Galois Theory and solvability of the nth degree polynomial equations

Miro Korhonen

21.5.2025

University of Helsinki
Faculty of Science
Master's Programme in Mathematics and Statistics
Thesis supervisor: Erik Elfving

Title: Galois Theory and solvability of the nth degree polynomial equations
Author: Miro Korhonen
Month and year: May 2025
Page count: 86

Abstract

The goal of the thesis is using Galois theory to prove Abel-Ruffini theorem, which states that for general polynomials of fifth degree or higher with coefficients in a field with characteristic zero there is no general solution formula. Galois theory gives way to a connection between group theory and field theory. Using this connection one can show by using groups instead of fields why Abel-Ruffini theorem holds, making the proof much simpler.

In the first chapter beyond the introduction, groups, rings, and fields were introduced along with important theorems and definitions that any graduate student of mathematics should be familiar with. After a short section about vector spaces I introduced Galois theory and field extensions. I wrote about the connections between Galois groups and fields, through which Galois groups can be connected to different types of polynomials. I then proved the Fundamental theorem of Galois, which states many important properties of Galois groups, that are helpful later on, especially with the Abel-Ruffini theorem.

I also wrote about polynomials and proved some theorems about their divisibility and irreducibility, and how the field the polynomial has its coefficients from matters when considering these concepts. From there I showed how some general solution formulas were formed for an linear, quadratic, cubic, and quartic polynomial equations, and gave examples on how to use the formulas. I then shared an example of a type of polynomial of fifth degree that has a solution formula, and introduced the idea that there is no general solution formula for fifth degree polynomial equations. After this I wrote briefly about symmetric polynomials, which are later used in the proof of the Abel-Ruffini theorem.

Having introduced Polynomial equations solution formulas, I went back to group theory. I shared some more important theorems around group theory and introduced the concept of solvable groups. I then introduced symmetric groups and key theorems about them. Using the previous definitions and proofs about solvable groups, I was able to show that the symmetry group S_n is solvable only when $n \leq 4$, and not solvable otherwise. Having shown that, I went back to showing how every group of order n is isomorphic to a subgroup of a symmetry group S_n, and showed a connection between radical field extensions and Galois groups.

Through connecting radical fields and Galois groups I was able to connect polynomials to symmetry groups S_n, and to determine that a general polynomial of nth degree is not solvable by radicals if $n \geq 5$ as S_n for $n \geq 5$ are not solvable. And so I had proved the

Abel-Ruffini theorem. The thesis comes to an end after a history portion about Évariste Galois, and solution formulas for polynomial equations.

Keywords: Galois theory, polynomial equations, Abel-Ruffini theorem, solvability, solution formula

Contents

Chapter 1

Introduction

The main goal of this thesis is to apply Galois Theory to Abel-Ruffini theorem, that states that there are no general solution formulas for the nth degree polynomials when n is greater or equal to five. Galois theory, invented by Évariste Galois in the 19th century, created a connection between group theory and field theory, and this connection made studying field theory much simpler. With Galois theory, we can connect the concepts of solvable groups to fields, to figure out if a polynomial with coefficients in that field is solvable.

The literary review on topics of algebra, more specifically group theory, field theory and the concepts around extension fields will be familiar to any graduate degree student of mathematics. Most of the review and the basis of Galois Theory is based on Joseph Rotman's book *Galois Theory* (2001), and most of the terminology and choice of language was based on this book.

In the review section of this thesis the book of Jokke Häsä and Johanna Rämö *Johdatus Abstraktiin Algebraan* (2016) was of great help, and the books by John B. Fraleigh (2003), Nathan Jacobson (1985) and R.B.J.T. Allenby (1991) on abstract algebra provided a greater understanding of the review topics and Galois theory. The books by E. T. Bell (1963) and Mario Livio (2005) provided a window to look back into the history of algebra and Galois theory specifically, pointing to motivations behind the creation and study of Galois theory.

Polynomials and some of their properties will be introduced, and some general solution formulas for quadratic, cubic and quartic polynomials will be defined and conducted in more detail in chapter 3 after a deep dive into Galois theory in chapter 2. In chapter 3 and 4 the concept of *solvability* is also introduced in the context of polynomials and groups respectively.

There is a quick introduction to symmetry groups and more group and field theory in chapter 4 with theorems connecting the concept of solvability to fields through Galois

theory. Abel-Ruffini theorem is proved at the end of this chapter. A brief look into the history of polynomial solution formulas, Abel-Ruffini theorem, Galois theory, and the man behind this theory is found in chapter 5 with some concluding words.

Chapter 2

Background information

In this chapter the most important definitions and theorems needed to understand the Fundamental Theorem of Galois Theory will be introduced. The most basic information on group theory and mappings will not be explained or proved in great detail and it will be assumed that the reader has some knowledge on these topics already.

Polynomials, polynomial rings and fields and some field theory will be introduced here too, as well as the basic information on Galois theory. Some more group theory, symmetry groups and permutations will be introduced in section 3 as they go well alongside the concept of solvability.

2.1 Group and field theory

Here are some basic definitions and notations concerning groups and rings. We will not go into detail on how or why these things are the way they are, but you can find further information and proofs from Jokke Häsä and Johanna Rämö's (2015) book *Johdatus abstraktiin algebraan*, the introductory chapters of Joseph Rotman's book on Galois Theory (2001), or Allenby's book (1983) on rings, fields and groups.

Definition 2.1. A pair $(G, *)$, where $*$ is some binary operation in G, is called a **group** if the following axioms are satisfied:

(G1) The operation $*$ is associative, i.e.

$$x * (y * z) = (x * y) * z$$

for all $x, y, z \in G$.

(G2) The operation has an identity element, $e \in G$ such that

$$e * x = x * e = x$$

for all $x \in G$. To differentiate between the identity elements of different groups, say groups G and H, the group the identity belongs to will be notated with indexes, like e_G and e_H.

(G3) For every $x \in G$ there exists an inverse element $y \in G$ such that

$$x * y = y * x = e.$$

If the group is also commutative, i.e.

$$x * y = y * x$$

for all $x, y \in G$, then the group is said to be Abelian.

Definition 2.2. Let G and H be groups. A mapping $f\colon G \to H$ is called a **group homomorphism** if

$$f(x * y) = f(x)f(y)$$

for all $x, y \in G$, where $*$ is a binary operation in G.

For the remainder of the thesis we will use the definition of a commutative ring with identity in place of just a ring.

Definition 2.3. A commutative ring with 1 is a set R equipped with two binary operations, addition and multiplication, such that:

(R1) R is an abelian group under addition,

(R2) multiplication is commutative and associative,

(R3) there is an element $1 \in R$ with $1r = r$ for all $r \in R$.

(R4) distribution law is satisfied,

$$r(s + t) = rs + rt \quad \text{for all } r, s, t \in R.$$

When dealing with multiple rings, say R and S, the identity elements for multiplication and addition are notated in this text in the forms 1_R and 0_R, and 1_S and 0_S respectively.

Some examples of commutative rings are the sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, all of which will be used in future examples.

Generally, the neutral elements 0 and 1 are not the same for a (commutative) ring, like for example in $\mathbb{R}$ we clearly have $1 \neq 0$. The special case of such ring is the trivial ring, as for the trivial ring $T = \{0\}$ we have $0_T = 1_T$.

Definition 2.4 (Congruence and Congruence Classes)**.** Two elements $a, b \in \mathbb{Z}$ are **congruent modulo** n, if $a - b$ is divisible by n. This is denoted by $a \equiv b \mod n$. The set of all congruence classes modulo n

$$[a]_n = \{b \in \mathbb{Z} \colon b \equiv a \mod n\}$$

is denoted by $\mathbb{Z}_n$. Here a is a representative of the congruence class $[a]_n$. Addition and multiplication are given by

$$[a]_n + [b]_n = [a + b]_n \quad \text{and} \quad [a]_n[b]_n = [ab]_n,$$

and $[1]_n$ is the identity element in $\mathbb{Z}_n$.

Congruence and congruence classes will mostly be used in some examples in this section and some important proofs in section 3.

Definition 2.5. A subset H of a group G is called a **subgroup** if

- $gh \in H$ for all $g, h, \in H$,
- the identity element of G is also in H,
- for all $g \in H$ also $g^{-1} \in H$.

We shall denote this by $H \leq G$. A subgroup is a **proper** subgroup if $H \neq G$, and a subgroup is called **trivial** if $H = \{1\}$, and nontrivial otherwise.

A subgroup $H \leq G$ is said to be **normal** if for for all $h \in H$ and $g \in G$ we have $ghg^{-1} \in H$. Meaning if

$$gHg^{-1} = \{ghg^{-1} : h \in H\} = H$$

then H is normal. Note, that all subgroups of abelian groups are normal, as for all $g \in G$ we have

$$ghg^{-1} = gg^{-1}h = h \in H.$$

Definition 2.6. A **subring** of a ring R is a subset S of R which contains the identity element $1 \in R$, and which is closed under subtraction and multiplication.

For example $\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$ and so on.

Definition 2.7. Let $g \in G$ and H be a subgroup of G. Then the left and right cosets of H in G are

$$gH = \{gh \mid h \in H\} \quad \text{and} \quad Hg = \{hg \mid h \in H\}.$$

These sets *partition* G, and the set of all left cosets is denoted by

$$G/H = \{gH \mid g \in G\}.$$

Definition 2.8. Let G be a group and N be a normal subgroup of it. The group G/N called the **quotient group of** G, is the family of cosets gN of N, the group operation defined by

$$gNhN = ghN$$

for all $g, h \in G$.

Quotient groups are especially important in the isomorphism theorems, which are some of the main important theorems in group theory. They will be introduced shortly.

Later in the thesis a similar notation to quotient group will be used for field extensions, but for clarity it will be specified when cosets and quotient groups are being used.

Definition 2.9. If R and S are rings, then a function $\varphi\colon R \to S$ is a **ring homomorphism** (ring map), if for all $r, r' \in R$:

$$\begin{aligned} \varphi(r + r') &= \varphi(r) + \varphi(r'); \\ \varphi(rr') &= \varphi(r)\varphi(r'); \\ \varphi(1_R) &= 1_S. \end{aligned}$$

A ring homomorphism $\varphi\colon R \to S$ is an **isomorphism** if φ is a bijection. If there is an isomorphism between two rings R and S, then we may say that they are isomorphic, which is denoted by $R \cong S$.

Definition 2.10. If $\varphi\colon R \to S$ is a ring map, then its **kernel** is

$$\ker \varphi = \{r \in R : \ \varphi(r) = 0\}$$

and its **image** is

$$\operatorname{im} \varphi = \{s \in S : \ s = \varphi(r) \text{ for some } r \in R\}.$$

It is easy to check that: If $\varphi\colon R \to S$ is a ring homomorphism, then the kernel $\ker \varphi$ is an additive subgroup of R that is closed under multiplication, and that $\operatorname{im} \varphi$ is a subring of S. The kernel on the other hand is not a subring of R because R does not contain 1_R as $\varphi(1_R) = 1_S$.

For a group homomorphism, the kernel is a subgroup of the domain of the map and, more specifically, is a normal subgroup.

Definition 2.11. The number of elements in the group G is denoted by $|G|$ and is called it's **order**.

Elements of groups also have an order; let $x \in G$, then the order of x is the least positive integer m, if any, such that $x^m = 1$. If there is no just integer, then the order is infinity.

Example 2.12. (ii) The group of real numbers $\mathbb{R}$ has infinite order as it has infinitely many elements;

(ii) The group $\mathbb{Z}_3$ has three elements, so it's order is 3.

Definition 2.13. Let $H \leq G$. The number of right (or left) cosets of H in G is called the index of H in G. It is denoted by $[G : H]$.

Theorem 2.14 (Lagrange's Theorem)**.** *Let $H \leq G$, G a finite group. Then $[G : H] = |G| : |H|$.*

Clearly $|H| \leq |G|$ for finite groups $H \leq G$, but Lagrange's theorem shows that the order of the subgroup H is a divisor of the group G.

Lemma 2.15. *If $h : G \to H$ is a group homomorphism, then h is an injection, if and only if $\ker h = \{e_G\}$.*

Proof. If h is an injection, then $x \neq e_G$ implies $h(x) \neq h(e_G) = e_H$, and so $x \notin \ker h$. Conversely assuming $\ker h = \{e_G\}$ and that $h(x) = h(y)$ for $x, y \in G$. Then

$$e_H = h(x)h(y)^{-1} = h(x)h(y^{-1}) = h(xy^{-1})$$

and $xy^{-1} \in \ker h = \{e_G\}$. So $x = y$ and h is an injection. □

The following isomorphism theorems will be useful when we move onto Galois theory. The latter two proofs have been emitted as they are assumed to be familiar to the reader.

Theorem 2.16 (First Isomorphism Theorem (for groups))**.** *Let G, H be groups. If $f : G \to H$ is a homomorphism, then $\ker f$ is a normal subgroup of G and*

$$G/\ker f \cong im\ f,$$

where $G/\ker f$ is the quotient group.

Proof. Let $K = \ker f$. We will now show that K is a subgroup of G:

Clearly K contains the identity e_G as f is a homomorphism and $f(e_G) = e_H$ as is necessary for the group identity.

If $x, y \in K$, then $f(xy) = f(x)f(y) = e_H$ and $xy \in K$. And if $x \in K$, then $f(x^{-1}) = f(x)^{-1} = e_H$ and $x^{-1} \in K$.

The subgroup is also normal, as when $x \in K$ and $g \in G$

$$f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)f(g)^{-1} = e_H$$

and so $gxg^{-1} \in K$.

Define $\phi\colon G/K \to \text{im } f$ by $\phi(gK) = f(g)$. It is well-defined because when $g'K = gK$ then $g' = gk$ for some $g \in K$, and

$$f(g') = f(gk) = f(g)f(k) = f(g).$$

It is also easy to check that ϕ is a homomorphism (as f is one) with $\text{im } \phi = \text{im } f$.

Lastly, using lemma 2.15 and by showing that $\ker \phi$ is a singleton, we can show that ϕ is injective: Let $\phi(xK) = e_H$, then $xK \in \ker \phi$ for some $x \in G$. This implies then $f(x) = e_H$, hence $x \in K$ and $xK = K$. So the kernel of ϕ is the singleton $\{K\} = \{e_{G/K}\}$, and so by lemma 2.15 ϕ is an injection. Now ϕ is clearly surjective, and so we have the isomorphism $G/K \cong \text{im } f$. □

From the previous theorem 2.16 we get that the group G is isomorphic with some quotient group of G. If N is a normal subgroup of G, we can define the surjective **canonical projection** or **natural map**

$$\pi : G \to G/N, \quad \text{such that} \quad \pi(g) = gN.$$

This mapping is surjective and its image is G/N. For more on the natural map, see [HR16].

Theorem 2.17 (Second Isomorphism Theorem)**.** *If K and H are subgroups of G, then $K \cap H$ is a normal subgroup of H and*

$$H/(K \cap H) \cong KH/K.$$

Theorem 2.18 (Third Isomorphism Theorem)**.** *If $S \subset K$ are normal subgroups of G, then K/S is a normal subgroup of G/S and*

$$(G/S)/(K/S) \cong G/K.$$

Here are definitions of fields, domains and ideals, and some useful theorems and examples for handling them. Some specific types of rings will also be introduced.

A field is a type of ring that we will be using for a good portion of this thesis. Domains are another type of ring that are mentioned here, but not used in this thesis outside of some examples.

Definition 2.19. An element $u \in R$ is a **unit**, if there exists $v \in R$ with $uv = 1$.

Definition 2.20. A **field** is a ring R in which every nonzero $r \in R$ is a unit.

Here are some examples of fields.

Example 2.21. 1. The rings $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields as all their nonzero elements have inverse elements.

2. The ring $\mathbb{Z}_p$ is a field if p is a prime number. Here is a proof of this claim:

   Suppose $[a] \in \mathbb{Z}_p$. If $[a]$ is not the zero congruence class, then the integer a is not divisible by p. We know that since p is a prime, its only divisors (in $\mathbb{Z}$) are 1 and p itself, and p is not a divisor of a. Then the greatest common divisor of a and p is 1. By Bezout's lemma (lemma 5.4. in [HR16] page 80) we have that 1 is a linear combination of a and p: $1 = ta + up$ for some $t, u \in \mathbb{Z}$. Then $ta - 1 = -up$, meaning $ta \equiv 1 \mod p$:

   $$[1] = [ta] = [t][a].$$

   Therefore the inverse of $[a]$ is $[t]$ and so $\mathbb{Z}_p$ is a field.

Theorem 2.22. *If R is a ring, then $U(R)$, the set of all units in R, is a group under multiplication. One calls $U(R)$ the group of units of R.*

Proof. From the definition of rings, we get that for R multiplication is associative, meaning the first condition of the definition of groups holds. There is also $1_R \in R$ for which $1_R \in U(R)$, meaning the second condition holds. And the third and last condition, every element of $U(R)$ having an inverse, holds by the definition of units. □

Theorem 2.23. *A ring R is a field if and only if $R^\# = R - 0$ is a group under multiplication. (And of course $U(R) = R^\#$ here.)*

Proof. First direction is clear by the previous theorem; from R being a ring we know that $U(R)$ is a group under multiplication, and as R is a field, then $U(R) = R^\#$.

If $R^\#$ is a group under multiplication, then clearly all nonzero elements of R are units, so R is a field. □

Note, that the group $R^\#$ is sometimes notated by R^* in some literature. Here we will be using the former.

