martínez i Sellarès

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

Barcelona, January 17, 2017

Abstract

“Given a field k and a finite group G , is there a Galois field extension $K|k$ such that its Galois group is isomorphic to G ?” Such an innocent question and yet it remains unsolved: this is what is known as the Inverse Galois Problem. In the present Bachelor thesis we show that this question has a positive answer if the field is \mathbb{Q} and the group is either S_n or A_n , following the strategy devised by David Hilbert in his paper *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten* (1892). We start with two basic examples and an exposition of relevant results from algebraic number theory, and then move on to proving Hilbert’s Irreducibility Theorem. As a consequence, we prove that the symmetric group S_n and the alternating group A_n are realisable as Galois groups over the field of rational numbers \mathbb{Q} .

Acknowledgements

I would like to thank...

...my supervisor Dr. Núria Vila, for listening to my wishes and guiding me towards attainable goals, and thereby doing more for my mathematical self-confidence than she probably knows.

...my faculty friends, for being on this journey with me and making me feel capable and loved.

...Guillem, for asking so many questions and not being satisfied with vague answers, thus directly contributing to making this thesis become much better than it would have been otherwise.

...my friends and family, specially my parents and my sister, for trying their best to understand what all the fuss is about, not quite succeeding, and still being always supportive and encouraging.

Contents

1	Introduction	1
1.1	The Inverse Galois Problem	1
1.2	Structure of the thesis	1
1.3	Notation	2
2	Groups of degree 3 and 4	3
2.1	Groups of order 3	4
2.2	Groups of order 4	4
3	Preliminary results	6
3.1	Hilbertian fields	6
3.2	Dedekind domains and algebraic number fields	7
3.3	Ramification of prime ideals	9
3.4	Hensel's Lemma	11
4	Hilbert's irreducibility theorem	14
5	S_n and A_n as Galois groups over \mathbb{Q}	23
5.1	The group S_n	25
5.2	The group A_n	26
5.2.1	Case n even	27
5.2.2	Case n odd	30
6	Conclusions	33

1 Introduction

1.1 The Inverse Galois Problem

Almost two hundred years ago Évariste Galois wrote down his revolutionary ideas about the resolution of algebraic equations. These ideas developed into what we nowadays call Galois theory, which provides a way to reformulate certain problems from field theory in terms of group theory. The Inverse Galois Problem arises when we wonder if it is possible to go in the opposite direction: if we fix a base field k and a finite group G , is it possible to find a Galois field extension of k having G as its Galois group? The answer to this question and the difficulty to find it depends greatly on k and G .

Setting $k = \mathbb{Q}$ leads to the classical formulation of the problem. One of the first mathematicians to ever explicitly work in that direction was David Hilbert. In a paper from 1892 titled *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten* [5] he proved that the Inverse Galois Problem has a positive answer for S_n and A_n over \mathbb{Q} . He constructed polynomials over a purely transcendental extension of \mathbb{Q} realising the desired groups, and then showed that this construction could be brought back down to the rational field. The mathematical language from his paper was updated and brought closer to the realm of algebra in two papers from the late 1970s and mid 1980s: a paper from Enric Nart and Núria Vila on the construction of the polynomials realising S_n and A_n [12], and a paper from Núria Vila on Hilbert's irreducibility theorem [19]. After Hilbert's paper came many other important results, such as the realisation of all solvable groups over \mathbb{Q} done by Shafarevich in the 1950s. Many new techniques have been developed since, giving new insight to the problem, but the Inverse Galois Problem as a whole remains still unsolved.

1.2 Structure of the thesis

The main goal of this thesis is to understand the results found by Hilbert, through the study of the chapter on hilbertian fields from Helmut Völkeim's *Groups as Galois groups* [20] and the aforementioned papers from Vila and Nart.

In chapter 2 we present two basic examples, namely, we show which groups can

be found as Galois groups of irreducible polynomials of degree 3 and 4. By doing so, we wish to familiarise the reader with the topic at hand and introduce them to a useful technique relating the discriminant of a polynomial and the alternating group.

Chapter 3 is a compilation of diverse results that we have had to study in order to have the necessary background knowledge for the next chapters. These preliminaries range from Hilbertian fields to ramification of prime ideals in Dedekind domains and Hensel's lemma. We are aware that these topics are not treated in full depth, but the reader should keep in mind that results and definitions included in chapter 2 are seen as tools that shall be needed later, and do not lie at the focus of this thesis. That is why theorems, propositions, and lemmas are stated without proof. We refer the interested reader back to the multiple references in each section and at the bibliography.

In chapter 4 we prove Hilbert's irreducibility theorem. We do so by first proving some auxiliary results and then giving the main proof. This allows for a more structured exposition and is intended to make the proof easier to follow.

Finally, chapter 5 offers a thorough revision of the paper «Sobre l'existència d'equacions que realitzen S_n i A_n com a grups de Galois d'un cos de números»[12], with extended proofs and commentary.

1.3 Notation

- In general, lowercase letters like a, b, c denote numbers or specific values, and uppercase letters like T, X, Y are used for polynomial indeterminates and transcendental elements. Lowercase letters like s, t, x, y, z can denote function variables, numbers, indeterminates, etc. depending on the context.
- Rings are commutative with unit element and fields have characteristic 0.
- Given a polynomial f with coefficients in a field k , and given a splitting field K of f over k , $\text{Gal}(f|k)$ denotes the Galois group of f over k . Similarly, $\text{Gal}(K|k)$ denotes the Galois group of the field extension $K|k$. These are obviously the same group.
- By 'for almost all' we mean 'for all but finitely many'.

2 Groups of degree 3 and 4

From Galois theory we know that the Galois group of an irreducible polynomial can be seen as a transitive subgroup of the symmetric group S_n , where n is the degree of the polynomial. Thus, given an irreducible polynomial of degree n there are only finitely many possibilities for its Galois group. In this section we consider irreducible polynomials of degree 3 and 4 over a field and give conditions to uniquely determine their Galois groups. We shall give general results for polynomials over any field K of characteristic 0; in particular, these apply in the case where $K = \mathbb{Q}$. References for this chapter are [7] and [21].

Definition 2.1. Let K be a field, $f(X) \in K[X]$ a monic polynomial of degree n , and let $\alpha_1, \dots, \alpha_n$ be the roots of f in an algebraic closure of K . The **discriminant** of f is

$$\Delta(f) = \prod_{i < j} (\alpha_i - \alpha_j)^2.$$

Note that $\Delta(f) = 0$ if, and only if, $\alpha_i = \alpha_j$ for some $i \neq j$. In characteristic 0 every irreducible polynomial of degree n has n distinct roots, so in our context all irreducible polynomials will have nonzero discriminant. Besides, the action of $\text{Gal}(f|K)$ on the roots fixes $\Delta(f)$ because the discriminant is a symmetric polynomial on the α_i 's, so $\Delta(f) \in K$.

Lemma 2.2. *Let f be an irreducible polynomial of degree n over a field K . Then $\text{Gal}(f|K)$ is a subgroup of A_n if, and only if, $\Delta(f)$ is a square in K .*

Proof. Let $\tau \in \text{Gal}(f|K)$. Then,

$$\tau(\sqrt{\Delta(f)}) = \tau\left(\prod_{i < j} (\alpha_i - \alpha_j)\right) = \prod_{i < j} (\alpha_{\tau(i)} - \alpha_{\tau(j)}) = \text{sign}(\tau) \prod_{i < j} (\alpha_i - \alpha_j)$$

Hence,

$$\tau(\sqrt{\Delta(f)}) = \sqrt{\Delta(f)} \Leftrightarrow \text{sign}(\tau) = 1 \Leftrightarrow \tau \in A_n,$$

which means that

$$\text{Gal}(f|K) \subseteq A_n \Leftrightarrow \text{Gal}(f|K) \text{ fixes } \sqrt{\Delta(f)} \Leftrightarrow \sqrt{\Delta(f)} \in K \Leftrightarrow \Delta(f) \in K^{*2}$$

as we wanted to see. □

2.1 Groups of order 3

Let K be a field and let $f(X) = X^3 + aX^2 + bX + c \in K[X]$.

Proposition 2.3. *Suppose $f(X)$ is irreducible over K . Then:*

$$\text{Gal}(f|K) \cong \begin{cases} S_3 & \text{if } \Delta(f) \notin K^{*2} \\ A_3 = C_3 & \text{if } \Delta(f) \in K^{*2}. \end{cases}$$

Proof. We have that $\{e\}$, A_3 and S_3 are exactly the transitive subgroups of S_3 . These are thus the options for $\text{Gal}(f|K)$ viewed as a group of permutations acting on the subindices of the roots $\alpha_1, \alpha_2, \alpha_3$ of $f(X)$. But if $\text{Gal}(f|K) \cong \{e\}$, then $\alpha_1, \alpha_2, \alpha_3 \in K$ and $f(X)$ wouldn't be irreducible. So the only two cases left to consider are S_3 and A_3 . Now the result is immediate by Lemma 2.2.: if $\Delta(f) \in K^{*2}$, then $\text{Gal}(f|K) \cong A_3$; if $\Delta(f) \notin K^{*2}$, then $\text{Gal}(f|K) \cong S_3$. \square

2.2 Groups of order 4

Again, let K be a field and let $f(X) = X^4 + aX^3 + bX^2 + cX + d \in K[X]$.

Definition 2.4. Let $\alpha_1, \dots, \alpha_4$ be the roots of f in an algebraic closure of K . The **cubic resolvent** of f is the polynomial

$$g(Y) = (Y - (\alpha_1\alpha_2 + \alpha_3\alpha_4))(Y - (\alpha_1\alpha_3 + \alpha_2\alpha_4))(Y - (\alpha_1\alpha_4 + \alpha_2\alpha_3)).$$

Since the coefficients of g are symmetric polynomials in $\alpha_1, \dots, \alpha_4$, they lie in K and thus $g(Y) \in K[X]$. A direct calculation shows that $\Delta(g) = \Delta(f)$.

The transitive subgroups of S_4 are the trivial group $\{e\}$, the Klein group V_4 , the cyclic group C_4 , the dihedral group D_4 , the alternating group A_4 , and S_4 itself.

