

UiO  **Faculty of Mathematics and Natural Sciences**
University of Oslo

Galois Theory of Palindromic Polynomials

Pia Lindstrøm
Master's Thesis, Spring 2015



Preface

Abstract

In 1862, substituting for professor O. J. Broch, Ludvig Sylow gives the first lectures ever given on the field of Galois theory in Norway, at the University of Christiania. He lectures on, amongst other things, what he calls “reciproke ligninger” (reciprocal equations), i.e. equations of the form

$$\begin{aligned} f(x) = x^{2n} + a_1x^{2n-1} + a_2x^{2n-2} + \dots + a_{n-1}x^{n+1} + a_nx^n \\ + a_{n-1}x^{n-1} + \dots + a_2x^2 + a_1x + 1 = 0, \end{aligned}$$

see [6, p.59-60]. It turns out that there are some interesting relations between the solutions of these equations.

About one hundred and fifty years later, the Norwegian Julie Kjennerud, who majored in mathematics at the University of Oslo in 1938 but later worked as university lecturer in botany, puzzles with some notes she has and tells an old colleague about them. She is then over 100 years old, but have discovered some interesting polynomials, which she calls “koeffisient symmetriske polynomer” (coefficient symmetrical polynomials) and which have roots with certain properties[1]. They turn out to be exactly the type of polynomials Sylow lectured about.

*These polynomials and their roots is exactly the theme of this thesis: we shall look into these special types of polynomials, calling them **palindromic polynomials**. What can a polynomial’s coefficients possibly tell us about its roots? And can certain connections between the roots help us calculate the polynomial’s Galois group?*

We will see how symmetry of the coefficient leads to special pairwise connections between the roots. Then we will use these connections to derive formulas for finding roots of these polynomials up to and including degree nine.

Having developed these tools we will consider the Galois groups of the palindromic polynomials, before we “upper our game” and consider polynomials which are not precisely palindromic, and which we shall call semipalindromic polynomials. Only some of their roots have the pairwise connection of the palindromic polynomials’. How can we detect that a polynomial is semipalindromic, and what do the Galois groups of the semipalindromic polynomials look like?

Acknowledgements

First of all I would like to thank my supervisor, Arne B. Sletsjøe. Ever since the beginning (and almost even before that) of this project you have been enthusiastic and interested, which has luckily turned out to be very contagious. Thank you for introducing me to the field of Galois theory, and for showing me that things can be easier, and more interesting, than I first realize myself - though I have also learned that things can take longer time and also be harder than first expected.

Next I would like to thank my dad, Tom Lindstrøm, for time and time again proofreading with critical eyes, but still not leaving me feeling completely screwed (just a bit, but always with good tools and hints for fixing it). And of course I owe the rest of my family, my mom Nann, brothers Jonas and Anders and sister Kaja, a big “thank you” as well. Thank you for accepting that I am in fact a math geek. Even though you make sure of mentioning it quite often (and almost always with a critical undertone...), I think we’re actually all in the same boat in that department - yes, you too, Kaja!

Also a huge “thank you” to you, Maren, for always being there for me! I would never have been where I am now if it wasn’t for you.

And lastly, but probably not least, I would like to thank my fellow students for making these five years five good ones. Amongst you a special thanks to Marthe, my “partner in crime” through subject after subject and on (almost) every event - without you these years would never have been the same. Along with one to all the other students of study hall B601 (both you present once but also you former), a thanks to both Astri and Fredrik, whom for no apparent reasons have been seated in study hall B606 instead - you are just as good as us B601’ers. Thank you all for making the years at Blindern not only about studies, but also about meeting friends and being social!

An extra thanks to Fredrik for proofreading, and for your love and care even when things got a bit too much for me. Even though I was a pain in the neck most of the time, almost never agreeing with you, I’m very grateful that you took time to “argue” with me, calm me down and help me improve my thesis.

This part is the only part which is proofread only by me, so if you find any misprints in other parts of the thesis, Fredrik, my dad and Arne are solely to blame for them (almost...). I take the blame for any potential misprints in the acknowledgments.

The years studying mathematics at the University of Oslo have given me a lot of knowledge, new friends and both fun and frustrating times. I’m grateful for the good learning environment the faculty has offered!

Oslo, 2015

Pia.

Contents

Preface	3
Abstract	3
Acknowledgements	5
Historical note	9
Introduction	17
1 Palindromic polynomials	21
1.1 Roots of palindromic polynomials	21
1.1.1 Finding the roots	29
2 Galois theory of palindromic polynomials	37
2.1 The Galois group	40
3 Characterization of a polynomial's roots	51
3.1 The usual discriminant of polynomials	51
3.2 The palindromic discriminant	54
3.3 Changing bases	55
3.4 The derived polynomials $P^{(2)}$ and P^*	61
4 Semipalindromic polynomials	65
4.1 The Galois groups of semipalindromic polynomials	66
Bibliography	81

Historical note

Before we start considering polynomials and their roots, let us take a second to shortly review the history of solving equations, starring both the Norwegian mathematician Niels Henrik Abel and the French genius Evariste Galois.

Finding the zeroes of different polynomials has been studied since the Babylonian time, about 1600 BC. The quadratic-, or *abc*-formula, for finding the roots of second degree polynomials is well known to most people. It is a quick and easy way to find the two complex roots of a quadratic equation. A little more tricky, and not so well known, is Cardano's formula for finding the three complex roots of a cubic polynomial. Still it exists and even a not very advanced calculator will use it to find the solutions of these equations. Actually, there is also an even more complicated formula for finding the roots of a quartic equation.

Even though these two last formulas look rather horrendous, only basic algebraic operations such as,

$$+, -, \times, \div, \sqrt{\quad}, \sqrt[3]{\quad}, \sqrt[4]{\quad}, \sqrt[5]{\quad}, \dots$$

and the coefficients of the polynomial are used to find expressions of its roots.

Some time (maybe even a very long time) after these formulas were derived, at least one mathematician asked himself for how high degrees he could find such expressions. The mathematician was the Norwegian Niels Henrik Abel, and he would be the one to show that it's impossible to find a formula for calculating the roots of a general polynomial of degree five or higher, using only algebraic operations. But it would take him some time even just to realize that this was the case.

As a matter of fact, while Abel was still a student at "Katedralskolen", he actually thought he had found a formula for calculating the five complex

roots of any quintic polynomial, and neither Abel nor any other Norwegian mathematician could find any flaws in it. But after some time Abel himself realized that this formula could not be correct for all polynomial fifth degree equations. With time his belief that no such formula existed grew stronger and stronger, but his suspicion was hard to prove. It turned out that the Italian mathematician Paolo Ruffini had actually given a proof of this some years earlier, which Abel did not know about at first, but was made aware of later. Eventually he found flaws in both Ruffini's and his own first attempted proof.

But Abel succeeded at last! In 1823 he presented a proof to what is now known as the *Abel-Ruffini* theorem: there is no general algebraic solution, meaning solution in radicals, to equations of degree five or higher.

Actually, Abel proved that there are *some* polynomials which can not be solved using radicals. What the proof doesn't include are conditions for saying which of the quintic (and higher degree) equations that are unsolvable by radicals. An example of an equation which can not be solved by radicals is $x^5 - x + 1 = 0$, while the equation $x^5 - x^4 - x + 1 = 0$, which may look more complicated, actually can be solved by an algebraic formula using radicals. As he became interested in other fields of mathematics, e.g. elliptic curves, Niels Henrik Abel never solved the question of which equations of degree five or higher could not be solved by radicals. His life ended at a young age, and his question was still unanswered.

Niels Henrik Abel was born on Finnøy in Ryfylke in Norway the 5th of August 1802. His father, Søren Georg Abel, was vicar and a prominent man. In 1804 Niels Henrik's grandfather, the vicar at Gjerstad in Aust-Agder died, and Søren Georg moved here with his family to fill the shoes of his dead father. Niels Henrik grew up at Gjerstad with an older brother, three younger brothers and one sister.

In 1815 he traveled to Christiania to attend "Katedralskolen". As his mathematics teacher was fired after beating a student to death, Bernt Michael Holmboe became Abel's new teacher. Holmboe was a different type of teacher, giving his students independent tasks, challenging them mathematically. Holmboe and his challenging tasks were probably what triggered Abel's interest in mathematics. It has been said that without the influence of Bernt Michael Holmboe, Abel would probably not have been the mathematician he

was.

Even as a young student, Abel probably had more mathematical knowledge than any other contemporary Norwegian. He had to study on his own. After publishing an article in *Magazin for Naturvidenskaberne* in the spring of 1823, some of the Norwegian professors understood that Abel needed to go abroad to widen his knowledge, but lack of funds forced him stay in Christiania. The same summer, though, he got the opportunity to go to Copenhagen. Here he started his work on elliptic curves, which he would later become famous for. After this visit, Abel became even more eager to travel further, and after writing a letter to the King he got funds to travel again the summer of 1825.



Figure 1: Niels Henrik Abel.

In Berlin he met an engineer with great interest in mathematics, August Leopold Crelle. Crelle wanted to publish a mathematical journal, and in 1826 the first number of *Journal für die reine und angewandte Mathematik* (often called *Crelle's Journal*) was published. In his first article for Crelle, Abel published an expansion of the *Abel-Ruffini* theorem. Abel would come to publish most of his articles in *Crelle's journal*, which quickly gave the magazine a reputation as the leading mathematical journal in Europe.

The summer of 1826 Abel finally reached the most important destination of his trip, Paris, which was the greatest mathematical center at that time. But his visit was a great disappointment. As he received no response on his big *Paris-thesis* from the “Academy of Science” and felt more and more unhappy in the city, Abel returned to Berlin in the beginning of 1827. In May the same year he returned to Norway. Having caught tuberculosis in Paris, he was already affected by the disease. Still he continued to work on his big thesis on elliptic functions, and as he finished the paper he resumed

his work on equations.

Being increasingly ill from his disease, Abel could not return to Christiania after spending Christmas with his fiancée, Christine Kemp, at Froland Verk in 1828. As he understood his life was coming to an end, Abel wrote down a resumé of a proof of what is these days called “Abel’s addition theorem”. The resumé was sent to Crelle. On the 6th of April 1829 Abel died in poverty at Froland Verk, having left the world of mathematics a lot of new and useful results and theories.

12 years after his death, in 1841 Abel’s *Paris-thesis* was published, and it was also included in his collected work, which was published in 1881.

A couple of years after Abel presented the *Abel-Ruffini* theorem, the young and promising student Evariste Galois wondered *why* the formulas Abel had been looking for didn’t exist. His idea was to study the symmetries of the solutions of polynomial equations. In 1846, long after his death, an independent proof of Abel’s theorem, proved by Galois, was published. In addition, Galois could describe which polynomials could, and which could not, be solved using radicals.

The story about the young and promising Galois is unfortunately both short and unsuccessful in many ways. Though Galois brought forth some very important mathematics, most of it was never presented during his own lifetime. There is little doubt that the loss of his potential, already at the age of 20, was a great tragedy for the scientific world.

Evariste Galois was born in France in 1811. As a young boy he was home taught by his mother, but as he was about to turn twelve, he started the famous school *Lycée Louis-le-Grand* in Paris. Being held back by the headmaster from entering the advanced rhetoric class at age fifteen, Galois was introduced to mathematics - which would become his life-long (although this was, as already revealed, not long) fascination. He lost interest for all other subjects and focused almost



Figure 2: Evariste Galois at Lycée Louis-le-Grand.

entirely on the problems of mathematics.

One of Galois' teachers, Louis Paul Emilie Richard, published his first paper, which was also his first sweep into what would become his new theories about groups and fields. He wanted to show, by first introducing the idea of a group, that to find the roots of certain polynomials, one would have to create a special group for the polynomial and some of its properties would determine whether or not the polynomial was solvable (meaning by radicals). This group is now known as the "Galois group" of the polynomial.

As Galois continued his studies at the Lycée, Richard encouraged him to submit two papers to the "Academy of Science", but Galois never got recognition for the work done in these papers.

Neither his academic nor his personal life treated Galois well. In 1829 his father committed suicide, and only days after, Galois re-failed the exam to be accepted to the *Ecole Polytechnique*, the greatest scientific college in France at that time. His only option was then to attend the next best college, the *Ecole Préparatoire*.

In February of 1830 the then 18 years old Galois again presented his ideas to the "Academy of Science", attempting to win the great mathematical honor "the Grand Prize". But again luck was against him, and the secretary died before even reading his paper.

During his time at the *Préparatoire* Galois became interested in politics, making him involved in protests and discussions. Living in poverty and serving time in prison due to political "battles", made his life tough. July of 1831 was really not a good month for him. He moved into his own apartment, breaking ties with his family. Again he was, due to leading a political protest, arrested and sentenced to six months in prison. As he got ill during his sentence, he got transferred to a hospital where he met a girl he fell head over heels in love with. But she turned his love down, and he insulted her somehow, which might have led to the notorious duel on the 31st of May 1832, ending his life the next day[2].

There is no historical agreement on the exact reason for the duel which

cost Evariste Galois his life. Some think it was a lovers' quarrel while others believe it was political. History is not even clear on whom he fought or how he got to the hospital, but the fact that he died from his injuries the next day, not yet 21 years old, is certain.

Whomever Galois fought and for whatever reason, Galois seems to have been pretty aware of and convinced of his impending death. The entire night before the duel Galois sat up, finishing his mathematical memoirs, consisting of a letter to Auguste Chevalier, outlining his ideas, and three attached manuscripts. During the night he also wrote letters to his Republican friends.

Not until 1843 were Galois' mathematical contributions published, we picture the first page of his memoirs on the next page. Joseph Liouville had reviewed the manuscripts Galois left behind, and declared them sound. Galois' collected work turned out just some 60 pages, but it contains many important ideas which have had consequences for nearly all branches of mathematics[3].

MÉMOIRE

Sur les conditions de résolubilité des équations par radicaux.

Le Mémoire ci-joint [*] est extrait d'un ouvrage que j'ai eu l'honneur de présenter à l'Académie il y a un an. Cet ouvrage n'ayant pas été compris, les propositions qu'il renferme ayant été révoquées en doute, j'ai dû me contenter de donner, sous forme synthétique, les principes généraux, et une *seule* application de ma théorie. Je supplie mes juges de lire du moins avec attention ce peu de pages.

On trouvera ici une *condition* générale à laquelle *satisfait toute équation soluble par radicaux*, et qui réciproquement assure leur résolubilité. On en fait l'application seulement aux équations dont le degré est un nombre premier. Voici le théorème donné par notre analyse :

« Pour qu'une équation de degré premier, qui n'a pas de diviseurs commensurables, soit soluble par radicaux, il *faut* et il *suffit* que toutes les racines soient des fonctions rationnelles de deux quelconques d'entre elles. »

Les autres applications de la théorie sont elles-mêmes autant de théories particulières. Elles nécessitent d'ailleurs l'emploi de la théorie des nombres, et d'un algorithme particulier : nous les réservons pour une autre occasion. Elles sont en partie relatives aux équations modulaires de la théorie des fonctions elliptiques, que nous démontrons ne pouvoir se résoudre par radicaux.

Ce 16 janvier 1831.

E. GALOIS.

[*] J'ai jugé convenable de placer en tête de ce Mémoire la préface qu'on va lire, bien que je l'aie trouvée biffée dans le manuscrit.

A. CII.

Figure 3: The first page of Galois' memoirs.

Introduction

Although they both died at a young age, Abel and Galois left the world of mathematics a lot of new ideas and theories. Both are perhaps most famous for their work on the solvability of polynomial equations, but using different methods.

To study the solvability of polynomials by radicals, Galois considered permutations of their roots leaving the coefficient field fixed. The modern approach is to study automorphisms determined by these permutations.

As mentioned earlier Galois first created what he called *groups*, and then one special group, the Galois group, associated to a polynomial. In this master thesis we are going to look at the Galois group of different types of polynomials. Let us first introduce some of the theory and the main result of Galois theory.

Definition 0.0.1. Let F be a field with algebraic closure \bar{F} . Let $f(x)$ be a polynomial in $F[x]$. A field $E \subseteq \bar{F}$ is the **splitting field of f over F** if it is the smallest subfield of \bar{F} containing F and all the zeroes of f in \bar{F} .

Definition 0.0.2. A polynomial $P(x)$ over a field K is **separable** if roots are distinct in an algebraic closure of K . The number of its distinct roots is equal to its degree.

The splitting field of a polynomial is an important part of its Galois theory. The next definition will also be quite useful as we start considering polynomials:

Definition 0.0.3. A finite extension K of F is a **finite normal extension of F** if K is a separable splitting field over F . A **separable extension** of a

field F is an algebraic field extension $K \supseteq F$ such that for every $\alpha \in K$, the minimal polynomial of α over F is a separable polynomial.

Having introduced the notion of a splitting field, we can “finally” reveal what this much spoken of Galois group is.

Definition 0.0.4. Let $P(x)$ be a polynomial in $F[x]$, F a field, and assume E with $F \subseteq E \subseteq \bar{F}$ is the splitting field of P over F . Then **the Galois group, $\text{Gal}(E/F)$, of P** is the group of all automorphisms of E which leaves F fixed. If $F \subseteq E \subseteq \bar{F}$, we also say $\text{Gal}(E/F)$ is the Galois group of E .

Galois theory has basically one main theorem. This is stated generally for fields, which is also how we state it here, but before we do so, we need to introduce one more definition.

Definition 0.0.5. Let $\{\sigma_i | i \in I\}$ be a collection of automorphisms of the field E . Then the field $E_{\{\sigma_i\}}$ is the fixed field of $\{\sigma_i | i \in I\}$. In our theorem below this means e.g. that $K_{\text{Gal}(K/E)}$ is the fixed field of all the automorphisms in $\text{Gal}(K/E)$.

We are now ready to state the main theorem of Galois theory [4, theorem 53.6, p.451]:

Theorem 0.0.6. *Let K be a finite normal extension of the field F and let its Galois group be $\text{Gal}(K/F)$. For a field E , where $F \subseteq E \subseteq K$, let $\lambda(E)$ be the subgroup of $\text{Gal}(K/F)$ which leaves E fixed. Then λ is a one-to-one map of the set of all such intermediate fields E onto the set of all subgroups of $\text{Gal}(K/F)$. The following properties hold for λ :*

1. $\lambda(E) = \text{Gal}(K/E)$
2. $E = K_{\text{Gal}(K/E)} = K_{\lambda(E)}$
3. For $H \subseteq \text{Gal}(K/F)$, $\lambda(K_H) = H$
4. The degree of K over E , $[K : E] = |\lambda(E)|$ and the degree of E over F , $[E : F] = (\text{Gal}(K/F) : \lambda(E))$, the number of left cosets of $\lambda(E)$ in $\text{Gal}(K/F)$.