Definition 2.24. A ring R is called a **domain** if the product of any two nonzero elements in R is itself nonzero.

Domains are a useful concept, as this tells a lot about the ring's elements; if we have a and b in a domain R with $ab = 0$, then clearly $a = 0$ or $b = 0$,

Now for example $\mathbb{Z}_4$ is not a domain because $[2] \neq [0]$ but $[2][2] = [4] = [0]$. But there are other $\mathbb{Z}_n$ that are domains:

Theorem 2.25. *$\mathbb{Z}_n$ is a domain if and only if n is a prime.*

Proof. If n is not a prime, then it is a product of some $a, b \in \mathbb{Z}$ with $1 < a < n$ and $1 < b < n$, and $n = ab$. It follows then that $[a]_n[b]_n = [ab]_n = [n]_n = [0]_n$, while $[a]_n, [b]_n \neq [0]_n$, so $\mathbb{Z}_n$ is not a domain.

Conversely, if $[a]_p[b]_p = [ab]_p = [0]_p$, then $ab \equiv 0 \mod p$ in $\mathbb{Z}_p$, and p is a divisor of ab. By Euclid's lemma for numbers (lemma 5.6. in [HR16] p.81) we have that p then divides either a or b, meaning $[a]_p = [0]_p$ or $[b]_p = [0]_p$.

□

Definition 2.26. Let R be a commutative ring with unity. A non-empty subset $I \subset R$ containing 0_R is called an **ideal** if

(i) $a, b \in I$ implies $a - b \in I$

(ii) $a \in I$ and $r \in R$ implies $ra \in I$.

An ideal I in a ring R is a **proper ideal** if $I \neq R$. Every ring R contains the ideals R itself and $\{0\}$.

We can define quotient rings and natural maps similarly to how we defined them for groups. Not considering the multiplication side of a ring R, now its ideal I is a subgroup of the additive group of R. And as R is abelian group, then I is a normal subgroup. From this we can continue defining the quotient R/I and the natural map.

Definition 2.27. The **natural map** for rings is $\pi : R \to R/I$, where I is an ideal of ring R, is the surjective group homomorphism defined by $r \mapsto r + I$.

Theorem 2.28. *Let I be a proper ideal in a ring R. Then the additive abelian group R/I can be equipped with a multiplication which makes it a ring and which makes the natural map $\pi : R \to R/I$ a surjective ring homomorphism.*

Definition 2.29. If I is an ideal in a ring R, then R/I is called the *quotient ring* of R *modulo* I.

Theorem 2.30. *If $\varphi\colon R \to S$ is a ring homomorphism, then $\ker\varphi$ is a proper ideal in R.*

Proof for this can be found in [Rot01].

Definition 2.31. If $a \in R$, then $\{ra\colon r \in R\}$ is the ideal generated by a. It is called the **principal ideal generated by** a, and it is denoted by (a).

Example 2.32. The ideals $n\mathbb{Z}$ of $\mathbb{Z}$, are generated by $n \in \mathbb{Z}$, therefore they are principal ideals of $\mathbb{Z}$.

Definition 2.33. A ring R is called a **principal ideal domain** (PID) if it is a domain in which every ideal is a principal ideal.

Example 2.34. The ring $\mathbb{Z}$ is a PID, as all of its ideals are principal ideals of the form $n\mathbb{Z}$, generated by n; As $\mathbb{Z}$ is an infinite cyclic group (cyclic groups will be defined later in section 3.1) therefore all its subgroups also have to be cyclic and of the form $n\mathbb{Z}$ where $n \in \mathbb{Z}$. For further explanations see [HR16].

Theorem 2.35 (First Isomorphism Theorem (for Rings))**.** *If I is an ideal of the ring R and $\varphi : R \to S$ is a ring homomorphism with $\ker \varphi = I$, then there is an isomorphism $R/I \to \text{im } \varphi$ given by $r + I \mapsto \varphi(r)$.*

Theorem 2.36. *Let I be an ideal in a ring R, let J be an ideal in a ring S, and let $\varphi : R \to S$ be a ring isomorphism with $\varphi(I) = J$. Then the function $\bar{\varphi} : r + I \mapsto \varphi(r) + J$ is a (well defined) isomorphism $R/I \to S/J$.*

Proof. There is a surjective natural mapping $\pi_S : S \to S/J$ defined by $s \mapsto s + J$ for all $s \in S$. Let $\delta : R \xrightarrow{\varphi} S \xrightarrow{\pi_S} S/J$, where now $\delta(r) = \varphi(r) + J$ for all $r \in R$. As φ and π_S are ring homomorphisms, so is δ for all $r, r' \in R$:

$$
\begin{aligned}
&(1) \quad \delta(r + r') = \varphi(r + r') + J = \varphi(r) + J + \varphi(r') + J = \delta(r) + \delta(r') \\
&(2) \quad \delta(rr') = \varphi(rr') + J = (\varphi(r) + J)(\varphi(r') + J) = \delta(r)\delta(r') \\
&(3) \quad \delta(1_R) = \varphi(1_R) + J = 1_S + J = (\text{the identity in } S/J).
\end{aligned}
$$

Also for all $r \in I$ we have $\varphi(r) \in J$, meaning $\delta(r) = J$ for all $r \in I$. Therefore $I \subset \ker \delta$.

Suppose that $\ker \delta \not\subset I$, so there is some $r' \in \ker \delta$ for which $r' \notin I$. Then $\varphi(r') \notin J$ which means that $\varphi(r') + J \neq J$. But as $r' \in \ker \delta$, then $\varphi(r') + J = \delta(r') = J$, which brings us to a contradiction with our assumption. Therefore $\ker \delta \subset I$.

So by the first isomorphism theorem there is an isomorphism $\bar{\varphi} : R/I \to \text{im } \delta$ given by $r + I \mapsto \delta(r) = \varphi(r) + J$. As π_S is surjective, then δ is surjective too, meaning $\text{im } \delta = S/J$. So we have found the wanted isomorphism $\bar{\varphi}$.

□

2.1.1 A summary of vector spaces

We will not get in depth about what vectors or vector spaces are, but a brief visit to their domain is necessary for the some of the definitions in Galois theory. A more in depth explanation can be found in [Rot15] and [OR13].

Before getting into vectors, let us define what a *group action* is.

Definition 2.37. Let G be a group and let S be a non-empty set. A function $\varphi : G \times S \to S$ where $\varphi(g, x) = gx$ is an *action* of G on S if

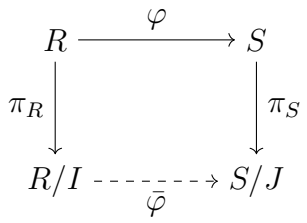

Figure 2.1: The mappings in theorem 2.36.

1. we have $\varphi(e_G, x) = x$ for every $x \in S$, and
2. we have
$$\varphi(g, \varphi(h, x)) = g(hx) = (gh)x = \varphi(gh, x)$$
for all $g, h \in G$ and $x \in S$.

A group action generalizes the definition of *permutations*; for a fixed $g \in G$ the map $\varphi_g : X \to X$ with $\varphi_g : x \mapsto gx$ is a bijection permutating all elements of the set by g. Group action gives a way for the elements of the set to interact with one another, while taking into account the structure of the group; for example, the neutral element leaves all the elements in their places.

Through group actions one may get a representation of the group as, for example, linear mappings of a vector space, when one will get to examine the group through much easily processable matrices.

A vector space is as follows:

Definition 2.38. Let V be a set with addition and scalar multiplication defined in it in some way. If the conditions below apply to all **vectors** $\bar{v}, \bar{w}, \bar{u} \in V$ and all **scalars** $a, b \in K$, where K is a field, then the set V is called a **vector space**.

1. $\bar{v} + \bar{w} = \bar{w} + \bar{v}$ for all $\bar{v}, \bar{w}, \in V$.
2. $(\bar{v} + \bar{w}) + \bar{u} = \bar{v} + (\bar{w} + \bar{u})$ for all $\bar{v}, \bar{w}, \bar{u} \in V$.
3. There exists a so called *zero vector* $\bar{0}$, for which $\bar{v} + \bar{0} = \bar{v}$ for all $\bar{v} \in V$.
4. For every vector $\bar{v} \in V$ there is an element $-\bar{v}$ called the *additive inverse* of $\bar{v}$, such that $\bar{v} + (-\bar{v}) = \bar{0}$.
5. $a(\bar{v} + \bar{w}) = a\bar{v} + a\bar{w}$ for all $\bar{v}, \bar{w} \in V$ and $a \in K$.
6. $(a + b)\bar{v} = a\bar{v} + b\bar{v}$ for all $\bar{v} \in V$ and $a, b \in K$.

7. $(ab)\bar{v} = a(b\bar{v})$ for all $\bar{v} \in V$ and $a, b \in K$.

8. $1_K\bar{v} = \bar{v}$ for all $\bar{v} \in V$.

Vector spaces have vectors that can generate any of the other vectors in the space. These generating vectors can form *spanning sets*, and in some cases they can be *bases* of the vector space:

Definition 2.39. Let V be some vector space and K be the field of scalars. Let $\bar{w}_1, \bar{w}_2, \ldots, \bar{w}_k \in V$. The set $\{\bar{w}_1, \bar{w}_2, \ldots, \bar{w}_k\}$ is a **basis** of the vector space V, if

1. the vectors $\bar{w}_1, \bar{w}_2, \ldots, \bar{w}_k$ span the vector space V, meaning that for any $v \in V$ there are $a_1, \ldots, a_k \in K$ such that $v = a_1\bar{w}_1 + a_2\bar{w}_2 + \cdots + a_k\bar{w}_k$.

2. $\{\bar{w}_1, \bar{w}_2, \ldots, \bar{w}_k\}$ is linearly independent, meaning if

$$c_1\bar{w}_1 + c_2\bar{w}_2 + \cdots + c_k\bar{w}_k = \bar{0},$$

for some $c_1, \ldots, c_k \in K$, then $c_i = 0$ for all $0 \leq i \leq k$.

By "dimension" of a vector space we mean the number of elements in a basis of the vector space. So for example the vector space $\mathbb{R}^2$ is of dimension 2 and has two base vectors in all its bases.

2.1.2 Polynomial Rings over Fields

Now back to rings, and more specifically polynomial rings. The following section is based on Rotman (2001). We will define polynomials, share some theorems and lemmas about their divisibility and bring them in to the context of rings and fields.

Let R be a commutative ring with unity. **A polynomial with one variable** is a sum of different powers of the variable with **coefficients** $c_i \in R$, $i \in \mathbb{N}_0$, i.e.

$$f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n = \sum_{i=0}^{n} c_ix^i,$$

where x is the variable.

The **zero polynomial** is the polynomial $f(x) = 0$, with no variables or coefficients in it. A polynomial $f(x) = c_0$, with $c_0 \neq 0$ in R, is a **constant** polynomial, and in this case c_0 is seen as the leading coefficient. If $f(x)$ is not the zero polynomial, the largest n with a nonzero c_n (*leading coefficient*) is called the **degree** of the polynomial. The constant polynomial has degree 0, and the zero polynomial on the other hand has no degree, as it does not have a leading coefficient.

We also say a polynomial is **monic**, if it's leading coefficient is 1. Using monic polynomials or constructing monic polynomials is useful when proving some aspects of solvable equations and some aspects of polynomial fields and extension fields, introduced in the next section and following chapter.

There are also some terms for different types of polynomials: **linear**, **quadratic**, **cubic**, **quartic** and **quintic**, and their degrees are 1, 2, 3, 4 and 5 respectively. We will not mention by name other polynomials of higher degrees in this thesis, as our interest lies in the polynomials up to 5th degree currently.

The **polynomial ring over** R is denoted by $R[x]$. It consists of single variable polynomials with coefficients in R. For a proof of the fact that $R[x]$ is indeed a ring, see [Jac85].

We can also define maps between polynomial rings. If $\varphi\colon R \to S$ is a ring map, then also $\varphi^*\colon R[x] \to S[x]$, defined by

$$\Sigma r_i x^i \mapsto \Sigma \varphi(r_i) x^i,$$

is a ring map: the second condition of a ring mapping follows from

$$\begin{aligned}
\varphi^*(\Sigma r_i x^i \cdot \Sigma r'_i x^i) &= \varphi^*(\Sigma_i \Sigma_k r_i x^i r'_k x^k) \\
&= \Sigma_i \Sigma_k \varphi(r_i r'_k) x^i x^k \\
&= \Sigma_i \Sigma_k \varphi(r_i)\varphi(r'_k) x^i x^k \\
&= \Sigma_i \varphi(r_i) x^i \Sigma_k \varphi(r'_k) x^k \\
&= \varphi^*(\Sigma r_i x^i)\varphi^*(\Sigma r'_i x^i);
\end{aligned}$$

and clearly $\varphi^*(1) = 1$.

Also, it is good to note that a ring of polynomials with multiple variables is also a ring. If R is a ring, then $R[x, y]$ is a ring for polynomials with two variables, and $R[x_0, \ldots, x_n]$ is the ring of polynomials with n many variables.

This thesis focuses on polynomials with a single variable, so polynomials with multiple different variables will not be discussed any further. For more information, you may read about them in [Jac85].

Next will be shown some qualities of polynomials and their relationships to fields.

Definition 2.40. Let $f(x) = \Sigma c_i x^i$ be a polynomial over a ring R. A **root** of $f(x)$ in R is an element $\alpha \in R$ such that

$$f(\alpha) = c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0.$$

Note that sometimes the roots lie in a ring larger than what we are considering:

Example 2.41. The polynomial $f(x) = x^2 + 1$ over $\mathbb{R}$ does not have roots in $\mathbb{R}$, but as a polynomial over $\mathbb{C}$ ($\geq \mathbb{R}$) it has roots i and $-i$.

Theorem 2.42. *If F is a field and $f(x) \in F[x]$ has degree $n \geq 0$, then F contains at most n roots of $f(x)$.*

Proof for this can be found in [Rot01].

Definition 2.43. Let F be a field. A nonzero polynomial $p(x) \in F[x]$ is **irreducible over** F if $\deg(p) \geq 1$ and there is no factorization $p(x) = f(x)g(x)$ in $F[x]$ with $0 < \deg(f) < \deg(p)$ and $0 < \deg(g) < \deg(p)$.

Example 2.44. Using the same polynomial as in example 2.41, the polynomial $f(x) = x^2+1$ is not irreducible over $\mathbb{C}$, as it can be written in the form $f(x) = (x+i)(x-i)$ using its roots. Over the ring $\mathbb{R}$ it is irreducible. Let us prove this fact:

Suppose $f(x)$ is not irreducible in $\mathbb{R}$. Then there are polynomials of some positive degree smaller than the degree of $f(x)$ that divide $f(x)$. Here that would mean we have two linear polynomials dividing $f(x)$. Suppose $f(x) = x^2 + 1 = (a_0x + b_0)(a_1x + b_1)$ for some $a_0, a_1, b_0, b_1 \in \mathbb{R}$. Then

$$x^2 + 1 = (a_0x + b_0)(a_1x + b_1) = a_0a_1x^2 + (a_0b_1 + a_1b_0)x + b_0b_1,$$

and by comparing the sides we get $a_0a_1 = 1$, $b_0b_1 = 1$ and $a_0b_1 + a_1b_0 = 0$. Solving a_1 and b_1 from the first two equations and placing them into the last one we get

$$a_0^2 = -b_0^2.$$

But as $a_0^2 \geq 0$ and $b_0^2 \geq 0$ for all $a_0, b_0 \in \mathbb{R}$, the above equation is impossible in $\mathbb{R}$ unless $a_0 = b_0 = 0$, which would then mean our linear polynomial $a_0x + b_0$ could not divide $f(x)$. So the polynomial $f(x)$ is irreducible over $\mathbb{R}$.

Lemma 2.45 (Euclid's Lemma)**.** *Let F be a field, and let $p(x) \in F[x]$ be irreducible; if $p(x)$ divides a product $q_1(x) \cdots q_n(x)$, then $p(x)$ divides $q_j(x)$ for some j. This fact can be notated by $p|q_j$.*

Proof for this lemma can be found in [Rot01].

The field that is being studied matters. For instance, it could be that a polynomial is not irreducible in some polynomial ring, while in some of its subrings it is. An example of that situation can be seen in the above example 2.44.

The lemmas and theorems in this section are useful when trying to find roots of polynomials, determining their solvability, which will be defined in chapter 3, and in finding some other qualities of these polynomials and polynomial rings. Before getting to that, here are some more theorems and definitions about the division of polynomials.

Definition 2.46. Let R be a domain, and let $f(x), g(x) \in R[x]$. The **greatest common divisor** (gcd) of $f(x)$ and $g(x)$ is a polynomial $d(x) \in R[x]$ such that:

(i) $d(x)$ is a common divisor of $f(x)$ and $g(x)$; that is, $d|f$ and $d|g$;

(ii) if $c(x)$ is any common divisor of $f(x)$ and $g(x)$, then $c(x)|d(x)$;

(iii) $d(x)$ is monic.

If for the above $d(x) = 1$, then $f(x)$ and $g(x)$ are called **relatively prime**.

Theorem 2.47 (Euclidean division)**.** *Let F be a field and $f, g \in F[x]$. Suppose $g \neq 0$. Then there are unique $q, r \in F[x]$ such that $f = gq + r$ and $r = 0$ or $\deg(r) < \deg(g)$.*

Proof. Consider the set $R = \{f - qg \,|\, q \in F[x]\}$. This set is non-empty as we have at least $f \in R$. Let then $r \in R$ be a polynomial that has the smallest degree in R. Then $f - qg = r$ for some $q \in F[x]$.