Proposition 2.5. *Suppose f is irreducible over K . Let g be its cubic resolvent and let K_g the corresponding splitting field, set $m = [K_g : K]$. Then $m \in \{1, 2, 3, 6\}$ and*

$$\text{Gal}(f|K) \cong \begin{cases} S_4 & \text{if } m = 6 \\ A_4 & \text{if } m = 3 \\ V_4 & \text{if } m = 1 \\ D_4 \text{ or } C_4 & \text{if } m = 2. \end{cases}$$

Proof. Once again, we do not need to consider the case $\text{Gal}(f|K) \cong \{e\}$ because we are assuming that the roots of f do not lie in K .

Clearly $m \mid 3!$ because $\text{Gal}(g|K) \subseteq S_3$ and $\#S_3 = 3! = 6$. It is also evident that $K_f = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ is a field extension of $K_g = K(\beta_1, \beta_2, \beta_3)$, where $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$, and $\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$ are the roots of g .

If $m = 6$, then $\text{Gal}(g|K) \cong S_3$ and by Lemma 2.2. we get $\Delta(g) \notin K^{*2}$. Since $\Delta(f) = \Delta(g)$, we have $\Delta(f) \notin K^{*2}$ as well, and so $\text{Gal}(f|K) \not\subseteq A_4$. But $m \mid [K_f : K]$, so the only option left is $\text{Gal}(f|K) \cong S_4$.

If $m = 3$, now $\text{Gal}(g|K) \cong A_3$. This implies $\Delta(f) = \Delta(g) \in K^{*2}$ and $\text{Gal}(f|K)$ is a subgroup of A_4 , but since $m \mid [K_f : K]$, the isomorphism $\text{Gal}(f|K) \cong A_4$ is the only possibility (the orders of the other groups are not divisible by 3).

We prove the remaining cases by contrapositive. Suppose $\text{Gal}(f|K) \not\cong V_4$. Then it has to be D_4 or C_4 and contains a 4-cycle. In that case there is a pair (i, j) such that β_i and β_j are swapped by said cycle, which means that $K_g \neq K$. Hence $m > 1$. Finally, suppose $\text{Gal}(f|K) \cong V_4$ (i.e. $\not\cong C_4$, $\not\cong D_4$). Now all β_i 's are fixed by the elements of the Galois group and thus $[K_g : K] = 1$. \square

3 Preliminary results

In this chapter we shall make a summary of the necessary definitions and results needed to prove the main theorems of chapters 4 and 5. If we aim to see that \mathbb{Q} is hilbertian, it is clear that we first need to know what a hilbertian field is, that is the purpose of section 3.1. In section 3.2. we define Dedekind domains and algebraic number fields. Section 3.3. presents the basic facts from ramification theory in the context of algebraic number fields. And finally, in Section 3.4. we make a minimal introduction to complete fields, just enough to state Hensel's Lemma.

3.1 Hilbertian fields

First, we recall the notion of a purely transcendental extension of a field and then define hilbertian fields. See [21] for the part on transcendental extensions and [20] for further treatment on hilbertian fields.

Definition 3.1. Let K be a field, L an extension field of K and let $x, x_1, \dots, x_m \in L$. We say x is **algebraically dependent** on x_1, \dots, x_m over K if x is algebraic over $K(x_1, \dots, x_m)$. In other words, if there exist $p_0, \dots, p_r \in K(x_1, \dots, x_m)$ such that $p_i \neq 0$ for some $i = 0, \dots, r$ and x satisfies an algebraic equation of the form

$$p_r x^r + p_{r-1} x^{r-1} + \dots + p_1 x + p_0 = 0 .$$

We say that x_1, \dots, x_m are **algebraically independent** if none of them is algebraically dependent on the others. We also call the elements x_1, \dots, x_m **independent transcendentals** over K .

If x_1, \dots, x_m are independent transcendentals and X_1, \dots, X_m are indeterminates over a field K , then there is a one-to-one correspondence between a polynomial $g(X_1, \dots, X_m) \in K[X_1, \dots, X_m]$ and a polynomial expression $g(x_1, \dots, x_m)$ with coefficients in K . Therefore $K[X_1, \dots, X_m] \cong K[x_1, \dots, x_m]$ and it follows that their fields of fractions are isomorphic too, $K(X_1, \dots, X_m) \cong K(x_1, \dots, x_m)$. Hence, the independent transcendentals x_1, \dots, x_m and the indeterminates X_1, \dots, X_m have the same algebraic properties with respect to the field K .

Definition 3.2. Given a field K , we say a field extension L is **purely transcendental** if $L = K(X_1, \dots, X_m)$, where X_1, \dots, X_m are algebraically independent.

Proposition 3.3. *Let X_1, \dots, X_m be algebraically independent over a field K and let \bar{K} be an algebraic closure of K . Set $X = (X_1, \dots, X_m)$.*

1. *If $K'|K$ is finite Galois, then $K'(X)|K(X)$ is also finite Galois and the restriction map $\text{Gal}(K'(X)|K(X)) \longrightarrow \text{Gal}(K'|K)$ is an isomorphism. In particular, every field between $K'(X)$ and $K(X)$ is of the form $K''(X)$, and $[K''(X) : K(X)] = [K'' : K]$.*
2. *Let $f(X, Y) \in K(X)[Y]$ be irreducible over $K(X)$ and let $L = K(X)[Y]/(f)$ be the corresponding field extension of $K(X)$. Then K is algebraically closed in L if, and only if, f is irreducible over $K(X)$. In that case, $f(X, Y)$ is irreducible over $K'(X)$ for every field extension $K'|K$ such that X_1, \dots, X_m, Y are independent transcendentals over L .*

Definition 3.4. A field K is called **hilbertian** if it satisfies any of the following equivalent conditions:

1. For each irreducible polynomial $f(X, Y) \in K[X, Y]$ with degree ≥ 1 in Y , there exist infinitely many $b \in K$ such that the specialised polynomial $f(b, Y)$ is also irreducible in $K[Y]$.
2. Given a finite extension $L|K$ and $g_1(X, Y), \dots, g_m(X, Y) \in L[X, Y]$ irreducible polynomials over $L(X)$ as polynomials in Y , there exist infinitely many $b \in K$ such that the specialised polynomials $g_1(b, Y), \dots, g_m(b, Y)$ are irreducible in $L[Y]$.
3. For any $p_1(X, Y), \dots, p_r(X, Y) \in K[X, Y]$, irreducible and of degree ≥ 2 as polynomials in Y over $K(X)$, there exist infinitely many $b \in K$ such that the specialised polynomials $p_1(b, Y), \dots, p_r(b, Y)$ are irreducible in $K[Y]$.

Observation 3.5. If K is hilbertian, every finitely generated extension of K is hilbertian as well.

3.2 Dedekind domains and algebraic number fields

We define the concept of Dedekind domain and show how it relates to algebraic number fields. For further reference see [1] and [14].

Definition 3.6. A **Dedekind domain** is a domain in which every nonzero ideal can be expressed uniquely as a product of prime ideals.

Observation 3.7. There are actually other three equivalent definitions of a Dedekind domain, which can be easily found in the literature (cf. for instance [14]). One of said definitions explicit an interesting property of Dedekind domains, namely, every nonzero prime ideal of a Dedekind domain is maximal. Therefore, if A is a Dedekind domain and \mathfrak{p} is a prime ideal of A , then the quotient ring A/\mathfrak{p} is a field.

Definition 3.8. Let B be a ring, A a subring of B . An element $x \in B$ is an **integer over A** if x is a root of a monic polynomial with coefficients in A , that is, if there exist $a_0, \dots, a_{n-1} \in A$, $n \geq 0$, such that $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$. If every $x \in B$ is an integer over A , B is said to be **integral over A** , and that $B|A$ is an **integral extension**.

If every $x \in B$ which is an integer over A actually lies in A , we say that A is **integrally closed in B** . If A is a domain, we say that it is an **integrally closed domain** if it is integrally closed in its field of fractions.

Proposition 3.9. *Let $A \subseteq B \subseteq C$ be rings. If C is integral over B and B is integral over A , then C is integral over A .*

Proposition 3.10. *Let B be a ring, $A \subseteq B$ a subring. Let A' be the set of $x \in B$ which are integral over A . Then A' is a subring of B , integrally closed in B and integral over A .*

Definition 3.11. The ring A' from the previous proposition is called the **integral closure of A in B** .

Suppose that K is an algebraic number field, i.e. a finite algebraic extension of \mathbb{Q} . Then we say that an algebraic number in K is an **algebraic integer** if it is a root of a monic polynomial with coefficients in \mathbb{Z} . The **ring of integers** of K is the integral closure of \mathbb{Z} in K . In particular, the elements of \mathbb{Z} are called **rational integers** because \mathbb{Z} is the integral closure of \mathbb{Z} in \mathbb{Q} .

Proposition 3.12. *Let A be a Dedekind domain, K its field of fractions, $L|K$ a finite field extension, and B the integral closure of A in L . Then B is a Dedekind domain.*

And since \mathbb{Z} is a Dedekind domain, we have the following result:

Corollary 3.13. *The ring of integers of an algebraic number field is a Dedekind domain.*

3.3 Ramification of prime ideals

In this section we introduce basic concepts and propositions from algebraic number theory. Results and their proofs can be found in [14], other consulted references are [10] and [13].

Let A be the ring of integers of an algebraic number field K . Let L be a finite field extension of K of degree $[L : K] = n$ and let B be its ring of integers. If \mathfrak{p} is a nonzero prime ideal of A , the extended ideal $\mathfrak{p}B$ can be written uniquely as

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} ,$$

where \mathfrak{P}_i are prime ideals of B . If $\mathfrak{P} = \mathfrak{P}_i$ for some i , we say that \mathfrak{P} lies over \mathfrak{p} or that \mathfrak{P} divides \mathfrak{p} , and write $\mathfrak{P}|\mathfrak{p}$. Note that $\mathfrak{P} \cap A = \mathfrak{p}$. The quotient B/\mathfrak{P} is a field containing A/\mathfrak{p} .

Definition 3.14. A prime ideal \mathfrak{P} of B is called **ramified** in $L|K$ if it has exponent $e > 1$ in the factorisation of $\mathfrak{p}B$ ($\mathfrak{p} = \mathfrak{P} \cap A$). Moreover, we say \mathfrak{P} is **totally ramified** in $L|K$ if $\mathfrak{p}B = \mathfrak{P}^n$. Similarly, \mathfrak{P} is called **unramified** in $L|K$ if it has exponent $e = 1$ and the residue field extension $B/\mathfrak{P}|A/\mathfrak{p}$ is separable.