5. E is a normal extension of F if and only if $\lambda(E)$ is a normal subgroup of $\text{Gal}(K/F)$. When $\lambda(E)$ is a normal subgroup of $\text{Gal}(K/F)$, then

$$\text{Gal}(E/F) \simeq \text{Gal}(K/F)/\lambda(E).$$

6. The diagram of subgroups of $\text{Gal}(K/F)$ is the inverted diagram of intermediate fields of K over F .

As we will use it quite often, we state 5. also for fields $\mathbb{Q} \subseteq E \subseteq F$, where F is a finite normal extension of the field \mathbb{Q} and $\text{Gal}(F/\mathbb{Q})$ is its Galois group:

5. E is a normal extension of \mathbb{Q} if and only if $\lambda(E)$ is a normal subgroup of $\text{Gal}(F/\mathbb{Q})$. When $\lambda(E)$ is a normal subgroup of $\text{Gal}(F/\mathbb{Q})$, then

$$\text{Gal}(E/\mathbb{Q}) \simeq \text{Gal}(F/\mathbb{Q})/\lambda(E).$$

We are now ready to start our work on the Galois theory of some special types of polynomials.

Chapter 1

Palindromic polynomials

Definition 1.0.7. A polynomial $P(x) \in \mathbb{Q}[x]$

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

of degree n is said to be *palindromic* if $a_{n-i} = a_i$ for $i = 0, 1, 2, \dots, n$.

Example 1.0.8. Examples of palindromic polynomials are:

- $x^2 + 2x + 1$
- $x^4 + 1$
- $4x^3 + 2x + 4$



1.1 Roots of palindromic polynomials

Since we are interested in finding the zeros of palindromic polynomials, we might as well assume that a_n (and thereby also a_0 , since the polynomial is palindromic) is equal to 1, because if $a_n \neq 1$ we simply divide all coefficients by a_n .

For simplicity we shall usually denote a palindromic polynomial with coefficients in \mathbb{Q} as

$$P(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_2 x^2 + a_1 x + 1.$$

Observation 1.1.1. Assume P has roots $\alpha_1, \alpha_2, \dots, \alpha_n$, where some of the roots may have multiplicity greater than 1. Then

$$P(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

And because every monic palindromic polynomial has constant term 1, this means

$$\begin{aligned} 1 &= (-\alpha_1)(-\alpha_2) \cdots (-\alpha_n) = (-1)^n \cdot \alpha_1 \alpha_2 \cdots \alpha_n \\ \implies \alpha_1 \alpha_2 \cdots \alpha_n &= \frac{1}{(-1)^n} = (-1)^n. \end{aligned}$$

So for palindromic polynomials the product of the roots always equals $(-1)^n$, where n is the degree of the polynomial.

Example 1.1.2. Consider the case $n = 2$. Since $(-1)^n = (-1)^2 = 1$ and every second degree polynomial has two roots (which might be the same with multiplicity 2), the roots are each other's inverses. In other words: if we call the roots α_1 and α_2 , for a palindromic second degree polynomial we must have


$$\alpha_2 = \frac{1}{\alpha_1}.$$

Let's see that using the well known *abc*-formula gives us the same result: A second degree palindromic polynomial looks like $P(x) = x^2 + bx + 1$, and the *abc*-formula gives

$$\alpha_1 = \frac{-b + \sqrt{b^2 - 4}}{2}, \quad \alpha_2 = \frac{-b - \sqrt{b^2 - 4}}{2}$$

If we now consider α_1 and $\frac{1}{\alpha_1}$, we see that

$$\alpha_1 = \frac{-b + \sqrt{b^2 - 4}}{2} \implies \frac{1}{\alpha_1} = \frac{2}{-b + \sqrt{b^2 - 4}} = \frac{-b - \sqrt{b^2 - 4}}{2} = \alpha_2.$$

Which again shows that the two roots of a second degree palindromic polynomial are each other's inverses. 

Example 1.1.3. Let $n = 3$ then if $\alpha_1, \alpha_2, \alpha_3$ are the roots of $P(x) = x^3 + ax^2 + ax + 1$, we have

$$\alpha_1 \cdot \alpha_2 \cdot \alpha_3 = (-1)^3 = -1.$$

Further we see that for third degree palindromic polynomials $\alpha = -1$ will always be a root:

$$P(-1) = (-1)^3 + a(-1)^2 + a(-1) + 1 = -1 + a - a + 1 = 0.$$

If we let $\alpha_1 = -1$ we must have $\alpha_2 \cdot \alpha_3 = 1$, or $\alpha_3 = \frac{1}{\alpha_2}$. In addition we have

$$\begin{aligned} P(x) &= x^3 + ax^2 + ax + 1 = (x + 1)(x - \alpha_2)(x - \alpha_3) \\ &= x^3 + (1 - \alpha_2 - \alpha_3)x^2 + (\alpha_2 \cdot \alpha_3 - \alpha_3 - \alpha_2)x + \\ &\quad \alpha_2 \cdot \alpha_3 \\ &= x^3 + (1 - \alpha_2 - \alpha_3)x^2 + (1 - \alpha_3 - \alpha_2)x + 1 \end{aligned}$$

(where we've used the fact that $\alpha_1 = -1$ and $\alpha_2 \cdot \alpha_3 = 1$), so we see that

$$a = 1 - \alpha_2 - \alpha_3.$$



As in the example above with $n = 3$ we can deduce that for all odd n , a palindromic polynomial of degree n has $\alpha = (-1)$ as a root (which might have multiplicity greater than 1).

Proposition 1.1.4. *If $P(x)$ is a palindromic polynomial of odd degree n , then (-1) is a root of $P(x)$.*

Proof. Let

$$P(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_2x^2 + a_1x + 1$$

be a polynomial of odd degree, $n = 2m + 1$. If we evaluate P at $x = -1$, we have

$$\begin{aligned} P(-1) &= (-1)^n + a_1(-1)^{n-1} + a_2(-1)^{n-2} + \dots + a_2(-1)^2 + a_1(-1) + 1 \\ &= (-1) + a_1 \cdot 1 + a_2 \cdot (-1) + \dots + a_2 \cdot 1 + a_1 \cdot (-1) + 1 \\ &= a_1 - a_2 + \dots + a_2 - a_1 \end{aligned}$$

From this it seems all terms will cancel, but let us take a look to be sure this is the case:

Assume first that i is even, say $i = 2k$. Since P is palindromic we know that $a_{n-i} = a_i$, and we see that evaluated at $x = -1$ we have

$$a_i(-1)^i = a_i \cdot (-1)^{2k} = a_i \cdot 1 = a_i.$$

But we also have that

$$n - i = 2m + 1 - 2k = 2(m - k) + 1$$

is odd, so

$$a_{n-i}(-1)^{n-i} = a_i(-1)^{n-i} = a_i \cdot (-1) = -a_i.$$

This shows that if i is even, then $n - i$ is odd, so evaluated at $x = -1$ the sum $a_i x^i + a_i x^{n-i}$ cancel.

Now if we assume i is odd, $i = 2k + 1$, evaluated at $x = -1$ we have

$$a_i(-1)^i = a_i(-1) = -a_i.$$

But then

$$n - i = 2m + 1 - (2k + 1) = 2(m - k),$$

is even, so

$$a_{n-i}(-1)^{n-i} = a_i(-1)^{n-i} = a_i \cdot 1 = a_i,$$

which shows that also if i is odd the sum $a_i x^i + a_i x^{n-i}$ evaluated at $x = -1$ cancel.

Lastly we make sure no terms are left uncanceled. Since n is odd, P has $n + 1$, which is even, terms. This means there is no “middle term” which is not cancelled, and we have

$$P(-1) = -1 + a_1 - a_2 + a_3 - a_4 + \dots + a_4 - a_3 + a_2 - a_1 + 1 = 0.$$

□

The next proposition, describing on more property of palindromic polynomials, will turn out to be surprisingly useful in the following.

Proposition 1.1.5. *A polynomial $P(x) \in \mathbb{Q}[x]$ of degree n is palindromic if and only if*

$$P(x) = x^n P\left(\frac{1}{x}\right).$$

Proof. \implies Assume first that $P(x)$ is palindromic:

$$P(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_2x^2 + a_1x + 1.$$

Then we have

$$\begin{aligned} x^n P\left(\frac{1}{x}\right) &= x^n \left(\left(\frac{1}{x}\right)^n + a_1 \left(\frac{1}{x}\right)^{n-1} + a_2 \left(\frac{1}{x}\right)^{n-2} + \dots \right. \\ &\quad \left. + a_2 \left(\frac{1}{x}\right)^2 + a_1 \left(\frac{1}{x}\right) + 1 \right) \\ &= 1 + a_1x + a_2x^2 + \dots + a_2x^{n-2} + a_1x^{n-1} + x^n = P(x) \end{aligned}$$

\Leftarrow Now assume $P(x) = x^n P\left(\frac{1}{x}\right)$, which means that

$$\begin{aligned} x^n P\left(\frac{1}{x}\right) &= x^n \left(a_n \left(\frac{1}{x}\right)^n + a_{n-1} \left(\frac{1}{x}\right)^{n-1} + a_{n-2} \left(\frac{1}{x}\right)^{n-2} + \dots \right. \\ &\quad \left. + a_2 \left(\frac{1}{x}\right)^2 + a_1 \left(\frac{1}{x}\right) + a_0 \right) \\ &= a_n + a_{n-1}x + a_{n-2}x^2 + \dots + a_2x^{n-2} + a_1x^{n-1} + a_0x^n = P(x). \end{aligned}$$

Comparing coefficients we see that we must have $a_{n-i} = a_i$ for all i , which means $P(x)$ is palindromic. \square

Lemma 1.1.6. *The product of two palindromic polynomials is a palindromic polynomial. If both $P(x)$ and $Q(x)$ are palindromic polynomials and Q is a factor in P , the quotient $R(x) = \frac{P(x)}{Q(x)}$ is also palindromic.*

Proof. Let $P(x)$ and $Q(x)$ be two palindromic polynomials of degrees n and m respectively. The product, $R(x)$, of P and Q is a polynomial of degree $n+m$, and we need to check that it is palindromic. According to proposition 1.1.5 it suffices to show that $R(x) = x^{n+m} R\left(\frac{1}{x}\right)$.

We know that $P(x) = x^n P\left(\frac{1}{x}\right)$ and that $Q(x) = x^m Q\left(\frac{1}{x}\right)$, so

$$\begin{aligned} R(x) &= P(x)Q(x) = x^n P\left(\frac{1}{x}\right) \cdot x^m Q\left(\frac{1}{x}\right) \\ &= x^{n+m} P\left(\frac{1}{x}\right) Q\left(\frac{1}{x}\right) \\ &= x^{n+m} R\left(\frac{1}{x}\right). \end{aligned}$$

So we have $R(x) = x^{n+m}R(\frac{1}{x})$ and hence the product of two palindromic polynomials is palindromic.

Now let

$$R(x) = \frac{P(x)}{Q(x)},$$

assume $n > m$, and that Q is a factor in P . Then

$$\begin{aligned} R(x) &= \frac{x^n P(\frac{1}{x})}{x^m Q(\frac{1}{x})} \\ &= x^{(n-m)} \frac{P(\frac{1}{x})}{Q(\frac{1}{x})} \\ &= x^{(n-m)} R\left(\frac{1}{x}\right), \end{aligned}$$

which shows that $R(x) = \frac{P(x)}{Q(x)}$ is a palindromic polynomial of degree $n - m$. \square

The previous lemma turns out to be quite useful as we try to characterize the roots of a palindromic polynomial. We will first use it to prove the following:

Lemma 1.1.7. *Let $P(x)$ be a palindromic polynomial. If $\alpha \neq \pm 1$ is a root of P , then so is $\frac{1}{\alpha}$, and their multiplicity is the same.*

Proof. We first show that if $\alpha \neq 0$ is a root of P , then so is $\frac{1}{\alpha}$. Since P is palindromic $P(x) = x^n P(\frac{1}{x})$, which means that if $\alpha \neq 0$ is a root of P , then

$$P(\alpha) = 0 \implies \underbrace{\alpha^n}_{\neq 0} \cdot P\left(\frac{1}{\alpha}\right) = 0 \implies P\left(\frac{1}{\alpha}\right) = 0,$$

so $\frac{1}{\alpha}$ is a root of P as well¹.

Now assume $\alpha \neq \pm 1$ is a root of multiplicity r , larger than the multiplicity, s , of $\frac{1}{\alpha}$. Then

$$P(x) = (x - \alpha)^r (x - \frac{1}{\alpha})^s (x - \alpha_1)^{n_1} (x - \alpha_2)^{n_2} \cdots (x - \alpha_m)^{n_m} (x-1)^t (x+1)^{n-1},$$

¹Note that since all palindromic polynomials have constant term equal to 1, 0 is never a root.

where $\alpha_1, \dots, \alpha_m, 1, (-1)$ are the rest of the roots of P with multiplicities $n_1, \dots, n_m, t, n_{-1}$ respectively (where t and n_{-1} could be zero). Observing that

$$\begin{aligned} (x - \alpha)\left(x - \frac{1}{\alpha}\right) &= x^2 - \left(\alpha + \frac{1}{\alpha}\right)x + 1 \\ \implies (x - \alpha)^s \left(x - \frac{1}{\alpha}\right)^s &= \left(x^2 - \left(\alpha + \frac{1}{\alpha}\right)x + 1\right)^s, \end{aligned}$$

by lemma 1.1.6 $(x - \alpha)^s \left(x - \frac{1}{\alpha}\right)^s$ is palindromic and hence so is

$$\begin{aligned} R(x) := \frac{P(x)}{(x - \alpha)^s \left(x - \frac{1}{\alpha}\right)^s} &= (x - \alpha)^{r-s} (x - \alpha_1)^{n_1} (x - \alpha_2)^{n_2} \dots \\ &\quad (x - \alpha_m)^{n_m} (x - 1)^t (x + 1)^{n_{-1}}. \end{aligned}$$

But now $R(x)$ is a palindromic polynomial where α is a root even though $\frac{1}{\alpha}$ isn't. As we saw in the start of the proof, this can not be the case. Hence if $\alpha \neq \pm 1$ is a root of P , then $\frac{1}{\alpha}$ is a root with the same multiplicity. \square

Before we state our theorem, we benefit from first stating, and proving, one more lemma.

Lemma 1.1.8. *If $\alpha = 1$ is a root of a palindromic polynomial, then it is of even multiplicity.*

Proof. We know from the lemma above that if $\alpha_i \neq \pm 1$ is a root of P , then $\frac{1}{\alpha_i}$ is a root as well and it has the same multiplicity, n_i . If we denote the multiplicity of the root (-1) as n_{-1} (might be 0) and the multiplicity of the root 1 as r , we can rewrite P as

$$\begin{aligned} P(x) &= (x - 1)^r (x + 1)^{n_{-1}} \left(x^2 - \left(\alpha_1 + \frac{1}{\alpha_1}\right)x + 1\right)^{n_1} \dots \\ &\quad \left(x^2 - \left(\alpha_m + \frac{1}{\alpha_m}\right)x + 1\right)^{n_m}. \end{aligned}$$

If we now assume the multiplicity of 1 is odd, say $r = 2k + 1, k \geq 0$, and note that $(x - 1)^2 = x^2 - 2x + 1$ is palindromic, we see that

$$\begin{aligned} P(x) &= (x - 1)^{2k+1} (x + 1)^{n_{-1}} \left(x^2 - \left(\alpha_1 + \frac{1}{\alpha_1}\right)x + 1\right)^{n_1} \dots \\ &\quad \left(x^2 - \left(\alpha_m + \frac{1}{\alpha_m}\right)x + 1\right)^{n_m} \\ &= (x - 1)(x^2 - 2x + 1)^k (x + 1)^{n_{-1}} \left(x^2 - \left(\alpha_1 + \frac{1}{\alpha_1}\right)x + 1\right)^{n_1} \dots \\ &\quad \left(x^2 - \left(\alpha_m + \frac{1}{\alpha_m}\right)x + 1\right)^{n_m}, \end{aligned}$$

where both $(x^2 - 2x + 1)^k$, $(x + 1)^{n-1}$ and $\left(x^2 - \left(\alpha_i + \frac{1}{\alpha_i}\right)x + 1\right)^{n_i}$ are palindromic for $i = 1, \dots, m$. This means the product of them is also palindromic, so their product has 1 as constant term. But when multiplied with the last factor $(x - 1)$, of P , we see that the constant term changes to -1 . Hence $P(x)$ can not be palindromic, which contradicts our assumption that the root 1 is of odd multiplicity. \square

We are now ready to state and prove the following result:

Theorem 1.1.9. *A polynomial $P(x) \in \mathbb{Q}[x]$ is palindromic if and only if the following two conditions are satisfied:*

- (1) *1 is a root of even multiplicity (possibly zero)*
- (2) *if $\alpha \neq \pm 1$ is a root, then $\frac{1}{\alpha}$ is a root with the same multiplicity.*

Also, if (-1) is a root of a palindromic polynomial, the multiplicity is always odd if the polynomial is of odd degree, and always even if the polynomial is of even degree.

Proof. We start by proving our “if and only if” statement:

\implies (1) is lemma 1.1.8, and (2) is lemma 1.1.7.

\impliedby We want to prove that if all roots not equal to ± 1 of a polynomial $P(x) \in \mathbb{Q}[x]$ come in inverse pairs, i.e. the fact that $\alpha_i \neq \pm 1$ is a root of multiplicity n_i implies that also $\frac{1}{\alpha_i}$ is a root of multiplicity n_i , and the multiplicity of the root 1 is even, then P is palindromic. If we let r and s be the multiplicities of the roots 1 and -1 respectively (they might be 0) and $\alpha_1, \frac{1}{\alpha_1}, \alpha_2, \frac{1}{\alpha_2}, \dots, \alpha_m, \frac{1}{\alpha_m}$ be the rest of the roots with multiplicities $n_1, n_1, n_2, n_2, \dots, n_m, n_m$ respectively, we have

$$P(x) = (x - 1)^r (x + 1)^s \prod_{i=1}^m \left(x^2 - \left(\alpha_i + \frac{1}{\alpha_i}\right)x + 1\right)^{n_i}$$

By assumption r is even, say $r = 2k, k \geq 0$, so the polynomial $(x - 1)^r = (x - 1)^{2k} = (x^2 - 2x + 1)^k$ is palindromic by lemma 1.1.6. Both $(x + 1)^s$ and the product $\prod_{i=1}^m \left(x^2 - \left(\alpha_i + \frac{1}{\alpha_i}\right)x + 1\right)^{n_i}$ are palindromic as well, which means $P(x)$ is a product of palindromic polynomial, so by lemma 1.1.6, P must be palindromic as well.

So we have proved our first statement and continue by proving the next; that if (-1) is a root the multiplicity is always odd if the polynomial is of odd degree, and always even if the polynomial is of even degree.

We know from the fundamental theorem of algebra (see e.g. [5, theorem 3.5.1]) that every polynomial of degree n has n complex roots, counted with multiplicity. So if n is odd, any polynomial of degree n has an odd number of roots. But from the result above we know that every other root than (-1) comes in inverse pairs $\{\alpha, \frac{1}{\alpha}\}$ with even multiplicity (the pair, since the multiplicity of α and $\frac{1}{\alpha}$ is the same).