If $r = 0$, then $f = qg$ and then clearly g and q are the polynomials dividing f. Suppose then that $r = \Sigma_{i=0}^{n} a_i x^i$ and $g = \Sigma_{i=0}^{m} b_i x^i$, where $a_n \neq 0 \neq b_m$. If $\deg(r) \geq \deg(g)$, then define a polynomial $q_1 = q + a_n b_m^{-1} x^{n-m}$. Then we have

$$\begin{aligned} f - q_i g &= f - qg - a_n b_m^{-1} x^{n-m} g \\ &= r - a_n b_m^{-1} x^{n-m}(b_m x^m + \cdots + b_0) \\ &= (a_n x^n + \cdots + a_0) + -a_n b_m^{-1} x^{n-m}(b_m x^m + \cdots + b_0). \end{aligned}$$

From this we can see that the coefficient of the term x^n is $a_n - a_n b_m^{-1} b_m = 0$, meaning that the degree of $f - q_i g$ is smaller than the degree of r, which is a contradiction with how we chose r.

To show that q and r are unique, suppose that for polynomials q_1, q_2, r_1 and r_2 the claim $f = q_i g + r_i$ holds. Then $q_1 g + r_1 = q_2 g + r_2$, which leads to $(q_1 - q_2)g = r_1 - r_2$.

If $q_1 \neq q_2$, then the degree of the polynomial $(q_1 - q_2)g$ is at least degree $\deg(g)$, which is greater than the degree of $r_1 - r_2$. This is in contradiction with $(q_1 - q_2)g = r_1 - r_2$, so it must be that $q_1 = q_2$ and $r_1 = r_2$. □

Theorem 2.48. *Let $k \subset K$ be fields and let $f(x), g(x) \in k[x] \subset K[x]$. Then the greatest common divisor of f and g computed in $K[x]$ is the same as the gcd of f and g computed in $k[x]$.*

Proof. The division algorithm in $K[x]$ gives us

$$f(x) = Q(x)g(x) + R(x),$$

where $Q(x), R(x) \in K[x]$ and $\deg(R) < \deg(g)$. As also $f(x), g(x) \in k[x]$, the division algorithm in $k[x]$ gives

$$f(x) = q(x)g(x) + r(x),$$

where $q(x), r(x) \in k[x]$ and $\deg(r) < \deg(g)$. But the equation $f(x) = q(x)g(x) + r(x)$ also holds in $K[x]$, so by the uniqueness of the quotient and remainder in the division algorithm in $K[x]$ it has to be that $Q(x) = q(x)$ and $R(x) = r(x)$. This means that the list of all equations occurring in the euclidean algorithm in $K[x]$ is the same as the list of all equations occurring in the algorithm of the smaller ring $k[x]$. Therefore the same gcd is obtained in both polynomial rings. □

The connection between polynomials and their respective rings can give us a way to determine some of the properties of the polynomials, including whether the polynomials are divisible or irreducible. This can be done with studying the ideals of the said polynomial rings and their properties.

Definition 2.49. An ideal I in a ring R is called a **prime ideal**, if it is a proper ideal and $ab \in I$ implies $a \in I$ or $b \in I$.

Theorem 2.50. *If F is a field, then a nonzero polynomial $p(x) \in F[x]$ is irreducible if and only if $(p(x))$ is a prime ideal.*

Proof. Suppose a nonzero $p(x) \in F[x]$ is irreducible. Then if $ab \in (p) = \{pf \colon f \in F[x]\}$, then by 2.45 either $p|a$ or $p|b$. So $a \in (p)$ or $b \in (p)$. Supposing that (p) isn't a proper ideal $1 \in F[x] = (p)$ would mean that there is some polynomial $f(x)$ such that $p(x)f(x) = 1$, but that gives us a contradiction as

$$\deg(pf) = \deg(p) + \deg(f) \geq \deg(p) \geq 1 \neq 0 = \deg(1).$$

So (p) is a proper ideal.

On the other hand, suppose that $p(x)$ is not irreducible, then there are some polynomials $a(x), b(x)$ in $F[x]$, with $\deg(a) < \deg(p)$ and $\deg(b) < \deg(p)$ for which

$$p(x) = a(x)b(x).$$

All nonzero polynomials in (p) have a degree at least $p(x)$, we get that neither $a(x)$ or $b(x)$ lies in (p), meaning (p) is not a prime ideal. □

Theorem 2.51. *A proper ideal I in R is a prime ideal if and only if R/I is a domain.*

Proofs of this and the following two theorems can be found in [Rot01].

Definition 2.52. An ideal I in a ring R is a **maximal ideal** if it is a proper ideal and there is no ideal J with $I \subsetneqq J \subsetneqq R$.

Theorem 2.53. *A proper ideal I in a ring R is a maximal ideal if and only if R/I is a field.*

Theorem 2.54. *If R is a principal ideal domain, then every nonzero prime ideal I is a maximal ideal.*

Theorem 2.55. *If F is a field, then $F[x]$ is a principal ideal domain.*

Theorem 2.56. *If F is a field and $p(x) \in F[x]$ is irreducible, then the quotient ring $F[x]/(p(x))$ is a field containing (an isomorphic copy of) F and a root of $p(x)$.*

Proof. As $p(x)$ is irreducible, then the principal ideal $I = (p(x))$ is a prime ideal and it is also nonzero, meaning it has more elements than just the zero element of $F[x]$. Since $F[x]$ is PID, I is a maximal ideal by 2.54, and so $E = F[x]/(p(x))$ is a field by 2.53.

The map $a \mapsto a + I$ is an isomorphism from F to $F' = \{a + I : a \in F\} \subset E$.

Let $\theta = x + I \in E$. We want to show that θ is a root of $p(x)$ in E. Write $p(x) = a_0 + a_1x + \cdots + a_nx^n$ where $a_i \in F$ and n is the degree of $p(x)$. Then, in E:

$$\begin{aligned} p(\theta) &= (a_0 + I) + (a_1 + I)\theta + \cdots + (a_n + I)\theta^n \\ &= (a_0 + I) + (a_1 + I)(x + I) + \cdots + (a_n + I)(x + I)^n \\ &= (a_0 + I) + (a_1x + I) + \cdots + (a_nx^n + I) \\ &= a_0 + a_1x + \cdots + a_nx^n + I \\ &= p(x) + I = I. \end{aligned}$$

But $I = 0 + I$ is the zero element of $E = F[x]/(p(x))$, and so θ is a root of $p(x)$. □

Definition 2.57. A polynomial $f(x) \in F[x]$ **splits over** F if it is a product of linear factors in $F[x]$.

Also, $f(x)$ splits over F, if and only if F contains all the roots of $f(x)$. Using the polynomial $f(x) = x^2+1$ again as an example; $f(x)$ splits over $\mathbb{C}$ as it has the factorization $f(x) = (x+i)(x-i)$ (a product of two linear factors) in $\mathbb{C}[x]$, but doesn't split over $\mathbb{R}$ as $\mathbb{R}$ doesn't contain the roots of $f(x)$. This example can be written in more general terms:

Theorem 2.58 (Kronecker)**.** *Let $f(x) \in F[x]$, where F is a field. There exists a field E containing F over which $f(x)$ splits.*

Proof. This proof is done by induction on $\deg(f)$:

If $\deg(f) = 1$, then $f(x)$ is linear and we can choose $E = F$.

If $\deg(f) > 1$, then let us write $f(x)$ as a product of two polynomials $p(x)$ and $g(x)$, where $p(x)$ is irreducible. By theorem 2.56 we have a field B containing F and a root a of $p(x)$, so $p(x) = (x - a)h(x)$ in $B[x]$ for some h, and then $f(x) = (x - a)h(x)g(x)$. By induction there is a field E containing B (which contains F), so that hg, therefore f, is a product of linear factors in $E[x]$. So f splits. □

Definition 2.59. Let $f(x) \in F[x]$ have the factorization into (not necessarily distinct) irreducibles:

$$f(x) = ap_1(x) \cdots p_t(x),$$

where $a \in F$; then $f(x)$ is **separable** if none of the p_i have repeated roots, meaning no p_i and p_j with $i \neq j$ can have any roots in common.

Using the polynomial $f(x) = x^2 + 1$ again as an example; $f(x)$ splits over $\mathbb{C}$ as it has the factorization $f(x) = 1(x + i)(x - i)$, a product of two linear factors in $\mathbb{C}[x]$, and $f(x)$ in $\mathbb{C}[x]$ is separable as none of its factors have repeated roots. An example of a non-separable polynomial would be $g(x) = x^2 + 2x + 1 \in \mathbb{R}[x]$ as $g(x) = 1(x + 1)(x + 1)$, where $x + 1$ appears in the factorization of $g(x)$ twice, giving us a repeated root -1.

Theorem 2.60. *Let R be a domain and F be a field, let $\sigma : R \to F$ be a ring map, and let $p(x) \in R[x]$. If $\deg(\sigma^*(p)) = \deg(p)$ and if $\sigma^*(p(x))$ is irreducible in $F[x]$, then $p(x)$ is not a product of two polynomials in $R[x]$ each of degree $< \deg(p)$.*

Proof. Suppose $p(x)$ is a product of some polynomials $f(x), g(x) \in R(x)$ with degrees smaller than $\deg(p(x))$. As σ^* is a well-defined ring map then $\sigma^*(fg) = \sigma^*(f)\sigma^*(g)$ in $F[x]$. Since $\sigma^*(p)$ is irreducible, we may assume $\deg(\sigma^*(f)) = 0$, but then

$$\begin{aligned} \deg(p) &= \deg(\sigma^*(p)) \\ &= \deg(\sigma^*(f)) + \deg(\sigma^*(g)) \\ &= \deg(\sigma^*(g)) \\ &\leq \deg(g) < \deg(p), \end{aligned}$$

which is a contradiction. So the theorem's statement holds. □

It is also worth mentioning characteristics of fields, and how they can be useful. Knowing the characteristic of a field gives us relations between the fields we study and the rational numbers and the commutative rings $\mathbb{Z}_p$ when p is a prime. It is also a useful concept when considering the solvability of polynomials. We will be mostly looking at fields of characteristic 0 in future sections. Some of the theorems and results used later on will apply to fields with characteristic 0, but not necessarily for fields of higher characteristics.

Definition 2.61. Let K be a field. The smallest possible integer n such that

$$\underbrace{1 + \cdots + 1}_{n \text{ many}} = 0$$

is called the **characteristic of** K and is denoted by $\text{char}(K)$. The characteristic of a field is always a prime. If such number doesn't exist, then we say that the characteristic is 0.

Examples of fields with characteristic zero are $\mathbb{Q}$ and $\mathbb{R}$; no sum of any amount of 1's larger than zero will we get a zero in $\mathbb{Q}$ or $\mathbb{R}$. An example of a field with characteristic larger than zero is $\mathbb{Z}_2$, as we have $[1]_2 + [1]_2 = [2]_2 = [0]_2$. This field has the characteristic $\text{char}(\mathbb{Z}_2) = 2$.

2.2 Field extensions and Galois groups

Galois groups give us a connection between groups and fields, and they can make studying certain qualities of fields and field extensions much simpler. To define what Galois groups and field extensions are, we'll have to define some concepts and notations used in the coming sections.

Rotman (2001) was the main source for this section with some additions from Häsä (2014) and Fraleigh (2003).

Definition 2.62. If F is a subfield of a field E, one also says that E is a **field extension** of F, and one writes E/F is a field extension.

The notation E/F is written as $E : F$ in some literature, but we'll use the former in this text. To be specific, E/F is not the same as forming quotients. The notation is used similarly, and in some sources they are written in the exact same way, but the point of this notation E/F by Rotman in [Rot01] was to emphasize the focus on larger fields E containing F, instead of the subfields F of E (like in the notation F/E for quotients).

A vector space over a field F means the scalars are from F. In the vector space E/F the scalars are from F.

Definition 2.63. The **degree** of a field extension E/F is the dimension of E as a F-vector space. We denote it by $[E : F]$, and it can either be a positive integer or infinity.

For example the extension $\mathbb{C}/\mathbb{R}$ is a finite extension: a basis of $\mathbb{C}$ is $\{1, i\}$, meaning the degree of the field extension is $[\mathbb{C} : \mathbb{R}] = 2$.

Definition 2.64. Let E/F be a field extension, and let $\alpha_1, \ldots, \alpha_n \in E$. Then the $F(\alpha_1, \ldots, \alpha_n)$, called the field obtained by adjoining $\alpha_1, \ldots, \alpha_n$ to F, is the intersection of all the subfields of E which contain F and $\{\alpha_1, \ldots, \alpha_n\}$.

An extension E/F is a **simple extension** if it is obtained by extending F by just one element $\alpha \in E$; that is

$$E = F(\alpha) = \{f(\alpha)/g(\alpha) : \ f(x), g(x) \in F[x] \text{ and } g(\alpha) \neq 0\}.$$

$F(\alpha)$ is the smallest field that contains both F and α.

The elements of a simple extension will get another definition a bit later on. But one easy example of these kinds of extensions is the complex field $\mathbb{C} = \mathbb{R}(i)$ over the field of real numbers.

Definition 2.65. Let $f \in F[x]$ be some polynomial that has roots in the field extension E/F. If $\alpha_1, \ldots, \alpha_n \in E$ are the roots of f, then we may define $F(\alpha_1, \ldots, \alpha_n)$ to be the **splitting field** of $f(x)$ in the extension E.

Example 2.66. Let $f(x) = x^3 - 1 \in \mathbb{Q}[x] = F[x]$. It splits over $\mathbb{C}$, as it can be written as a product of linear factors; if $\omega = e^{2\pi i/3}$ is a cube root of unity, then here

$$f(x) = (x - \omega)(x - \omega^2)(x - 1).$$

Roots of unity will be explained in a future section 3.1. Now the splitting field of $f(x)$ is $\mathbb{Q}(1, \omega, \omega^2) = \mathbb{Q}(\omega)$, as $1 \in \mathbb{Q}$ and $\omega^2 = 1/\omega \in \mathbb{Q}(\omega)$.

Theorem 2.67. *If F is a field, then every polynomial $f(x) \in F[x]$ has a splitting field.*

Proof. By Kronecker theorem 2.58 there exists a field E containing F over which $f(x)$ splits. Let n be the degree of f and let $\alpha_1, \ldots, \alpha_n$ be the roots of f in E. We may define $E = F(\alpha_1, \ldots, \alpha_n)$, and it becomes clear that $f(x)$ splits over E, and $f(x)$ does not split over any proper subfield of E, as it would not then contain some element α_i. □

Definition 2.68. Given a field extension E/F, an **intermediate field** is a field B with $F \subset B \subset E$.

Lemma 2.69 (Degree formula)**.** *If $F \subset B \subset E$ are fields with finite $[E : B]$ and $[B : F]$, then E/F is finite and*

$$[E : F] = [E : B][B : F].$$

Definition 2.70. Let E/F be a field extension, and let $\alpha \in E$. Then α is **algebraic over** F if α is a root of some monic polynomial in $F[x]$; otherwise α is **transcendental over** F**.** A field extension E/F is called **algebraic** if every element of E is algebraic over F.

Theorem 2.71. *If E/F is a finite extension, then it is an algebraic extension.*

Proof. Assume $[E : F] = n$ and that $\alpha \in E$. In any n-dimensional vector space any sequence of $n+1$ vectors is linearly dependent. So there are scalars $c_i \in F$ for $i = 0, 1, \ldots, n$ not all are 0, with

$$\Sigma_{i=0}^{n} c_i \alpha^i = 0.$$

This means that there is a nonzero polynomial $f(x) = \Sigma_{i=0}^{n} c_i x^i$ in $F[x]$ that has α as its root, and so α is algebraic over F. □

By the above theorem the field extension $\mathbb{C}/\mathbb{R}$ is algebraic as it is a finite extension.

Example 2.72. Some examples of algebraic elements.

(i) For example π is transcendental over the field of rational numbers $\mathbb{Q}$; there is no monic polynomial in $\mathbb{Q}[x]$ that has π as its root. To read a proof of this, see *Abstract Modern Algebra* (2015) by Joseph Rotman.

(ii) Let us look at the function $f(x) = x^2 + 1 \in \mathbb{R}[x]$. It has now two complex roots, i and $-i$, and no real roots.

These complex roots are algebraic over $\mathbb{R}$, as they have $f(x)$ as their monic polynomial in $\mathbb{R}[x]$; there are no linear monic polynomials of type $x - a \in \mathbb{R}[x]$ that has i or $-i$ as their root.

The following theorem will be useful for us for determining elements of algebraic field extensions, more specifically in theorem 2.77.

Theorem 2.73 (The Evaluation Homomorphism for Field Theory)**.** *Let F be a subfield of a field E, let β be any element of E, and let x be a variable. The map $\Phi_\beta : F[x] \to E$ defined by*

$$\Phi_\beta(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1\beta + \cdots a_n\beta^n$$

for $a_0 + a_1x + \cdots + a_nx^n \in F[x]$ is a homomorphism of $F[x]$ into E. Also, $\Phi_\beta(x) = \beta$, and Φ_β maps F isomorphically by the identity map; that is $\Phi_\beta(a) = a$ for $a \in F$. The homomorphism Φ_β is an evaluation *at β.*

Proof. The map Φ_β is well defined, meaning, independent of the representation of $f(x) = a_0 + a_1x + \cdots a_nx^n \in F[x]$ as a finite sum, such finite sums can be changed only by insertion or deletion of terms $0x^i$, which does not change the value of $\Phi_\beta(f(x))$.