We say that a prime ideal \mathfrak{p} of A is **unramified** in $L|K$ if each prime factor \mathfrak{P}_i of \mathfrak{p} in B is unramified in $L|K$. Otherwise we say it is **ramified**.

The field extension $L|K$ is called **unramified** if all prime ideals of A are unramified.

Definition 3.15. In the context above,

- for each $1 \leq i \leq g$, the exponent e_i is called the **ramification index** of \mathfrak{P}_i over \mathfrak{p} ;
- for each $1 \leq i \leq g$, the degree of the residue field extension, $f_i := [B/\mathfrak{P}_i : A/\mathfrak{p}]$, is called the **inertia degree** of \mathfrak{P}_i over \mathfrak{p} .
- the number g is called the **decomposition number** of \mathfrak{p} in $L|K$.

Proposition 3.16. *Let K be an algebraic number field with ring of integers A , and let L be a finite field extension of K of degree n with ring of integers B . Moreover, let \mathfrak{p} be a prime ideal of A which factors in B as $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ and, for each i , let $f_i = [B/\mathfrak{P}_i : A/\mathfrak{p}]$. Then*

$$\sum_{i=1}^g e_i f_i = n .$$

The result above can be proved more generally for separable field extensions, but since we are working with algebraic number fields, which are perfect because they have characteristic 0, every extension of algebraic number fields is separable and so the result always applies.

For the rest of this section let us further assume that $L|K$ is a Galois extension and set $G = \text{Gal}(L|K)$.

Proposition 3.17. *Let \mathfrak{p} be a nonzero prime ideal of A . Then G acts transitively on $\{\mathfrak{P}_1, \dots, \mathfrak{P}_g\}$, the set of primes of B above \mathfrak{p} .*

Corollary 3.18. *If $L|K$ is Galois, one has that $e = e_1 = \dots = e_g$ and $f = f_1 = \dots = f_g$, and so the identity in Proposition 3.16. becomes*

$$efg = n .$$

Now, fix a prime \mathfrak{P} over \mathfrak{p} and set $\bar{L} := B/\mathfrak{P}$ and $\bar{K} := A/\mathfrak{p}$.

Definition 3.19. The **decomposition group** of \mathfrak{P} in $L|K$ is the stabiliser of \mathfrak{P} by G , $D_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$. The subfield of L fixed by $D_{\mathfrak{P}}$ is called the **decomposition field** of \mathfrak{P} in $L|K$ and we shall denote it by $L^{D_{\mathfrak{P}}}$.

The decomposition group $D_{\mathfrak{P}}$ acts on the residue field \bar{L} as follows; $\sigma(x \bmod \mathfrak{P}) = \sigma(x) \bmod \mathfrak{P}$. This action is indeed well defined, because $x \equiv y \pmod{\mathfrak{P}}$ implies $\sigma(x) \equiv \sigma(y) \pmod{\sigma(\mathfrak{P})}$ and for all $\sigma \in D_{\mathfrak{P}}$ one has $\sigma(\mathfrak{P}) = \mathfrak{P}$.

Definition 3.20. The kernel of the homomorphism $D_{\mathfrak{P}} \longrightarrow \text{Aut}(\bar{L}|\bar{K})$, that is, the normal subgroup $I_{\mathfrak{P}} = \{\sigma \in D_{\mathfrak{P}} \mid \sigma(x) \equiv x \pmod{\mathfrak{P}}\}$, is known as the **inertia group** of \mathfrak{P} in $L|K$. The subfield of L fixed by $I_{\mathfrak{P}}$ is called the **inertia field** of \mathfrak{P} in $L|K$ and is denoted by $L^{I_{\mathfrak{P}}}$.

Proposition 3.21. *The residue field extension $\bar{L}|\bar{K}$ is normal, and the homomorphism $D_{\mathfrak{P}} \longrightarrow \text{Gal}(\bar{L}|\bar{K})$ defines an isomorphism between $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ and $\text{Gal}(\bar{L}|\bar{K})$.*

Proposition 3.22. *The tower of field extensions $L|L^{I_{\mathfrak{P}}}|L^{D_{\mathfrak{P}}}|K$ has extension degrees $[L : L^{I_{\mathfrak{P}}}] = e$, $[L^{I_{\mathfrak{P}}} : L^{D_{\mathfrak{P}}}] = f$, $[L^{D_{\mathfrak{P}}} : K] = g$.*

Observation 3.23. The inertia field will play an important role in this thesis, so we need to do a further remark about it. For a much more detailed presentation see [14]. We have a prime ideal \mathfrak{P} in B and consider its inertia group $I_{\mathfrak{P}}$ and inertia

field $L^{\mathfrak{P}}$. Then the ideal $\mathfrak{P} \cap L^{\mathfrak{P}}$ is unramified in $L^{\mathfrak{P}}|K$, and \mathfrak{P} is ramified in any field extension of K between $L^{\mathfrak{P}}$ and L .

To finish this section, we consider the relationship between the discriminant and the ramification of prime ideals in the particular case of a monogenic field. Once again, consult [14] for a more general and comprehensive treatment of discriminants and ramification. Here we shall only state the particular results that will be needed later.

Observation 3.24. We know what the discriminant of a polynomial is (Definition 2.1.), but the notion of discriminant can in fact be extended to a more general context. For instance, let K be an algebraic field, A its ring of integers, and L a finite extension of K . One can define $\delta_{L|K}$, the **relative discriminant of $L|K$** , which is an ideal of A . Turns out that, in the case where L is a monogenic field extension of K , i.e. $L = K(\theta)$ for some $\theta \in L$, and if f is the minimal polynomial of θ in K , then $\delta_{L|K} = (\Delta(f))$.

Lastly, we state two important results which nail down the relationship between discriminant and ramification:

Proposition 3.25. *Let \mathfrak{p} be a nonzero prime ideal of A . Then \mathfrak{p} is ramified in $L|K$ if, and only if, \mathfrak{p} divides $\delta_{L|K}$. In particular, there are only finitely many prime ideals of A which are ramified in $L|K$.*

Proposition 3.26. *Let $K \subseteq L \subseteq N$ be algebraic number fields such that N is the smallest field containing L for which $N|K$ is Galois, and let \mathfrak{p} be a nonzero prime ideal of A , the ring of integers of K . Then \mathfrak{p} is ramified in $L|K$ if, and only if, \mathfrak{p} is ramified in $N|L$.*

3.4 Hensel's Lemma

In this section we introduce the concept of a complete field with respect to a valuation and state Hensel's lemma. We follow [2] and [13].

Definition 3.27. Let K be a field. A **discrete valuation** on K is a function $\nu : K \rightarrow \mathbb{Z} \cup \{\infty\}$ satisfying

$$(i) \quad \nu(x) = \infty \Leftrightarrow x = 0,$$

- (ii) for all $x, y \in K$, $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$,
- (iii) the restriction of ν to K^* is a homomorphism onto \mathbb{Z} .

The ring $A_\nu = \{x \in K \mid \nu(x) \geq 0\}$ is called the **valuation ring** of ν , and the subset $\mathfrak{p}_\nu = \{x \in K \mid \nu(x) > 0\}$ of A_ν is an ideal, called the **valuation ideal** of ν .

In the case where A is a Dedekind domain with field of fractions K (for example, if A is the ring of integers of an algebraic number field K) and if \mathfrak{p} is a nonzero prime ideal of A , one can define a discrete valuation on K as follows: for $x \in K$ we set $\nu(x) = e_{\mathfrak{p}}$, where $e_{\mathfrak{p}}$ is the exponent of \mathfrak{p} in the unique factorisation of the principal fractional ideal xA , and $\nu(0) = \infty$. We call this discrete valuation on K a **\mathfrak{p} -adic valuation**. Conversely, if K is the field of fractions of a Dedekind domain A and ν is a discrete valuation on K such that $A \subseteq A_\nu$, then ν is a \mathfrak{p} -adic valuation for some prime ideal \mathfrak{p} of A .

We now introduce the concept absolute value and see how discrete valuations can be used to define absolute values.

Definition 3.28. An **absolute value** on a field K is a function $|\cdot| : K \rightarrow \mathbb{R}$ satisfying

- (i) $|x| \geq 0$ for all $x \in K$ and $|x| = 0 \Leftrightarrow x = 0$,
- (ii) $|xy| = |x||y|$,
- (iii) $|x + y| \leq |x| + |y|$ (triangle inequality).

Our interest lies in the following relation between absolute values and discrete valuations: if K is a field with a discrete valuation ν , then we can define an absolute value setting $|x| = C^{-\nu(x)}$ for some $C \in \mathbb{R}$, $C > 1$. In the case where K is the field of fractions of a Dedekind domain and ν is a \mathfrak{p} -adic valuation for some prime ideal \mathfrak{p} in A , we say $|\cdot|$ is a **\mathfrak{p} -adic absolute value**.

Definition 3.29. Let K be a field with an absolute value $|\cdot|$. We say that a sequence $(x_n)_{n \in \mathbb{N}}$ of elements of K is a **Cauchy sequence** if

$$\forall \epsilon > 0, \exists N \in \mathbb{N}; \forall m, n > N, |x_m - x_n| < \epsilon .$$

The field K is said to be **complete** with respect to $|\cdot|$ if the limit of every Cauchy sequence lies in K . Given a field K with an absolute value $|\cdot|$ and a field \widehat{K} with absolute value $\|\cdot\|$, and if $\|\cdot\|$ extends $|\cdot|$ in the sense that $|x| = \|x\|$ for all $x \in K$, then we say that \widehat{K} is the **completion** of K if \widehat{K} is complete and is the closure of K in \widehat{K} for $\|\cdot\|$.

The following shows we can really refer to \widehat{K} as *the* completion of K :

Proposition 3.30. *Every field K with an absolute value has a completion, and this completion is unique up to isomorphism of fields with an absolute value.*

With all this notation, we can finally state

Proposition 3.31. (Hensel's Lemma) *Let A be a discrete valuation ring with maximal ideal \mathfrak{p} , and suppose its field of fractions K is complete with respect to the \mathfrak{p} -adic absolute value. Let $f(X) \in A[X]$ be a primitive polynomial and let $\bar{f}(X) \in A/\mathfrak{p}[X]$ be its reduction mod \mathfrak{p} . Suppose there exist relatively prime polynomials $\bar{g}(X), \bar{h}(X) \in A/\mathfrak{p}[X]$ such that*

$$\bar{f}(X) \equiv \bar{g}(X)\bar{h}(X) \pmod{\mathfrak{p}} .$$

Then $f(X)$ factors in $A[X]$ as

$$f(X) = g(X)h(X)$$

where $g(X), h(X) \in A[X]$, $\deg(g) = \deg(\bar{g})$ and

$$g(X) \equiv \bar{g}(X) \pmod{\mathfrak{p}} \quad \text{and} \quad h(X) \equiv \bar{h}(X) \pmod{\mathfrak{p}} .$$

4 Hilbert's irreducibility theorem

In this section we prove Hilbert's irreducibility theorem, i.e. \mathbb{Q} is a hilbertian field. Theorems and proofs are taken mainly from [20]. See [19] for a more succinct proof of the main theorem.