From the first statement we know that if 1 is a root it is of even multiplicity $2k$ where k could be 0 . Now let $2n_1$ be the multiplicity of the pair of roots $\{\alpha_1, \frac{1}{\alpha_1}\}$, $2n_2$ be the multiplicity of the pair of roots $\{\alpha_2, \frac{1}{\alpha_2}\}$ and so on, until the “last” roots $\{\alpha_r, \frac{1}{\alpha_r}\}$ ($r \leq n$). Let the multiplicity of (-1) be n_{-1} . Then the number of roots are

$$\left(\sum_{i=1}^r 2n_i\right) + 2k + n_{-1} = \left(2\sum_{i=1}^r n_i\right) + 2k + n_{-1}.$$

And since n is odd and both $(2\sum_{i=1}^r n_i)$ and $2k$ are even, we must have n_{-1} odd.

Now, in the case of an even degree polynomial, n would be even, so since $(2\sum_{i=1}^r n_i)$ and $2k$ are even, so must n_{-1} .

□

Remark 1.1.10. Note that if α_i and $\frac{1}{\alpha_i}$ don't have the same multiplicity, even though $P(\alpha_i) = 0 \implies P\left(\frac{1}{\alpha_i}\right) = 0$, $P(x)$ need not be palindromic. Just consider the example $P(x) = (x-2)^2(x-\frac{1}{2}) = x^3 - \frac{9}{2}x^2 + 6x - 2$. $P(x)$ is not palindromic, but if $P(\alpha) = 0$, then $P\left(\frac{1}{\alpha}\right) = 0$ also.

1.1.1 Finding the roots

Knowing that all roots (other than possibly $\alpha = -1$) of a palindromic polynomial come in inverse pairs $\{\alpha_i, \frac{1}{\alpha_i}\}$, where α_i and $\frac{1}{\alpha_i}$ have the same multiplicity, will turn out to be very handy as we try to calculate the roots of

palindromic polynomials of different degrees.

Let $P(x) \in \mathbb{Q}[x]$ be a monic polynomial of degree n . As mentioned earlier P has exactly n complex roots, counted with multiplicity. Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the roots of P . If we assume that all the roots are different, and that they are the minimal number of elements we need to be able to express all the roots of $P(x)$ and that none of them are in \mathbb{Q} , then the splitting field of P would be

$$\mathbb{Q}(\alpha_1, \dots, \alpha_n)$$

and the Galois group of P would be

$$\text{Gal}(\mathbb{Q}(\alpha_1, \dots, \alpha_n)/\mathbb{Q})$$

which has order (at most) $n!$

As mentioned in the historical note, Niels Henrik Abel proved that one can not find a formula for calculating roots of general polynomials of degree five or higher. In fact, Galois showed that the solvability of its Galois group determines whether or not a polynomial can be solved using radicals, as is the case for 2nd, 3rd and 4th degree “normal” polynomials. As we just saw, these polynomials have Galois groups of order at most $2! = 4$, $3! = 6$ and $4! = 24$ respectively. More importantly we have $\text{Gal}(\mathbb{Q}(\alpha_1, \dots, \alpha_n)/\mathbb{Q}) \simeq S_n$, and S_n is solvable for all $n \leq 4$, but unsolvable for $n \geq 5$. Which means we can find the roots of 2nd, 3rd and 4th degree “normal” polynomials using radicals.

But we’ve just seen that for palindromic polynomials, every root is the inverse of another root. So if we need to extend \mathbb{Q} with the root α_k to have the splitting field of a palindromic polynomial $P(x) \in \mathbb{Q}[x]$, then this extension also contains the root $\frac{1}{\alpha_k}$, so we get this root “for free”. This means that for a palindromic polynomial of degree n with coefficients in \mathbb{Q} , the splitting field is an extension of \mathbb{Q} with at most $\frac{n}{2}$ elements if n is even, or $\frac{n-1}{2}$ if n is odd, because (-1) is already in \mathbb{Q} . If we assume that $\frac{n}{2}$ or $\frac{n-1}{2}$ of these roots are different and algebraically independent, we see that the Galois group is

$$\text{Gal}(\mathbb{Q}(\alpha_1, \dots, \alpha_{n/2})/\mathbb{Q}) \text{ or } \text{Gal}(\mathbb{Q}(\alpha_1, \dots, \alpha_{(n-1)/2})/\mathbb{Q})$$

which has order (at most) $\frac{n}{2}!$ or $\frac{n-1}{2}!$, in the even and odd cases respectively.

This means that there should be formulas for finding the roots of palindromic polynomials of up to and including degree nine! Let's figure out how to do this:

We first consider the easiest case, $n = 5$. Since we know that (-1) is a root, we simply divide our 5th degree polynomial by $(x + 1)$ to find a 4th degree polynomial of which we can find the roots, using the formula for roots of a polynomial of degree 4.

We now consider the cases $n = 6$ and $n = 7$. In the case $n = 7$, (-1) is a root, so we simply divide the polynomial by $(x + 1)$. Since $(x + 1)$ is a palindromic polynomial, according to lemma 1.1.6 the quotient of a palindromic polynomial of degree 7 and $(x + 1)$ is a palindromic polynomial of degree 6. Hence we only need to consider polynomials of degree 6.

Let

$$P(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_2x^2 + a_1x + 1$$

be our palindromic 6th degree polynomials, where $a_1, a_2, a_3 \in \mathbb{Q}$.

This polynomial has six roots, which we denote $\alpha_1, \alpha_2, \alpha_3, \frac{1}{\alpha_1}, \frac{1}{\alpha_2}$ and $\frac{1}{\alpha_3}$. Then

$$\begin{aligned} P(x) &= (x - \alpha_1) \left(x - \frac{1}{\alpha_1}\right) (x - \alpha_2) \left(x - \frac{1}{\alpha_2}\right) (x - \alpha_3) \left(x - \frac{1}{\alpha_3}\right) \\ &= \left(x^2 - \left(\alpha_1 + \frac{1}{\alpha_1}\right)x + 1\right) \left(x^2 - \left(\alpha_2 + \frac{1}{\alpha_2}\right)x + 1\right) \\ &\quad \left(x^2 - \left(\alpha_3 + \frac{1}{\alpha_3}\right)x + 1\right) \end{aligned}$$

If we define

$$\beta_1 = \alpha_1 + \frac{1}{\alpha_1}, \quad \beta_2 = \alpha_2 + \frac{1}{\alpha_2} \quad \text{and} \quad \beta_3 = \alpha_3 + \frac{1}{\alpha_3},$$

we can rewrite our polynomial as

$$\begin{aligned} P(x) &= (x^2 - \beta_1x + 1)(x^2 - \beta_2x + 1)(x^2 - \beta_3x + 1) \\ &= (x^4 - (\beta_1 + \beta_2)x^3 + (2 + \beta_1\beta_2)x^2 - (\beta_1 + \beta_2)x + 1)(x^2 - \beta_3x + 1) \\ &= x^6 - (\beta_1 + \beta_2 + \beta_3)x^5 + (3 + \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3)x^4 \\ &\quad - (2\beta_1 + 2\beta_2 + 2\beta_3 + \beta_1\beta_2\beta_3)x^3 + (3 + \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3)x^2 \\ &\quad - (\beta_1 + \beta_2 + \beta_3)x + 1. \end{aligned}$$

Let

$$\begin{aligned} S_1 &= \beta_1 + \beta_2 + \beta_3, \\ S_2 &= \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3, \\ S_3 &= \beta_1\beta_2\beta_3 \end{aligned}$$

be the elementary symmetric polynomials in the three “variables” β_1 , β_2 and β_3 . Then we have

$$\begin{aligned} S_1 &= -a_1 \\ S_2 &= a_2 - 3 \\ S_3 &= -a_3 - 2S_1 = 2a_1 - a_3 \end{aligned}$$

This is a set of equations which we can solve; β_1 , β_2 and β_3 are the three solutions of the equation

$$\begin{aligned} x^3 - S_1x^2 + S_2x - S_3 &= 0 \\ \implies x^3 + a_1x^2 + (a_2 - 3)x - (2a_1 - a_3) &= 0. \end{aligned}$$

And once we find β_1 , β_2 and β_3 , we easily find α_1 , α_2 and α_3 by solving

$$\begin{aligned} \beta_i &= \alpha_i + \frac{1}{\alpha_i} \\ \implies \alpha_i\beta_i &= \alpha_i^2 + 1 \\ \alpha_i^2 - \beta_i\alpha_i + 1 &= 0, \end{aligned}$$

which is easy using the *abc*-formula.

The last case we consider is $n = 8$ and $n = 9$. It suffices to find the roots of a 8th degree polynomial, since we know that (-1) is a root of every 9th degree palindromic polynomial. So let us consider the polynomial

$$P(x) = x^8 + a_1x^7 + a_2x^6 + a_3x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + 1.$$

Again we let the roots be $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \frac{1}{\alpha_1}, \frac{1}{\alpha_2}, \frac{1}{\alpha_3}$ and $\frac{1}{\alpha_4}$. If we now define

$$\beta_1 = \alpha_1 + \frac{1}{\alpha_1}, \quad \beta_2 = \alpha_2 + \frac{1}{\alpha_2}, \quad \beta_3 = \alpha_3 + \frac{1}{\alpha_3}, \quad \beta_4 = \alpha_4 + \frac{1}{\alpha_4},$$

we have

$$\begin{aligned}
P(x) &= (x^2 - \beta_1x + 1)(x^2 - \beta_2x + 1)(x^2 - \beta_3x + 1)(x^2 - \beta_4x + 1) \\
&= x^8 - (\beta_1 + \beta_2 + \beta_3 + \beta_4)x^7 \\
&\quad + (4 + \beta_1\beta_2 + \beta_1\beta_3 + \beta_1\beta_4 + \beta_2\beta_3 + \beta_2\beta_4 + \beta_3\beta_4)x^6 \\
&\quad - (3\beta_1 + 3\beta_2 + 3\beta_3 + 3\beta_4 + \beta_1\beta_2\beta_3 + \beta_1\beta_2\beta_4 + \beta_1\beta_3\beta_4 + \beta_2\beta_3\beta_4)x^5 \\
&\quad + (6 + 2\beta_1\beta_2 + 2\beta_1\beta_3 + 2\beta_1\beta_4 + 2\beta_2\beta_3 + 2\beta_2\beta_4 + 2\beta_3\beta_4 + \beta_1\beta_2\beta_3\beta_4)x^4 \\
&\quad - (3\beta_1 + 3\beta_2 + 3\beta_3 + 3\beta_4 + \beta_1\beta_2\beta_3 + \beta_1\beta_3\beta_4 + \beta_1\beta_3\beta_4 + \beta_2\beta_3\beta_4)x^3 \\
&\quad + (4 + \beta_1\beta_2 + \beta_1\beta_3 + \beta_1\beta_4 + \beta_2\beta_3 + \beta_2\beta_4 + \beta_3\beta_4)x^2 \\
&\quad - (\beta_1 + \beta_2 + \beta_3 + \beta_4)x + 1
\end{aligned}$$

In the same manner as above we now define

$$\begin{aligned}
S_1 &= \beta_1 + \beta_2 + \beta_3 + \beta_4, \\
S_2 &= \beta_1\beta_2 + \beta_1\beta_3 + \beta_1\beta_4 + \beta_2\beta_3 + \beta_2\beta_4 + \beta_3\beta_4, \\
S_3 &= \beta_1\beta_2\beta_3 + \beta_1\beta_2\beta_4 + \beta_1\beta_3\beta_4 + \beta_2\beta_3\beta_4, \\
S_4 &= \beta_1\beta_2\beta_3\beta_4,
\end{aligned}$$

and see that we then have

$$\begin{aligned}
S_1 &= -a_1 \\
S_2 &= a_2 - 4 \\
S_3 &= -3S_1 - a_3 = 3a_1 - a_3 \\
S_4 &= a_4 - 6 - 2S_2 = a_4 - 6 - 2(a_2 - 4) = a_4 - 2a_2 + 2
\end{aligned}$$

Then $\beta_1, \beta_2, \beta_3$ and β_4 are the solutions to the equation

$$\begin{aligned}
&x^4 - S_1x^3 + S_2x^2 - S_3x + S_4 = 0 \\
\implies &x^4 + a_1x^3 + (a_2 - 4)x^2 - (3a_1 - a_3)x + (a_4 - 2a_2 + 2) = 0,
\end{aligned}$$

which can be solved, using radicals. Again we can easily solve

$$\alpha_i^2 - \beta_i\alpha_i + 1 = 0$$

to find $\alpha_1, \alpha_2, \alpha_3$ and α_4 .

Result 1.1.11.

In this box we summarize the methods derived above:

We let α_i be the roots of $P(x)$, and $\beta_i = \alpha_i + \frac{1}{\alpha_i}$. If n is odd, divide P by $(x+1)$ to find a palindromic polynomial of even degree $n-1$.

$n = 6$ (and 7):

$$P(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_2x^2 + a_1x + 1$$

to find $\beta_1, \beta_2, \beta_3$, solve

$$x^3 + a_1x^2 + (a_2 - 3)x - (2a_1 - a_3) = 0.$$

then solve $\alpha_i^2 - \beta_i\alpha_i + 1 = 0$ to find the roots.

$n = 8$ (and 9):

$$P(x) = x^8 + a_1x^7 + a_2x^6 + a_3x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + 1$$

to find $\beta_1, \beta_2, \beta_3, \beta_4$ solve

$$x^4 + a_1x^3 + (a_2 - 4)x^2 - (3a_1 - a_3)x + (a_4 - 2a_2 + 2) = 0.$$

then solve $\alpha_i^2 - \beta_i\alpha_i + 1 = 0$ to find the roots.

Example 1.1.12. As an example, let us consider the polynomial

$$P(x) = x^6 - \frac{9}{2}x^5 + 8x^4 - 9x^3 + 8x^2 - \frac{9}{2}x + 1,$$

and find its zeroes, using the method derived above.

We see that in our example

$$a_1 = -\frac{9}{2}, \quad a_2 = 8 \quad \text{and} \quad a_3 = -9,$$

which means that

$$S_1 = -a_1 = \frac{9}{2},$$

$$S_2 = a_2 - 3 = 5$$

$$S_3 = 2a_1 - a_3 = 0.$$

So to find β_1 , β_2 and β_3 , we need to solve the equation

$$x^3 - S_1x^2 + S_2x - S_3 = 0 \implies x^3 - \frac{9}{2}x^2 + 5x = 0$$

This gives us

$$\beta_1 = 0, \beta_2 = 2 \text{ and } \beta_3 = \frac{5}{2},$$

which means we have

$$\alpha_1^2 - 0\alpha_1 + 1 = 0 \implies \alpha_1 = i$$

$$\alpha_2^2 - 2\alpha_2 + 1 = 0 \implies \alpha_2 = 1$$

$$\alpha_3^2 - \frac{5}{2}\alpha_3 + 1 = 0 \implies \alpha_3 = 2$$

We can now conclude that

$$\begin{aligned} P(x) &= (x - i)(x - 1)(x - 2)\left(x - \frac{1}{i}\right)\left(x - \frac{1}{1}\right)\left(x - \frac{1}{2}\right) \\ &= (x - i)(x - 1)^2(x - 2)(x + i)\left(x - \frac{1}{2}\right). \end{aligned}$$



Example 1.1.13. Let $P(x) = x^6 - \frac{5}{2}x^3 + 1$. Again we use the method derived above to find its zeroes.

We observe that $a_1 = a_2 = 0$ and $a_3 = -\frac{5}{2}$, which means

$$S_1 = -a_1 = 0$$

$$S_2 = a_2 - 3 = -3$$

$$S_3 = 2a_1 - a_3 = -\frac{5}{2}.$$

This leads us to solving the equation

$$\begin{aligned} x^3 - 0x^2 + (-3)x - \left(-\frac{5}{2}\right) &= 0 \\ \implies x^3 - 3x + \left(\frac{5}{2}\right) &= 0 \end{aligned}$$

Solving this equation, together with some algebraic manipulation, we obtain

$$\beta_1 = \sqrt[3]{2} + \frac{1}{\sqrt[3]{2}}, \quad \beta_2 = \sqrt[3]{2}\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) + \frac{1}{\sqrt[3]{2}\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)}$$

$$\text{and } \beta_3 = \sqrt[3]{2} \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i \right) + \frac{1}{\sqrt[3]{2} \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i \right)},$$

so the zeroes of $P(x)$ are

$$\begin{aligned} \alpha_1 &= \sqrt[3]{2}, & \alpha_2 &= \sqrt[3]{2} \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i \right), & \alpha_3 &= \sqrt[3]{2} \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i \right), \\ \alpha_4 &= \frac{1}{\sqrt[3]{2}}, & \alpha_5 &= \frac{1}{\sqrt[3]{2} \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i \right)}, & \alpha_6 &= \frac{1}{\sqrt[3]{2} \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i \right)}. \end{aligned}$$



Chapter 2

Galois theory of palindromic polynomials

As seen, the fact that a polynomial is palindromic at least halves the number of elements of which we have to extend \mathbb{Q} to have the splitting field of the polynomial. Letting F be the splitting field of the palindromic polynomial $P(x)$, we know that the Galois group of $P(x)$, $\text{Gal}(F/\mathbb{Q})$, is the group of all automorphisms $\phi : F \rightarrow F$ which leave \mathbb{Q} fixed. In fact, it turns out that these are all the automorphisms which permutes the roots of $P(x)$ which are not in \mathbb{Q} .

Now, we know that all the roots of $P(x)$ come in “inverse pairs” (except for possibly $\alpha = -1$, which is already in \mathbb{Q}). Since all the elements of $\text{Gal}(F/\mathbb{Q})$ are group isomorphisms, we see that if $\alpha_2 = \frac{1}{\alpha_1}$ and $\phi \in \text{Gal}(F/\mathbb{Q})$ is such that $\phi(\alpha_1) = \alpha_2$, we must also have $\phi(\alpha_2) = \alpha_1$, because

$$\phi(\alpha_2) = \phi\left(\frac{1}{\alpha_1}\right) = \frac{\phi(1)}{\phi(\alpha_1)} = \frac{1}{\alpha_2} = \alpha_1.$$

In the calculations and discussions of this chapter, the following result will turn out quite handy.

Lemma 2.0.14. *The expression $x^n + \frac{1}{x^n}$ can be written as a polynomial in $x + \frac{1}{x}$, with coefficients in \mathbb{Q} , for all $n \in \mathbb{N}$.*

Proof. We prove the result using induction on n .