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $g(x) = b_0 + b_1x + \cdots + b_nx^m$, and without loss of generality we can choose $\deg(f) \leq \deg(g)$, and denote the sum as $h(x) = f(x) + g(x) = c_0 + c_1x + \cdots + c_mx^m$, with $c_i = a_i + b_i$ for all i.

Then

$$\begin{aligned}
\Phi_\beta(f(x) + g(x)) &= \Phi_\beta(h(x)) \\
&= c_0 + c_1\beta + \cdots + c_s\beta^s \\
&= (a_0 + b_0) + (a_1 + b_1)\beta + \cdots + (a_n + b_n)\beta^n + b_{n+1}\beta^{n+1} + \cdots + b_m\beta^m \\
&= (a_0 + a_1\beta + \cdots + a_n\beta^n) + (b_0 + b_1\beta + \cdots + b_n\beta^m) \\
&= \Phi_\beta(f(x)) + \Phi_\beta(g(x)).
\end{aligned}$$

Denoting the multiplication by $f(x)g(x) = d_0 + d_1x + \cdots + d_rx^r$, where by definition of polynomial multiplication $d_j = \Sigma_{i=0}^{j} a_i b_{j-i}$. Now

$$\begin{aligned}\Phi_\beta(f(x)g(x)) &= d_0 + d_1\beta + \cdots + d_r\beta^r \\ &= (a_0 + a_1\beta + \cdots + a_n\beta^n)(b_0 + b_1\beta + \cdots + b_n\beta^m) \\ &= \Phi_\beta(f(x))\Phi_\beta(g(x)).\end{aligned}$$

Thus Φ_β is a homomorphism.

For any constant polynomial $a \in F[x]$ where $a \in F$, the map gives $\Phi_\beta(a) = a$, so Φ_β maps F isomorphically by the identity map. And clearly by the definition of Φ_β we have $\Phi_\beta(x) = \Phi_\beta(1x) = 1\beta = \beta$.

□

Definition 2.74. Suppose $\alpha \in E$ is algebraic over F. The **minimal polynomial** of α is a nonzero monic polynomial $p(x) \in F[x]$, for which $p(\alpha) = 0$ and which is of minimal degree.

The minimal polynomial of an algebraic element α is irreducible and unique, and divides every polynomial which has α as a root. This is fairly easy to prove:

Suppose the minimal polynomial $p(x) \in F[x]$ of α is not irreducible. Then there are some non-constant $f(x), g(x) \in F[x]$ such that $p(x) = f(x)g(x)$ where $0 < \deg(f) < \deg(p)$ and $0 < \deg(g) < \deg(p)$. Then α is a root of at least one of them; without loss of generality we may say $f(\alpha) = 0$. But as $f(x)$ has a smaller degree than $p(x)$, there is a contradiction with $p(x)$ being the minimal polynomial of α. So $p(x)$ is irreducible.

To prove that the minimal polynomial is unique we assume the contrary. So suppose both $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $q(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ for some $0 < n$, are minimal polynomials of α. Then

$$\begin{gathered}f(\alpha) = 0 = g(\alpha) \\ \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = \alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_0\end{gathered}$$

from which we get

$$(a_{n-1} - b_{n-1})\alpha^{n-1} + \cdots + (a_1 - b_1)\alpha + (a_0 - b_0) = 0,$$

which means there is some polynomial $g(x) = (a_{n-1}-b_{n-1})x^{n-1}+\cdots+(a_1-b_1)x+(a_0-b_0)$ in $F[x]$ that has α as its root. But as $g(x)$ has a smaller degree than either $p(x)$ or $q(x)$, it has to be $g(x) = 0$ to avoid contradiction. But then $a_i = b_i$ for all $0 \leq i \leq n$, meaning $p(x) = q(x)$. So the minimal polynomial is unique.

Suppose then that there is some polynomial $f(x) \in F[x]$ that has α as one of its roots and $p(x)$ does not divide $f(x)$. We can write $f(x)$ in the form $g(x)p(x) + r(x)$ where

$q(x), r(x) \in F[x]$ and either $r(x) = 0$ or $0 < \deg(r) < \deg(p)$. Since α is a root of f, we either have $r(x) = 0$ or $r(\alpha) = 0$. But as $\deg(r) < \deg(p)$ the option $r(\alpha) = 0$ would go against $p(x)$ being the minimal polynomial of α, so it has to be that $r(x) = 0$. Therefore any $f(x) \in F[x]$ that has α as one of its roots can be divided by $p(x)$.

Example 2.75. The element $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$. The minimal polynomial of i in $\mathbb{R}[x]$ is $f(x) = x^2 + 1$ as it is a nonzero monic polynomial of minimal degree; there is no linear monic polynomial $x - a \in \mathbb{R}[x]$ that has i as its root.

The minimal polynomial of i in $\mathbb{C}[x]$ on the other hand is $x - i$.

Example 2.76. Let $f(x) = 2x^2 - 2x - 12$, which has real roots 3 and -2. Now 3 is algebraic over $\mathbb{R}$, as it is a root of at least the monic polynomial $\frac{1}{2}f(x) = x^2 - x - 6$.

Now f is a reducible polynomial that can be written as a product of linear polynomials, so we may write it in the form

$$f(x) = 2x^2 - 2x - 12 = 2(x + 2)(x - 3),$$

where the factor $p(x) = x - 3$ is minimal polynomial of 3 (as it is a monic nonzero irreducible polynomial of the smallest degree possible for which $p(3) = 0$).

So any polynomial that can be divided by $p(x)$ with the result still being a polynomial, will have 3 as one of its roots.

With algebraic elements we may define the elements of simple extensions.

Theorem 2.77. *Let E be a simple extension $F(\alpha)$ of a field F, and let α be algebraic over F. Let the degree of the minimal polynomial of α be $n \geq 1$. Then every element β of $E = F(\alpha)$ can be uniquely expressed in the form*

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},$$

where the b_i are in F.

Proof. Using the evaluation homomorphism (2.73) for α the simple extension $F(\alpha)$ can be defined as $\Phi_\alpha(F[x])$, and each element is of the form $\Phi_\alpha(f(x)) = f(\alpha)$, a polynomial at α with coefficients in F. Let

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$$

be the minimal polynomial of α. Then $p(\alpha) = 0$, so

$$\begin{aligned} 0 &= \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \\ \alpha^n &= -a_{n-1}\alpha^{n-1} - \cdots + a_1\alpha - a_0. \end{aligned}$$

This equation in $F(\alpha)$ can be used to express all α^m for which $m \geq n$ in terms of powers of α that are less than n. For example

$$\begin{aligned}\alpha^{n+1} &= \alpha\alpha^n = \alpha(-a_{n-1}\alpha^{n-1} - \cdots + a_1\alpha - a_0) \\ &= -a_{n-1}\alpha^n - \cdots + a_1\alpha^2 - a_0\alpha \\ &= -a_{n-1}(-a_{n-1}\alpha^{n-1} - \cdots - a_0) - a_{n-2}\alpha^{n-1} - \cdots - a_0\alpha\end{aligned}$$

Thus, if $\beta \in F(\alpha)$, β can be expressed in the required form

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}.$$

Then to show the uniqueness of the form: suppose there are some $b_i' \in F$ such that

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = b_0' + b_1'\alpha + \cdots + b_{n-1}'\alpha^{n-1},$$

then there is a polynomial

$$(b_0 - b_0') + (b_1 - b_1')x + \cdots + (b_{n-1} - b_{n-1}')x^{n-1} = g(x)$$

in $F[x]$ with $g(\alpha) = 0$. Now the degree of $g(x)$ is less than the degree of $p(x)$, meaning $g(x)$ has to be zero. Therefore $b_i - b_i' = 0$, meaning $b_i = b_i'$, and so the elements b_i are unique.

□

With the concept of algebraic elements and monic polynomials we can now prove more theorems in previous topics around fields extensions, and show the connection between simple extensions and polynomial rings.

Theorem 2.78. *Let E/F be a field extension, and let $\alpha \in E$ be algebraic over F with its minimal polynomial being $p(x) \in F[x]$. Then*

$$F[x]/(p(x)) \cong F(\alpha);$$

in fact there is an isomorphism $\Phi : F[x]/(p(x)) \to F(\alpha)$, fixing F pointwise, with $\Phi(x + (p(x))) = \alpha$.

Proof. Define $\varphi : F[x] \to E$ to be the function $f(x) \mapsto f(\alpha)$. It is a ring map as it is the restriction of the evaluation mapping $E[x] \to E$ to $F[x]$.

As $(p(x))$ is an ideal of $F[x]$, and clearly $\ker\varphi = (p(x))$, then by first isomorphism theorem (2.35) the map $\Phi : F[x]/(p(x)) \to \operatorname{im}\varphi$, for which $f(x) + (p(x)) \mapsto f(\alpha)$, is an isomorphism. Thus $\Phi : x + (p(x)) \mapsto \alpha$ and $\Phi : c + (p(x)) \mapsto c$ for each $c \in F$. Then identify the subfield $F' = \{c + (p(x)) \colon c \in F\}$ with F, and so one may say that Φ fixes F pointwise.

Finally note that $\operatorname{im}\varphi = \operatorname{im}\Phi = \{f(\alpha) : f(x) \in F[x]\}$ is a subfield of E by 2.56, as $p(x)$ is irreducible. So clearly $F \subset \operatorname{im}\Phi \subset E$ and $\operatorname{im}\Phi$ contains both F and α, so $\operatorname{im}\Phi = F(\alpha)$. □

Theorem 2.79. *Let E/F be a field extension, and let $\alpha \in E$ be algebraic over F, and let $p(x)$ be the minimal polynomial that has α as one of its roots. Then $[F(\alpha) : F] = \deg(p)$.*

Proof. As by theorem 2.78, now $F[x]/(p(x)) \cong F(\alpha)$. So we may choose to prove instead that $[F[x]/(p(x)) : F] = \deg(p(x))$. Denote $K = F[x]/(p(x))$, $I = (p(x))$, and let α represent the element $x + I \in K$. To prove $[K : F] = \deg(p(x))$, it suffices to show that $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is a basis of K over F.

If for $0 \leq i \leq d-1$ there are $c_i \in F$, not all 0, with $\Sigma c_i \alpha^i = 0$, then α is a root of the polynomial $f(x) = c_i x^i$, a polynomial of smaller degree than d. And as $f(\alpha) = 0$ then $f(x) \in I$, but since $\deg(f) < \deg(p)$, this gives us a contradiction with p being a polynomial of the smallest degree with α as a root. Hence $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is linearly independent.

Every element of K has the form $f(x) + I$. By division algorithm there are some $q(x), r(x) \in F[x]$ with $f(x) = q(x)p(x) + r(x)$, where either $r(x) = 0$ or $\deg(r) < \deg(p) = d$. Now clearly $q(x)p(x) + I = I$ and so

$$f(x) + I = (q(x)p(x) + r(x)) + I = r(x) + I.$$

Now $r(x) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1}$ for some $a_0, \ldots, a_{d-1} \in F$, so then

$$f(x) + I = r(x) + I = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1},$$

and as $f(x)$ was arbitrarily chosen and is now a linear combination of the elements in $\{1, \alpha, \ldots, \alpha^{d-1}\}$, hence this set is a basis of K. □

Lemma 2.80. *Let E/F and E'/F' be some extension fields, let $\sigma : F \to F'$ be an isomorphism of fields, let $\sigma^* : F[x] \to F'[x]$, defined by $\Sigma r_i x^i \mapsto \Sigma \sigma(r_i)x^i$, be the corresponding isomorphism of rings, let $p(x) \in F[x]$ be irreducible and let $p^*(x) = \sigma^*(p(x)) \in F'[x]$.*

If $\beta \in E$ is a root of $p(x)$ and $\beta' \in E'$ is a root of $p^*(x)$, then there is a unique isomorphism $\hat{\sigma} : F(\beta) \to F'(\beta')$ extending σ with $\hat{\sigma}(\beta) = \beta'$.

Proof. The mapping $\sigma^* : F[x] \to F'[x]$ carries the ideal $(p(x))$ over onto the ideal $(p^*(x))$. Then by theorem 2.36, there is an isomorphism

$$\varepsilon : F[x]/(p(x)) \to F'[x]/(p^*(x))$$

with $c + (p(x)) \mapsto \sigma(c) + (p^*(x))$ for all $c \in F$ and $x + (p(x)) \mapsto x + (p^*(x))$. By the theorem 2.78 we have the isomorphisms

$$\varphi : F[x]/(p(x)) \to F(\beta) \quad \text{and} \quad \psi : F'[x]/(p^*(x)) \to F'(\beta).$$

We may then define $\hat{\sigma}$ as the composition

$$F(\beta) \xrightarrow{\varphi^{-1}} F[x]/(p(x)) \xrightarrow{\varepsilon} F'[x]/(p^*(x)) \xrightarrow{\psi} F'(\beta').$$

Clearly $\hat{\sigma}$ is an isomorphism as it is a composition of isomorphisms, extending σ to map β to β'. Uniqueness of this mapping follows from theorem 2.84, which will be shown and proven later.

$$\begin{array}{ccc} F[x]/(p(x)) & \xrightarrow{\varphi} & F(\beta) \\ \varepsilon \downarrow & & \downarrow \hat{\sigma} \\ F'[x]/(p^*(x)) & \xrightarrow[\psi]{} & F'(\beta') \end{array}$$

□

Theorem 2.81. *Let $\sigma\colon F \to F'$ be an isomorphism of fields, let $f(x) \in F[x]$, and let $f^*(x) = \sigma^*(f(x))$ be the corresponding polynomial in $F'[x]$; let E be a splitting field of $f(x)$ over F and let E' be a splitting field of $f^*(x)$ over F'.*

(i) There is an isomorphism $\tilde{\sigma}\colon E \to E'$ extending σ.

(ii) If $f(x)$ is separable, then σ has exactly $[E : F]$ many extensions $\tilde{\sigma}$.

$$\begin{array}{ccc} E & \overset{\tilde{\sigma}}{\dashrightarrow} & E' \\ | & & | \\ F & \xrightarrow[\sigma]{} & F' \end{array}$$

Proof. Both proofs will be done by induction, with the part (ii) being a modification of the first one.

(i) If $[E : F] = 1$, then clearly $E = F$ and $f(x)$ is a product of linear factors in $F[x]$. It then follows that $f^*(x)$ is also a product of linear factors, and that $E' = F'$. So we may define $\tilde{\sigma}$ as σ.

If $[E : F] > 1$ we may choose an irreducible factor $p(x)$ of $f(x)$ that has degree 2 or higher, and choose some root β of it, which is also a root of $f(x)$ and then must be in E. Let $p^*(x) = \sigma^*(p(x))$ and let $\beta' \in E'$ be a root of $p^*(x)$. By lemma 2.80 for each such β' there is a unique isomorphism $\hat{\sigma} : F(\beta) \to F'(\beta')$ extending σ with $\hat{\sigma}(\beta) = \beta'$. Now E is a splitting field of f over $F(\beta)$ and similarly E' is a splitting field of f^* over $F'(\beta')$.

As f is a polynomial of at least degree 2, it has finitely many roots, therefore $[E : F]$ is finite. So by the degree formula (2.69) $[E : F] = [E : F(\beta)][F(\beta) : F]$, and as $[F(\beta) : F] \geq 2$, it follows $[E : F(\beta)] < [E : F]$.

By induction, there exists $\tilde{\sigma} : E \to E'$ extending all of the $\hat{\sigma}$ and hence extending σ.

(ii) If $[E : F] = 1$, then $E = F$ and there is only one extension $\tilde{\sigma}$ of σ, specifically σ itself.

If $[E : F] > 1$ and $f(x)$ is separable, let $f(x) = p(x)g(x)$, where $p(x)$ is irreducible and of some degree d. If $d = 1$, then we may replace $f(x)$ with $g(x)$ and study it without loss of generality. If $d > 1$, let us choose a root β of $p(x)$. If $\tilde{\sigma}$ is any extension of σ to E, then $\tilde{\sigma}(\beta) = \beta'$ is a root of $p^*(x)$. Since $f^*(x)$ is separable $p^*(x)$ has exactly d roots $\beta' \in E'$. By lemma 2.80, there are exactly d isomorphisms $\hat{\sigma} : F(\beta) \to F'(\beta')$, for each β', extending σ. Now E is a splitting field of f over $F(\beta)$ and E' is a splitting field of f^* over $F'(\beta')$.

Since $[E : F(\beta)] = [E : F]/[F(\beta) : F] = [E : F]/d$ by theorem 2.79 and 2.69, by induction each of the d isomorphisms $\hat{\sigma}$ has exactly $[E : F]/d$ extensions from $F(\beta)$ to E. Therefore σ has exactly $[E : F]$ many extensions $\tilde{\sigma}$, because every isomorphism τ extending σ has $\tau|F(\beta) =$ some $\hat{\sigma}$.

□

Next automorphisms and the sets of automorphisms will be introduced, along with Galois groups and extensions. These are the first steps into Galois theory beyond the group and field theory we have established prior.

Definition 2.82. If E is a field, then an **automorphism** of E is an isomorphism of E with itself. If E/F is a field extension, then an automorphism σ of E **fixes** F **pointwise** if $\sigma(c) = c$ for every $c \in F$. We denote the set of all automorphisms of E by $\mathrm{Aut}(E)$.