Before actually proving Hilbert's irreducibility theorem, we shall see some previous results in order to make the final proof much simpler and easy to follow.

Definition 4.1. A set $\Omega \subset \mathbb{N}$ is **sparse** if there exists $\delta \in \mathbb{R}$, $0 < \delta < 1$, such that

$$|\Omega \cap \{1, \dots, N\}| \leq N^\delta$$

for almost all $N \in \mathbb{N}$.

Lemma 4.2. *Every finite set is sparse. More generally, a finite union of sparse sets is sparse.*

Proof. Let $\Omega = \{a_1, \dots, a_n\}$ be a finite set, we can assume $a_n = \max_{1 \leq i \leq n} a_i$. Then $|\Omega| \leq a_n$ and so $|\Omega \cap \{1, \dots, N\}| \leq a_n$ always holds. Let $N_0 = a_n + 1 > a_n$ and note that $\log_{N_0} a_n < 1$. For every $N \geq N_0$ we have $\log_N a_n \leq \log_{N_0} a_n$, therefore $|\Omega \cap \{1, \dots, N\}| \leq a_n = N^{\log_N a_n} \leq N^{\log_{N_0} a_n}$. This proves the first statement of the lemma.

To see the second statement, let $m \in \mathbb{N}$ and $\Theta = \bigcup_{i=1}^m \Theta_i$, where Θ_i are sparse sets for all $i = 1, \dots, m$, that is, for every i there exists $0 < \delta_i < 1$ such that $|\Theta_i \cap \{1, \dots, N\}| \leq N^{\delta_i}$ for almost all N . Set $\delta_0 := \max_{1 \leq i \leq m} \delta_i$. Now,

$$\begin{aligned} |\Theta \cap \{1, \dots, N\}| &= \left| \left(\bigcup_{i=1}^m \Theta_i \right) \cap \{1, \dots, N\} \right| \\ &= \left| \bigcup_{i=1}^m (\Theta_i \cap \{1, \dots, N\}) \right| \\ &= \sum_{i=1}^m |\Theta_i \cap \{1, \dots, N\}| \\ &= \sum_{i=1}^m N^{\delta_i} \\ &\leq m N^{\delta_0} = N^{\log_N m + \delta_0} . \end{aligned}$$

This time let $N_0 \in \mathbb{N}$ be large enough, so that $\log_{N_0} m < 1 - \delta_0$. Then, for all $N \geq N_0$,

$$|\Theta \cap \{1, \dots, N\}| \leq N^{\log_N m + \delta_0} \leq N^{\log_{N_0} m + \delta_0},$$

where $\log_{N_0} m + \delta_0 < 1$. Thus, Θ is a sparse set. \square

The following lemma states a property that will be needed to prove the next proposition.

Lemma 4.3. *Let $s_0 < \dots < s_m \in \mathbb{R}$, $m \geq 1$; let $\chi(s)$ be a real-valued function defined for $s_0 \leq s \leq s_m$ and m times continuously differentiable; and let V_m be the Vandermonde determinant*

$$V_m = \begin{vmatrix} 1 & s_0 & s_0^2 & \cdots & s_0^m \\ 1 & s_1 & s_1^2 & \cdots & s_1^m \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & s_m & s_m^2 & \cdots & s_m^m \end{vmatrix} = \prod_{0 \leq j < i \leq m} (s_i - s_j)$$

Then there exists $\xi \in \mathbb{R}$ with $s_0 \leq \xi \leq s_m$ such that

$$\frac{\chi^{(m)}(\xi)}{m!} = \frac{1}{V_m} \begin{vmatrix} 1 & s_0 & s_0^2 & \cdots & s_0^{m-1} & \chi(s_0) \\ 1 & s_1 & s_1^2 & \cdots & s_1^{m-1} & \chi(s_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & s_m & s_m^2 & \cdots & s_m^{m-1} & \chi(s_m) \end{vmatrix}.$$

Proof. First we define the function

$$F(s) = \begin{vmatrix} 1 & s_0 & s_0^2 & \cdots & s_0^{m-1} & \chi(s_0) \\ 1 & s_1 & s_1^2 & \cdots & s_1^{m-1} & \chi(s_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & s & s^2 & \cdots & s^{m-1} & \chi(s) \end{vmatrix}$$

and set

$$c = \frac{F(s_m)}{(s_m - s_0) \cdots (s_m - s_{m-1})}.$$

We then define another function

$$G(s) = F(s) - c(s - s_0) \cdots (s - s_{m-1})$$

such that $G(s) = 0$ at the $m+1$ points $s = s_0, \dots, s_m$. Thus, $G^{(m)}(s) = F^{(m)}(s) - m!c$ equals to zero at least at one point ξ between s_0 and s_m and we get

$$F^{(m)}(\xi) = m!c .$$

Besides, if we expand the determinant that defines $F(s)$ we obtain

$$F(s) = \sum_{i=0}^{m-1} c_i s^i + V_{m-1} \chi(s) ,$$

where c_i are constants which depend on s_0, \dots, s_m and V_{m-1} is the Vandermonde determinant of s_0, \dots, s_{m-1} . This way,

$$F^{(m)}(\xi) = V_{m-1} \chi^{(m)}(\xi) ,$$

and if we compare the two expressions for $F^{(m)}(\xi)$ we get

$$\frac{\chi^{(m)}(\xi)}{m!} = \frac{c}{V_{m-1}} = \frac{F(s_m)}{(s_m - s_0) \cdots (s_m - s_{m-1}) V_{m-1}} = \frac{F(s_m)}{V_m}$$

as desired. □

Proposition 4.4. *Let*

$$\psi(t) = \sum_{i=n}^{\infty} a_i t^i$$

be a Laurent series with complex coefficients, i.e. $n \in \mathbb{Z}$ and $a_i \in \mathbb{C}$ for all i , converging for all $t \neq 0$ in a neighbourhood U of 0 in \mathbb{C} . If ψ is not a Laurent polynomial (that is, if it has infinitely many nonzero terms), then the set $B(\psi) := \{b \in \mathbb{N} \mid \psi(\frac{1}{b}) \in \mathbb{Z}\}$ is sparse.

Proof. Assume that $B(\psi)$ is infinite (otherwise by Lemma 4.2. it would trivially be sparse). We first prove three claims. To begin with, let us see that (1) *all coefficients a_i lie in \mathbb{R} .* Consider the Laurent series

$$\bar{\psi}(t) = \sum_{i=n}^{\infty} \bar{a}_i t^i ,$$

obtained by replacing each coefficient a_i with its complex conjugate \bar{a}_i . This series has the same radius of convergence as ψ , because

$$R_\psi = \frac{1}{\limsup_{n \rightarrow \infty} \sqrt[n]{|a_n|}} = \frac{1}{\limsup_{n \rightarrow \infty} \sqrt[n]{|\bar{a}_n|}} = R_{\bar{\psi}} .$$

Furthermore, $\bar{\psi}(\frac{1}{b}) = \psi(\frac{1}{b})$ for all $b \in B(\psi)$ because $\psi(\frac{1}{b}) \in \mathbb{Z}$ and thus $\text{Im}(\psi(\frac{1}{b})) = 0 = -\text{Im}(\bar{\psi}(\frac{1}{b}))$. Since we assumed $B(\psi)$ to be infinite, it follows that $\bar{\psi} = \psi$. Hence, all coefficients a_i must be real.

Then

$$\chi(s) := \psi(s^{-1}) = \sum_{i=n}^{\infty} a_i s^{-i}$$

is a real valued function, defined for large values of s . Note that the condition in $B(\psi)$ can also be expressed in terms of χ : $B(\psi) = \{b \in \mathbb{N} \mid \chi(b) \in \mathbb{Z}\}$.

Secondly, we claim that (2) there exist $\lambda > 0$ and $m, S \in \mathbb{N}$ such that, if $s_0, \dots, s_m \in \mathbb{N}$ with $\chi(s_0), \dots, \chi(s_m) \in \mathbb{Z}$ and $S < s_0 < \dots < s_m$, then

$$s_m - s_0 \geq s_0^\lambda .$$

To see this, let m large enough, so that the series

$$\chi^{(m)}(s) := \sum_{i=r}^{\infty} d_i s^{-i}$$

has only negative powers of s , i.e. $r > 0$. We have $d_i \in \mathbb{R}$ for all i , and we can assume $d_r \neq 0$ because χ is not a Laurent polynomial and has therefore infinitely many nonzero coefficients. Then

$$\begin{aligned} \lim_{s \rightarrow \infty} s^r \chi^{(m)}(s) &= \lim_{s \rightarrow \infty} s^r \sum_{i=r}^{\infty} d_i s^{-i} \\ &= \lim_{s \rightarrow \infty} s^r \left(\frac{d_r}{s^r} + \frac{d_{r+1}}{s^{r+1}} + \dots \right) \\ &= \lim_{s \rightarrow \infty} \left(d_r + \frac{d_{r+1}}{s} + \dots \right) \\ &= d_r . \end{aligned}$$

Hence there exists $S \in \mathbb{N}$ such that, for $s \geq S$,

$$0 < |s^r \chi^{(m)}(s)| < |2d_r|$$

and so

$$0 < \frac{s^r}{|2d_r|} < \frac{1}{|\chi^{(m)}(s)|}.$$

Now assume $s_0, \dots, s_m \in \mathbb{N}$ to be as desired, i.e. $S < s_0 < \dots < s_m$, and take ξ satisfying Lemma 4.3., that is, $s_0 < \xi < s_m$ and

$$\frac{\chi^{(m)}(\xi)}{m!} = \frac{1}{V_m} \begin{vmatrix} 1 & s_0 & s_0^2 & \cdots & s_0^{m-1} & \chi(s_0) \\ 1 & s_1 & s_1^2 & \cdots & s_1^{m-1} & \chi(s_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & s_m & s_m^2 & \cdots & s_m^{m-1} & \chi(s_m) \end{vmatrix}$$