For $n = 1$ this is trivially true, since

$$x + \frac{1}{x} = \left(x + \frac{1}{x}\right)^1.$$

Assume now that the claim holds for all n up to $n = k$. In particular this means that we can find polynomials $P_{k-1}(x + \frac{1}{x})$ and $P_k(x + \frac{1}{x})$ in $\mathbb{Q}\left[x + \frac{1}{x}\right]$ such that

$$P_{k-1}\left(x + \frac{1}{x}\right) = x^{k-1} + \frac{1}{x^{k-1}}$$

and

$$P_k\left(x + \frac{1}{x}\right) = x^k + \frac{1}{x^k}.$$

Now, we have

$$\begin{aligned} \left(x^k + \frac{1}{x^k}\right)\left(x + \frac{1}{x}\right) &= x^{k+1} + x^{k-1} + \frac{1}{x^{k-1}} + \frac{1}{x^{k+1}} \\ \implies P_k\left(x + \frac{1}{x}\right)\left(x + \frac{1}{x}\right) &= x^{k+1} + \frac{1}{x^{k+1}} + P_{k-1}\left(x + \frac{1}{x}\right), \end{aligned}$$

which gives

$$x^{k+1} + \frac{1}{x^{k+1}} = \left(x + \frac{1}{x}\right)P_k\left(x + \frac{1}{x}\right) - P_{k-1}\left(x + \frac{1}{x}\right),$$

which is a polynomial in $x + \frac{1}{x}$ and coefficients in \mathbb{Q} . □

With this in mind, let us now consider the Galois group of palindromic polynomials. Since every palindromic polynomial of odd degree has (-1) as a root, and (-1) is a rational number (which means it doesn't add anything to the Galois group), it suffices¹ to consider palindromic polynomials of even degree $2n$, where n is a natural number. Hence we explore the palindromic polynomial

$$P(x) = x^{2n} + a_1x^{2n-1} + a_2x^{2n-2} + \dots + a_2x^2 + a_1x + 1,$$

¹by prop. 1.1.4 and lemma 1.1.6 it follows that a palindromic polynomial of odd degree $2n + 1$ divided by $(x + 1)$ is a palindromic polynomial of even degree $2n$.

and assume it has $2n$ distinct roots; $\alpha_1, \frac{1}{\alpha_1}, \alpha_2, \frac{1}{\alpha_2}, \dots, \alpha_n, \frac{1}{\alpha_n}$, none of which belongs to \mathbb{Q} . This means that

$$F = \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$$

is the splitting field of $P(x)$ over \mathbb{Q} .

Consider the rational function

$$\begin{aligned} Q(x) &= \frac{P(x)}{x^n} = \frac{x^{2n} + a_1x^{2n-1} + a_2x^{2n-2} + \dots + a_2x^2 + a_1x + 1}{x^n} \\ &= x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + \frac{a_2}{x^{n-2}} + \frac{a_1}{x^{n-1}} + \frac{1}{x^n} \\ &= x^n + \frac{1}{x^n} + a_1\left(x^{n-1} + \frac{1}{x^{n-1}}\right) + a_2\left(x^{n-2} + \frac{1}{x^{n-2}}\right) + \dots \\ &\quad + a_{n-1}\left(x + \frac{1}{x}\right) + a_n. \end{aligned}$$

According to lemma 2.0.14 this means that we can write $\frac{P(x)}{x^n}$ as a polynomial $Q_P(x + \frac{1}{x})$ with all coefficients in \mathbb{Q} .

More general; if $P(x)$ is a polynomial with coefficients in a field E , the rational function $\frac{P(x)}{x^n}$ has coefficients in E , and then by the construction in lemma 2.0.14, we must also have $Q_P(x + \frac{1}{x}) \in E[x + \frac{1}{x}]$.

Definition 2.0.15. If $P(x)$ is a palindromic polynomial of degree $2n$ in $E[x]$, E a field, with roots $\alpha_1, \frac{1}{\alpha_1}, \alpha_2, \frac{1}{\alpha_2}, \dots, \alpha_n, \frac{1}{\alpha_n}$, we define the **the x^n -derived polynomial of P , $Q_P(x + \frac{1}{x})$** , to be the polynomial obtained by dividing P by x^n and rewriting it as a polynomial in $E[x + \frac{1}{x}]$.

Proposition 2.0.16. $\alpha \neq 0$ is a root of $P(x)$ if and only if $\alpha + \frac{1}{\alpha}$ is a root of $Q_P(x + \frac{1}{x})$.

Proof. \implies First assume $P(\alpha) = 0$, where $\alpha \neq 0$. Then we have

$$\begin{aligned} Q_P\left(x + \frac{1}{x}\right) &= \frac{P(x)}{x^n} \\ \implies Q_P\left(\alpha + \frac{1}{\alpha}\right) &= \frac{P(\alpha)}{\alpha^n} = \frac{0}{\alpha^n} = 0 \end{aligned}$$

\Leftarrow Now assume $Q_P(\alpha + \frac{1}{\alpha}) = 0$, where $\alpha \neq 0$. This means

$$\begin{aligned} P(x) &= Q_P\left(x + \frac{1}{x}\right) \cdot x^n \\ \implies P(\alpha) &= Q_P\left(\alpha + \frac{1}{\alpha}\right) \cdot \alpha^n = 0 \cdot \alpha^n = 0. \end{aligned}$$

□

2.1 The Galois group

It is now clear that if α is a root of a palindromic polynomial $P(x)$, then $\alpha + \frac{1}{\alpha}$ is a root of $Q_P(x + \frac{1}{x})$. Continuing to consider

$$P(x) = x^{2n} + a_1x^{2n-1} + a_2x^{2n-2} + \dots + a_2x^2 + a_1x + 1,$$

this means the splitting field of Q_P is

$$E = \mathbb{Q}\left(\alpha_1 + \frac{1}{\alpha_1}, \alpha_2 + \frac{1}{\alpha_2}, \dots, \alpha_n + \frac{1}{\alpha_n}\right).$$

And since the coefficients of Q_P lie in \mathbb{Q} , E is a splitting field over \mathbb{Q} . According to Galois theory, since E is a splitting field over \mathbb{Q} , E is a **finite normal extension of \mathbb{Q}** . Furthermore, according to point 5. in the main theorem of Galois theory, since E is a normal extension of \mathbb{Q} , $\text{Gal}(F/E)$ is a normal subgroup of $\text{Gal}(F/\mathbb{Q})$. Thus

$$\text{Gal}(E/\mathbb{Q}) \simeq \text{Gal}(F/\mathbb{Q})/\text{Gal}(F/E),$$

or equivalently the exactness of the short sequence

$$1 \rightarrow \text{Gal}(F/E) \rightarrow \text{Gal}(F/\mathbb{Q}) \rightarrow \text{Gal}(E/\mathbb{Q}) \rightarrow 1.$$

It's trivial to see that $E \subseteq F$, but we can even say something about the degree of F over E :

Proposition 2.1.1. *F is of order 2^m over E , with $m \leq n$.*

Proof. Assume $\alpha_i + \frac{1}{\alpha_i}$ is a root of Q_P , such that

$$\begin{aligned}\beta_i &= \alpha_i + \frac{1}{\alpha_i} \in E \\ \implies \alpha_i^2 - \beta_i \alpha_i + 1 &= 0.\end{aligned}$$

This shows that $\alpha_i \in F$ is the solution of a second degree equation with coefficients in E , which means α_i is quadratic over E . This holds for every $i = 1, 2, \dots, n$. So each time we extend E by an element of F , we extend it with an element of degree 2. We see that

$$\begin{aligned}E(\alpha_1) &= \mathbb{Q}\left(\alpha_1, \alpha_2 + \frac{1}{\alpha_2}, \dots, \alpha_n + \frac{1}{\alpha_n}\right) \\ E(\alpha_1, \alpha_2) &= \mathbb{Q}\left(\alpha_1, \alpha_2, \alpha_3 + \frac{1}{\alpha_3}, \dots, \alpha_n + \frac{1}{\alpha_n}\right) \\ &\vdots \\ E(\alpha_1, \dots, \alpha_n) &= \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n) = F\end{aligned}$$

Each time we extend E by an α_i , as seen this element is quadratic over E , so the degree increases by a factor 2, or it doesn't increase at all since we can not be sure that for example

$$\begin{aligned}E\left(\alpha_1, \dots, \alpha_{i-1}, \alpha_i, \alpha_{i+1} + \frac{1}{\alpha_{i+1}}, \dots, \alpha_n + \frac{1}{\alpha_n}\right) &\neq \\ E\left(\alpha_1, \dots, \alpha_{i-1}, \alpha_{i+1} + \frac{1}{\alpha_{i+1}}, \dots, \alpha_n + \frac{1}{\alpha_n}\right)\end{aligned}$$

(which means that $E(\alpha_1, \dots, \alpha_i) = E(\alpha_1, \dots, \alpha_{i-1})$). Hence we only know that $[F : E] = 2^m$, where $m \leq n$. \square

How many elements there are in $\text{Gal}(F/\mathbb{Q})$ is not that easy to “spot”. As we have seen, not all automorphisms of F which leaves \mathbb{Q} fixed are included in $\text{Gal}(F/\mathbb{Q})$.

So to find out more about the number of elements in F , we try to consider the Galois groups of the x^n -derived polynomial Q_P and $\text{Gal}(F/E)$. Hence, by considering the two other Galois groups in our exact sequence

$$1 \rightarrow \text{Gal}(F/E) \rightarrow \text{Gal}(F/\mathbb{Q}) \rightarrow \text{Gal}(E/\mathbb{Q}) \rightarrow 1,$$

we can find out more about the Galois group of F .

Let us first consider $\text{Gal}(E/\mathbb{Q})$:

$\text{Gal}(E/\mathbb{Q})$ is the group of all automorphisms of E which keeps \mathbb{Q} fixed. As we have seen these are all the automorphisms of E which permutes the roots of Q_P . Since there are n roots, we have generically

$$\text{Gal}(E/\mathbb{Q}) \simeq S_n.$$

So since $|S_n| = n!$, we get

$$|\text{Gal}(E/\mathbb{Q})| = n!$$

Next we consider $\text{Gal}(F/E)$:

This is the group of all automorphisms of F leaving E fixed, meaning that for all i only the automorphisms of F which send α_i either to α_i or $\frac{1}{\alpha_i}$ can be in $\text{Gal}(F/E)$, because if it sends α_i to either α_j or $\frac{1}{\alpha_j}$, $j \neq i$, then it sends $\alpha_i + \frac{1}{\alpha_i}$ to $\alpha_j + \frac{1}{\alpha_j}$, not leaving E fixed.

When the “destination of” α_i by an element $\phi \in \text{Gal}(F/E)$ is decided, so is the destination of $\frac{1}{\alpha_i}$. So there are n different α 's which can be sent to two different values by $\phi \in \text{Gal}(F/E)$. Hence we must have

$$|\text{Gal}(F/E)| = 2^n.$$

This provides us with enough information to say something about how many elements are in $\text{Gal}(F/\mathbb{Q})$. As we have seen, due to Galois theory we know that $\text{Gal}(E/\mathbb{Q})$ is the quotient of $\text{Gal}(F/\mathbb{Q})$ with $\text{Gal}(F/E)$, which means that

$$\begin{aligned} |\text{Gal}(E/\mathbb{Q})| &= |\text{Gal}(F/\mathbb{Q})|/|\text{Gal}(F/E)| \\ \implies |\text{Gal}(F/\mathbb{Q})| &= |\text{Gal}(F/E)| \cdot |\text{Gal}(E/\mathbb{Q})| \\ \implies |\text{Gal}(F/\mathbb{Q})| &= 2^n \cdot n! \end{aligned}$$

Assuming we need to extend \mathbb{Q} with all the n different roots of P (not including the inverse roots because they come “for free”) to have the splitting field of P , we have now used Galois theory and appropriate splitting fields to find a formula for the order of the Galois group of F over \mathbb{Q} . To see how this actually looks for a general polynomial, we include an example.

Example 2.1.2. Let us consider these groups for a palindromic polynomial of degree 4, meaning we let $n = 2$, so $2n = 4$, and

$$P(x) = x^4 + ax^3 + bx^2 + ax + 1.$$

Now suppose $\alpha_1, \frac{1}{\alpha_1}, \alpha_2$ and $\frac{1}{\alpha_2}$ are the roots of P , and that its splitting field is

$$F = \mathbb{Q}(\alpha_1, \alpha_2).$$

We know from our arguments above that if F is a maximal extension, then

$$|\text{Gal}(F/\mathbb{Q})| = 2^n \cdot n! = 2^2 \cdot 2! = 4 \cdot 2 = 8.$$

But what kind of elements are these?

For simplicity, let us rename our roots such that $\{\alpha_1, \frac{1}{\alpha_1}, \alpha_2, \frac{1}{\alpha_2}\} = \{1, 2, 3, 4\}$. We see that if we e.g. send $1 \mapsto 3$ then we must send $2 \mapsto 4$, so for example the permutation $(1, 3, 4, 2) \in S_n$ is not in $\text{Gal}(F/\mathbb{Q})$. We’re left with these elements:

- Order 0: $\{e\}$
- Order 2: $\{(12), (34), (12)(34), (13)(24), (14)(23)\}$
- Order 3: none
- Order 4: $\{(1324), (1423)\}$

This is a non-commutative group, just note that if $h = (34)$ and $k = (13)(24)$, both in $\text{Gal}(F/\mathbb{Q})$, then

$$hk = (34) \cdot (13)(24) = (1423)$$

while

$$kh = (13)(24) \cdot (34) = (1324),$$

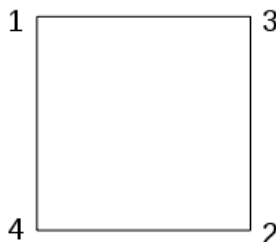
so $hk \neq kh$.

Up to isomorphism there are only two non-commutative groups of order 8, the dihedral group of 8 elements, D_4 , and the quaternion group, Q_8 . It should not be too hard to see that we have

$$\text{Gal}(F/\mathbb{Q}) \simeq D_4,$$

but we include a geometrical explanation:

D_4 , the dihedral group of eight elements, is often associated with the symmetries of the square. If we let our roots $\{1, 2, 3, 4\}$ represent the corners of a square like this,



we can represent each of our automorphism with a symmetry of the square. Let us first consider rotating the square to the right:

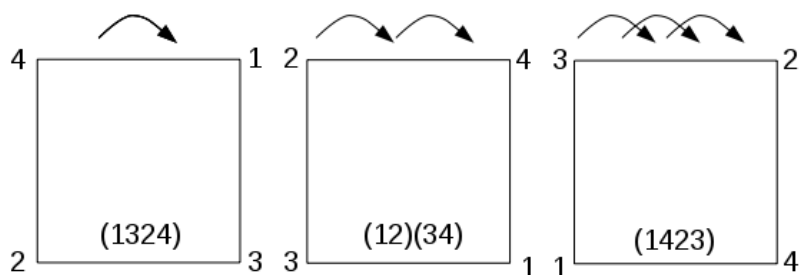


Figure 2.1: Rotating once, twice and three times to the right. The automorphism the rotations corresponds to is written inside the squares.

Next the square can be reflectet around one of the diagonals, and then first reflected and then rotated:

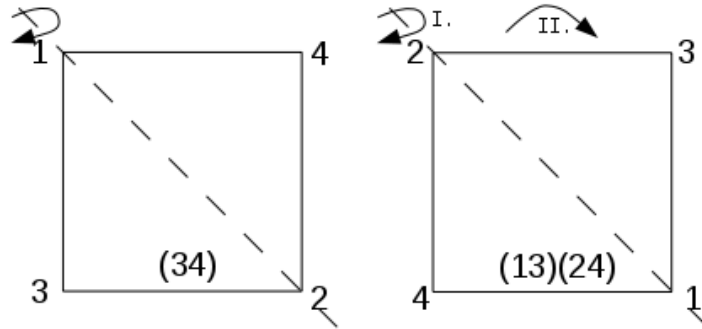
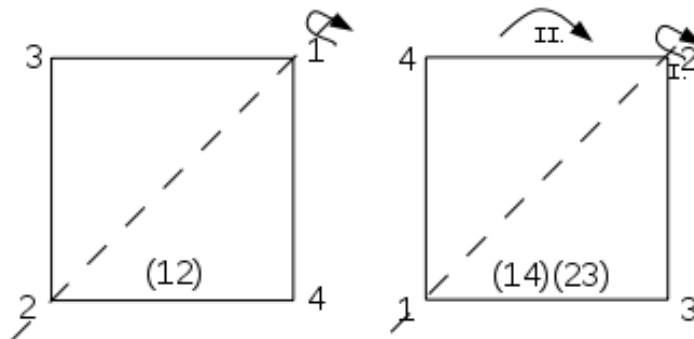
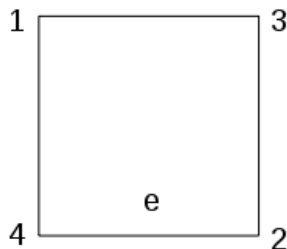


Figure 2.2: Again the permutation corresponding to the symmetry is written inside the squares.

The last two symmetries consist of (the first) reflecting around the other diagonal, then (the second) first reflecting then rotating:



The last automorphism is the identity, simply leaving the edges fixed:



Hopefully this gives, for those who were doubtful, greater consensus that we in fact have

$$\text{Gal}(F/\mathbb{Q}) \simeq D_4.$$

We also want to consider the Galois group of the x^2 -derived polynomial of P , $Q_P(x + \frac{1}{x})$. Let us first compute $Q_P(x + \frac{1}{x})$:

$$\begin{aligned} Q(x) &= \frac{P(x)}{x^2} = x^2 + ax + b + \frac{a}{x} + \frac{1}{x^2} \\ &= \left(x^2 + \frac{1}{x^2}\right) + a\left(x + \frac{1}{x}\right) + b \\ &= \left(x + \frac{1}{x}\right)^2 - 2 + a\left(x + \frac{1}{x}\right) + b \\ \implies Q_P\left(x + \frac{1}{x}\right) &= \left(x + \frac{1}{x}\right)^2 + a\left(x + \frac{1}{x}\right) + (b - 2). \end{aligned}$$

We know that the roots of Q_P are $\alpha_1 + \frac{1}{\alpha_1}$ and $\alpha_2 + \frac{1}{\alpha_2}$, so let us assume² the splitting field of Q_P is

$$E := \mathbb{Q}\left(\alpha_1 + \frac{1}{\alpha_1}, \alpha_2 + \frac{1}{\alpha_2}\right),$$

which we have seen is a splitting field over \mathbb{Q} (in this example it is easy to see that the coefficients of $Q_P(x + \frac{1}{x})$ are in \mathbb{Q}).

²The reason we need to, time and time again, assume something about the splitting fields of these polynomials is because even though there is no relation between α_1 and α_2 (since the splitting field of P is $\mathbb{Q}(\alpha_1, \alpha_2)$), we could have $\mathbb{Q}\left(\alpha_1 + \frac{1}{\alpha_1}, \alpha_2 + \frac{1}{\alpha_2}\right) = \mathbb{Q}\left(\alpha_1 + \frac{1}{\alpha_1}\right)$, and by assuming the splitting field is $\mathbb{Q}\left(\alpha_1 + \frac{1}{\alpha_1}, \alpha_2 + \frac{1}{\alpha_2}\right)$ we avoid this.