Theorem 2.83. *Let $f(x) \in F[x]$ and let E/F be an extension field of F. If $\sigma\colon E \to E$ is an automorphism fixing F pointwise, and if $\alpha \in E$ is a root of $f(x)$, then $\sigma(\alpha)$ is also a root of $f(x)$.*

Proof. Let $f(x) = \Sigma_{i=0}^{n} c_i x^i$, for which $f(\alpha) = 0$ for some α. Applying σ gives

$$\begin{aligned} 0 = \sigma(0) = \sigma(f(\alpha)) &= \sigma(c_0) + \sigma(c_1)\sigma(\alpha) + \cdots + \sigma(c_n)\sigma(\alpha)^n \\ &= c_0 + c_1\sigma(\alpha) + \cdots + c_n\sigma(\alpha)^n \\ &= f(\sigma(\alpha)), \end{aligned}$$

as σ fixes F. This makes $\sigma(\alpha)$ a root of $f(x)$.

□

Theorem 2.84. *Let F be a field. If σ is an isomorphism of $F(\alpha_1, \ldots, \alpha_n)$ to itself such that $\sigma(\alpha_i) = \alpha_i$, for $i, \ldots, n$, and $\sigma(c) = c \in F$, then σ is the identity.*

Moreover, if E is a field extension of F and if $\sigma, \tau \colon F(\alpha_1, \ldots, \alpha_n) \to E$ fix F pointwise and $\sigma(\alpha_i) = \tau(\alpha_i)$ for all i, then $\sigma = \tau$.

Proof. Let $b = c_0 + c_1\alpha_1 + \cdots + c_n\alpha_n \in F(\alpha_1, \ldots, \alpha_n)$ where $c_1, \ldots, c_n \in F$, and let id denote the identity mapping. Then clearly

$$\begin{aligned}
\sigma(b) &= \sigma(c_0 + c_1\alpha_1 + \cdots + c_n\alpha_n) \\
&= \sigma(c_0) + \sigma(c_1)\sigma(\alpha_1) + \cdots + \sigma(c_n)\sigma(\alpha_n) \\
&= c_0 + c_1\alpha_1 + \cdots + c_n\alpha_n \\
&= id(c_0) + id(c_1)id(\alpha_1) + \cdots + id(c_n)id(\alpha_n) \\
&= id(c_0 + c_1\alpha_1 + \cdots + c_n\alpha_n) \\
&= id(b),
\end{aligned}$$

so σ maps any linear combination of elements in $F(\alpha_1, \ldots, \alpha_n)$ back to themselves, just as the identity mapping does, so $\sigma = id$.

Let $b \in F(\alpha_1, \ldots, \alpha_n)$ be the same as above and let $\sigma, \tau : F(\alpha_1, \ldots, \alpha_n) \to E$ fix F pointwise and $\sigma(\alpha_i) = \tau(\alpha_i)$ for all i. Then

$$\begin{aligned}
\sigma(b) &= \sigma(c_0) + \sigma(c_1)\sigma(\alpha_1) + \cdots + \sigma(c_n)\sigma(\alpha_n) \\
&= c_0 + c_1\sigma(\alpha_1) + \cdots + c_n\sigma(\alpha_n) \\
&= c_0 + c_1\tau(\alpha_1) + \cdots + c_n\tau(\alpha_n) \\
&= \tau(c_0) + \tau(c_1)\tau(\alpha_1) + \cdots + \tau(c_n)\tau(\alpha) \\
&= \tau(b).
\end{aligned}$$

So for any linear combination of elements of $F(\alpha_1, \ldots, \alpha_n)$ we have that $\sigma = \tau$. □

Definition 2.85. Let E/F be a field extension. Its **Galois group** is

$$\mathrm{Gal}(E/F) = \{\text{automorphisms } \sigma \text{ of } E \text{ fixing } F \text{ pointwise}\}$$

under the binary operation of composition. If $f(x) \in F[x]$ has splitting field E, then the Galois group of $f(x)$ is $\mathrm{Gal}(E/F)$.

Galois groups are a fundamental part of Galois theory. They give us a way to study the fields, and additionally polynomials with their coefficients in those fields, in a much simpler way, letting us look at things through isomorphisms. For example, in the next theorem, which will be proved in chapter 4, we are able to find properties of Galois groups and the field extensions through their connections to symmetry groups. This theorem is shared here to provide motivation and insight into the usefulness of Galois groups.

Theorem 2.86. *If $f(x) \in F[x]$ has n distinct roots in its splitting field E, then $Gal(E/F)$ is isomorphic to a subgroup of the symmetric group S_n (definition 4.20), and so its order is a divisor of $n!$.*

Example 2.87. Using the polynomial $f(x) = x^2 + 1$ as an example once more, we know from before that the splitting field of $x^2 + 1$ over $\mathbb{R}$ is $\mathbb{C}$. And as it has two roots, $-i$ and i, the order of the Galois group is $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| \leq 2 = 2!$.

In fact $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = 2$, because the Galois group contains the automorphism

$$\sigma \,:\, z = a + ib \mapsto \bar{z} = a - ib,$$

and the identity automorphism; the above mapping $\sigma \colon \mathbb{C} \to \mathbb{C}$ is clearly an automorphism:

Now for all real elements a of $\mathbb{C}$ map to themselves, $\sigma(a) = a$ (including $\sigma(1) = 1$), clearly fixing $\mathbb{R}$. Now let $a + bi, c + di \in \mathbb{C}$. Then

$$\begin{aligned}
\sigma((a + bi) + (c + di)) &= \sigma((a + c) + (bi + di)) \\
&= a + c - bi - di \\
&= a - bi + c - di \\
&= \sigma(a + bi) + \sigma(c + di),
\end{aligned}$$

and

$$\begin{aligned}
\sigma((a + bi) \cdot (c + di)) &= \sigma((ac - bd) + (adi + bci)) \\
&= ac - bd - adi - bci \\
&= a(c - di) - b(d + ci) \\
&= a(c - di) - bi(c - di) \\
&= (a - bi)(c - di) \\
&= \sigma(a + bi) \cdot \sigma(c + di).
\end{aligned}$$

So the map σ fulfills all the terms to be a homomorphism. And it is clearly a bijection, so it is an automorphism of $\mathbb{C}$.

Example 2.88. Let $E = \mathbb{Q}(\sqrt{2})$. There are now two automorphisms of E fixing $\mathbb{Q}$, the identity automorphism, and for all $a, b \in \mathbb{Q}$

$$\sigma \,:\, a + b\sqrt{2} \;\mapsto\; a - b\sqrt{2}$$

which fixes all elements of $\mathbb{Q}$ and changes the signs of the multiples of $\sqrt{2}$.

There is also a polynomial $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ with E as its splitting field as the roots of $f(x)$ are $\pm\sqrt{2}$, so $\mathrm{Gal}(E/\mathbb{Q})$ is the Galois group of $f(x)$.

Lemma 2.89. *If $f(x) \in F[x]$ is a separable polynomial and if E/F is its splitting field, then*

$$|Gal(E/F)| = [E : F].$$

Proof. Let $F' = F$ and $E' = E$ and the $\sigma\colon F \to F$ to be the identity mapping. By theorem 2.81 as $f(x) = \sigma^*(f(x))$ is separable, then σ has exactly $[E : F]$ many extensions $\tilde{\sigma}\colon E \to E'$ of E fixing F. So $[E : F] = |\mathrm{Gal}(E/F)|$. □

Lemma 2.90. *Let $F \subset B \subset E$ be a tower of fields with B/F the splitting field of some polynomial $f(x) \in F[x]$. If $\sigma \in Gal(E/F)$, then $\sigma|B \in Gal(B/F)$.*

Proof. We may just show that $\sigma(B) = B$. If $\alpha_1, \ldots, \alpha_n$ are the distinct roots of polynomial $f(x) \in F[x]$, then $B = F(\alpha_1, \ldots, \alpha_n)$. Now clearly $\sigma(F) = F$, and $\sigma(\alpha_i) \in B$ for all i by 2.83, then

$$\sigma(B) = \sigma(F(\alpha_1, \ldots, \alpha_n)) = F(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = B.$$

□

Theorem 2.91. *Let $F \subset B \subset E$ be a tower of fields with B/F the splitting field of some polynomial $f(x) \in F[x]$ and E/F the splitting field of some $g(x) \in F[x]$. Then $Gal(E/B)$ is a normal subgroup of $Gal(E/F)$, and*

$$Gal(E/F)/Gal(E/B) \cong Gal(B/F).$$

Proof. Define a new map $\psi\colon \mathrm{Gal}(E/F) \to \mathrm{Gal}(B/F)$ by $\sigma \mapsto \sigma|B$. The previous lemma 2.90 says that ψ does in fact take its values in $\mathrm{Gal}(B/F)$.

Now ψ is clearly a homomorphism, and if $\sigma|B$ is the identity automorphism, then $\sigma \in \mathrm{Gal}(E/B)$ and so $\ker \psi = \mathrm{Gal}(E/B)$. This in turn means that $\mathrm{Gal}(E/B)$ is a normal subgroup of $\mathrm{Gal}(E/F)$.

Next we need to show that ψ is surjective to get the wanted isomorphism. Let $\tau \in \mathrm{Gal}(B/F)$, then by theorem 2.81 there is an automorphism $\tilde{\tau}$ of E with $\psi(\tilde{\tau}) = \tilde{\tau}|B = \tau$. Therefore ψ is surjective and so by the first isomorphism theorem 2.16 we have

$$\mathrm{Gal}(E/F)/\mathrm{Gal}(E/B) \cong \mathrm{Gal}(B/F).$$

Surjectivity gives us proof that the above quotient is isomorphic to $\mathrm{Gal}(B/F)$ and not to just some subgroup of it. □

Theorem 2.92. *Let $f(x) \in F[x]$, let E/F be a splitting field, and let $G = Gal(E/F)$ be the Galois group.*

*(i) If $f(x)$ is irreducible, then G acts **transitively** on the set of all roots of $f(x)$, meaning if α and β are any two roots of $f(x)$ in E, there exists $\sigma \in G$ with $\sigma(\alpha) = \beta$.*

(ii) If $f(x)$ has no repeated roots and G acts transitively on the roots, then $f(x)$ is irreducible.

Proof. (i) To show this we only need to reference lemma 2.80. Let now the isomorphism $\sigma \in G$ in the lemma be the identity automorphism fixing F. Then, as $f(x)$ is irreducible, then by lemma 2.80 for any two roots α and β there is some $\hat{\sigma}\,(\in G)$ for which $\hat{\sigma}(\alpha) = \beta$.

(ii) Let $f(x)$ have no repeated roots and G act transitively on the roots of $f(x)$. We assume the contrary, that $f(x)$ is not irreducible, and so $f(x) = g(x)h(x)$ where $g(x), h(x) \in F[x]$ and $\gcd(g(x), h(x)) = 1$. Let α be a root of $g(x)$. As G acts transitively on the roots of $f(x)$, there has to be an automorphism $\sigma \in G$ such that $\sigma(\alpha)$ is a root of $h(x)$. Therefore by theorem 2.83 $g(x)$ and $h(x)$ have a common root, meaning $f(x)$ has a repeated root, giving us a contradiction with the hypothesis. So it has to be that $f(x)$ is irreducible. □

Definition 2.93. Let $\mathrm{Aut}(E)$ be the group of all the automorphisms of a field E. If G is a subset of $\mathrm{Aut}(E)$, then

$$E^G = \{\alpha \in E : \sigma(\alpha) = \alpha, \text{ for all } \sigma \in G\}$$

is called the **fixed field**.

Now E^G is clearly a subset of E. It is also a field, as for all $a, b \in E^G$ and $\sigma \in G$, then

$$\sigma(a \pm b) = \sigma(a) \pm \sigma(b) = a \pm b,$$
$$\sigma(ab) = \sigma(a)\sigma(b) = ab,$$

and when $b \neq 0_{E^G} = 0_E$

$$\sigma(a/b) = \sigma(a)/\sigma(b) = a/b,$$

meaning E^G is closed under these operations. Also $\sigma(0_E) = 0_E$ and $\sigma(1_E) = 1_E$ as all σ preserve the addition and multiplication identities, so $0_E, 1_E \in E^G$. Thus E^G is a subfield of E, and therefore a field.

Note that $H \subset G\ (\subset \mathrm{Aut}(E))$ implies $E^G \subset E^H$; if $\alpha \in E$ and $\sigma(\alpha) = \alpha$ for all $\sigma \in G$, then $\sigma(\alpha) = \alpha$ for all $\sigma \in H \subset G$.

Here G is a group of automorphisms of E.The operations between the automorphisms here are

$$f + g\colon s \mapsto f(s) + g(s)$$

and

$$fg\colon s \mapsto f(s)g(s),$$

where $f, g\colon E \to E$ and $s \in E$.

There is an interesting example of the relationship between F, E and the Galois group of the field extension E/F using fixed fields: If E/F is a field extension with Galois group $G = \mathrm{Gal}(E/F)$, then

$$F \subset E^G \subset E.$$

Lemma 2.94. *If $G = \{\sigma_1, \ldots, \sigma_n\}$ is a set of automorphisms of E, then*

$$[E : E^G] \geq n.$$

Proof. Assume the opposite, that $[E : E^G] = r < n$, and let $\{\alpha_1, \ldots \alpha_r\}$ be a basis of E/E^G. Consider the linear system over E of r equations in n unknowns:

$$\begin{aligned}
\sigma_1(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_1)x_n &= 0 \\
\sigma_1(\alpha_2)x_1 + \cdots + \sigma_n(\alpha_2)x_n &= 0 \\
&\cdots \\
\sigma_1(\alpha_r)x_1 + \cdots + \sigma_n(\alpha_r)x_n &= 0
\end{aligned}$$

As $r < n$, there is a nontrivial solution $(x_1, \ldots, x_n)$. For any $\beta \in E$, we have $\beta = \Sigma b_i \alpha_i$ where $b_i \in E^G$. Multiply the ith row of the above system by b_i to obtain the system with the ith row;

$$b_i\sigma_1(\alpha_i)x_1 + \cdots + b_i\sigma_n(\alpha_i)x_n = 0.$$

But now $b_i = \sigma_j(b_i)$ for all i, j because $b_i \in E^G$, then the ith row can be written as

$$\sigma_1(b_i\alpha_i)x_1 + \cdots + \sigma_n(b_i\alpha_i)x_n = 0.$$

But then

$$\sigma_1(\beta)x_1 + \cdots + \sigma_n(\beta)x_n = 0,$$

and the independence of the characters $\{\sigma_1, \ldots, \sigma_n\}$ is violated, as β is an arbitrarily chosen element of E. This gives us an contradiction, so $[E : E^G] \geq n$. □

Theorem 2.95. *(p.78) If $G = \{\delta_1, \ldots, \delta_n\}$ is a subgroup of $Aut(E)$, then*

$$[E : E^G] = |G|.$$

Proof. We already know $[E : F^G] \geq n = |G|$ by lemma 2.94, and we want to show that the equality holds here. So let us show that $[E : E^G] \leq |G| = n$ holds too. It will be shown here through an antithesis.

Let $\{\omega_1, \ldots, \omega_{n+1}\}$ be linearly independent vectors in E/E^G. Consider the system of n equations in $n+1$ unknowns

$$\begin{aligned}
\sigma_1(\omega_1)x_1 + \cdots + \sigma_1(\omega_{n+1})x_{n+1} &= 0 \\
\sigma_i(\omega_1)x_1 + \cdots + \sigma_i(\omega_{n+1})x_{n+1} &= 0 \\
&\vdots \\
\sigma_n(\omega_1)x_1 + \cdots + \sigma_n(\omega_{n+1})x_{n+1} &= 0.
\end{aligned}$$

There is a nontrivial solution $(x_1, \ldots, x_{n+1})$ over E. We proceed to normalize it. Choose a solution that has the least number r of nonzero components, say $(a_1, \ldots, a_r, 0, \ldots, 0)$. By reindexing the ω_i we may assume that all nonzero components come first.

A few notes and assumptions next. Note that $r \neq 1$, so as not to have $\sigma_1(\omega_1)a_1 = 0$ imply $a_1 = 0$. Multiplying by its inverse if necessary, we may assume that $a_r = 1$. Not all $a_i \in E^G$ so as not to have the row of the above system corresponding to identity of G violate the linear independence of $\{\omega_1, \ldots, \omega_{n+1}\}$. Assume also that a_1 does not lie in E^G, which can be accomplished by reindexing the ω_i if necessary. There then exists σ_k with $\sigma_k(a_1) \neq a_1$.

The original system has jth row

$$\sigma_j(\omega_1)a_1 + \cdots + \sigma_j(\omega_{r-1})a_{r-1} + \sigma_j(\omega_r) = 0.$$

Applying σ_k to this system we obtain

$$\sigma_k\sigma_j(\omega_1)\sigma_k(a_1) + \cdots + \sigma_k\sigma_j(\omega_{r-1})\sigma_k(a_{r-1}) + \sigma_k\sigma_j(\omega_r) = 0.$$

Since G is a group, $\sigma_k\sigma_1, \ldots, \sigma_k\sigma_n$ is just a permutation of $\sigma_1, \ldots, \sigma_n$. Setting $\sigma_k\sigma_j = \sigma_i$, the system then has ith row

$$\sigma_i(\omega_1)\sigma_k(a_1) + \cdots + \sigma_i(\omega_{r-1})\sigma_k(a_{r-1}) + \sigma_i(\omega_r) = 0.$$

Subtracting this from the original ith row to obtain a new system with the following ith row:

$$\sigma_i(\omega_1)(a_1 - \sigma_k(a_1)) + \cdots + \sigma_i(\omega_{r-1})(a_{r-1} - \sigma_k(a_{r-1})) = 0.$$

Since we had assumed $\sigma_k(a_1) \neq a_1$, we have found a non trivial solution of the original system having fewer than r nonzero components, which brings us to a contradiction. □

Theorem 2.96. *If G, H, are finite subgroups of $Aut(E)$ with $E^G = E^H$, then $G = H$.*

Proof. If $\sigma \in G$, then clearly σ fixes E^G. To prove the converse, suppose σ fixes E^G and $\sigma \notin G$. Then E^G is fixed by the $n+1$ elements in $G \cup \{\sigma\}$, so lemma 2.94 and theorem 2.95 give us the contradiction:

$$n = |G| = [E : E^G] \geq [E : E^{G\cup\{\sigma\}}] \geq n + 1,$$

therefore, if σ fixes E^G, then $\sigma \in G$.