Then

$$0 \neq \frac{V_m \chi^{(m)}(\xi)}{m!} \in \mathbb{Z},$$

so its absolute value is ≥ 1 and therefore

$$V_m \geq \frac{m!}{|\chi^{(m)}(\xi)|} \geq \frac{1}{|\chi^{(m)}(\xi)|}.$$

Besides, one has

$$V_m = \prod_{0 \leq j < i \leq m} (s_i - s_j) \leq \prod_{0 \leq j < i \leq m} (s_m - s_0) = (s_m - s_0)^{\sum_{k=1}^{m+1} k} = (s_m - s_0)^{\frac{(m+1)(m+2)}{2}}.$$

Combining both inequalities we obtain

$$(s_m - s_0)^{\frac{(m+1)(m+2)}{2}} \geq V_m \geq \frac{1}{|\chi^{(m)}(\xi)|} \geq \frac{\xi^r}{|2d_r|} \geq \frac{s_0^r}{|2d_r|}$$

and so

$$s_m - s_0 \geq \left(\frac{s_0^r}{|2d_r|} \right)^{\frac{2}{(m+1)(m+2)}} = \left(\frac{1}{|2d_r|} \right)^{\frac{2}{(m+1)(m+2)}} s_0^{\frac{2r}{(m+1)(m+2)}}.$$

Thus, there is always a $0 < \lambda < \frac{2r}{(m+1)(m+2)}$ that satisfies the claim.

Next, (3) let $b_1 < b_2 < b_3 < \dots$ be a sequence of positive integers with $b_{i+1} - b_i \geq b_i^\delta$ for some $\delta > 0$ and for every $i \in \mathbb{N}$. We want to see that the set $B = \{b_1, b_2, \dots\}$ is sparse. For each $N \in \mathbb{N}$ let $\tilde{N} = \#\{b \in B \mid \sqrt{N} < b \leq N\}$ and let $b_{i_1} < \dots < b_{i_{\tilde{N}}}$ be the \tilde{N} consecutive elements of B satisfying $1 \leq \sqrt{N} \leq b_{i_1} < \dots < b_{i_{\tilde{N}}} \leq N$ and therefore $b_{i_{\tilde{N}}} - b_{i_1} \leq N - 1$.

Then

$$\begin{aligned}
N &\geq b_{i_{\tilde{N}}} - b_{i_1} \\
&\geq (b_{i_{\tilde{N}}} - b_{i_{\tilde{N}-1}}) + (b_{i_{\tilde{N}-1}} - b_{i_{\tilde{N}-2}}) + \cdots + (b_{i_2} - b_{i_1}) \\
&\geq b_{i_{\tilde{N}-1}}^\delta + b_{i_{\tilde{N}-2}}^\delta + \cdots + b_{i_1}^\delta \\
&\geq (\tilde{N} - 1)b_{i_1}^\delta \\
&\geq (\tilde{N} - 1)\sqrt{N}^\delta
\end{aligned}$$

Hence,

$$\tilde{N} \leq N^{1-\frac{\delta}{2}} + 1$$

and so

$$|B \cap \{1, \dots, N\}| \leq \sqrt{N} + \tilde{N} \leq \sqrt{N} + N^{1-\frac{\delta}{2}} + 1,$$

which implies that B is a sparse set.

Let us finally see that $B(\psi) = \{b \in \mathbb{N} \mid \chi(b) \in \mathbb{Z}\}$ is sparse. Take $S, m \in \mathbb{N}$ as in our second claim. Consider $B' = B(\psi) \setminus \{s \leq S\}$, and assume

$$S < b_0 < b_1 < \cdots < b_m < b_{m+1} < \cdots < b_{2m} < \cdots$$

where b_i are the elements of B' . Take the first $m+1$ elements and apply claim (2): $b_m - b_0 \geq b_0^\delta$. This also applies for $b_{m+1} - b_1 \geq b_1^\delta$, and in fact one has that $b_{tm+i} - b_{(t-1)m+i} \geq b_{(t-1)m+i}^\delta$ for every $t \in \mathbb{Z}^+$ and $i = 0, \dots, m-1$. Thus, we define the m sets

$$B_i := \{b_i, b_{m+i}, b_{2m+i}, \dots\}$$

and each of these sets satisfies the condition from our third claim, which shows that each B_i is sparse. Since the equality $B' = \bigcup_{i=0}^{m-1} B_i$ holds, the set $B(\psi)$ is sparse as well. \square

We want to see that \mathbb{Q} is hilbertian by using condition (3) in Definition 3.4. In order to do so, we first need a couple of technical results concerning specialised polynomials and their roots.

Lemma 4.5. *Let K be a field and $f(X, Y) \in K[X, Y]$ separable as a polynomial in Y over K . Then the specialised polynomial $f(b, Y) \in K[Y]$ is separable for almost all $b \in K$.*

Proof. We may assume f is monic in Y . Its discriminant $D(X)$ is a polynomial in X which lies in $K[X]$ and is not identically zero because f is separable in Y . For each $b \in K$ the specialised polynomial $f(b, Y) \in K[Y]$ has discriminant $D(b)$, so $f(b, Y)$ is separable for all $b \in K$ which are not roots of $D(X)$. \square

Proposition 4.6. *Let $p(X, Y) \in \mathbb{Q}[X][Y]$ be an irreducible polynomial over $\mathbb{Q}(X)$, of degree $r > 1$ in Y . Then for almost all $x_0 \in \mathbb{Z}$ the following holds:*

- (i) *There exist $\epsilon > 0$ and holomorphic functions $\alpha_1(t), \dots, \alpha_r(t)$ defined for $t \in \mathbb{C}$, $|t| < \epsilon$, such that $\alpha_1(t), \dots, \alpha_r(t)$ are the roots of the polynomial $p(x_0 + t, Y) \in \mathbb{Q}[Y]$.*
- (ii) *If, for some i , $\alpha_i(t)$ is a rational function with complex coefficients, then there are only finitely many $q \in \mathbb{Q}$ with $\alpha_i(q) \in \mathbb{Q}$.*
- (iii) *The set $B(p, x_0) := \{b \in \mathbb{N} \mid p(x_0 + \frac{1}{b}, c) = 0 \text{ for some } c \in \mathbb{Q}\}$ is sparse.*

Proof. By Lemma 4.5. the specialised polynomial $p(x_0, Y)$ is separable for almost all $x_0 \in \mathbb{Q}$, thus for almost all $x_0 \in \mathbb{Z}$. Consider only such integer x_0 for the rest of the proof.

Claim (i) follows directly from this result from complex analysis ([20, Chapter 1, Theorem 1.18]):

Lemma 4.7. *Let $f(X, Y) \in \mathbb{C}[X, Y]$ be a polynomial of degree $n \geq 1$ in Y . Let $c_0 \in \mathbb{C}$ such that the specialised polynomial $f(c_0, Y) \in \mathbb{C}[Y]$ is separable of degree n . Then there exist holomorphic functions $\alpha_1(t), \dots, \alpha_n(t)$, defined in a neighbourhood U of c_0 , such that for each $c \in \mathbb{C}$ the roots of the polynomial $f(c, Y)$ are exactly $\alpha_1(c), \dots, \alpha_n(c)$ ($\alpha_i(c) \neq \alpha_j(c)$ for $i \neq j$).*

To see (ii), assume $\alpha(t) := \alpha_i(t)$ is a rational function with coefficients in \mathbb{C} . Then $p(x_0 + t, \alpha(t)) \equiv 0$ (as a function in t) and so $p(x_0 + X, \alpha(X)) = 0$ in $\mathbb{C}(X)$, where X is transcendental over \mathbb{C} . Thus, $\alpha(X) \in \mathbb{C}(X)$ is a root of a polynomial with coefficients in $\mathbb{Q}(X)$, so it is algebraic over $\mathbb{Q}(X)$ and also over $\bar{\mathbb{Q}}(X)$. But Proposition 3.3. tells us that any irreducible polynomial over $\bar{\mathbb{Q}}(X)$ is also irreducible over $\mathbb{C}(X)$, so $\bar{\mathbb{Q}}(X)$ is algebraically closed in $\mathbb{C}(X)$. Hence, it must be $\alpha(X) \in \bar{\mathbb{Q}}(X)$.

Now, for each $\sigma \in \text{Gal}(\bar{\mathbb{Q}}|\mathbb{Q})$, let σ act on α by applying σ to the coefficients of the rational function α , set $\alpha_\sigma := \sigma(\alpha)$. Then, for all $q \in \mathbb{Q}$ such that $\alpha(q) \in \mathbb{Q}$,

we have $\alpha_\sigma(q) = \sigma(\alpha(q)) = \alpha(q)$ because σ fixes the elements of \mathbb{Q} . If we suppose there are infinitely many such $q \in \mathbb{Q}$, we get $\alpha_\sigma = \alpha$ for each $\sigma \in \text{Gal}(\bar{\mathbb{Q}}|\mathbb{Q})$. But by Artin's theorem $\bar{\mathbb{Q}}^{\text{Gal}(\bar{\mathbb{Q}}|\mathbb{Q})} = \mathbb{Q}$, so it follows that α has coefficients in \mathbb{Q} . In that case $\alpha(X - x_0)$ would be a root of $p(X, Y)$ over $\mathbb{Q}(X)$, contradicting the hypothesis that $p(X, Y)$ is irreducible over $\mathbb{Q}(X)$. Therefore there can only be finitely many $q \in \mathbb{Q}$ such that $\alpha(q) \in \mathbb{Q}$.