Now we can consider both $\text{Gal}(F/E)$ and $\text{Gal}(E/\mathbb{Q})$: $\text{Gal}(E/\mathbb{Q})$ is the group of all automorphisms of E that leaves \mathbb{Q} fixed. This means that the only automorphisms we can have in $\text{Gal}(E/\mathbb{Q})$ are the identity map and the automorphism which sends $\alpha_1 + \frac{1}{\alpha_1}$ to $\alpha_2 + \frac{1}{\alpha_2}$ and vice versa. Hence the order of $\text{Gal}(E/\mathbb{Q})$, $|\text{Gal}(E/\mathbb{Q})|$, is 2, as we have already seen, in the previous theory, that it should be.

$\text{Gal}(F/E)$ is the set of automorphisms of F which leaves E fixed, so this means we can either send α_i to α_i or $\frac{1}{\alpha_i}$ for $i = 1, 2$. This leaves us, as we have already discussed, with $|\text{Gal}(F/E)| = 2^2 = 4$.

We have the exact sequence

$$1 \rightarrow \text{Gal}(F/E) \rightarrow \text{Gal}(F/\mathbb{Q}) \rightarrow \text{Gal}(E/\mathbb{Q}) \rightarrow 1,$$

and as we have seen, this means that $\text{Gal}(F/E)$ is a normal subgroup of $\text{Gal}(F/\mathbb{Q}) \simeq D_4$. If we note that

$$\text{Gal}(F/E) = \{e, (12), (34), (12)(34)\}.$$

it is easy³ to see that we must have

$$\text{Gal}(F/E) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \subseteq D_4.$$

The elements of the Galois group of F is simply a composition of one element from $\text{Gal}(E/\mathbb{Q})$ and one element from $\text{Gal}(F/E)$. Let us look at an example. Let the permutation $(1423) \in \text{Gal}(F/\mathbb{Q})$, which means

$$\alpha_1 \mapsto \frac{1}{\alpha_2} \mapsto \frac{1}{\alpha_1} \mapsto \alpha_2 \mapsto \alpha_1.$$

If we first lift this to $\text{Gal}(E/\mathbb{Q})$ it is equal to sending $\alpha_1 + \frac{1}{\alpha_1}$ to $\alpha_2 + \frac{1}{\alpha_2}$, and since we see no difference in $\alpha_1 + \frac{1}{\alpha_1}$ and $\frac{1}{\alpha_1} + \alpha_1$, this is equal to (1324) , which means

$$\alpha_1 \mapsto \alpha_2 \mapsto \frac{1}{\alpha_1} \mapsto \frac{1}{\alpha_2} \mapsto \alpha_1.$$

On the other hand, in $\text{Gal}(F/E)$, where we need to keep $\alpha_1 + \frac{1}{\alpha_1}$ and $\alpha_2 + \frac{1}{\alpha_2}$ fixed, this equals the map $\alpha_1 \mapsto \frac{1}{\alpha_1}$ and $\alpha_2 \mapsto \frac{1}{\alpha_2}$, i.e. the permutation $(12)(34)$.

³Let one of the \mathbb{Z}_2 's be $\{e, (12)\}$ and the other one $\{e, (34)\}$

Hence the permutation (1423) in $\text{Gal}(F/\mathbb{Q})$ is equal to the product

$$(1423) = (12)(34) \cdot (1324).$$



We can exploit the fact that any palindromic polynomial can be “turned into” a polynomial of half the degree in $x + \frac{1}{x}$ to find formulas for the roots of palindromic polynomials of low degrees. Let’s have a look.

Example 2.1.3. We want to find a formula for calculating the roots of a palindromic polynomial of degree 4.

Assume $P(x) = x^4 + ax^3 + bx^2 + ax + 1$. As we have seen we can find a polynomial $Q_p(x + \frac{1}{x})$ such that if $\alpha + \frac{1}{\alpha}$ is a root of Q_p , then α is a root of P . In the case $P(x) = x^4 + ax^3 + bx^2 + ax + 1$, we find (as we’ve already seen in example 2.1.2)

$$\begin{aligned} Q(x) &= \frac{P(x)}{x^2} = x^2 + ax + b + \frac{a}{x} + \frac{1}{x^2} \\ \implies Q_p\left(x + \frac{1}{x}\right) &= \left(x + \frac{1}{x}\right)^2 - 2 + a\left(x + \frac{1}{x}\right) + b \\ &= \left(x + \frac{1}{x}\right)^2 + a\left(x + \frac{1}{x}\right) + (b - 2) \end{aligned}$$

For simplicity we let $y = x + \frac{1}{x}$, and see that we can solve

$$Q_P(y) = y^2 + ay + (b - 2) = 0 \implies y^2 = -ay - b + 2$$

by using the *abc*-formula:

$$y = \frac{-a \pm \sqrt{a^2 - 4b + 8}}{2}.$$

So

$$x + \frac{1}{x} = y \implies x^2 - yx + 1 = 0$$

and hence

$$\begin{aligned}
 x &= \frac{y \pm \sqrt{y^2 - 4}}{2} \\
 x &= \frac{\frac{-a \pm \sqrt{a^2 - 4b + 8}}{2} \pm \sqrt{\frac{a^2 \mp a\sqrt{a^2 - 4b + 8} - 2b + 4 - 8}{2}}}{2} \\
 x &= -\frac{a}{4} \pm \frac{\sqrt{a^2 - 4b + 8}}{4} \pm \frac{1}{2\sqrt{2}} \sqrt{a^2 \mp \sqrt{a^4 - 4a^2b + 8a^2} - 2b - 4}
 \end{aligned}$$

We have now found a formula for the four roots of $P(x)$. ♣

Remark 2.1.4. As we saw in the last example we have

$$\begin{aligned}
 y &= \frac{-a \pm \sqrt{a^2 - 4b + 8}}{2} \\
 \implies x + \frac{1}{x} &= \frac{-a \pm \sqrt{a^2 - 4b + 8}}{2} \\
 \implies \alpha_1 + \frac{1}{\alpha_1} &= -\frac{a}{2} + \frac{1}{2}\sqrt{a^2 - 4b + 8} \text{ and } \alpha_2 + \frac{1}{\alpha_2} = -\frac{a}{2} - \frac{1}{2}\sqrt{a^2 - 4b + 8}.
 \end{aligned}$$

Chapter 3

Characterization of a polynomial's roots

We are interested in using the roots of polynomials to consider the properties of their Galois groups. But finding roots of polynomials can be both hard and time consuming. Luckily, to find the Galois group of a polynomial we can be satisfied just knowing certain connections between its roots. We both have and can construct tools for finding different kind of connections, which is exactly the aim of this chapter.

3.1 The usual discriminant of polynomials

The discriminant of a polynomial is one tool for giving us some information about the roots of the polynomial.

Definition 3.1.1. If we have a polynomial

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

the discriminant of P is given by

$$\Delta = a_n^{2n-2} \prod_{i < j} (\alpha_i - \alpha_j)^2,$$

where $\alpha_1, \alpha_2, \dots, \alpha_n$ are the n roots of P .

It's not difficult to see that the discriminant of a polynomial is 0 if and only if at least one of the roots has multiplicity more than 1. This, as mentioned, gives us at least some kind of information about the roots. Could it perhaps be useful for us to create other types of discriminants to tell us something different about the relations of some of the roots? We will look into this question a bit later, but let us first have a closer look at our current discriminant.

The formula for the discriminant actually gives us a homogeneous polynomial of degree $2(n - 1)$ in the coefficients of P . Let us have a look at the two easiest examples to illustrate this:

Example 3.1.2. Let $n = 2$, so $P(x) = ax^2 + bx + c$, and assume α_1 and α_2 are its roots. This gives us

$$\begin{aligned}\Delta &= a^{2 \cdot 2 - 2}(\alpha_1 - \alpha_2)^2 \\ &= a^2(\alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2).\end{aligned}$$

Now we also know that

$$\begin{aligned}P(x) &= a(x - \alpha_1)(x - \alpha_2) = ax^2 - a(\alpha_1 + \alpha_2)x + a\alpha_1\alpha_2 \\ \implies b &= -a(\alpha_1 + \alpha_2) \text{ and } c = a\alpha_1\alpha_2 \\ \implies b^2 &= a^2(\alpha_1^2 + 2\alpha_1\alpha_2 + \alpha_2^2).\end{aligned}$$

This means that

$$\Delta = a^2\alpha_1^2 - 2a^2\alpha_1\alpha_2 + a^2\alpha_2^2 = b^2 - 4a^2\alpha_1\alpha_2 = b^2 - 4ac.$$

Note that this is a polynomial of degree $2(n - 1) = 2(2 - 1) = 2$ in the coefficients of P , like stated above. We recognize this expression from the *abc*-formula, as the term under the square root sign. This means that P has two different real roots if $\Delta > 0$, one real root of multiplicity 2 if $\Delta = 0$ and two complex roots if $\Delta < 0$. ♣

Example 3.1.3. Doing similar calculation we find that letting $n = 3$, the discriminant of $P(x) = ax^3 + bx^2 + cx + d$ is

$$\Delta = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

We note that this is a polynomial of degree $2(n-1) = 2(3-1) = 4$ in the coefficients of P . ♣

As seen, the discriminant of a polynomial is 0 if and only if at least one of the roots has multiplicity more than 1. But could we somehow use the discriminant to see if, for example, a polynomial has a root of multiplicity at least three?

Let us first have a look at the easiest case. We let $n = 3$ such that

$$P(x) = x^3 + bx^2 + cx + d$$

and assume $\Delta = 0$. Can we tell, using the coefficients of P if the root α has multiplicity 2 or 3?

Let us assume P only has one root, α , of multiplicity 3. Then we know

$$\begin{aligned} P(x) &= (x - \alpha)^3 = x^3 - 3\alpha x^2 + 3\alpha^2 x - \alpha^3 \\ \implies b &= -3\alpha, \quad c = 3\alpha^2, \quad d = -\alpha^3 \\ \implies b^2 &= 9\alpha^2 = 3c, \quad b^3 = -27\alpha^3 = 27d, \quad c^3 = 27\alpha^6 = 27d \end{aligned}$$

If we now define three *subdiscriminants*,

$$\begin{aligned} \Delta_1 &:= b^2 - 3c \\ \Delta_2 &:= b^3 - 27d \\ \Delta_3 &:= c^3 - 27d, \end{aligned}$$

for P we have

$$\Delta_1 = 0, \quad \Delta_2 = 0, \quad \Delta_3 = 0.$$

We can now rewrite the discriminant using these subdiscriminants (recall that we assume $a = 1$).

$$\begin{aligned} \Delta &= b^2c^2 - 4c^3 - 4b^3d - 27^2d^2 + 18bcd \\ &= c^2(b^2 - 3c) - c^3 - 4b^3d + d(b^3 - 27d) - b^3d + 18bcd \\ &= c^2(b^2 - 3c) - c^3 + d(b^3 - 27d) - 5b^3d - 6bd(b^2 - 3c) + 6b^3d \\ &= (c^2 - 6bd)(b^2 - 3c) + d(b^3 - 27d) + b^3d - c^3 \\ &= (c^2 - 6bd)\Delta_1 + d\Delta_2 + b^3d - c^3 \end{aligned}$$

Recognizing that

$$b^3d - c^3 = d(b^3 - 27d) - (c^3 - 27d^2) = d\Delta_2 - \Delta_3,$$

we have

$$\begin{aligned}\Delta &= (c^2 - 6bd)\Delta_1 + d\Delta_2 + b^3d - c^3 \\ &= (c^2 - 6bd)\Delta_1 + d\Delta_2 + d\Delta_2 - \Delta_3 \\ &= (c^2 - 6bd)\Delta_1 + 2d\Delta_2 - \Delta_3\end{aligned}$$

We have now found a new expression for the discriminant, using the subdiscriminants Δ_1, Δ_2 and Δ_3 . And we know that if and only if all these three are 0, then P has one root of multiplicity 3.

3.2 The palindromic discriminant

To obtain more information about various polynomials we can create different types of discriminants. Let us consider one discriminant which will be zero for all palindromic polynomials.

Definition 3.2.1. We define the *palindromic discriminant*, Δ_p , of a polynomial as

$$\Delta_p = a_n^{2n-n} \prod_{i \neq j} \left(\alpha_i - \frac{1}{\alpha_j} \right).$$

Let us see what this discriminant looks like for a 2nd degree polynomial:

Example 3.2.2. Let $P(x) = ax^2 + bx + c$ have roots α_1 and α_2 . Then

$$\begin{aligned}\Delta_p &= a^2 \left(\alpha_1 - \frac{1}{\alpha_2} \right) \left(\alpha_2 - \frac{1}{\alpha_1} \right) \\ &= a^2 \left(\alpha_1 \alpha_2 - 2 + \frac{1}{\alpha_1 \alpha_2} \right) \\ &= a^2 \left(S_2 - 2 + \frac{1}{S_2} \right) = \frac{a^2}{S_2} (S_2^2 - 2S_2 + 1) \\ &= \frac{a^2}{S_2} (S_2 - 1)^2 = \frac{a^2 (S_2 - 1)^2}{S_2},\end{aligned}$$

where S_2 is the second symmetric elementary polynomial in the two “variables” α_1 and α_2 , i.e. $S_2 = \alpha_1\alpha_2 = \frac{c}{a}$, which means

$$\Delta_p = \frac{a^2\left(\frac{c}{a} - 1\right)^2}{\frac{c}{a}} = \frac{a(c-a)^2}{c}.$$



Clearly Δ_p is zero for all palindromic polynomials, but it’s important to note that there are other polynomials also satisfying this. Recall e.g. the non-palindromic polynomial $P(x) = (x-2)(x-2)\left(x-\frac{1}{2}\right)$, which gives

$$\Delta_p = \left(\frac{1}{2} - \frac{1}{2}\right)\left(\frac{1}{2} - \frac{1}{2}\right)\left(2 - \frac{1}{2}\right) = 0.$$

Remark 3.2.3. We could of course also create different discriminants for detecting other pairwise connections of roots. If we e.g. are looking for connections like $\alpha_i = \frac{a\alpha_j+b}{c\alpha_j+d}$, where $\phi(z) = \frac{az+b}{cz+d}$, we could construct the discriminant

$$\Delta_\phi = a_n^{2n-2} \prod_{i \neq j} \left(\alpha_i - \frac{a\alpha_j + b}{c\alpha_j + d} \right),$$

for detecting this.

3.3 Changing bases

The following may seem misplaced, but we will soon make use of it.

A basis for a vector space, V , of dimension n is a sequence of n vectors (ν_1, \dots, ν_n) such that every vector in V can be uniquely expressed as a linear combination of these vectors. If we express our vector space using another basis, (ν'_1, \dots, ν'_n) , we can always create a transformation which transforms the representation of a vector with respect to the first basis to a representation with respect to the other. A transformation like this is called a change of basis.

Example 3.3.1. We’re not interested in complicated changes of bases. Actually all we need is to understand what a change of basis over \mathbb{Q} is. The easiest is the map

$$\phi(x)_n = x - n \quad n \in \mathbb{Q}.$$

If we e.g. consider the polynomial $P(x) = 2x^2 - 3x + 5$ in $\mathbb{Q}[x]$, we see that

$$\begin{aligned} P(\phi(x)) &= 2(x - n)^2 - 3(x - n) + 5 \\ &= 2(x^2 - 2nx + n^2) - 3x + 3n + 5 \\ &= 2x^2 - (2n + 3)x + (2n^2 + 3n + 5) \end{aligned}$$

which is also a polynomial in $\mathbb{Q}[x]$. ♣

How can we say something more about the Galois group of a polynomial if we don't know what its roots are? As we have seen we may sometimes exploit the properties of the coefficients (if the polynomial is palindromic) and we can use discriminants to identify if at least two of our roots satisfy a given "connection". But we may also say something in general about the Galois group of a polynomial if it can be written as another polynomial just by using a change of basis over \mathbb{Q} . If we know more about the Galois group of the polynomial we can "turn" our original polynomial into, we know more about the Galois group of the original polynomial as well, due to the following lemma:

Lemma 3.3.2. *If $R(x) \in \mathbb{Q}[x]$ is a polynomial of degree n which we can rewrite as the polynomial $P(x) \in \mathbb{Q}[x]$ of degree n , using a change of basis over \mathbb{Q} , then R and P have the same splitting field.*

Proof. Let $\phi(x)$ be a function making a change of basis over \mathbb{Q} , such that we may assume $R(x) = P(\phi(x))$. We know that

$$P(x) = (x - \alpha_1)(x - \alpha_2) \cdot \dots \cdot (x - \alpha_n)$$

where $\alpha_1, \alpha_2, \dots, \alpha_n$ are the n roots of P . If not all, or none, of these are in \mathbb{Q} , the splitting field, F , of P is larger than \mathbb{Q} ;

$$F = \mathbb{Q}(\beta_1, \beta_2, \dots, \beta_r),$$

where the β_i 's are the elements of which we need to extend \mathbb{Q} .
Now we have

$$R(x) = P(\phi(x)) = (\phi(x) - \alpha_1)(\phi(x) - \alpha_2) \cdot \dots \cdot (\phi(x) - \alpha_n)$$

and since ϕ is a change of basis over \mathbb{Q} , we see that the splitting field of R must be the same as the splitting field of P . □

Let us have a look at two simple examples:

Example 3.3.3. Let $P(x) = x^2 + 2x + 5$ and let $\phi_n(x) = x - n$ with $n \in \mathbb{Q}$. If we now denote $R_n(x) = P(\phi_n(x)) = P(x - n)$ we see that

$$\begin{aligned} R_n(x) &= (x - n)^2 + 2(x - n) + 5 \\ &= x^2 + (2 - 2n)x + (n^2 + 5 - 2n), \end{aligned}$$

which gives us:

$$\begin{aligned} R_{-2}(x) &= x^2 + 6x + 13 \\ R_{-1}(x) &= x^2 + 4x + 8 \\ R_0 = P(x) &= x^2 + 2x + 5 \\ R_1(x) &= x^2 + 4 \\ R_2(x) &= x^2 - 2x + 5 \\ R_3(x) &= x^2 - 4x + 8 \\ R_4(x) &= x^2 - 6x + 13. \end{aligned}$$

We can easily find the roots of these polynomials, and if we do, we see that the splitting field in any case is

$$F = \mathbb{Q}(i).$$



Example 3.3.4. Let $P(x) = x^3 - 3x^2 + 12x - 10$ and let again $\phi_n(x) = x - n$ with $n \in \mathbb{Q}$. Then if $R_n(x) = P(\phi_n(x)) = P(x - n)$ we see that


$$\begin{aligned} R_n(x) &= (x - n)^3 - 3(x - n)^2 + 12(x - n) - 10 \\ &= x^3 - 3nx^2 + 3n^2x - n^3 - 3x^2 + 6nx - 3n^2 + 12x - 12n - 10 \\ &= x^3 - (3n + 3)x^2 + (3n^2 + 6n + 12)x - (n^3 + 3n^2 + 12n + 10), \end{aligned}$$

which gives

$$\begin{aligned} R_{-1}(x) &= x^3 - (-3 + 3)x^2 + (3 - 6 + 12)x - (-1 + 3 - 12 + 10) \\ &= x^3 + 9 \\ R_0(x) = P(x) &= x^3 - 3x^2 + 12x - 10 \\ R_1(x) &= x^3 - (3 + 3)x^2 + (3 + 6 + 12)x - (1 + 3 + 12 + 10) \\ &= x^3 - 6x^2 + 21x - 26. \end{aligned}$$

Further calculations give us:

$$\begin{aligned} P(x) &= (x - 1 + 3i)(x - 1 - 3i)(x - 1) \\ R_{-1}(x) &= (x - 3i)(x + 3i) \\ R_1(x) &= (x - 2 + 3i)(x - 2 - 3i)(x - 2) \end{aligned}$$

so all these polynomials have splitting field $F = \mathbb{Q}(i)$, just as in the example above. 