If $\sigma \in G$, then σ fixes $E^G = E^H$, and hence $\sigma \in H$. The reverse inclusion is proved the same way. □

The following theorem connects some of the above definitions and theorems together nicely with Galois groups:

Theorem 2.97. *The following conditions are equivalent for a finite extension E/F with Galois group $G = Gal(E/F)$.*

(i) $F = E^G$;

(ii) every irreducible $p(x) \in F[x]$ with one root in E is separable and has all its roots in E; that is, $p(x)$ splits over E;

(iii) E is a splitting field of some separable polynomial $f(x) \in F[x]$.

Proof. $(i) \Rightarrow (ii)$: Let $p(x) \in F[x]$ be an irreducible polynomial with $\alpha \in E$ as its root, and let the distinct elements of the set $\{\sigma(\alpha) : \sigma \in G\}$ be $\alpha_1, \ldots, \alpha_n$. Now $\alpha = \alpha_i$ for some i.

Define $g(x) \in E[x]$ by

$$g(x) = \Pi_{i=1}^{n}(x - \alpha_i).$$

Each $\sigma \in G$ permutes the α_i so that each σ fixes each of the coefficients of $g(x)$. That is, the coefficients of $g(x)$ lie in $E^G = F$. And so $g(x) \in F[x]$, and has no repeated roots (as all α_i are distinct).

Now $p(x)$ and $g(x)$ have the common root α in E, so their gcd is not 1 in $E[x]$. And by theorem 2.48 their gcd in $F[x]$ is not 1 either. Since $p(x)$ is irreducible, then it must divide $g(x)$. Therefore $p(x)$ has no repeated roots, hence is separable, and it splits over E.

$(ii) \Rightarrow (iii)$: Choose $\alpha_1 \in E$ with $\alpha_1 \notin F$. Since E/F is a finite extension, α_1 must be algebraic over F by theorem 2.71. Let $p_1(x) \in F[x]$ be its irreducible polynomial. By hypothesis $p_1(x)$ is a separable polynomial which splits over E; let $K_1 \subset E$ be its splitting field. If $K_1 = E$ then all is good. If $K_1 \neq E$, choose $\alpha_2 \in E$ with $\alpha_2 \notin K_1$. By hypothesis there is a separable polynomial $p_2(x) \in F[x]$ that has α_2 as a root. Let $K_2 \subset E$ be the splitting field of $p_1(x)p_2(x)$, a separable polynomial.

If $K_2 = E$ then we are done. If not, then we iterate this and keep going with this process. The process must end with some $K_m \subset E$ for some m as E/F is finite.

(iii) $\Rightarrow$ *(i)* By theorem 2.89 we have $[E : F] = |G|$, and by theorem 2.95 we have $|G| = [E : E^G]$, and so

$$[E : F] = |G| = [E : E^G].$$

Since $F \subset E^G$, it follows that $F = E^G$. □

This gives us the term Galois extension; a finite field extension E/F is **Galois** (or normal) if it satisfies any of the equivalent conditions in the above theorem.

Note that $F = E^G$ does not hold true in general. For example, if $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt[3]{2})$, then $\mathrm{Gal}(E/F) = \{1\}$; if $\sigma \in G$, then $\sigma(\sqrt[3]{2})$ is a root of $x^3 - 2$, but E does not contain the other two roots of this polynomial as they are complex. Hence $E^G = E \neq F$.

Definition 2.98. Let E/F be a Galois extension and let B and C be intermediate fields. If there exists an isomorphism $B \to C$ fixing F, then C is called a **conjugate** of B.

Theorem 2.99. *Let E/F be a Galois extension, and let B be an intermediate field. The following conditions are equivalent.*

(i) B has no conjugates other than itself;

(ii) If $\sigma \in Gal(E/F)$, then $\sigma|B \in Gal(B/F)$;

(iii) B/F is a Galois extension.

Proof. (i)$\Rightarrow$(ii) is clear.

(ii)$\Rightarrow$(iii): Let $p(x) \in F[x]$ be some irreducible polynomial with some root β in B. As $B \subset E$ and E/F is Galois, then by theorem 2.97 $p(x)$ is a separable polynomial with all its roots in E. Let $\beta' \in E$ be one of those roots. By 2.80 there is an isomorphism $\tau : F(\beta) \to F(\beta')$, which by theorem 2.81 extends to $\sigma \in \mathrm{Gal}(E/F)$ as E/F is Galois. By condition (ii) we have that $\sigma(B) = B$, so $\beta' = \sigma(\beta) \in \sigma(B) = B$, meaning B contains all of the roots of $p(x)$, and so $p(x)$ splits in B. And as $p(x)$ splits in B, by 2.97 B/F is Galois.

(iii)$\Rightarrow$(i): As B/F is Galois, it is a splitting field of some polynomial $f(x) \in F[x]$, so $B = F(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are all the roots of $f(x)$. By the proof of 2.83 we can see that any injection $\nu : B \to E$ fixing F permute the roots of $f(x)$. Therefore

$$\nu(B) = \nu(F(\alpha_1, \ldots, \alpha_n)) = F(\nu\alpha_1, \ldots, \nu\alpha_n) = B.$$

So there can be no conjugates of B other than itself.

□

Theorem 2.100. *If E/F is a Galois extension and B is an intermediate field, then E/B is a Galois extension.*

Proof. Suppose $f(x) \in F[x] \subset B[x]$ is some separable polynomial with E being its splitting field. Then $f(x)$ clearly is a separable polynomial in $B[x]$ with E being its splitting field, and so by theorem 2.97 E/B is Galois.

□

2.3 Lattices and intermediate fields

Here are some definitions and theorems that will be needed for The Fundamental Theorem of Galois Theory and its proof. We will be using lattices in the context of towers of sets and define the bounds in a lattice by using intersections and unions of sets.

This section is mainly based on [Rot01]. More on lattices and partially ordered sets can be found in [Jac85].

Definition 2.101. A **partially ordered set** is a set L together with relation $a \leq b$ satisfying the following conditions:

- $a \leq a$ (reflexivity),
- If $a \leq b$ and $b \leq a$ then $a = b$ (anti-symmetry),
- If $a \leq b$ and $b \leq c$, then $a \leq c$ (transitivity).

If also $a \leq b$ or $b \leq a$ for all $a, b \in \mathcal{P}$, then the set L is said to have linear order.

Definition 2.102. A **lattice** is a partially ordered set $(L, \preceq)$ in which each pair of elements $a, b \in L$ has a least upper bound $a \vee b$ and a greatest lower bound $a \wedge b$.

For example, if X is a set, and let L be the family of all subsets of X, and define $A \leq B$ to mean $A \subset B$ when $A, B \in L$, then L is a lattice with

$$A \vee B = A \cup B \quad \text{and} \quad A \wedge B = A \cap B.$$

Definition 2.103. When B and C are subfields of E, their **compositum** $B \vee C$ is the intersection of all the subfields of E containing B and C.

One use of this this definition is with field extensions, like in the definition 2.64: For a field extension E/F, and elements $\alpha_1, \ldots, \alpha_n \in E$, the field $F(\alpha_1, \ldots, \alpha_n)$ is the intersection of all the subfields of E which contain F and $\{\alpha_1, \ldots, \alpha_n\}$.

Theorem 2.104. *If $\alpha_1, \ldots, \alpha_n \in E \supset F$, then*

$$F(\alpha_1) \vee \cdots \vee F(\alpha_n) = F(\alpha_1, \ldots, \alpha_n)$$

is an extension of F.

Proof. Let $B_1, B_2, \ldots$ be the subfields of E containing each $F(\alpha_i)$ for $i = 1, \ldots, n$. Then by definition

$$F(\alpha_1) \vee F(\alpha_2) \vee \cdots \vee F(\alpha_n) = \cap_{j=1}^{\infty} B_j.$$

Clearly $F(\alpha_1, \ldots, \alpha_n) \subset \cap_{j=1}^{\infty} B_j$ as all B_j contain both F and the adjoined elements $\alpha_1, \ldots, \alpha_n$.

Suppose then there is some $x \in \cap_{j=1}^{\infty} B_j$ for which $x \notin F(\alpha_1, \ldots, \alpha_n)$. Then for every j we have $x \in B_j$. Remember, that $F(\alpha_1, \ldots, \alpha_n)$ is a subfield of E by definition that contains F and each α_i, so it also contains each $F(\alpha_i)$. Therefore $F(\alpha_1, \ldots, \alpha_n) = B_j$ for some j. But then $x \in F(\alpha_1 \ldots, \alpha_n)$, which is a contradiction with how we picked x. So $\cap_{j=1}^{\infty} B_j \subset F(\alpha_1, \ldots, \alpha_n)$.

Therefore $\cap_{j=1}^{\infty} B_j = F(\alpha_1) \vee F(\alpha_2) \vee \cdots \vee F(\alpha_n) = F(\alpha_1, \ldots, \alpha_n)$. □

Another concrete example using lattices with field extensions:

Example 2.105. Let E/F be a field extension, let $\mathrm{Lat}(E/F)$ be the **family of all intermediate fields**, and define $B \preceq C$ to mean $B \subset C$ when $B, C \in \mathrm{Lat}(E/F)$. Then $\mathrm{Lat}(E/F)$ is a lattice with $B \vee C$ being their compositum and $B \wedge C = B \cap C$.

We will be using lattices of fields in the next section.

Theorem 2.106. *If L and L' are lattices and $\gamma : L \to L'$ is a bijection such that both γ and γ^{-1} are **order reversing** (i.e. $a \preceq b$ implies $\gamma(b) \preceq \gamma(a)$), then*

$$\gamma(a \vee b) = \gamma(a) \wedge \gamma(b) \quad \text{and} \quad \gamma(a \wedge b) = \gamma(a) \vee \gamma(b).$$

A proof for this theorem can be found in Rotman's book [Rot01] on page 84.

Example 2.107. If G is a group, let $\mathrm{Sub}(G)$ be the **family of all the subgroups of** G, and define $H \preceq K$ to mean $H \subset K$ (when $H, K \in \mathrm{Sub}(G)$). Then $\mathrm{Sub}(G)$ is a lattice with $H \vee K$ the subgroup generated by H and K, and $H \wedge K = H \cap K$.

2.4 Fundamental Theorem of Galois Theory

Now The Fundamental Theorem of Galois Theory (FTGT) will be introduced and proved. The version of Fundamental Theorem of Galois Theory presented here is from Rotman's book *Galois Theory* [Rot01]. In other literature this theorem may have only the parts (1), (4) and (5) with the other parts combined to the other ones or left out as their own lemmas or theorems.

Theorem 2.108 (Fundamental Theorem of Galois Theory)**.** *Let E and F be finite fields, and let E/F be a Galois extension with Galois group $G = Gal(E/F)$.*

1. *The function $\gamma : Sub(G) \to Lat(E/F)$, defined by $H \mapsto E^H$, is an order reversing bijection with inverse $\delta : B \mapsto Gal(E/B)$.*
2. *$E^{Gal(E/B)} = B$ and $Gal(E/E^H) = H$.*
3. $$\begin{aligned} E^{H\vee K} &= E^H \cap E^K; \\ E^{H\cap K} &= E^H \vee E^K; \\ Gal(E/B \vee C) &= Gal(E/B) \cap Gal(E/C); \\ Gal(E/B \cap C) &= Gal(E/B) \vee Gal(E/C). \end{aligned}$$
4. *$[B : F] = [G : Gal(E/B)]$ and $[G : H] = [E^H : F]$.*
5. *B/F is a Galois extension if and only if $Gal(E/B)$ is a normal subgroup of G.*

Proof. 1. Let the function $\gamma : \mathrm{Sub}(G) \to \mathrm{Lat}(E/F)$ be defined by $H \mapsto E^H$.

Now if $H \subset K$ when $H, K \in \mathrm{Sub}(G)$ then $E^K \subset E^H$, in other words, $\gamma(K) = E^K \subset E^H = \gamma(H)$. So γ is order reversing.

By theorem 2.96 the mapping γ is injective, as for any $H, K \in \mathrm{Sub}(G)$, if $E^K = E^H$, then $K = H$. For surjectivity, consider the composite

$$\mathrm{Lat}(E/F) \xrightarrow{\delta} \mathrm{Sub}(G) \xrightarrow{\gamma} \mathrm{Lat}(E/F),$$

for which $\gamma \circ \delta : B \mapsto \mathrm{Gal}(E/B) \mapsto E^{\mathrm{Gal}(E/B)}$.

Now by 2.100 E/F being Galois implies that E/B is Galois for every intermediate field B, which by theorem 2.97 gives $B = E^{\mathrm{Gal}(E/B)}$. Therefore $\gamma\delta$ is the identity and γ has to be surjective. It then follows that δ is an inverse of γ that is bijective.

2. As γ is bijective and it has an inverse δ, making $\gamma \circ \delta$ and $\delta \circ \gamma$ the same as the identity mapping, the statements $E^{\mathrm{Gal}(E/B)} = B$ and $\mathrm{Gal}(E/E^H) = H$ hold:

$$B \overset{\delta}{\mapsto} \mathrm{Gal}(E/B) \overset{\gamma}{\mapsto} E^{\mathrm{Gal}(E/B)},$$

and

$$H \overset{\gamma}{\mapsto} E^H \overset{\delta}{\mapsto} \mathrm{Gal}(E/E^H).$$

3. The order reversing bijection γ gives us

$$E^{H \vee K} = \gamma(H \vee K) = \gamma(H) \wedge \gamma(K) = E^H \cap E^K,$$

and

$$E^{H \cap K} = \gamma(H \wedge K) = \gamma(H) \vee \gamma(K) = E^H \vee E^K.$$

The following two equations follow from δ also being an order reversing bijection:

$$\mathrm{Gal}(E/(B \vee C)) = \delta(B \vee C) = \delta(B) \wedge \delta(C) = \mathrm{Gal}(E/B) \cap \mathrm{Gal}(E/C),$$

and

$$\mathrm{Gal}(E/(B \cap C)) = \delta(B \wedge C) = \delta(B) \vee \delta(C) = \mathrm{Gal}(E/B) \vee \mathrm{Gal}(E/C).$$

4. Using the Degree formula 2.69 and lemma 2.89

$$\begin{aligned}[B : F] &= [E : F]/[E : B] \\ &= |\mathrm{Gal}(E/F)|/|\mathrm{Gal}(E/B)| \\ &= [G : \mathrm{Gal}(E/B)].\end{aligned}$$

So the degree of B/F is the index of $\mathrm{Gal}(E/B)$ in G.

Now as $F \subset E^H \subset E$ and $H = \mathrm{Gal}(E/E^H)$, then

$$\begin{aligned}[G : H] &= [\mathrm{Gal}(E/F) : H] \\ &= [E : F] : |H| \\ &= [E : E^H][E^H : F] : |\mathrm{Gal}(E/E^H)| \\ &= [E^H : F].\end{aligned}$$

5. "B/F is a Galois extension if and only if $\mathrm{Gal}(E/B)$ is a normal subgroup of G."

Proof in the first direction, that if B/F is Galois then $\mathrm{Gal}(E/B)$ is a normal subgroup of G:

Now B is such that $F \subset B \subset E$, and let $G = \mathrm{Gal}(E/F)$ and $\mathrm{Gal}(B/F)$ to be Galois groups. Theorem 2.91 says that B/F being Galois implies $\mathrm{Gal}(E/B)$ is then a normal subgroup of G.

Then the proof in the other direction, that if $\mathrm{Gal}(E/B)$ is a normal subgroup of $G = \mathrm{Gal}(E/F)$ then B/F is Galois:

Suppose $H = \mathrm{Gal}(E/B)$ is a normal subgroup of G. If $\sigma \in G$, $\tau \in H$, and $\alpha \in E^H$, then $\tau\sigma(\alpha) = \sigma\tau'(\alpha)$ for some $\tau \in H$ by normality of H in $\mathrm{Gal}(E/F)$ in the theorem 2.91, and $\sigma\tau'(\alpha) = \sigma(\alpha)$ because τ' fixes α. Now $\alpha \in E^H$ implies $\sigma(\alpha) \in E^H$, meaning that $\sigma(E^H) \subset E^H$.

In fact, $\sigma(E^H) = E^H$ because both have the same dimension over F. Then by 2.99, $E^H/F = E^{\mathrm{Gal}(E/B)}/F = B/F$ is a Galois extension.

□

With this theorem plenty of mathematical problems can be solved and different theorems can be proved; for example, using FTGT we could prove the Fundamental Theorem of Algebra or solve different types of ruler-compass problems. To read more on those, see [Rot01]. This theorem also provides connections between intermediate fields and subgroups, that are useful in the end when proving the Abel-Ruffini theorem. We will prove this theorem in section 4.3.