For (iii): assume $p(X, Y) \in \mathbb{Z}[X][Y]$:

$$p(X, Y) = \sum_{i=0}^r p_i(X)Y^i$$

with $p_i \in \mathbb{Z}[X]$. One can take R large enough that

$$X^R p\left(x_0 + \frac{1}{X}, Y\right) = \sum_{i=0}^r X^R p_i\left(x_0 + \frac{1}{X}\right) Y^i$$

is still an element of $\mathbb{Z}[X][Y]$. Let $\tilde{p}_i(X)$ denote the coefficient of Y^i in the above expression; set $h(X) := \tilde{p}_R(X)$ and define a new polynomial

$$\tilde{p}(X, T) = T^r + \sum_{i=0}^{r-1} \tilde{p}_i(X) h(X)^{r-i-1} T^i \in \mathbb{Z}[X, T],$$

monic in T . Now take $b \in B(p, x_0)$ and a suitable c , that is, $b \in \mathbb{N}$ and $c \in \mathbb{Q}$ such that $p(x_0 + \frac{1}{b}, c) = 0$. Then $\tilde{p}(b, h(b)c) = 0$ and it follows that $h(b)c \in \mathbb{Q}$ is integral over \mathbb{Z} because $\tilde{p}(b, T) \in \mathbb{Z}[T]$ is monic. Thus, $h(b)c \in \mathbb{Z}$. Moreover, if there is $\epsilon > 0$ such that $|\frac{1}{b}| < \epsilon$, by (i) we have $c = \alpha_i(\frac{1}{b})$ for some $i = 1, \dots, r$. Hence $h(b)\alpha_i(\frac{1}{b}) \in \mathbb{Z}$.

Finally, set $\psi_i(t) = h(\frac{1}{t})\alpha_i(t)$, $i = 1, \dots, r$, defined for $0 < |t| < \epsilon$. According to the reasoning we just saw, if $b \in B(p, x_0)$ with $\frac{1}{b} < \epsilon$ then $\psi_i(\frac{1}{b}) = h(b)\alpha_i(\frac{1}{b}) \in \mathbb{Z}$ for some $i = 1, \dots, r$. It follows that, up to a finite number of elements, the set $B(p, x_0)$ lies in $\cup_{i=1}^r B(\psi_i)$ (using the notation from Proposition 4.4.) If ψ_i is not a rational function, then by Proposition 4.4. we have that $B(\psi_i)$ is sparse. And if ψ_i is a rational function, then α_i is a rational function as well and by (ii) there are only finitely many $q \in \mathbb{Q}$ for which $\alpha_i(q) \in \mathbb{Q}$. Thus, $B(\psi_i)$ is finite. By Lemma 4.2. we obtain that $B(p, x_0)$ is sparse. \square

We finally have all the tools we need to prove the main theorem:

Theorem 4.8. (Hilbert's Irreducibility Theorem) *The field \mathbb{Q} is hilbertian.*

Proof. We will see the claim using condition (3) in Definition 3.4. Let $p_1(X, Y), \dots, p_t(X, Y) \in \mathbb{Q}[X][Y]$ be polynomials, irreducible and of degree > 1 as polynomials in Y over $\mathbb{Q}[X]$. Take $x_0 \in \mathbb{Z}$ as in Proposition 4.6. and so that it works for all $p_i, i = 1, \dots, t$. Let S be the set of $b \in \mathbb{N}$ such that none of the specialised polynomials $p_i(x_0 + \frac{1}{b}, Y) \in \mathbb{Q}[Y]$ has a root in \mathbb{Q} . Our goal is to see that S is infinite.

Set $B = \mathbb{N} \setminus S$. Then, with the notation from Proposition 4.6., $B = \cup_{i=1}^t B(p_i, x_0)$. But by Proposition 4.6. we know that $B(p_i, x_0)$ is sparse for all $i = 1, \dots, t$. Hence, by Lemma 4.2., B itself is sparse and so its complement S is infinite: \mathbb{Q} is hilbertian.

□

5 S_n and A_n as Galois groups over \mathbb{Q}

In this chapter, we see that S_n and A_n are realisable as Galois groups over \mathbb{Q} . We develop the arguments in [12], which follows the ideas in [5]. Prior to that, we introduce the concept of resultant of a polynomial in one variable, because it will be needed later during the argumentation. We state some of its properties and show how it relates to the discriminant. See [3] and [4] for further reference.

Definition 5.1. Let K be a field, and let $f(X), g(X) \in K[X]$ be polynomials,

$$f(X) = a_m(X - x_1) \cdots (X - x_m) \quad g(X) = b_n(X - y_1) \cdots (X - y_n)$$

with $m, n \geq 0$. We define the **resultant** of f and g as

$$Res(f, g) = a_m^n b_n^m \prod_{i=1}^m \prod_{j=1}^n (x_i - y_j) .$$

It is clear that $Res(f, g)$ vanishes if, and only if, f and g have a root in common. Some of the properties of the resultant are:

1. $Res(f, g) = (-1)^{mn} Res(g, f)$.
2. If $m = 0$, i.e. if $f(X) = a_0$ is constant, then $Res(f, g) = a_0^n$.
3. If $h(X) \in K[X]$, $Res(hf, g) = Res(h, g)Res(f, g)$.
4. Since $g(X) = b_n \prod_{i=1}^n (X - y_i)$, it follows that $Res(f, g) = a_m^n \prod_{i=1}^m g(x_i)$.

Given a polynomial $f(X) \in K[X]$ as above, its derivative $f'(X) \in K[X]$ is obviously also a polynomial. Setting

$$f'(X) = \sum_{i=1}^m a_m(X - x_1) \cdots (\widehat{X - x_i}) \cdots (X - x_m)$$

and using property 4, we get:

$$Res(f, f') = a_m^{m-1} \prod_{i=1}^m f'(x_i) = a_m^{m-1} \prod_{i=1}^m \left(a_m \prod_{j \neq i} (x_i - x_j) \right) = a_m^{2m-1} \prod_{i=1}^m \prod_{j \neq i} (x_i - x_j)$$

Observation 5.2. If we now assume $f(X)$ to be monic, according to Definition 2.1. we get

$$\text{Res}(f, f') = \prod_{i=1}^m \prod_{j \neq i} (x_i - x_j) = \prod_{i < j} (x_i - x_j)^2 = \Delta(f) .$$

After this short digression, we come back to our main concern: proving that S_n and A_n are realisable as Galois groups over \mathbb{Q} . We start by proving that, if one considers the Galois group G of a polynomial with coefficients in a purely transcendental field extension of an algebraic number field, and then specialises the independent transcendentals to elements of \mathbb{Z} , then the Galois group of the specialised polynomial is isomorphic to G . This result assures that if we work over a purely algebraic extension $\mathbb{Q}(T)$ and find a solution to our problem there, we will have infinitely many ways to go back down to \mathbb{Q} and still have a positive answer.

Theorem 5.3. *Let k be an algebraic number field, $K = k(T_1, \dots, T_r)$ a purely transcendental extension of k , $r \leq 1$, $F = F(T_1, \dots, T_r, X) \in K[X]$ a polynomial. There exist infinitely many r -tuples $t = (t_1, \dots, t_r) \in \mathbb{Z}^r$ such that the specialised polynomial $F_t(X) := F(t_1, \dots, t_r, X) \in k[X]$ satisfies $\text{Gal}(F|K) \cong \text{Gal}(F_t|k)$.*

Proof. Let $A = k[T_1, \dots, T_r]$ be the ring of integers of K , L the splitting field of F over K , B the integral closure of A in L . Since $L|K$ is finite and separable, there exists $b \in B$ such that $L = K(b)$; let $H(X) \in A[X]$ be the minimal polynomial of b over K and let $t = (t_1, \dots, t_r)$ be one of the infinitely many r -tuples such that the specialised polynomial $H_t(X) \in k[X]$ is irreducible (Theorem 4.8.).

Now consider the ideal $\mathfrak{p} = (T_1 - t_1, \dots, T_r - t_r)$, which is prime because the quotient $A/\mathfrak{p} \cong k$ is a field and thus a domain. Let e, f and g be the ramification index, the inertia degree and the decomposition number, respectively, of $\mathfrak{p}B$. Let \mathfrak{P} be a prime ideal of B over \mathfrak{p} , let $D_{\mathfrak{P}}$ and $I_{\mathfrak{P}}$ be the corresponding decomposition group and inertia group, and $\bar{L} = B/\mathfrak{P}$ and $\bar{K} = A/\mathfrak{p}$ the respective residue fields. \bar{K} has characteristic 0 because it is isomorphic to k ; therefore the field extension $\bar{L}|\bar{K}$ is separable. Hence, $\bar{L}|\bar{K}$ is Galois and by Proposition 3.21. we have $\text{Gal}(\bar{L}|\bar{K}) \cong D_{\mathfrak{P}}/I_{\mathfrak{P}}$.

Besides, the polynomial H is irreducible mod \mathfrak{p} because $H \equiv H_t \pmod{\mathfrak{p}}$ and H_t is irreducible. This implies $f \geq n$, where $n = [L : K] = \text{deg}(H)$. However, the

equality $efg = n$ holds (Corollary 3.18.), so it must be $f = n$ and $e = g = 1$. Thus, by Artin's theorem and Proposition 3.22., $D_{\mathfrak{p}} = \text{Gal}(L|K)$ and $I_{\mathfrak{p}} = \{id\}$. Consequently $D_{\mathfrak{p}}/I_{\mathfrak{p}} \cong D_{\mathfrak{p}}$ and we get

$$\text{Gal}(F|K) = \text{Gal}(L|K) \cong \text{Gal}(\bar{L}|\bar{K}) = \text{Gal}(F_t|K)$$

as desired. □

Our goal from now on is clear: we want to find polynomials with coefficients in some purely transcendental extension K of \mathbb{Q} , so that we can specialise them and have polynomials with coefficients in \mathbb{Q} with the desired Galois group, namely S_n and A_n .

5.1 The group S_n

In this section we follow [16].

Definition 5.4. Let $n \geq 2$, $A = \mathbb{Z}[T_n, x_1, \dots, x_n]$ the ring of polynomials in $n + 1$ indeterminates with coefficients in \mathbb{Z} , $K = \mathbb{Q}(T_n, x_1, \dots, x_n)$ its field of fractions. The **general polynomial of degree n** is the polynomial

$$F(X) = T_n(X - x_1)(X - x_2) \cdots (X - x_n) \in A[X].$$

By developing the product, $F(X)$ can be written as

$$F(X) = T_n X^n + T_{n-1} X^{n-1} + \cdots + T_1 X^1 + T_0 \in A[X],$$

whose coefficients are

$$T_i := (-1)^{n-i} T_n s_{n-i}(x_1, \dots, x_n)$$

for every $i \in \{0, \dots, n-1\}$, where the $s_i(x_1, \dots, x_n)$ are the elementary symmetrical polynomials in x_1, \dots, x_n . The group S_n acts trivially on K by permuting x_1, \dots, x_n , so the elements of S_n can be seen as automorphisms of K . Therefore, by Artin's theorem the field extension $K|K^{S_n}$ is finite and Galois, and $\text{Gal}(K|K^{S_n}) \cong S_n$. Now, any element of S_n acting on K fixes not only \mathbb{Q} and T_n , but also s_1, \dots, s_n , so it fixes T_0, \dots, T_{n-1} as well. Thus $K^{S_n} = \mathbb{Q}(T_0, \dots, T_n)$, and we get $F(X) \in \mathbb{Q}(T_0, \dots, T_n)$.