This technique could actually be quite useful if we can use it to “turn” a non-palindromic polynomial in to a palindromic one. This would for example make it a lot easier to compute the Galois group of non-palindromic polynomials of degrees 5, 6, 7, 8 and 9. We include an example showing how this can be useful:

Example 3.3.5. We consider the polynomial

$$P(x) = x^6 + 6x^5 + \frac{27}{2} + 14x^3 + \frac{9}{2}x^2 - 3x - 1.$$

Using the map $\phi(x) = x - 1$ we have

$$\begin{aligned} R(x) &= P(\phi(x)) = (x - 1)^6 + 6(x - 1)^5 + \frac{27}{2}(x - 1)^4 + 14(x - 1)^3 + \\ &\quad \frac{9}{2}(x - 1)^2 - 3(x - 1) - 1 \\ &= x^6 - 6x^5 - 20x^3 + 15x^2 - 6x + 1 + 6x^5 - 30x^4 + 60x^3 - \\ &\quad 60x^2 + 30x - 6 + \frac{27}{2}x^4 - 54x^3 + 81x^2 - 54x + \frac{27}{2} + 14x^3 - \\ &\quad 42x^2 + 42x - 14 + \frac{9}{2}x^2 - 9x + \frac{9}{2} - 3x + 3 - 1 \\ &= x^6 - \frac{3}{2}x^4 - \frac{3}{2}x^2 + 1, \end{aligned}$$

which is a palindromic polynomial. This means we can use the techniques we developed earlier to find the roots of R and hence the splitting field of (both R and) P .

Using the notation of result 1.1.11 we now have

$$a_1 = 0, a_3 = -\frac{3}{2} \text{ and } a_5 = 0,$$

which means

$$\begin{aligned} S_1 &= -a_1 = 0 \\ S_2 &= a_2 - 3 = -\frac{3}{2} - 3 = -\frac{9}{2} \\ S_3 &= 2a_1 - a_3 = 0. \end{aligned}$$

Hence β_1, β_2 and β_3 are the three solutions of the equation

$$\begin{aligned} x^3 - 0x^2 - \frac{9}{2}x - 0 &= 0 \\ \implies x^3 - \frac{9}{2}x &= 0, \end{aligned}$$

which gives us

$$\beta_1 = 0, \beta_2 = \frac{3}{\sqrt{2}} \text{ and } \beta_3 = -\frac{3}{\sqrt{2}}.$$

So solving for the roots α_1, α_2 and α_3 , we find

$$\begin{aligned} \alpha_1^2 - \beta_1\alpha_1 + 1 &= \alpha_1^2 - 0\alpha_1 + 1 = 0 \implies \alpha_1 = i \\ \alpha_2^2 - \beta_2\alpha_2 + 1 &= \alpha_2^2 - \frac{3}{\sqrt{2}}\alpha_2 + 1 = 0 \implies \alpha_2 = \frac{1}{\sqrt{2}} \\ \alpha_3^2 - \beta_3\alpha_3 + 1 &= \alpha_3^2 + \frac{3}{\sqrt{2}}\alpha_3 + 1 = 0 \implies \alpha_3 = -\frac{1}{\sqrt{2}}. \end{aligned}$$

So the roots of R are

$$\alpha_1 = i, \alpha_2 = \frac{1}{\sqrt{2}}, \alpha_3 = -\frac{1}{\sqrt{2}}, \alpha_4 = -i, \alpha_5 = \sqrt{2} \text{ and } \alpha_6 = -\sqrt{2}$$

Writing

$$R(x) = (x - i)(x + i)(x - \sqrt{2})(x - \frac{1}{\sqrt{2}})(x + \sqrt{2})(x + \frac{1}{\sqrt{2}}),$$

doing the same backwards gives us

$$\begin{aligned} P(x) &= R(\phi^{-1}(x)) = ((x + 1) - i)((x + 1) + i)((x + 1) - \sqrt{2})((x + 1) - \frac{1}{\sqrt{2}}) \\ &\quad \left((x + 1) + \sqrt{2} \right) \left((x + 1) + \frac{1}{\sqrt{2}} \right) \\ &= (x - (i - 1))(x - (-i - 1))(x - (\sqrt{2} - 1))(x - (\frac{1}{\sqrt{2}} - 1)) \\ &\quad \left(x - (-\sqrt{2} - 1) \right) \left(x - \left(-\frac{1}{\sqrt{2}} - 1 \right) \right). \end{aligned}$$

Showing that the splitting field of both P and R is $\mathbb{Q}(\sqrt{2}, i)$. And knowing this, we could say more about the Galois groups of these polynomials. ♣

Before we leave the topic of changing bases to find the splitting field of polynomials, the next question could be useful:

Question 3.3.6. Given a monic polynomial of degree two, $P(x) = x^2 + bx + c \in \mathbb{Q}[x]$, with roots α_1 and α_2 , we know that the discriminant of P is

$$\Delta_{P(x)} = (\alpha_1 - \alpha_2)^2.$$

Can we then find a palindromic polynomial of degree 2 with coefficients in \mathbb{Q} and discriminant equal to $\Delta_{P(x)}$?

Let's try to find out what this palindromic polynomial would have to look like. We know that a palindromic polynomial has constant term 1, so we can assume

$$Q(x) = x^2 + b'x + 1,$$

with roots α and $\frac{1}{\alpha}$, so its discriminant is

$$\Delta_{Q(x)} = \left(\alpha - \frac{1}{\alpha}\right)^2.$$

This means that if we have $\Delta_{Q(x)} = \Delta_{P(x)} =: \Delta$, we must have

$$\Delta = \left(\alpha - \frac{1}{\alpha}\right)^2.$$

Let us have a closer look at it:

$$\begin{aligned} \Delta = \left(\alpha - \frac{1}{\alpha}\right)^2 &\implies \Delta = \alpha^2 - 2 + \frac{1}{\alpha^2} \\ &\implies \alpha^4 - (2 + \Delta)\alpha^2 + 1 = 0 \end{aligned}$$

Solving this equation gives us

$$\alpha^2 = \frac{2 + \Delta \pm \sqrt{(-2 - \Delta)^2 - 4}}{2} = \frac{2 + \Delta}{2} \pm \sqrt{\frac{\Delta^2 + 4\Delta}{4}}$$

It's not easy to decide whether or not this gives an α such that we have $(\alpha + \frac{1}{\alpha}) \in \mathbb{Q}$, which is what we need to have for the polynomial

$$Q(x) = (x - \alpha)\left(x - \frac{1}{\alpha}\right) = x^2 - \left(\alpha + \frac{1}{\alpha}\right)x + 1$$

to have coefficients in \mathbb{Q} . It is certainly not trivial to see that this is true for all such α . If we can find one counter example, we're done.

Let us consider the polynomial

$$P(x) = x^2 - 10x + 16 = (x - 8)(x - 2).$$

Then $\Delta_{P(x)} = (8 - 2)^2 = 6^2 = 36$. For a palindromic polynomial to have the same discriminant, we have to have

$$\begin{aligned}\alpha^2 &= \frac{2 + 36}{2} \pm \sqrt{\frac{36^2 + 4 \cdot 36}{4}} \\ &= 19 \pm \frac{\sqrt{1440}}{2} = 19 \pm 6\sqrt{10}.\end{aligned}$$

This means

$$\begin{aligned}\alpha &= \pm\sqrt{19 \pm 6\sqrt{10}} = \pm\sqrt{10 \pm 2 \cdot 3\sqrt{10} + 9} \\ &= \pm\sqrt{(\sqrt{10} \pm 3)^2} = \pm(\sqrt{10} \pm 3).\end{aligned}$$

No matter which of these α 's we choose, we have

$$\alpha + \frac{1}{\alpha} = \pm 2\sqrt{10},$$

which is an irrational number. So we conclude that there is no palindromic polynomial with coefficients in \mathbb{Q} and discriminant $\Delta = 36$.

Hence we can not for every 2nd degree polynomial with coefficients in \mathbb{Q} , find a palindromic polynomial which has coefficients in \mathbb{Q} and the same discriminant.

3.4 The derived polynomials $P^{(2)}$ and P^*

Let us now, before we explore more complicated Galois groups, consider one way of detecting how many inverse pairs of roots a polynomial has.

Let $P(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Q}[x]$ be a monic polynomial of even degree $n = 2m$, with roots $\alpha_1, \alpha_2, \dots, \alpha_n$. Then we have

$$P(x) = \prod_{i=1}^n (x - \alpha_i)$$

where the coefficients of P are the elementary symmetric polynomials, i.e. $a_i = S_{n-i}$. Let

$$P^{(2)}(x) = \prod_{i < j} (x - a_i a_j).$$

Then the coefficients of $P^{(2)}(x)$ are symmetrical polynomials in $\alpha_1, \dots, \alpha_n$ and thereby polynomial functions in the coefficients of $P(x)$.

Example 3.4.1. If $n = 2$, $P^{(2)}(x)$ is a polynomial of degree 1, given by

$$P^{(2)}(x) = x - \alpha_1\alpha_2 = x - a_0.$$

If $n = 4$, $P^{(2)}(x)$ is a polynomial of degree 6, given by

$$P^{(2)}(x) = x^6 - a_2x^5 + (a_1a_3 - a_0)x^4 - (a_1^2 + a_3^2a_0 - 2a_2a_0)x^3 + (a_1a_3 - a_0)a_0x^2 - a_2a_0^2x + a_0^3.$$

For example, calculation of the coefficient of x^4 shows that it's given by

$$\sum_{\{i < j\} < \{k < l\}} \alpha_i\alpha_j\alpha_k\alpha_l,$$

where $\{i < j\} < \{k < l\}$ means $\{i, j\} \neq \{k, l\}$ or $i = k$ and $j < l$. We can split the index set

$$\begin{aligned} \{\{i < j\} < \{k < l\}\} &= \{i < j < k < l\} \cup \{i < k < j < l\} \cup \{i < k < l < j\} \\ &\cup \{i = k < j < l\} \cup \{i < j = k < l\} \cup \{i < k < j = l\}. \end{aligned}$$

Meanwhile

$$a_1a_3 - a_0 = \left(\sum_{i=1}^4 \alpha_i \cdot \sum_{j < k < l} \alpha_j\alpha_k\alpha_l \right) - \alpha_1\alpha_2\alpha_3\alpha_4.$$

Those terms in the product which do not contain four different α_i 's will be indexed by

$$\{i = j < k < l\}, \{j < i = k < l\}, \{j < k < i = l\},$$

while there will be $4 - 3 = 1$ terms of the type $\{i < j < k < l\}$, and the result follows. ♣

For degrees higher than $n = 4$, it may be both hard and time consuming to calculate the polynomial $P^{(2)}(x)$ in terms of the coefficients of P by hand, but using a computer we would (more quickly) be able to find $P^{(2)}(x)$ for polynomials of degree higher than 4 as well.

What use can we then have of this “new” polynomial?

If we assume P has one inverse pair amongst its roots, which we could detect by calculating Δ_p , we must have

$$P^{(2)}(1) = 0.$$

But $P^{(2)}(1) = 0$ means that 1 is a root of $P^{(2)}(x)$, so dividing by $x - 1$ gives a new polynomial. We now check again if 1 is a root in this new polynomial and if it is, there is at least two inverse pairs amongst the roots of P . If we keep on like this, we will eventually end up with

Result 3.4.2.

$$P^{(2)}(x) = (x - 1)^m \cdot P^*(x)$$

where $P^*(x)$ is a polynomial in $\mathbb{Q}[x]$ with $P^*(1) \neq 0$. Then the polynomial we started out with, $P(x)$, has m inverse pairs amongst its roots.

Remark 3.4.3. We note that the result holds because we have $P^{(2)}(1) = 0$ if and only if there is at least one i and $j \in \{1, 2, \dots, n\}$ such that $\alpha_j = \frac{1}{\alpha_i}$. Finding the number m such that $P^{(2)}(x) = (x - 1)^m \cdot P^*(x)$ tells us nothing about whether or not some of these m pairs are equal.

Chapter 4

Semipalindromic polynomials

We have just found a way of calculating how many inverse pairs of roots a given polynomial has. The higher the degree, the more difficult and time consuming the calculations become, and the method only gives us information about how many such pairs there are amongst the roots, it doesn't tell us anything about whether or not any of them are equal to each other or whether or not they are in \mathbb{Q} .

But if we could somehow find a way to know all these properties about the roots of a general polynomial, P in $\mathbb{Q}[x]$ of degree n , what could we then say about its Galois group?

Definition 4.0.4. Let $P(x)$ be a polynomial of degree n in $\mathbb{Q}[x]$, with roots $\alpha_1, \alpha_2, \dots, \alpha_n$. If P has at least one inverse pair of roots, i.e. for at least one i there is one j such that $\alpha_i = \frac{1}{\alpha_j}$, we say that P is a **semipalindromic polynomial of degree n in $\mathbb{Q}[x]$** .

Let $P(x) \in \mathbb{Q}[x]$ be a polynomial of degree n and let F be its splitting field. If we need to expand \mathbb{Q} with all the n roots, $\alpha_1, \alpha_2, \dots, \alpha_n$, the splitting field will be

$$F = \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n).$$

If we don't have any dependencies amongst the roots, then

$$|\text{Gal}(F/\mathbb{Q})| = n!$$

But what happens to the order of the group if some of the roots come in

“inverse pairs”?

4.1 The Galois groups of semipalindromic polynomials

Let $P(x)$ be a semipalindromic polynomial of order n in $\mathbb{Q}[x]$. First assume it has exactly one “inverse pair” amongst its roots, and that the splitting field is $\mathbb{Q}(\alpha_1, \alpha_3, \alpha_4, \dots, \alpha_n)$ (we order the roots such that $\alpha_2 = \frac{1}{\alpha_1}$). Since all the elements of $\text{Gal}(F/\mathbb{Q})$ are automorphisms, if we have an element $\phi \in \text{Gal}(F/\mathbb{Q})$ such that $\phi(\alpha_1) = \alpha_i$ then we must also have $\phi(\alpha_2) = \phi(\frac{1}{\alpha_1}) = \frac{1}{\alpha_i}$. But $\frac{1}{\alpha_i}$ is a root of P if and only if $i = 1$ or 2 . This means that all elements of the Galois group must map α_1 to either α_1 or α_2 . And which of these two, α_1 and α_2 , α_1 is sent to, determines which root α_2 is sent to.

This means we only have two options for which roots the automorphisms of $\text{Gal}(F/\mathbb{Q})$ can send α_1 to; namely α_1 and α_2 . And then α_2 must be sent to the inverse root. Further we have $n - 2$ options for which roots α_3 can be sent to, which leaves $n - 3$ options for α_4 and so on. This means

$$|\text{Gal}(F/\mathbb{Q})| = 2 \cdot 1 \cdot (n-2) \cdot (n-3) \cdot \dots \cdot (n-(n-2)) \cdot (n-(n-1)) = 2 \cdot (n-2)!$$

Realizing the fact that a root which is one part of an “inverse pair” can only be sent to another root which is also a part of such a pair can help us say something more general about the order of the Galois group of semipalindromic polynomials:

Proposition 4.1.1. *Assume $P(x) \in \mathbb{Q}[x]$ is of degree n and that we can detect exactly m inverse pairs amongst its roots. Assume also that if we order the roots as $\alpha_1, \alpha_2 = \frac{1}{\alpha_1}, \alpha_3, \alpha_4 = \frac{1}{\alpha_3}, \dots, \alpha_{2m-1}, \alpha_{2m} = \frac{1}{\alpha_{2m-1}}, \alpha_{2m+1}, \alpha_{2m+2}, \dots, \alpha_n$, the splitting field of $P(x)$ is*

$$F = \mathbb{Q}(\alpha_1, \alpha_3, \dots, \alpha_{2m-1}, \alpha_{2m+1}, \alpha_{2m+2}, \dots, \alpha_n).$$

Then we have

$$|\text{Gal}(F/\mathbb{Q})| = 2^m \cdot m! (n - 2m)!$$

Proof. Since there are $2m$ roots which are one part of an inverse pair of roots, we can send the root α_1 to $2m$ different roots (including itself). Then the “destination” of $\alpha_2 = \frac{1}{\alpha_1}$ is already decided, so we only have one option for the “destination” of this root. Now one pair of inverse roots is “used”, so α_3 can be sent to $2m - 2$ different roots. This leaves $2m - 4$ options for α_5 , and so on. The first root which is not a part of such a pair can then be sent to $n - 2m$ different roots, the next $n - (2m + 1)$ and so on. This gives

$$\begin{aligned} |\text{Gal}(F/\mathbb{Q})| &= 2m(2m - 2)(2m - 4)(2m - 6)\dots(2m - (2m - 2)) \cdot \\ &\quad (n - 2m)(n - (2m + 1))\dots 1 \\ &= 2m \cdot 2(m - 1) \cdot 2(m - 2) \cdot 2(m - 3) \cdot \dots \cdot (n - 2m)! \\ &= \underbrace{2 \cdot 2 \cdot 2 \cdot \dots \cdot 2}_m \cdot m!(n - 2m)! \\ &= 2^m \cdot m!(n - 2m)! \end{aligned}$$

□

Let $P(x)$ be an irreducible polynomial of degree n in $\mathbb{Q}[x]$, with m pairs of inverse roots. Then we know that

$$\begin{aligned} P(x) &= (x - \alpha_1) \left(x - \frac{1}{\alpha_1}\right) (x - \alpha_2) \left(x - \frac{1}{\alpha_2}\right) \dots (x - \alpha_m) \left(x - \frac{1}{\alpha_m}\right) \\ &\quad (x - \alpha_{m+1})(x - \alpha_{m+2}) \dots (x - \alpha_{n-m}), \end{aligned}$$

where $\alpha_1, \frac{1}{\alpha_1}, \alpha_2, \frac{1}{\alpha_2}, \dots, \alpha_m, \frac{1}{\alpha_m}, \alpha_{m+1}, \alpha_{m+2}, \dots, \alpha_{n-m}$ are the n roots of P . This means we can write

$$P(x) = \underbrace{(x^{2m} + a_1x^{2m-1} + a_2x^{2m-2} + \dots + a_2x^2 + a_1x + 1)}_{:=Q(x)} \cdot R_{n-2m}(x),$$

where the first part is a palindromic polynomial, $Q(x)$, of degree $2m$ and the rest is a polynomial of degree $n - 2m$. Note that since P was irreducible in \mathbb{Q} , these polynomials are not (at least not both) in $\mathbb{Q}[x]$.