Chapter 3

Polynomials and solution formulas

We have defined polynomials, groups, and fields in the previous chapter, and will now move on to the concept of *solvability* in the context of polynomials.

In this chapter we will first introduce roots of unity and then show how some classical solution formulas were formed. The classical solution formulas give us insight into how centuries ago mathematicians and scientists would start to formulate, or start to wonder *how* to formulate solution formulas for different types of polynomials, and if it was possible for polynomials of higher and higher degrees.

But when we are talking about solvability, what do we mean? By *solving* a polynomial, we generally are talking about finding its roots. One could try to find them by trial and error, but there are some more efficient ways.

We can sometimes express the roots of a polynomial in terms of its coefficients and field operations: we say a polynomial is **solvable by radicals** when there is an expression for its roots in terms of its coefficients, the field operations and extraction of roots.

A classic example of such an expression that one might remember from primary school is the quadratic formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

that can give us the solutions of any general quadratic equation $ax^2 + bx + c = 0$ where, for example, $a, b, c \in \mathbb{R}$.

This concept will be useful when constructing solution formulas for polynomial equations of different degrees.

3.1 Roots of unity

Roots of unity are useful for finding roots of polynomials, and they are used in the next section about classical solution formulas. For this we will give a brief introduction to cyclic groups, based on an appendix in [Rot01], and some chapters in [HR16] and [Fra03] on the topic.

Definition 3.1. A group G is called a **cyclic group**, if G is generated by some element $g \in G$. This group can then be denoted by $G = \langle g \rangle$.

Cyclic groups are also abelian, and all their subgroups and quotient groups are also cyclic. If the cyclic group has order n, the elements of a cyclic group G with the generator g can be written as some power of g, meaning if $a \in G$ then $a = g^m$ for some $m \in \mathbb{N}$, where $m \leq n$. The cyclicity of the group comes from the fact that for n we have $g^n = 1$, where 1 is the identity element of G. We call this n the order of the element g. We can also write the cyclic group in the following form:

$$\langle g \rangle = \{1, g^1, g^2, \ldots, g^{n-1}\}.$$

Roots of unity in this case are the elements of the above group, written with the form g^k, where $0 \leq k \leq n-1$.

Lemma 3.2. *If p is a prime, then every group G of order p is cyclic.*

Proof. If $g \in G$ and $g \neq 1$, then g has order $d > 1$ which is a divisor of p. But as p is a prime, it has to be that $d = p$, meaning G is generated by g, and is therefore cyclic. □

Theorem 3.3. *(i) If $a \in G$ is an element of order n, then $a^m = 1$ if and only if $n \mid m$.*

(ii) If $G = \langle a \rangle$ is a cyclic group of order n, then a^k is a generator of G if and only if the greatest common divisor of n and k is 1.

Proof. (i) Let $a \in G$ be an element of order n. Suppose $a^m = 1$. Then either $m < n$ or $m \geq n$. If $m < n$, then m is the order of a, contradicting how n was defined. If $m = n$, clearly $n \mid m$. Suppose then that $m > n$ and that $n \nmid m$. Then there are some $k, r \in \mathbb{N}$ for which $m = kn + r$ where $0 < r < n$. Recall, that for any $k \in \mathbb{Z}$ we have $a^{kn} = 1$. Then

$$1 = a^m = a^{kn+r} = a^{kn}a^r = a^r,$$

but as $0 < r < n$ then $a^r \neq 1$, contradicting $a^m = 1$. So it has to be that $m = kn$ for some $k \in \mathbb{Z}$, meaning $n \mid m$.

Suppose then that $n \mid m$. Then there is some $k \in \mathbb{Z}$ for which $m = nk$, and meaning $g^m = g^{nk} = (g^n)^k = 1$.

(*ii*) Recall that two integers are relatively prime if and only if some integral linear combination of them is 1. Two elements are relatively prime when there are no common factors but 1, meaning their greatest common divisor is 1.

Let $G = \langle a \rangle$ be a cyclic group of order n. Suppose a^k is a generator of G, then $a \in \langle a^k \rangle$ so that $a = a^{kt}$ for some $t \in \mathbb{Z}$. Then

$$\begin{aligned} a &= a^{kt} \\ a^{kt}a^{-1} &= 1 \\ a^{kt-1} &= 1. \end{aligned}$$

By the previous part (*i*), $n \mid kt - 1$, meaning there is some $u \in \mathbb{Z}$ with $nu = kt - 1$. Therefore 1 is a linear combination of k and n, so their gcd is 1.

Suppose their gcd is 1, then there are some $t, u \in \mathbb{Z}$ such that $nu + kt = 1$. Therefore

$$a = a^{nu+kt} = a^{nu}a^{kt} = a^{kt} \in \langle a^k \rangle$$

So every power of a also lies in $\langle a^k \rangle$, and so $G = \langle a \rangle$. □

Definition 3.4. Let n be a positive integer. An element α of a field is an n**th root of unity** if $\alpha^n = 1$.

Theorem 3.5. *Let n be a positive integer. The solutions of the equation $z^n = 1$ in $\mathbb{C}$ form a cyclic group $\mathbb{C}_n$ or order n. The group is generated by the element*

$$e^{2\pi i/n}.$$

For example, the roots of $x^3 - 1$ are 1, $e^{2\pi i/3}$ and $e^{4\pi i/3}$.

Theorem 3.6. *The set of all nth roots of unity in a field E form a group under multiplication.*

Proof. Define $X \subset E$ as the set of all nth roots of unity.

Firstly, multiplication is associative and commutative in X as it is in the field E, meaning for any $x, y, z \in X$ we have $(xy)z = x(yz)$ and $xy = yx$. The set X contains an unique identity element 1_X which is also the identity of the field E, and for which $1_X^n = 1_X$. For any $x, y \in X$ we have

$$(xy)^n = x^n y^n = 1_X,$$

so $xy \in X$. For all x there is an inverse $x^{-1} \in X$, since

$$(x^{-1})^n = (x^n)^{-1} = 1_X^{-1} = 1_X.$$

So the set X is a group under multiplication. □

The type of elements depends on the field E and its characteristic. If the field is of characteristic zero, then the nth roots of unity are algebraic complex numbers, and the group is in fact the cyclic group $X = \mathbb{C}_n$. This is seen above in the theorem 3.5. We will be focusing on fields of characteristic zero, so to read more about this topic for fields of other characteristics, see [Rot15].

Definition 3.7. Let n be a fixed positive integer and let F be a field. A generator of the group of all nth roots of unity is called a **primitive root of unity**.

For example, a primitive root of unity in $\mathbb{C}$ is $e^{2\pi i/n}$, which happens to be the generator of $\mathbb{C}_n$ mentioned in theorem 3.5.

Recall the theorem 2.22: if R is a ring, then it has a multiplicative group of units, $U(R)$. In particular,

$$U(\mathbb{Z}_n) = \{[i] \in \mathbb{Z}_n : \gcd(i, n) = 1\}.$$

And when p is a prime we have $U(\mathbb{Z}_p) = \mathbb{Z}_p^{\#}$, where $\mathbb{Z}_p^{\#}$ is the multiplicative group of all nonzero elements of $\mathbb{Z}_p$.

Theorem 3.8. *If F is a field and $E = F(\alpha)$, where α is a primitive nth root of unity, then Gal(E/F) is isomorphic to a subgroup of $U(\mathbb{Z}_n)$, and hence Gal(E/F) is an abelian group.*

Proof. Now every $\sigma \in \mathrm{Gal}(E/F)$ is determined by its value on α, meaning: if $\sigma(\alpha) = \alpha^i$ for some unique $i \mod n$, we may denote $\sigma = \sigma_i$ where $0 \leq i \leq n-1$. Theorem 3.3 says that i has to be relatively prime to n, for $\sigma|\langle\alpha\rangle$ is an automorphism of $\langle\alpha\rangle$. Therefore the function $\psi : \sigma \mapsto [i]$ is a function $\psi : \mathrm{Gal}(E/F) \to U(\mathbb{Z}_n)$. This ψ is now a homomorphism, as

$$\sigma_j\sigma_i(\alpha) = \sigma_j(\alpha^i) = (\alpha^i)^j = \alpha^{ij} = \alpha^{ji},$$

hence $\psi(\sigma_j\sigma_i) = [ji] = [j][i] = \psi(\sigma_j)\psi(\sigma_i)$. By theorem 2.84 the map ψ is injective. Therefore $\mathrm{Gal}(E/F)$ is isomorphic to a subgroup of $U(\mathbb{Z}_n)$. □

Theorem 3.9. *Let F contain a primitive nth root of unity, and let $f(x) = x^n - c \in F[x]$. If E/F is a splitting field of $f(x)$ then there is an injection*

$$\varphi\colon G = \mathit{Gal}(E/F) \to \mathbb{Z}_n.$$

Moreover, $f(x)$ is irreducible if and only if φ is surjective.

Proof. Let ω be a primitive nth root of unity, and if α is a root of $f(x)$ given above, then $\alpha^n = c$, and all the roots of $f(x)$ are $\alpha, \alpha\omega, \ldots, \alpha\omega^{n-1}$. If $\sigma \in G$, then $\sigma(\alpha) = \alpha\omega^i$ for some i and σ is now determined by that i. Define then $\varphi(\sigma) = [i]$ if $\sigma(\alpha) = \alpha\omega^i$.

Next we show that $\varphi : G \to \mathbb{Z}_n$ is a homomorphism, where $\mathbb{Z}_n$ is the additive group. If $\tau \in G$, then $\tau(\omega) = \omega$ because $\omega \in F$ and $\tau(\alpha) = \alpha\omega^j$ for some j. Therefore

$$\begin{aligned}\tau\sigma : \alpha \mapsto \alpha\omega^i &\mapsto \tau(\alpha\omega^i) \\ &= \tau(\alpha)\tau(\omega^i) \\ &= (\alpha\omega^j)\omega^i \\ &= \alpha\omega^{j+i},\end{aligned}$$

so now $\varphi(\tau\sigma) = [j+i] = \varphi(\tau) + \varphi(\sigma)$, meaning φ is a homomorphism. And as $\varphi(id) = [0]$ with no other automorphism mapping to $[0]$ in $\mathbb{Z}_n$ (by theorem 2.84), we have that $\ker\varphi = \{id\}$ and so by lemma 2.15 φ is injective.

Now φ is surjective if and only if G acts transitively on the roots of $f(x)$. By theorem 2.92 there is an equivalence between G acting transitively on the roots of $f(x)$ and $f(x)$ being irreducible. Therefore φ is surjective if and only if $f(x)$ is irreducible.

□

Corollary 3.10. *Let p be a prime, let F be a field containing a primitive pth root of unity, and let $f(x) = x^p - c \in F[x]$ have a splitting field E. Then either $f(x)$ splits and $Gal(E/F) = 1$ or it is irreducible and $Gal(E/F) \cong \mathbb{Z}_p$.*

Proof. Let us consider the mapping $\mathrm{Gal}(E/G) \to \mathbb{Z}_p$. If f splits, then $\mathrm{Gal}(E/F) = \{id\}$ and its image is trivial. If $f(x)$ does not split, then its image is a nontrivial subgroup of $\mathbb{Z}_p$. But the only subgroups of $\mathbb{Z}_p$ are the trivial subgroup and $\mathbb{Z}_p$ itself, so then the map must be surjective, meaning $\mathrm{Gal}(E/F) \cong Z_p$ and $f(x)$ is irreducible.

□

3.2 Some classical solution formulas

This section is based on Rotman's [Rot01] introduction to classical formulas for finding roots of polynomials, and how they were constructed. The introductions to Viète's trigonometric solution formula to the cubics are excluded from this, but the reader may find them from Rotman's book.

Theorem 3.11. *If $f(X) = a_nX^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots$, then replacing X by $x - (a_{n-1}/n)$ gives a reduced polynomial*

$$\tilde{f}(x) = f(x - \frac{a_{n-1}}{n})$$

where $\tilde{f}$ now doesn't have a x^{n-1} term. Moreover, if u is a root of $\tilde{f}(x)$, then $u - (a_{n-1}/n)$ is a root of f(X).

Proof. The first part is clear as a straightforward calculation (which can be seen in the next example). And the latter part follows from $0 = \tilde{f}(u) = f(u - (a_{n-1}/n))$. □

Example 3.12. Let $f(X) = X^2 + 2X - 1$. It has two real roots $-\sqrt{2} - 1$ and $\sqrt{2} - 1$. Now the reduced polynomial

$$\begin{aligned}\tilde{f}(x) &= f(x - \frac{2}{2}) = f(x - 1)\\ &= (x-1)^2 + 2(x-1) - 1\\ &= x^2 - 2x + 1 + 2x - 2 - 1\\ &= x^2 - 2,\end{aligned}$$

and has roots $u_1 = \sqrt{2}$ and $u_2 = -\sqrt{2}$. Clearly, for either root u_i of $\tilde{f}(x)$, $u_i - (2/2) = u_i - 1$ is a root of $f(X)$.

Using the above theorem 3.11 we can find solution formulas for quadratics, cubics and quartics. To introduce the quartic solution formula we will use method constructed by Descartes.

3.2.1 Quadratic solution formula

If we consider the quadratic

$$f(X) = X^2 + bX + c$$

and substitute X by $x - \frac{1}{2}b$, we get the reduced quadratic

$$\begin{aligned}\tilde{f}(x) &= f(x - \frac{1}{2}b)\\ &= (x - \frac{1}{2}b)^2 + b(x - \frac{1}{2}b) + c\\ &= x^2 - b + \frac{1}{4}b^2 + bx - \frac{1}{2}b^2 + c\\ &= x^2 + c - \frac{1}{4}b^2,\end{aligned}$$

that has roots $u = \pm\frac{1}{2}\sqrt{b^2 - 4c}$. By the previous lemma 3.11 we obtain the formula for the roots of the original quadratic

$$-\frac{1}{2}b \pm \frac{1}{2}\sqrt{b^2 - 4c}.$$

Example 3.13. In the previous example we had the polynomial $f(X) = X^2 + 2X - 1$, and the roots were given. But to find the roots we could use the above solution formula:

$$-\frac{1}{2} \cdot 2 \pm \frac{1}{2}\sqrt{2^2 + 4 \cdot 1} = -1 \pm \frac{\sqrt{8}}{2} = -1 \pm \sqrt{2}.$$

Reminder: to use the solution formulas given in this section, our polynomials have to be monic. So if for example we were to find the roots for the polynomial $5x^2 + 3x - 1$, one can easily turn it monic by dividing it by the leading coefficient, which here is 5. So the monic form for this polynomial would be $x^2 + \frac{3}{5}x - \frac{1}{5}$.

3.2.2 Cubic solution formula

For the solution formula for the cubic polynomials, we need some temporary notations and constraints, but otherwise this formulation of it goes similarly as above. So, for the cubic

$$g(X) = X^3 + aX^2 + bX + c$$

has a reduced form $\tilde{g}(x) = x^3 + qx + r$. By lemma 3.11 we have that a formula for the roots of $\tilde{g}(x)$ will give a formula for the roots of the original one. Let u be a root of $\tilde{g}(x)$, and choose numbers y and z such that $u = y + z$. Then

$$\begin{aligned} u^3 &= (y+z)^3 \\ &= (y+z)(y^2 + z^2 + 2yz) \\ &= y^3 + z^3 + 3y^2z + 3yz^2 \\ &= y^3 + z^3 + 3uyz. \end{aligned}$$

Therefore

$$\tilde{g}(u) = y^3 + z^3 + u(3yz + q) + r = 0. \tag{3.14}$$

Using the previous constraint $u = y+z$ for the root, we want to use another constraint using y and z, namely yz in the above equation.

To find such constraint we may consider the following situation: If we have a polynomial

$$p(x) = (x-a)(x-b) = x^2 - (a+b)x + ab,$$

finding its roots a and b we can find the terms $a + b$ and ab. Using this idea, it is easy to find a form needed for the term yz in our case, when we have the given root $u = y + z$.

Next we want the linear term $3yz+q$ to vanish in (3.14), so we may use the constraint that $yz = -q/3$. Then we have

$$\begin{aligned} y^3 + z^3 + u(3(-q/3) + q) + r &= 0 \\ y^3 + z^3 &= -r, \end{aligned}$$

and

$$\begin{aligned} y^3 z^3 &= -q^3/27 \\ \Leftrightarrow \quad z^3 &= \frac{q^3}{27y^3} \\ \Leftrightarrow \quad z &= \frac{q}{3y}. \end{aligned} \tag{3.15}$$

Solving the former equation for y^3 using the latter one, we get

$$\begin{aligned} y^3 - \frac{q^3}{27y^3} &= -r \\ y^6 + ry^3 - q^3/27 &= 0. \end{aligned}$$

Using the quadratic solution formula to solve for y^3, we get

$$\begin{aligned} y^3 &= \frac{1}{2}(-r + \sqrt{r^2 + 4q^3/27}) \\ \Leftrightarrow \quad y &= \sqrt[3]{\frac{1}{2}(-r + \sqrt{r^2 + 4q^3/27})}. \end{aligned} \tag{3.16}$$

Combining the information from above equations 3.15 and 3.16 we have then found the root $u = y + z = y - \frac{q}{3y}$ of $\tilde{g}(x)$.