Now, F is irreducible in $\mathbb{Q}(T_0, \dots, T_n)$, its splitting field is $K = \mathbb{Q}(T_n, x_1, \dots, x_n)$, and $\text{Gal}(K|\mathbb{Q}(T_0, \dots, T_n)) = S_n$. By Hilbert's Irreducibility Theorem there exist infinitely many $(n + 1)$ -tuples $t = (t_0, \dots, t_n)$ so that the specialised polynomial $F_t(X) \in \mathbb{Q}[X]$ is also irreducible and has Galois group isomorphic to S_n (Theorem 5.3.).

Note that an analogous reasoning can be used over an arbitrary number field k : indeed, letting F have coefficients in the ring of integers of k delivers the same result. That proves the following result as a corollary of Theorem 4.8. and Theorem 5.3.

Corollary 5.5. *There exist infinitely many Galois extensions over any number field with Galois group isomorphic to S_n . In particular, S_n is realisable as a Galois group over \mathbb{Q} .* \square

5.2 The group A_n

Our next goal is to find polynomials realising A_n over a purely transcendental extension of a given number field k . Here we go back to following [12].

We are looking for a polynomial $F \in \mathbb{Q}(T)[X]$ (and so $F \in k(T)[X]$ for any algebraic number field k) satisfying two conditions:

- (1) $\Delta(F) \in \mathbb{Q}(T)^{*2}$, and
- (2) $\text{Gal}(F|\mathbb{C}(T)) = A_n$.

These two conditions ensure that F has Galois group over $k(T)$ isomorphic to A_n : on the one hand, the first condition implies $\text{Gal}(F|k(T)) \subseteq A_n$ by Lemma 2.2.; on the other hand, since $\text{Gal}(F|\mathbb{C}(T)) \subset \text{Gal}(F|k(T))$ because any automorphism that fixes $\mathbb{C}(T)$ must fix $k(T)$ as well, the second condition implies $A_n \subset \text{Gal}(F|k(T))$.

The construction of said polynomial depends on the parity of n , so we shall develop each case separately.

5.2.1 Case n even

The case $n = 2$ has already been covered because $A_2 \cong C_2 \cong S_2$ and therefore the general quadratic polynomial solves the problem.

For $n > 2$, let $r = (n - 2)/2$ and let a_1, \dots, a_r be positive integers such that $a_i \neq a_j$ if, and only if, $i \neq j$. Let $f = f(X)$ be the only polynomial such that

$$f'(X) = nX(X - a_1)^2 \cdots (X - a_r)^2 \quad \text{and} \quad f(0) = 0 .$$

The derivative $f'(X)$ is positive for any $X > 0$, which means that f is monotonically increasing when viewed as a polynomial function. Therefore, $f(a_i) \neq 0$ for every $i = 1, \dots, r$ (implying 0 is a double root of f and all its other roots are simple) and $f(a_i) \neq f(a_j)$ if $i \neq j$.

We then define the polynomial

$$F = F(T, X) = T^2 + f(X) \in \mathbb{Q}(T)[X] ,$$

so that $F' = f'$ (with respect to X). Using the property stated in Observation 5.2. and property 4 of the resultant, we get

$$\Delta(F) = \text{Res}(F, F') = \text{Res}(F, f') = n^n F(0) \prod_{i=1}^r F(a_i)^2 = n^n T^2 \prod_{i=0}^r (T^2 + f(a_i))^2 .$$

Hence $\Delta(F) \in \mathbb{Q}(T)^{*2}$ and the polynomial F satisfies condition (1). Moving on to seeing the second condition, we give a lemma that characterises A_n in terms of the permutations that generate it.

Lemma 5.6. *Let G be a transitive subgroup of A_n . If G is generated by 3-cycles, then $G = A_n$.*

Proof. Remember that a group G acting on the set $X = \{1, \dots, n\}$ is a transitive subgroup of A_n if every permutation of G is even and for every $i, j \in X$ there exists $\sigma \in G$ such that $\sigma(i) = j$. Remember also that A_n is a transitive group itself. If $Y \subseteq X$, let $A(Y)$ denote the subgroup of A_n of permutations which fix $X \setminus Y$ and note that $A(X) = A_n$.

If $(a \ b \ c)$ is one of the generators of G , then $A(\{a, b, c\}) = \langle (a \ b \ c) \rangle \subseteq G$. That

means that there exists a subset $Y \subseteq X$ containing at least 3 elements such that $A(Y) \subseteq G$. If $Y = X$, $A(Y) = A(X) = A_n \subseteq G$ and the lemma is proved. If $Y \subsetneq X$, there is at least one 3-cycle in G that permutes some element of Y with another element of $X \setminus Y$, because otherwise the action of G would leave Y and $X \setminus Y$ invariant, contradicting the transitivity of G . Accordingly, let $(i j k) \in G$ and assume, for example, $i \in Y$, $j \notin Y$. Now let $r, s \in Y$, r, s different from i, k . We have $(i r s), (i s r) \in A(Y) \subseteq G$ and:

$$(i r s)(i j k)(i s r) = (j k r) .$$

Thus, $(j k r) \in G$ for each $r \in Y \setminus \{k\}$ and it follows that $A(Y \cup \{j, k\}) \subseteq G$. But X is a finite set, so by iterating this process finitely many times we reach $Y = X$ and therefore $G = A(X) = A_n$. \square

We have finally reached the peak of our argumentation. In the next proposition we shall see that the inertia groups of certain prime ideals are generated by 3-cycles. This result, combined with the lemma we just proved, will allow us to show later that indeed $\text{Gal}(F|\mathbb{C}(T)) = A_n$, where $F(T, X) = T^2 + f(X) \in \mathbb{Q}(T)[X]$.

Let $A = \mathbb{C}[T]$, $K = \mathbb{C}(T)$ its field of fractions, and $G = \text{Gal}(F|K) \subseteq \text{Gal}(F|k(T)) \subseteq A_n$. Let L be the splitting field of F in an algebraic closure \bar{K} of K , and let B be the integral closure of A in L .

Since \mathbb{C} is a field, A is a principal ideal domain and so it is a Dedekind domain; hence, B is a Dedekind domain as well. The extension $L|K$ is Galois because L is the splitting field of F and we are working in characteristic 0.

Proposition 5.7. *The inertia groups of the prime ideals of B in the field extension $L|K$ are either trivial or generated by one 3-cycle.*

Proof. Let

$$\mathfrak{p}_0 = (T), \quad \mathfrak{p}_j = \left(T + \sqrt{-f(a_j)} \right), \quad \mathfrak{p}_{j+r} = \left(T - \sqrt{-f(a_j)} \right) \quad \text{for } j = 1, \dots, r$$

be $2r + 1$ prime ideals in A .

Let $b \in L$ be a root of F and consider the field extension $K(b)$ of K . Let A' be the ring of integers of $K(b)$. Since $K(b)$ is generated by one element and the minimal

polynomial of b is F , according to Observation 3.24. we have that $\delta_{K(b)|K}$ is the principal ideal $(\Delta(F))$. Besides, the prime ideals \mathfrak{p}_i , $i = 0, 1, \dots, 2r$, are the only ones in A that divide $(\Delta(F)) = \delta_{K(b)|K}$. Therefore, by Proposition 3.25. these are the only prime ideals that are ramified in $K(b)$ and thus by Proposition 3.26. the ideals \mathfrak{p}_i , $i = 0, 1, \dots, 2r$, are the only prime ideals that are ramified in L . Therefore we can focus our study on these specific ideals, because the inertia group of any other ideal in $L|K$ will be trivial.

Moreover, for each prime ideal \mathfrak{p}_i of A the residue field A/\mathfrak{p}_i is isomorphic to \mathbb{C} . But the complex field is algebraically closed, so all algebraic extensions of \mathbb{C} are trivial. Therefore all residue degrees are equal to 1.

Let us see how F decomposes in each of the residue fields A/\mathfrak{p}_i . For $i = 0$, the image of F in A/\mathfrak{p}_0 is f . This polynomial has 0 as a root of multiplicity 2, since it is also a root of f' , and $n - 2$ simple roots. For $i \neq 0$, the image of F in A/\mathfrak{p}_i is $f - f(a_i)$, which has a_i as a root of multiplicity 3 (because a_i is a double root of f'), and $n - 3$ simple roots.

Hensel's Lemma (Proposition 3.31.) allows us to lift these decompositions to $K_{\mathfrak{p}_i}$, the completion of K for the respective \mathfrak{p}_i -adic absolute value. Thus we get the following: if $i = 0$, then

$$F = G_0 \cdots G_{n-2} ,$$

where $\deg(G_0) = 2$ and $\deg(G_j) = 1$ for $j > 0$; if $i \neq 0$, then

$$F = H_{i,0} \cdots H_{i,n-3} ,$$

with $\deg(H_{i,0}) = 3$ and $\deg(H_{i,j}) = 1$ for $j > 0$.