We want to consider the rational function

$$\begin{aligned}
\overline{P}(x) &= \frac{P(x)}{x^m} = \frac{\overbrace{(x^{2m} + a_1x^{2m-1} + a_2x^{2m-2} + \dots + a_2x^2 + a_1x + 1)}{=Q(x)}}{x^m} \\
&= \frac{R_{n-2m}(x)}{R_{n-2m}(x)} \\
&= \left(x^m + a_1x^{m-1} + a_2x^{m-2} + \dots + \frac{a_2}{x^{m+2}} + \frac{a_1}{x^{m+1}} + \frac{1}{x^m} \right) \cdot R_{n-2m}(x) \\
&= \left(x^m + \frac{1}{x^m} + a_1 \left(x^{m+1} + \frac{1}{x^{m+1}} \right) + a_2 \left(x^{m+2} + \frac{1}{x^{m+2}} \right) + \dots \right. \\
&\quad \left. + a_m \right) \cdot R_{n-2m}(x).
\end{aligned}$$

As we have seen earlier this means that \overline{P} can be written as the product of the x^m -derived polynomial of Q (the palindromic part of P), by abuse of notation we shall call it $Q_P(x + \frac{1}{x})$, of degree m in $x + \frac{1}{x}$ and the polynomial R_{n-2m} in x , i.e.

$$\overline{P}(x, x + \frac{1}{x}) = Q_P(x + \frac{1}{x})R_{n-2m}(x).$$

So the roots of \overline{P} are $\alpha_1 + \frac{1}{\alpha_1}, \alpha_2 + \frac{1}{\alpha_2}, \dots, \alpha_m + \frac{1}{\alpha_m}, \alpha_{m+1}, \dots, \alpha_{n-m}$, which gives \overline{P} the splitting field

$$M = \mathbb{Q}\left(\alpha_1 + \frac{1}{\alpha_1}, \alpha_2 + \frac{1}{\alpha_2}, \dots, \alpha_m + \frac{1}{\alpha_m}, \alpha_{m+1}, \dots, \alpha_{n-m}\right).$$

But as we have seen, the coefficients of \overline{P} are not (at least not all) rational numbers. To have an exact sequence as we have seen earlier we need to detect which field M is a splitting field over.

We start by considering an example:

Example 4.1.2. Let $P(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_4x^2 + a_5x + a_6$ be a polynomial with roots $\alpha_1, \frac{1}{\alpha_1}, \alpha_2, \frac{1}{\alpha_2}, \alpha_3, \alpha_4$ and splitting field $F = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ ($n = 6, m = 2$). We have

$$\begin{aligned}
P(x) &= (x - \alpha_1)\left(x - \frac{1}{\alpha_1}\right)(x - \alpha_2)\left(x - \frac{1}{\alpha_2}\right)(x - \alpha_3)(x - \alpha_4) \\
&= \left(x^4 - \left(\alpha_1 + \frac{1}{\alpha_1} + \alpha_2 + \frac{1}{\alpha_2}\right)x^3 + \left(\alpha_1\alpha_2 + \frac{\alpha_2}{\alpha_1} + \frac{\alpha_1}{\alpha_2} + \frac{1}{\alpha_1\alpha_2} + 2\right)x^2 \right. \\
&\quad \left. - \left(\alpha_1 + \frac{1}{\alpha_1} + \alpha_2 + \frac{1}{\alpha_2}\right)x + 1\right) \cdot (x^2 - (\alpha_3 + \alpha_4)x + \alpha_3\alpha_4)
\end{aligned}$$

so¹

$$\begin{aligned} Q(x) &:= \frac{P(x)}{x^2 \cdot R_2(x)} \\ &= x^2 + \frac{1}{x^2} - \left(\alpha_1 + \frac{1}{\alpha_1} + \alpha_2 + \frac{1}{\alpha_2} \right) \left(x + \frac{1}{x} \right) + \alpha_1 \alpha_2 + \frac{\alpha_1}{\alpha_2} + \frac{\alpha_2}{\alpha_1} + \frac{1}{\alpha_1 \alpha_2} + 2, \end{aligned}$$

where $R_2(x) = x^2 - (\alpha_3 + \alpha_4)x + \alpha_3 \alpha_4$. Recalling that $x^2 + \frac{1}{x^2} = \left(x + \frac{1}{x} \right)^2 - 2$, gives us

$$Q_P \left(x + \frac{1}{x} \right) = \left(x + \frac{1}{x} \right)^2 - \left(\alpha_1 + \frac{1}{\alpha_1} + \alpha_2 + \frac{1}{\alpha_2} \right) \left(x + \frac{1}{x} \right) + \alpha_1 \alpha_2 + \frac{\alpha_1}{\alpha_2} + \frac{\alpha_2}{\alpha_1} + \frac{1}{\alpha_1 \alpha_2}.$$

By proposition 2.0.16, Q_P has roots $\alpha_1 + \frac{1}{\alpha_1}, \alpha_2 + \frac{1}{\alpha_2}$.

We want to consider the “polynomial”

$$P \left(x, x + \frac{1}{x} \right) = x^2 Q_P \left(x + \frac{1}{x} \right) R_2(x),$$

which has roots $x + \frac{1}{x} = \alpha_1 + \frac{1}{\alpha_1}, \alpha_2 + \frac{1}{\alpha_2}$ and $x = \alpha_3, \alpha_4$.

This means the splitting field of $P \left(x, x + \frac{1}{x} \right)$ is $\mathbb{Q} \left(\alpha_1 + \frac{1}{\alpha_1}, \alpha_2 + \frac{1}{\alpha_2}, \alpha_3, \alpha_4 \right)$, but in which field does the coefficients of this polynomial lie?

We know that for all polynomials the coefficients are elementary symmetric polynomials of the roots. So since the coefficients of $R_2(x)$ are $1, \alpha_3 + \alpha_4$ and $\alpha_3 \alpha_4$, we must have $R_2(x) \in \mathbb{Q}(\alpha_3, \alpha_4)$. But are the coefficients of $Q_P \left(x + \frac{1}{x} \right)$ also in $\mathbb{Q}(\alpha_3, \alpha_4)$? It turns out they are! Let’s have a look:

Recalling that we have $P(x) = x^6 + a_1 x^5 + a_2 x^4 + a_3 x^3 + a_4 x^2 + a_5 x + a_6$ with roots $\alpha_1, \frac{1}{\alpha_1}, \alpha_2, \frac{1}{\alpha_2}, \alpha_3, \alpha_4$, we can calculate the first two (excluding the coefficient 1 of x^6) coefficients of P to be

$$\begin{aligned} a_1 &= \alpha_1 + \frac{1}{\alpha_1} + \alpha_2 + \frac{1}{\alpha_2} + \alpha_3 + \alpha_4 \\ a_2 &= 2 + \alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_1 \alpha_4 + \alpha_2 \alpha_3 + \alpha_2 \alpha_4 + \alpha_3 \alpha_4 + \\ &\quad \frac{\alpha_2}{\alpha_1} + \frac{\alpha_3}{\alpha_1} + \frac{\alpha_4}{\alpha_1} + \frac{\alpha_1}{\alpha_2} + \frac{\alpha_3}{\alpha_2} + \frac{\alpha_4}{\alpha_2} + \frac{1}{\alpha_1 \alpha_2}. \end{aligned}$$

And as we have already seen the coefficient of $\left(x + \frac{1}{x} \right)$ and the constant term of $Q_P \left(x + \frac{1}{x} \right)$ are (note that the coefficient of $\left(x + \frac{1}{x} \right)^2$ is 1):

$$\begin{aligned} b &:= - \left(\alpha_1 + \frac{1}{\alpha_1} + \alpha_2 + \frac{1}{\alpha_2} \right) \\ \text{and } c &:= \alpha_1 \alpha_2 + \frac{\alpha_2}{\alpha_1} + \frac{\alpha_1}{\alpha_2} + \frac{1}{\alpha_1 \alpha_2} - 2. \end{aligned}$$

¹Note that the new expression for P shows that $\alpha_3 \alpha_4 \in \mathbb{Q}$.

We want to show that both b and c are in $\mathbb{Q}(\alpha_3, \alpha_4)$.

As we saw

$$\begin{aligned} a_1 &= \alpha_1 + \frac{1}{\alpha_1} + \alpha_2 + \frac{1}{\alpha_2} + \alpha_3 + \alpha_4, \\ a_2 &= 2 + \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 + \\ &\quad \frac{\alpha_2}{\alpha_1} + \frac{\alpha_3}{\alpha_1} + \frac{\alpha_4}{\alpha_1} + \frac{\alpha_1}{\alpha_2} + \frac{\alpha_3}{\alpha_2} + \frac{\alpha_4}{\alpha_2} + \frac{1}{\alpha_1\alpha_2}, \end{aligned}$$

which means these expressions are both in \mathbb{Q} . Hence

$$\begin{aligned} a_1 &= b + \alpha_3 + \alpha_4 \\ \implies b &= a_1 - \alpha_3 - \alpha_4 \in \mathbb{Q}(\alpha_3, \alpha_4) \\ a_2 &= c + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2 + \alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 + \frac{\alpha_3}{\alpha_1} + \frac{\alpha_4}{\alpha_1} + \frac{\alpha_3}{\alpha_2} + \frac{\alpha_4}{\alpha_2} + 4 \\ \implies c &= a_2 - 4 - \alpha_3\alpha_4 - \left(\alpha_1 + \alpha_2 + \frac{1}{\alpha_1} + \frac{1}{\alpha_2}\right)\alpha_4 - \left(\alpha_1 + \alpha_2 + \frac{1}{\alpha_1} + \frac{1}{\alpha_2}\right)\alpha_3 \\ &= a_2 - 4 - \alpha_3\alpha_4 - (a_1 - \alpha_3 - \alpha_4)(\alpha_3 + \alpha_4) \\ &= a_2 - 4 - \alpha_3\alpha_4 - a_1\alpha_3 - a_1\alpha_4 + \alpha_3\alpha_4 + \alpha_3^2 + \alpha_3\alpha_4 + \alpha_3\alpha_4 + \alpha_4^2 \\ &= \underbrace{a_2 - 4 - \alpha_3\alpha_4 + 2\alpha_3\alpha_4}_{\in \mathbb{Q}} - \underbrace{a_1\alpha_3}_{\in \mathbb{Q}(\alpha_3, \alpha_4)} - \underbrace{a_1\alpha_4}_{\in \mathbb{Q}(\alpha_3, \alpha_4)} + \underbrace{\alpha_3^2}_{\in \mathbb{Q}(\alpha_3, \alpha_4)} + \underbrace{\alpha_4^2}_{\in \mathbb{Q}(\alpha_3, \alpha_4)} \\ \implies c &\in \mathbb{Q}(\alpha_3, \alpha_4) \end{aligned}$$

This result shows that $P(x, x + \frac{1}{x})$ has coefficients in $\mathbb{Q}(\alpha_3, \alpha_4)$, which means $M := \mathbb{Q}\left(\alpha_1 + \frac{1}{\alpha_1}, \alpha_2 + \frac{1}{\alpha_2}, \alpha_3, \alpha_4\right)$ is a splitting field over $L := \mathbb{Q}(\alpha_3, \alpha_4)$. Then we know that M is a finite normal extension of L , and using Galois theory again, this means $\text{Gal}(F/M)$ is a normal subgroup of $\text{Gal}(F/L)$, and then

$$\text{Gal}(M/L) \simeq \text{Gal}(F/L)/\text{Gal}(F/M),$$

which gives us an exact sequence

$$1 \rightarrow \text{Gal}(F/M) \rightarrow \text{Gal}(F/L) \rightarrow \text{Gal}(M/L) \rightarrow 1.$$



Lemma 4.1.3. *Let $P(x)$ be an irreducible, monic polynomial of degree n in $\mathbb{Q}[x]$. Assume we can factor P as*

$$P(x) = F(x) \cdot G(x)$$

with $G(x) \in E[x]$ where E is a field $E \supseteq \mathbb{Q}$. Then we also have $F(x) \in E[x]$.

Proof. Assume $P(x) = \sum_{i=0}^n a_i x^i$, $F(x) = \sum_{i=0}^r b_i x^i$ and $G(x) = \sum_{i=0}^s c_i x^i$, where $r + s = n$ and $a_n = b_r = c_s = 1$ (we could of course have $b_r = c_s^{-1}$, but this doesn't change anything later). If we let m be a rational number, the element $P(m) = F(m) \cdot G(m)$ is also a rational number. Further, $G(m)$ is an element of $E \supseteq \mathbb{Q}$, which means that also $F(m) = \frac{P(m)}{G(m)}$ is in E . We want to show that for every $i \in \{1, \dots, r\}$, $b_i \in E$ and we do it by induction. We note first that

$$\begin{aligned} F(x) \cdot G(x) &= (x^r + b_{r-1}x^{r-1} + \dots + b_1x + b_0)(x^s + c_{s-1}x^{s-1} + \dots + c_1x + c_0) \\ &= x^{r+s} + (b_{r-1} + c_{s-1})x^{r+s-1} + \dots + b_0c_0 \\ &= x^n + a_{n-1}x^{n-1} + \dots + a_0 = P(x). \end{aligned} \tag{4.1.1}$$

From this we find

$$a_{k+1} = \sum_{i=0}^{k+1} b_i \cdot c_{k+1-i}.$$

We are now ready to start our induction, wanting to show that for every $k \in \{0, 1, \dots, r\}$, b_k is in E .

Consider the case $k = 0$. We know from equation (4.1.1) that $b_0c_0 \in \mathbb{Q}$, say $b_0c_0 = t$. Since E is a field, we have $c_0^{-1} \in E$, and hence $b_0 = t \cdot c_0^{-1}$ is in E as well.

Now assume that the claim that $b_0, b_1, b_2, \dots, b_k$ are in E holds. Then we need to show that also b_{k+1} is in E . But as we saw

$$\begin{aligned} a_{k+1} &= \sum_{i=0}^{k+1} b_i \cdot c_{k+1-i} = \sum_{i=0}^k b_i \cdot c_{k+1-i} + b_{k+1} \cdot c_0 \\ \implies b_{k+1} &= \underbrace{a_{k+1}}_{\in \mathbb{Q} \implies \in E} - \underbrace{\sum_{i=0}^k b_i \cdot c_{k+1-i}}_{\in E} \\ \implies b_{k+1} &\in E, \end{aligned}$$

where $\sum_{i=0}^k b_i \cdot c_{k+1-i}$ is in E because we assumed $b_0, b_1, b_2, \dots, b_k$ are in E and already know that all c_i are in E . \square

Proposition 4.1.4. *Both polynomials $Q_P(x + \frac{1}{x})$ and $R_{n-2m}(x)$ have coefficients in $\mathbb{Q}(\alpha_{m+1}, \alpha_{m+2}, \dots, \alpha_{n-m})$, which means the field*

$$M = \mathbb{Q}\left(\alpha_1 + \frac{1}{\alpha_1}, \alpha_2 + \frac{1}{\alpha_2}, \dots, \alpha_m + \frac{1}{\alpha_m}, \alpha_{m+1}, \dots, \alpha_{n-m}\right)$$

is a splitting field over $\mathbb{Q}(\alpha_{m+1}, \alpha_{m+2}, \dots, \alpha_{n-m})$.

Proof. This follows almost immediately from the lemma above.

To make notation easier we rename the roots of P as

$$\alpha_1, \alpha_2 = \frac{1}{\alpha_1}, \alpha_3, \alpha_4 = \frac{1}{\alpha_3}, \dots, \alpha_{2m-1}, \alpha_{2m} = \frac{1}{\alpha_{2m-1}}, \alpha_{2m+1}, \alpha_{2m+2}, \dots, \alpha_n.$$

Recalling that the coefficients of all polynomials are symmetric polynomials in its roots, since the roots of R_{n-2m} are $\alpha_{2m+1}, \dots, \alpha_n$, $R_{n-2m}(x) \in \mathbb{Q}(\alpha_{2m+1}, \dots, \alpha_n)[x] \supseteq \mathbb{Q}$.

Now, constructing the x^m -derived polynomial $Q_P(x + \frac{1}{x})$, we first split P into two polynomials, the palindromic part, $Q(x)$, and the “rest polynomial”, $R_{n-2m}(x)$, see page 67. It follows from lemma 4.1.3 that the coefficients of $Q(x)$ are also in $\mathbb{Q}(\alpha_{2m+1}, \dots, \alpha_n)[x]$. Further we know that when dividing $Q(x)$ by x^m and “turning it into” $Q_P(x + \frac{1}{x})$ we do not change the coefficients other than possibly by elements of \mathbb{Q} . This means that $Q_P(x + \frac{1}{x}) \in \mathbb{Q}(\alpha_{2m+1}, \dots, \alpha_n)[x + \frac{1}{x}]$. Which means that the field M is a splitting field over $\mathbb{Q}(\alpha_{m+1}, \alpha_{m+2}, \dots, \alpha_{n-m})$. □

The results above may at first eyesight seem a bit weird. Let us compare² the first two coefficients (not including the ones of the highest terms, since they're 1) of the polynomials $Q_P(x + \frac{1}{x})$ and $P(x)$, which have roots $\alpha_1 + \alpha_2, \alpha_3 + \alpha_4, \dots, \alpha_{2m-1} + \alpha_{2m}$ and $\alpha_1, \alpha_2, \dots, \alpha_n$ respectively, to see how it can actually be true that we have $Q_P(x + \frac{1}{x}) \in \mathbb{Q}(\alpha_{2m+1}, \dots, \alpha_n)[x + \frac{1}{x}]$. Computing the coefficients of $P(x)$ using elementary symmetric polynomials

²using the notation from proposition 4.1.4

in its roots, we have:

$$\begin{aligned}
 a_1 &= \sum_{1 \leq i \leq n} \alpha_i = \alpha_1 + \alpha_2 + \dots + \alpha_n \\
 a_2 &= \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j = \alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \dots + \alpha_1 \alpha_n + \alpha_2 \alpha_3 + \dots + \alpha_2 \alpha_n + \alpha_3 \alpha_4 + \dots \\
 &\quad + \alpha_3 \alpha_n + \alpha_4 \alpha_5 + \dots + \alpha_4 \alpha_n + \alpha_5 \alpha_n + \alpha_5 \alpha_3 + \dots + \alpha_6 \alpha_n \\
 &\quad + \alpha_6 \alpha_4 + \dots + \alpha_6 \alpha_n + \dots + \alpha_i \alpha_{i+1} + \dots + \alpha_i \alpha_n + \dots \\
 &\quad + \alpha_{n-2} \alpha_{n-1} + \alpha_{n-2} \alpha_n + \alpha_{n-1} \alpha_n \\
 a_3 &= \sum_{1 \leq i < j < k \leq n} \alpha_i \alpha_j \alpha_k \\
 &\quad \vdots \\
 a_n &= \alpha_1 \alpha_2 \cdots \alpha_n
 \end{aligned}$$