Let \mathfrak{p} be one of the ideals \mathfrak{p}_i , $i = 0, 1, \dots, 2r$, and let \mathfrak{P} a prime ideal of B over \mathfrak{p} . Let b_1, \dots, b_n be the roots of F in an algebraic closure of K . Then, by [15, ch. 2, sec. 3, corol. 1],

$$L_{\mathfrak{P}} \cong LK_{\mathfrak{p}} \cong K_{\mathfrak{p}}(b_1, \dots, b_n)$$

According to our previous reasoning, one has $b_i \in K$ for $i \geq 4$ and so we get $L_{\mathfrak{P}} \cong K_{\mathfrak{p}}(b_1, b_2, b_3)$. Thus, the inertia group $I_{\mathfrak{P}}$ lies in S_3 . But we already saw that $I_{\mathfrak{P}} \subseteq \text{Gal}(F|\mathbb{C}(T)) \subseteq A_n$, so in fact we have $I_{\mathfrak{P}} \subseteq A_3$. Since the alternating group is generated by 3-cycles, $I_{\mathfrak{P}}$ must be generated by 3-cycles as well. If the prime ideal considered is \mathfrak{p}_0 , the reasoning is analogue to that which we just saw, the only

difference now being that $L_{\mathfrak{P}} \cong K_{\mathfrak{p}}(b_1, b_2)$. In that case, since the only possible non-trivial permutation of the roots would be a transposition and these do not lie in A_n , the only option left is for $I_{\mathfrak{P}}$ to be the trivial group. \square

Finally, we define I to be the subgroup of G generated by all the inertia groups and set $N := L^I$, which is then the largest unramified subextension of $L|K$. Applying the Hurwitz genus formula for N and K [9, ch.I, sec.6],

$$2g_N - 2 = [N : K](2g_K - 2) + \sum_{\mathfrak{P}} (e - 1) ,$$

where g_N and g_K are the genera of N and K , respectively, \mathfrak{P} runs through all prime ideals of N , and $e_{\mathfrak{P}}$ denotes the ramification index of \mathfrak{P} . We know that $K = \mathbb{C}(T)$ has genus 0 and $e_{\mathfrak{P}} = 1$ for all \mathfrak{P} because $N|K$ is unramified. Thus, we obtain a simplified expression:

$$g_N - 1 = -[N : K]$$

where $g_N \geq 0$ and $[N : K] \geq 1$. Hence, the only values that satisfy the equality are $g_N = 0$ and $[N : K] = 1$. This implies that actually $N = K$, i.e. there exist no unramified extensions of K , and we get $I = G$. Therefore, G is generated by 3-cycles.

Besides, seeing $F = T^2 + f = T^2 - (-f)$ as a polynomial in T , $F \in \mathbb{C}[X][T]$, it becomes clear that it is irreducible because $-f$ is not a square in $\mathbb{C}[X]$. Thus, G is transitive and by Lemma 5.6. we get the desired result: $G = A_n$. This proves that F really is the polynomial we needed, because it satisfies conditions (1) and (2) and so $\text{Gal}(F|k(T)) = A_n$.

5.2.2 Case n odd

We just proved the existence of a polynomial satisfying our conditions in the case it has even degree. We shall do a similar construction now for a polynomial with odd degree.

This time set $r = (n - 1)/2$ and let a_1, \dots, a_r be strictly positive integers with $a_i \neq a_j$ for $i \neq j$. Set

$$a = -\frac{1}{2 \sum_{i=1}^r \frac{1}{a_i}} \in \mathbb{Q}$$

and define the polynomial

$$g(X) = (n-1)(X-a) \prod_{i=1}^r (X-a_i)^2 \in \mathbb{Q}(X).$$

Because of how we defined a , the coefficient of X is 0. This condition is necessary and sufficient for the existence of a polynomial $f(X) \in \mathbb{Q}(X)$ such that $g = Xf' - f$. Note that $f = Xf' - g$ and $g' = Xf''$.

Given this polynomial f we define a polynomial $F = F(T, X) \in \mathbb{Q}(T)[X]$,

$$F = f + (T^2 - f'(a))X = Xf' - g + (T^2 - f'(a))X = -g + (T^2 + f' - f'(a))X,$$

for which

$$F' = -g' + Xf'' + (T^2 + f' - f'(a)) = T^2 + f' - f'(a).$$

That means F can be rewritten as $F = -g + XF'$, so by Observation 5.2. and using the properties right after Definition 5.1. one has

$$\begin{aligned} \Delta(F) &= \text{Res}(F, F') \\ &= \text{Res}(-g + XF', F') \\ &= \text{Res}((-1)(g - XF'), F') \\ &= (-1)^{n-1} \text{Res}(g - XF', F') \\ &= \text{Res}(g, F') \\ &= (n-1)^{n-1} F'(a) \prod_{i=1}^r F'(a_i) \\ &= (n-1)^{n-1} T^2 \prod_{i=1}^r (T^2 + f'(a_i) - f'(a))^2. \end{aligned}$$

This is a square in $\mathbb{Q}(T)$ because $n-1$ is even, so F satisfies condition (1). To see F satisfies condition (2) as well, we take prime ideals in A

$$\mathfrak{p}_0 = (T), \quad \mathfrak{p}_j = \left(T + \sqrt{-f'(a_j) + f'(a)} \right), \quad \mathfrak{p}_{j+r} = \left(T - \sqrt{-f'(a_j) + f'(a)} \right)$$

for $j = 1, \dots, r$, and from there on we can proceed exactly as in the case n even, using Proposition 5.7. Indeed, the image of F in A/\mathfrak{p}_0 is $-g + (f' - f'(a))X$, which

has a as a double root and $n - 2$ simple roots (because $g(0) \neq 0$ and $f' - f'(a)$ vanishes only at a), and for $i \neq 0$ the image of F in A/\mathfrak{p}_i is $-g + (f' - f'(a_i))X$, which has a_i as a triple root and $n - 3$ simple roots. For the reasoning after Proposition 5.7., note that considering F as an element of $\mathbb{C}[X][T]$ makes it clear that it is irreducible.

Hence, we have proved the next theorem.

Theorem 5.8. *For every $n \in \mathbb{N}$ one can construct polynomials of degree n with Galois group over $\mathbb{Q}(T)$ isomorphic to A_n . \square*

So, just like with S_n , we get the following result as a corollary from Theorem 4.8. and Theorem 5.3.

Corollary 5.9. *There exist infinitely many Galois extensions over any number field with Galois group isomorphic to A_n . In particular, A_n is realisable as a Galois group over \mathbb{Q} . \square*

6 Conclusions

Having reached this point, it is time to reflect on what we have achieved and its implications. Throughout this thesis we have become acquainted with many new mathematical concepts and techniques from abstract algebra and algebraic number theory, which have provided us with the necessary knowledge to successfully reach our initial goal. Even further: not only have we proved that S_n and A_n are indeed realisable as Galois groups over $\mathbb{Q}(T)$ and thus over the rational field, but we have found general results for any algebraic number field.

The aim to solve the Inverse Galois Problem brings together many areas of mathematics such as number theory, group theory, topology, algebraic geometry and complex analysis. Each of these fields comes with its own perspective on the topic and its own set of tools, and the variety of techniques offers a very diverse and fruitful approach to the problem. Consequently, the research needed for this thesis suggests that mathematics is much more than the sum of isolated areas of knowledge. We suspect there is no such thing as ‘pure algebra’, ‘pure analysis’, ‘pure number theory’, ‘pure topology’... Boundaries between different disciplines are not clearly defined and it is precisely the intertwinement of mathematical ideas what allows for progress and discovery.

Bibliography

- [1] ATIYAH, Michael F.; MACDONALD, Ian G. *Introduction to Commutative Algebra*. Reading (Mass.): Addison-Wesley, 1969. (Addison-Wesley series in mathematics).
- [2] CORNELISSEN, Gunther. «Lecture Notes on p -adic Numbers. Utrecht University Summer School 2016 on Geometry». Utrecht, the Netherlands, August 11, 2016.
- [3] GELFAND, Israel M.; KAPRANOV, Mikhail M.; ZELEVINSKY, Andrei V. *Discriminants, Resultants, and Multidimensional Determinants*. Boston: Birkhäuser, 1994. (Mathematics: Theory & Applications).
- [4] GUÀRDIA, Jordi; VILA, Núria. *Àlgebra I: de la pràctica a la teoria*. Barcelona: Publicacions Universitat de Barcelona, 1997. (Textos docents; 53. Text-guia).
- [5] HILBERT, David. «Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten». *Journal für die reine und angewandte Mathematik*, 1892, vol. 110, num. 18, p. 104-129.
- [6] JANUSZ, Gerald J. *Algebraic Number Fields*. New York: Academic Press, 1973. (Pure and Applied Mathematics; 55).
- [7] JENSEN, Christian U.; LEDET, Arne; YUI, Noriko. *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*. Cambridge [etc.]: Cambridge University Press, cop. 2002. (Mathematical Sciences Research Institute publications; 45).
- [8] LANG, Serge. *Algebra*. 3rd ed. Reading (Mass.) [etc.]: Addison-Wesley, cop. 1993.
- [9] LANG, Serge. *Introduction to Algebraic and Abelian Functions*. 2nd ed. New York: Springer, 1982. (Graduate texts in mathematics; 89).
- [10] LONG, Robert L. *Algebraic Number Theory*. New York: Marcel Dekker, 1977. (Monographs and textbooks in pure and applied mathematics; 41).
- [11] MORANDI, Patrick. *Field and Galois Theory*. New York [etc.]: Springer, 1996. (Graduate texts in mathematics; 167).

- [12] NART, Enric; VILA, Núria. «Sobre l'existència d'equacions que realitzen S_n i A_n com a grups de Galois d'un cos de números». *Publicacions de la Secció de Matemàtiques, UAB*, July 1979, num. 13, p. 79-87.
- [13] NEUKIRCH, Jürgen. *Algebraic Number Theory*. Translated from the German by Norbert Schappacher. Berlin: Springer, 1999. (Grundlehren der mathematischen Wissenschaften; 322).
- [14] RIBENBOIM, Paulo. *Algebraic Numbers*. New York: Wiley-Interscience, 1972. (Pure and applied mathematics; 27).
- [15] SERRE, Jean-Pierre. *Local Fields*. Translated from the French by Marvin Jay Greenberg. New York: Springer, cop. 1979. (Graduate texts in mathematics; 67).
- [16] TRAVESA, Artur. *Curs d'àlgebra*. [Online]
<<https://atlas.mat.ub.edu/personals/travesa>> [January 13, 2017]
- [17] TRAVESA, Artur. *Teoria de nombres*. [Online]
<<https://atlas.mat.ub.edu/personals/travesa>> [January 13, 2017]
- [18] VILA, Núria. «On the Inverse Problem of Galois Theory». *Publicacions Matemàtiques*, 1992, vol. 36, p. 1053-1073.
- [19] VILA, Núria. «Sobre el teorema d'irreductibilitat de Hilbert». *Publicacions de la Secció de Matemàtiques, UAB*, December 1986, vol. 30, num. 2-3.
- [20] VÖLKLEIN, Helmut. *Groups as Galois Groups: an Introduction*. Cambridge: Cambridge University Press, 1996. (Cambridge Studies in Advanced Mathematics; 53).
- [21] WAERDEN, Bartel L. van der. *Modern Algebra*. Volume 1. Translated from the second revised German edition by Fried Blum. New York: Frederick Ungar, 1953.