Since the roots of $Q_P(x + \frac{1}{x})$ are $\beta_1 = \alpha_1 + \alpha_2, \beta_2 = \alpha_3 + \alpha_4, \dots, \beta_m = \alpha_{2m-1} + \alpha_{2m}$, denoting its coefficients b_i for $i = 1, \dots, m$, the first coefficient is given by

$$\begin{aligned}
 b_1 &= \sum_{1 \leq i \leq m} \beta_i = \sum_{1 \leq i \leq 2m} \alpha_i = \underbrace{a_1}_{\in \mathbb{Q}} - \underbrace{\sum_{2m+1 \leq i \leq n} \alpha_i}_{\in \mathbb{Q}(\alpha_{2m+1}, \alpha_{2m+2}, \dots, \alpha_n)} \\
 \implies b_1 &\in \mathbb{Q}(\alpha_{2m+1}, \alpha_{2m+2}, \dots, \alpha_n)
 \end{aligned}$$

And for the second

$$\begin{aligned}
b_2 &= \sum_{1+\leq i < j \leq 2m} \beta_i \beta_j = \sum_{\substack{1+\leq i < j \leq 2m \\ i, j \text{ odd}}} (\alpha_i + \alpha_{i+1})(\alpha_j + \alpha_{j+1}) \\
&= a_2 - \underbrace{\alpha_1 \alpha_2}_{=1} - \alpha_1(\alpha_{2m+1} + \alpha_{2m+2} + \dots + \alpha_n) - \\
&\quad \alpha_2(\alpha_{2m+1} + \alpha_{2m+2} + \dots + \alpha_n) - \underbrace{\alpha_3 \alpha_4}_{=1} \\
&\quad - \alpha_3(\alpha_{2m+1} + \alpha_{2m+2} + \dots + \alpha_n) - \\
&\quad \alpha_4(\alpha_{2m+1} + \alpha_{2m+2} + \dots + \alpha_n) - \dots - \underbrace{\sum_{2m+1 \leq i < j \leq n} \alpha_i \alpha_j}_{\in \mathbb{Q}(\alpha_{2m+1}, \dots, \alpha_n)} \\
&= \underbrace{a_2 - m}_{\in \mathbb{Q}} - \underbrace{a_1}_{\in \mathbb{Q}} \underbrace{(\alpha_{2m+1} + \alpha_{2m+2} + \dots + \alpha_n)}_{\in \mathbb{Q}(\alpha_{2m+1}, \dots, \alpha_n)} + \underbrace{\sum_{2m+1 \leq i \leq n} \alpha_i^2}_{\in \mathbb{Q}(\alpha_{2m+1}, \dots, \alpha_n)} + \\
&\quad \underbrace{\sum_{2m+1 \leq i < j \leq n} \alpha_i \alpha_j}_{\in \mathbb{Q}(\alpha_{2m+1}, \dots, \alpha_n)} \\
&\implies b_2 \in \mathbb{Q}(\alpha_{2m+1}, \dots, \alpha_n).
\end{aligned}$$

Proposition 4.1.4 has great interest for us as we are going to consider the Galois group of P . It shows that the field³

$$M = \mathbb{Q}\left(\alpha_1 + \frac{1}{\alpha_1}, \dots, \alpha_m + \frac{1}{\alpha_m}, \alpha_{m+1}, \dots, \alpha_{n-m}\right),$$

which is not (necessarily) a splitting field over \mathbb{Q} , actually is a splitting field over the field $L = \mathbb{Q}(\alpha_{m+1}, \dots, \alpha_{n-m})$. And since F is a splitting field over \mathbb{Q} , it is also a splitting field over M , which according to Galois theory gives us the exact sequence

$$1 \rightarrow \text{Gal}(F/M) \rightarrow \text{Gal}(F/L) \rightarrow \text{Gal}(M/L) \rightarrow 1.$$

Let us consider what these groups look like and their orders:

³We're back to our "usual" notation

$\text{Gal}(F/M)$ is the group of all automorphisms of F which leaves $\alpha_1 + \frac{1}{\alpha_1}, \dots, \alpha_m + \frac{1}{\alpha_m}, \alpha_{m+1}, \dots, \alpha_{n-m}$ fixed. This means an element $\phi \in \text{Gal}(F/M)$ must send α_i to either α_i or $\frac{1}{\alpha_i}$ for the first m i 's, and then keep the rest of the roots fixed. Counting our options this leaves us with

$$|\text{Gal}(F/M)| = 2^m.$$

Next we look at $\text{Gal}(F/L)$. These automorphisms need to keep all the roots $\alpha_{m+1}, \dots, \alpha_{n-m}$ fixed, but can, for $i = 1, \dots, m$, send α_i to all α_j or $\frac{1}{\alpha_j}$ for $j = 1, \dots, m$ (also $j = i$). This gives $2m$ options for where to send α_1 , and then $2m - 2$ options for where to send α_2 (remember it can't be sent to neither the same root as α_1 or that root's inverse). This leaves $2m - 4$ options for the image of α_3 , and so on, up to and including $i = m$. This gives us

$$\begin{aligned} |\text{Gal}(F/L)| &= \underbrace{2m \cdot (2m - 2) \cdot (2m - 4) \cdots 2}_{m \text{ factors of } 2} \\ &= 2^m \cdot m(m - 1)(m - 2) \cdots 1 \\ &= 2^m \cdot m! \end{aligned}$$

Since we have our exact sequence, we can now calculate the order of $\text{Gal}(M/L)$ to be

$$|\text{Gal}(M/L)| = |\text{Gal}(F/L)| / |\text{Gal}(F/M)| = 2^m \cdot m! / 2^m = m!,$$

but let us also check this by “counting” the automorphisms.

$\text{Gal}(M/L)$ is the group of all automorphisms of F which permutes $\alpha_i + \frac{1}{\alpha_i}$'s for $i = 1, 2, \dots, m$, but leaves the $n - 2m$ other roots of P fixed. This means an element $\phi \in \text{Gal}(M/L)$ can send $\alpha_1 + \frac{1}{\alpha_1}$ to $\alpha_i + \frac{1}{\alpha_i}$ for m different i 's ($1, 2, \dots, m$). This leaves $m - 1$ options for $\phi\left(\alpha_2 + \frac{1}{\alpha_2}\right)$, $m - 2$ options for $\phi\left(\alpha_3 + \frac{1}{\alpha_3}\right)$, and so on, until there is only one option for $\phi\left(\alpha_m + \frac{1}{\alpha_m}\right)$. The rest of the roots, the ones not part of an inverse pair, must be kept fixed, which leaves us with

$$|\text{Gal}(M/L)| = m \cdot (m - 1) \cdots (m - 2) \cdots 2 \cdot 1 \cdot \underbrace{1 \cdots 1}_m = m!,$$

which is the same as we just saw.

Finally, let us consider an example, which turns out to be quite special, using the theory just developed.

Example 4.1.5. Let $P(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_4x^2 + a_5x + a_6$ with roots $\alpha_1, \frac{1}{\alpha_1}, \alpha_2, \frac{1}{\alpha_2}, \alpha_3, \alpha_4$ be as in example 4.1.2, where we saw that $Q_P(x + \frac{1}{x})$ had coefficients in $\mathbb{Q}(\alpha_3, \alpha_4)$. Hence $M := \mathbb{Q}\left(\alpha_1 + \frac{1}{\alpha_1}, \alpha_2 + \frac{1}{\alpha_2}, \alpha_3, \alpha_4\right)$ is a splitting field over $L = \mathbb{Q}(\alpha_3, \alpha_4)$.

Then we have

$$\begin{aligned} P(x) &= (x - \alpha_1)\left(x - \frac{1}{\alpha_1}\right)(x - \alpha_2)\left(x - \frac{1}{\alpha_2}\right)(x - \alpha_3)(x - \alpha_4) \\ &= \left(x^2 - \left(\alpha_1 + \frac{1}{\alpha_1}\right)x + 1\right)\left(x^2 - \left(\alpha_2 + \frac{1}{\alpha_2}\right)x + 1\right) \\ &\quad \left(x^2 - (\alpha_3 + \alpha_4)x + \alpha_3\alpha_4\right). \end{aligned}$$

If we assume that the polynomial $P(x)$ is not palindromic, we must have $\alpha_3\alpha_4 = a_6 \neq 1 \in \mathbb{Q}$, because if $\alpha_3\alpha_4 = 1$ then $\alpha_3 = \frac{1}{\alpha_4}$ and then all roots of P are inverse pairs, so P would be palindromic. If we now define

$$\beta_1 := \alpha_1 + \frac{1}{\alpha_1}, \quad \beta_2 := \alpha_2 + \frac{1}{\alpha_2}, \quad \gamma := \alpha_3 + \alpha_4$$

and note that $a_6 = \alpha_3\alpha_4$,

we have

$$\begin{aligned} P(x) &= (x^2 - \beta_1x + 1)(x^2 - \beta_2x + 1)(x^2 - \gamma x + \alpha_3\alpha_4) \\ &= x^6 - (\beta_1 + \beta_2 + \alpha_3 + \alpha_4)x^5 + (a_6 + 2 + \beta_1 + \beta_2a_6 + (\beta_1 + \beta_2)\gamma)x^4 \\ &\quad - (\beta_1\beta_2\gamma + (\beta_1 + \beta_2)a_6 + 2\gamma)x^3 + (2a_6 + 1 + \beta_1\beta_2a_6 + (\beta_1 + \beta_2)\gamma)x^2 \\ &\quad - ((\beta_1 + \beta_2)a_6 + \gamma)x + a_6, \end{aligned}$$

which means

$$\begin{aligned} a_1 &= -(\beta_1 + \beta_2 + \gamma), & a_2 &= 2 + a_6(1 + \beta_1\beta_2) + (\beta_1 + \beta_2)\gamma, \\ a_3 &= -(2 + \beta_1\beta_2)\gamma - (\beta_1 + \beta_2)a_6, & a_4 &= 1 + a_6(2 + \beta_1\beta_2) + (\beta_1 + \beta_2)\gamma, \\ a_5 &= a_6(\beta_1 + \beta_2) + \gamma. \end{aligned}$$

We know from our assumption that $a_6 \neq 1$ and that all the a_i 's are in \mathbb{Q} , which means

$$\begin{aligned} -a_5 + a_1a_6 &= a_6(\beta_1 + \beta_2) + \gamma - a_6(\beta_1 + \beta_2) - a_6\gamma \\ \implies -a_5 + a_1a_6 &= (1 - a_6)\gamma \\ \implies \gamma &= \frac{-a_5 + a_1a_6}{1 - a_6} \in \mathbb{Q}. \end{aligned}$$

And since $a_6 = \alpha_3\alpha_4$ is rational as well, we must have

$$R(x) := x^2 + \gamma x + a_6 \in \mathbb{Q}[x],$$

which again means that $\mathbb{Q}(\alpha_3, \alpha_4) = \mathbb{Q}(\alpha_3)^4$ is a splitting field over \mathbb{Q} , so the relation:

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha_3) \subseteq F = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4),$$

gives rise to the exact sequence

$$1 \rightarrow \text{Gal}(F/\mathbb{Q}(\alpha_3)) \rightarrow \text{Gal}(F/\mathbb{Q}) \rightarrow \text{Gal}(\mathbb{Q}(\alpha_3)/\mathbb{Q}) \rightarrow 1.$$

Let's see what the field $\text{Gal}(\mathbb{Q}(\alpha_3)/\mathbb{Q})$ looks like. This is the group of automorphisms permuting the roots α_3 and α_4 , but keeping \mathbb{Q} fixed. The only possible automorphisms are then the identity map, and the map ϕ , sending α_3 to α_4 , and vice versa, which shows that $\text{Gal}(\mathbb{Q}(\alpha_3)/\mathbb{Q}) \simeq \mathbb{Z}_2$.

Further we note that

$$\begin{aligned} \beta_1 + \beta_2 &= -a_1 - \gamma \implies \beta_1 + \beta_2 \in \mathbb{Q} \\ \text{and } (2 + \beta_1\beta_2)\gamma &= -a_3 - (\beta_1 + \beta_2)a_6 = -a_3 + (a_1 + \gamma)a_6 \\ \implies \beta_1\beta_2 &= \frac{-a_3 + (a_1 + \gamma)a_6}{\gamma} - 2 \implies \beta_1\beta_2 \in \mathbb{Q}, \end{aligned}$$

which shows that also

$$\begin{aligned} Q(x) &:= (x^2 - \beta_1x + 1)(x^2 - \beta_2x + 1) \\ &= x^4 - (\beta_1 + \beta_2)x^3 + (2 + \beta_1\beta_2)x^2 - (\beta_1 + \beta_2)x + 1 \end{aligned}$$

is an irreducible⁵ polynomial in $\mathbb{Q}[x]$.

⁴because $\alpha_3 + \alpha_4 \in \mathbb{Q}$

⁵recall that we assumed neither root of P was in \mathbb{Q}

We see that taking in account our assumptions about the roots and coefficients of $P(x)$, it must be a reducible polynomial in $\mathbb{Q}[x]$. But this means that also $\mathbb{Q}(\beta_1, \beta_2) = \mathbb{Q}(\beta_1)$ and that this is actually also a splitting field over \mathbb{Q} . Hence we have an exact sequence

$$1 \rightarrow \text{Gal}(F/\mathbb{Q}(\beta_1)) \rightarrow \text{Gal}(F/\mathbb{Q}) \rightarrow \text{Gal}(\mathbb{Q}(\beta_1)/\mathbb{Q}) \rightarrow 1.$$

And for the same reasons as for $\text{Gal}(\mathbb{Q}(\alpha_3)/\mathbb{Q})$ we have $\text{Gal}(\mathbb{Q}(\beta_1)/\mathbb{Q}) \simeq \mathbb{Z}_2$.

We now claim that:

Claim 4.1.6. $\text{Gal}(F/\mathbb{Q}(\beta_1)) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. This claim is not hard to prove. We first note that this is the set of all automorphisms which permutes the roots of P , $\alpha_1, \frac{1}{\alpha_1}, \alpha_2, \frac{1}{\alpha_2}, \alpha_3, \alpha_4$, but keeps $\alpha_1 + \frac{1}{\alpha_1}$ and $\alpha_2 + \frac{1}{\alpha_2}$ fixed. This means we can only send α_1 to itself or its inverse. The same holds for α_2 . This means α_3 can only be sent to itself or α_4 , which determines the image of α_4 leaving only the option of the root α_3 is not sent to (either α_3 or α_4). This means

$$|\text{Gal}(F/\mathbb{Q}(\beta_1))| = 2 \cdot 2 \cdot 2 \cdot 1 = 8,$$

which is the same as $|\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2|$.

If we rename our roots again, just like we did in example 2.1.2, as $\{\alpha_1, \frac{1}{\alpha_1}, \alpha_2, \frac{1}{\alpha_2}, \alpha_3, \alpha_4\} = \{1, 2, 3, 4, 5, 6\}$, and let

$$\mathbb{Z}_2^{(1)} = \{e, (12)\}, \quad \mathbb{Z}_2^{(2)} = \{e, (34)\}, \quad \mathbb{Z}_2^{(3)} = \{e, (56)\}$$

we have

$$\begin{aligned} \mathbb{Z}_2^{(1)} \times \mathbb{Z}_2^{(2)} \times \mathbb{Z}_2^{(3)} &= \{(e, e, e), (e, e, (56)), (e, (34), e), (e, (34), (56)), \\ &\quad ((12), e, e), ((12), (34), e), ((12), e, (56)), ((12), (34), (56))\} \\ &\simeq \text{Gal}(F/\mathbb{Q}(\beta_1)). \end{aligned}$$

□

So we have $\text{Gal}(F/\mathbb{Q}(\beta_1)) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Our last claim is:

Claim 4.1.7. $\text{Gal}(F/\mathbb{Q}) \simeq D_4 \times \mathbb{Z}_2$.

Proof. We let the \mathbb{Z}_2 be the set $\{e, (56)\}$. We know that when permuting the roots of P while keeping \mathbb{Q} fixed, we can not send α_3 and α_4 to any other roots than each other or themselves.

So we're basically left with $\text{Gal}(\mathbb{Q}(\alpha_1, \alpha_2)/\mathbb{Q})$ which by example 2.1.2 is isomorphic to D_4 . \square

After detecting which groups our Galois groups are isomorphic to, we can now rewrite the exact sequence as

$$1 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow D_4 \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_2 \rightarrow 1.$$

To illustrate the elements of $\text{Gal}(F/\mathbb{Q})$ we list them according to order:

- Order 0: $\{e\}$
- Order 2: $\{(12), (34), (56), (12)(34), (12)(34)(56), (13)(24), (13)(24)(56), (14)(23), (14)(23)(56), (12)(56), (34)(56)\}$
- Order 4: $\{(1423), (1423)(56), (1324), (1324)(56)\}$

If we consider these elements a bit further, we find that

$$\text{Gal}(F/\mathbb{Q}) = \langle a, x, y \mid a = (1324), x = (12), y = (56) \rangle,$$

which is just another way of showing that $\text{Gal}(F/\mathbb{Q}) \approx D_4 \times \mathbb{Z}_2$. To illustrate the structure of the group we also include a figure of the cycle graph of $D_4 \times \mathbb{Z}_2$:

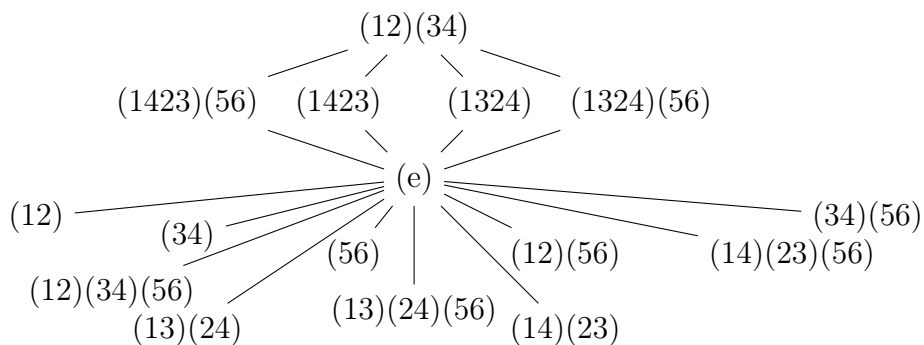


Figure 4.1: The cycle graph of $D_4 \times \mathbb{Z}_2$



Bibliography

- [1] *Handwritten private notes of Julie Kjennerud.*
- [2] The Life of Evariste Galois and his Theory of Field Extension. <http://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=1129&context=honors>. Accessed: 2015-04-17.
- [3] Wikipedia article on Evariste Galois. http://en.wikipedia.org/wiki/%C3%89variste_Galois. Accessed: 2015-04-24.
- [4] John B. Fraleigh. *A first course in abstract algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1967.
- [5] Tom L. Lindstrøm. *Kalkulus*. Universitetsforlaget, 2006.
- [6] Ludvig Sylow. *Forelæsninger over algebraisk Lignings og Substitutions theorie*. Universitetsforlaget, 1862.