To find the two other roots of $\tilde{g}(x)$, we will use roots of unity. If $\omega = e^{2\pi i/3}$ is a cube root of unity then we have three values for y:

$$y, \quad \omega y, \quad \omega^2 y.$$

The corresponding values for z are

$$z = -\frac{q}{3y}, \quad \omega z = \frac{q}{3\omega^2 y}, \quad \text{and} \quad \omega^2 z = \frac{-q}{3\omega y}.$$

In conclusion, the roots of the cubic polynomial $\tilde{g}(x)$, and the original polynomial, are

$$y + z, \quad \omega y + \omega^2 z, \quad \text{and} \quad \omega^2 y + \omega z,$$

with the formula

$$y^3 = \frac{1}{2}(-r + \sqrt{R}) \tag{3.17}$$

where $R = r^2 + 4q^3/27$ and $z = -q/3y$.

Example 3.18. Let $f(X) = X^3 - X$. Using the above formula (3.17), now $q = -1$ and $r = 0$, so

$$\begin{aligned} y^3 &= \frac{1}{2}(-r + \sqrt{r^2 + 4q^3/27}) \\ &= \frac{1}{2}\sqrt{-4/27} \\ &= \frac{\sqrt{-4}}{2}\frac{1}{\sqrt{27}} \\ &= \frac{i}{3\sqrt{3}} \\ \Leftrightarrow \quad y &= \frac{1}{2} + \frac{i}{2\sqrt{3}} \end{aligned}$$

and

$$\begin{aligned} z = -q/3y &= \frac{1}{3 \cdot (\frac{1}{2} + \frac{i}{2\sqrt{3}})} \\ &= \frac{2}{3 + i\sqrt{3}} \\ &= \frac{1}{2} - \frac{i}{2\sqrt{3}}. \end{aligned}$$

Then the roots of $f(x)$ are

$$\begin{aligned} y + z &= (\frac{1}{2} + \frac{i}{2\sqrt{3}}) + (\frac{1}{2} - \frac{i}{2\sqrt{3}}) = 1, \\ \omega y + \omega^2 z &= e^{2\pi i/3}(\frac{1}{2} + \frac{i}{2\sqrt{3}}) + e^{4\pi i/3}(\frac{1}{2} - \frac{i}{2\sqrt{3}}) = -1, \\ \omega^2 y + \omega z &= e^{4\pi i/3}(\frac{1}{2} + \frac{i}{2\sqrt{3}}) + e^{2\pi i/3}(\frac{1}{2} - \frac{i}{2\sqrt{3}}) = 0. \end{aligned}$$

Example 3.19. We want to find the roots of the polynomial $f(X) = X^3 - 15X - 4$. To

use the formula (3.17), here $q = -15$ and $r = -4$. Then

$$\begin{aligned} y^3 &= \frac{1}{2}(4 + \sqrt{16 - 4 \cdot 15^3/27}) \\ &= 2 + \sqrt{-121} \\ &= 2 + 11i \\ \Leftrightarrow \quad y &= \sqrt[3]{2 + 11i}, \end{aligned}$$

and

$$\begin{aligned} z &= -\frac{-15}{3y} \\ &= \frac{5}{\sqrt[3]{2 + 11i}}. \end{aligned}$$

Then the roots are

$$\begin{aligned} y + z &= \sqrt[3]{2 + 11i} + \frac{5}{\sqrt[3]{2 + 11i}}, \\ \omega y + \omega^2 z &= e^{2\pi i/3}\sqrt[3]{2 + 11i} + e^{4\pi i/3}\frac{5}{\sqrt[3]{2 + 11i}}, \\ \omega^2 y + \omega z &= e^{4\pi i/3}\sqrt[3]{2 + 11i} + e^{2\pi i/3}\frac{5}{\sqrt[3]{2 + 11i}}. \end{aligned}$$

The complex looking expressions can in this case be written more simply, as 4, $-2 - \sqrt{3}$ and $\sqrt{3} - 2$. Simplifying the roots is not always possible but this example shows us the kind of expressions this solution formula gives us.

Example 3.20. Let $f(X) = X^3 + 2X^2$. Then the reduced form of it is $\tilde{f}(x) = f(x - 2/3) = x^3 - \frac{4}{3}x + \frac{16}{27}$. With the formula (3.17) we have $q = -\frac{4}{3}$ and $r = \frac{16}{27}$, and so

$$\begin{aligned} y^3 &= \frac{1}{2}(-\frac{16}{27} + \sqrt{(\frac{16}{27})^2 + \frac{4}{27}(-\frac{4}{3})^3}) \\ &= -\frac{8}{27} + \frac{1}{2}\sqrt{\frac{256}{729} - \frac{4}{27} \cdot \frac{64}{27}} \\ &= -\frac{8}{27} + \frac{1}{2}\sqrt{\frac{4}{27} \cdot \frac{64}{27} - \frac{4}{27} \cdot \frac{64}{27}} \\ &= -\frac{8}{27}, \end{aligned}$$

from where we get

$$\begin{aligned} y &= \sqrt[3]{-\frac{8}{27}} = \frac{2}{3}e^{2i\pi/6} \\ &= \frac{1}{3} + \frac{i}{\sqrt{3}}. \end{aligned}$$

The form $y = \frac{2}{3}e^{(i\pi)/3}$ will be used in the next steps as it is simplifies the next step. Then also

$$\begin{aligned} z &= -(-\frac{4}{3})/(3 \cdot (\frac{2}{3}e^{2i\pi/6}) \\ &= \frac{4}{3} \cdot \frac{1}{2}e^{-2i\pi/6} \\ &= \frac{2}{3}e^{-2i\pi/6} \\ &= \frac{1}{3} - \frac{i}{\sqrt{3}}. \end{aligned}$$

So the roots of $\tilde{f}(x)$ are

$$\begin{aligned} y + z &= \frac{1}{3} + \frac{i}{\sqrt{3}} + \frac{1}{3} - \frac{i}{\sqrt{3}} \\ &= \frac{2}{3}, \end{aligned}$$

and, using the other forms for y and z,

$$\begin{aligned} \omega y + \omega^2 z &= e^{2\pi i/3}\frac{2}{3}e^{2i\pi/6} + e^{4\pi i/3}\frac{2}{3}e^{-2i\pi/6} \\ &= \frac{2}{3}(e^{i\pi} + e^{i\pi}) = \frac{2}{3}(-1-1) = -\frac{4}{3}, \end{aligned}$$

and it happens that $y + z = \omega^2 y + \omega z$:

$$\begin{aligned} \omega^2 y + \omega z &= e^{4\pi i/3}\frac{2}{3}e^{2i\pi/6} + e^{2\pi i/3}\frac{2}{3}e^{-2i\pi/6} \\ &= \frac{2}{3}e^{2i\pi/6} + \frac{2}{3}e^{-2i\pi/6} \\ &= \frac{2}{3} = y + z. \end{aligned}$$

So this polynomial happens to have two roots instead of three, and they are $-\frac{4}{3}$ and $\frac{2}{3}$. Then by lemma 3.11 the roots of the original polynomial $f(X)$ are $-\frac{4}{3} - \frac{2}{3} = -2$ and $\frac{2}{3} - \frac{2}{3} = 0$.

3.2.3 Quartic solution formula

Let us next consider the quartic polynomial

$$X^4 + aX^3 + bX^2 + cX + d.$$

Setting $X = x - (a/4)$, we get the reduced polynomial

$$h(x) = x^4 + qx^2 + rx + s.$$

Again, by lemma 3.11, a formula for the roots of $h(x)$ gives us the formula for the roots of the original polynomial.

Let's write the polynomial in the following form:

$$x^4 + qx^2 + rx + s = (x^2 + kx + l)(x^2 - kx + m),$$

where we will determine k, l and m. Expanding the right side

$$\begin{aligned} x^4 + qx^2 + rx + s &= x^4 - kx^3 + mx^2 + kx^3 - k^2x^2 + kmx + lx^2 - klx + lm \\ &= x^4 + (l + m - k^2)x^2 + (km - kl)x + lm \end{aligned}$$

and equating the terms gives us:

$$l + m - k^2 = q; \tag{3.21}$$

$$km - kl = r; \tag{3.22}$$

$$lm = s. \tag{3.23}$$

Finding the value of m from the equation (3.22) we get

$$\begin{aligned} km - kl &= r \\ km &= r + kl \\ m &= \frac{r}{k} + l \end{aligned}$$

then inputting that to equation (3.21)

$$\begin{aligned} l + m - k^2 &= q \\ l + \frac{r}{k} + l - k^2 &= q \\ 2l &= k^2 - \frac{r}{k} + q. \end{aligned}$$

Similarly we can find that $2m = k^2 + \frac{r}{k} + q$. Inputting them to the last equation of (3.23) gives us

$$\begin{aligned} lm &= s \qquad || \cdot 4 \\ 4lm &= 4s \\ (k^2 - \frac{r}{k} + q)(k^2 + \frac{r}{k} + q) &= 4s \\ k^4 + 2qk^2 - \frac{r^2}{k^2} + q^2 &= 4s \qquad || \cdot k^2 \\ k^6 + 2qk^4 + (q^2 - 4s)k^2 - r^2 &= 0. \end{aligned}$$

By replacing $y = k^2$, we get a cubic polynomial, and using the cubic solution formula we can find values for k, l and m are, and then we can determine the roots of $h(x)$ and the original quartic formula.

Example 3.24. Let $f(x) = x^4 - 15x^2 - 20x - 6 \in \mathbb{R}[x]$. We will show here two ways of finding the roots in this case. The equation can be written in the form

$$f(x) = (x + 3)(x + 1)(x^2 - 4x - 2),$$

where $x^2 - 4x - 2$ has roots $2 \pm \sqrt{6}$ by the quadratic solution formula, therefore the roots of $f(x)$ are

$$-3, \quad -1, \quad 2 - \sqrt{6}, \quad \text{and} \quad 2 + \sqrt{6}.$$

Using the quartic solution formula method, we have that

$$f(x) = x^4 - 15x^2 - 20x - 6 = (x^2 + kx + l)(x^2 - kx + m)$$

from which we get the cubic in k^2:

$$k^6 - 30k^4 + 249k^2 - 400,$$

and using the cubic solution formula we have the roots 16, $7 + 2\sqrt{6}$ and $7 - 2\sqrt{6}$ for the above formula in k^2. From there we can easily figure out $l = 3$ and $m = -2$ when $k = 4\,(= +\sqrt{16})$ (and $l = -2$ and $m = 3$ when $k = -4\,(= -\sqrt{16})$ and so on), and find the roots

$$-1, \quad -3, \quad 2 - \sqrt{6}, \quad \text{and} \quad 2 + \sqrt{6}.$$

There have also been different types of solution formulas through out history for different types of polynomials of degrees ≤ 4. For example, the dal Ferro-Tartaglia-Cardano formula [Liv05] to find a root of a cubic of the form $x^3 + px - q = 0$ is

$$\sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}},$$

which has a fairly complicated look to it. In fact, mathematicians used to study thirteen different forms of cubics [Liv05], where some terms were missing or negative, as they did not have a general solution formula yet.

As time went on and mathematicians and scientists found new ways to solve a polynomial for higher and higher degrees, one may have started to wonder why could it not be formed similarly for the quintics.

Different forms of fifth degree polynomial equations do have solution formulas (similarly to how cubics had plenty of formulas as mentioned above) but there is no *general* solution formula for quintics, as we will find out in section 4.3 when proving the Abel-Ruffini theorem.

A simple example of the type of fifth degree polynomial that we can solve easily is $f(x) = x^5 - a$, where $a \in \mathbb{C}$: it is easy to see that one root of $f(x)$ is $\sqrt[5]{a}$, and with the primitive root of unity one can find all the other roots:

$$\sqrt[5]{a}, \qquad \omega\sqrt[5]{a}, \qquad \omega^2\sqrt[5]{a}, \qquad \omega^3\sqrt[5]{a}, \qquad \text{and} \qquad \omega^4\sqrt[5]{a}.$$

3.2.4 A brief look into symmetric polynomials

Here is a brief introduction to *symmetric polynomials* with multiple variables. By calling polynomials symmetric we mean that the polynomial does not change if we were to change the order of its variables, in other words, we are able to permute the variables. For example the polynomials

$$x^2 + 2xy + y^2, \quad x^2 - xy + y^2, \quad \text{and} \quad xy + xz + yz,$$

with variables x, y and z are symmetric polynomials. As said before, we will not go more in depth into polynomials with multiple variables, but this concept is useful when figuring out the roots of polynomials with one variable. Say we have a polynomial

$$f(x) = X^n + s_{n-1}X^{n-1} + \cdots + s_1X + s_0$$

with coefficients $s_1, \ldots, s_{n-1}$ in some field $F \subset E$. Assume the polynomial has n roots and that they are $x_1, \ldots, x_n \in E$. The roots are not necessarily distinct, but using all its roots the polynomial can be expressed as

$$\begin{aligned} f(x) &= X^n + s_{n-1}X^{n-1} + \cdots + s_1X + s_0 \\ &= (X - x_1)(X - x_2)\cdots(X - x_n). \end{aligned}$$

From this equality we get that each s_i is some *elementary symmetric polynomial* consisting of only the roots $x_1, \ldots, x_n$ and operations of the field F. The s_i are in the form

$$\begin{aligned} s_{n-1} &= -(x_1 + \cdots + x_n), \\ s_{n-2} &= x_1x_2 + x_1x_3 + \cdots + x_2x_3 + \ldots x_{n-1}x_n \\ &\vdots \\ s_0 &= (-1)^n x_1 \cdots x_n. \end{aligned}$$

These are also called *Vieta's formulas*. We will be using these symmetric polynomials in the proof of the Abel-Ruffini theorem in the end of next chapter.

Chapter 4

Further group and field theory, and solvability of groups

When thinking of the words *solvable* or *solvability* in context of mathematics, the general public usually thinks of different types of numerical or geometrical problems and may come to think of polynomials and equations. By solving polynomials, we usually mean finding the roots of the polynomials like in the previous chapter. But what does it mean when a group is solvable? And how are Galois groups and field extensions connected to this concept? In this chapter we will answer these questions.

To prove Abel-Ruffini theorem, we will have to introduce symmetric groups and their solvability. First some more group theory will be introduced, along side the concept of solvability, then permutations and symmetry groups. After that we can connect solvability to field extensions through Galois groups and symmetry groups. All of the following sections are based on Rotman's book (2001) on Galois theory, with some theorems from Häsä (2014), Clark (1984) and Fraleigh (2003).

4.1 More group theory

In the following part about group theory and the theorems and definitions about solvability we will assume the groups to be finite, as we will mainly apply this concept to finite symmetry groups in this thesis. Some of these definitions and theorems do work for infinite groups too, but not all will.

Theorem 4.1. *Let H and N be subgroups of group G, and let N be normal. Then $H \cap N$ is a normal subgroup of N.*

Proof. First we show $H \cap N \subset G$ is a subgroup of G. Let $g, h \in H \cap N$, then $g, h \in H$ and $g, h \in N$. Therefore as H and N are subgroups of G as

- $gh \in H$ and $gh \in N$ means $gh \in H \cap N$;
- as $1_G \in H$ and $1_G \in N$ then $1_G \in H \cap N$;
- for all $g \in H \cap N$ we have $g^{-1} \in H \cap N$ as $g^{-1} \in H$ and $g^{-1} \in N$.

Hence $H \cap N \leq G$. With the same logic, as $H \cap N \subset N$, we find $H \cap N \leq N$.

Next we show that $H \cap N$ is normal in N. Let $g \in N$ and $x \in H \cap N$. Then clearly $g \in G$ also. As N is a normal subgroup of G, we know that for all $n \in N$ and for any $g \in G$ we have $gng^{-1} \in N$.

Since $H \leq G$ is closed in G, then for all $x \in H \cap N$ and for all $g \in N$ (and hence $g \in G$) we also have $gxg^{-1} \in H$. Similarly, for any $x \in H \cap N$ we get that $gxg^{-1} \in N$. Therefore for any $x \in H \cap N$ and $g \in N$ we have $gxg^{-1} \in H \cap N$, meaning $H \cap N$ is a normal subgroup of N. □

This first theorem gives us some useful information about normal subgroups and their intersections with other groups. This will be important when discussing some subgroups of different symmetry groups in the next subsection 4.1.1.

Next we will take a look at the some more advanced algebra and group theory, that graduate level students should know. For further reading on this level see [Fra03] or [Rot15].

Definition 4.2. A group G *acts* on a set X if there is a function

$$G \times X \to X,$$

denoted by $(g, x) \mapsto g \cdot x$, such that

(i) $1_G \cdot x = x$ for all $x \in X$;

(ii) $(gh) \cdot x = g \cdot (h \cdot x)$ for all $x \in X$ and for all $g, h \in G$.

Definition 4.3. If group G acts on a set X and $x \in X$, then the **orbit** of x is

$$\mathcal{O}(x) = \{g \cdot x : g \in G\} \subset X,$$

and the **stabilizer** of x is the subgroup

$$G_x = \{g \in G : g \cdot x = x\} \subset G.$$

A group G acts *transitively* on X if, for each $x, y \in X$, there exists $g \in G$ with $g \cdot x = y$. In this case $\mathcal{O}(x) = X$.

Definition 4.4. Two elements x and y in a group G are called **conjugate** if there exists $g \in G$ with $y = gxg^{-1}$.

Definition 4.5. Every group G acts on itself by conjugation. So define action $g \cdot x = gxg^{-1}$.

The orbit $\mathcal{O}(x)$ of $x \in G$ is its *conjugacy class*:

$$\{y \in G : y = gxg^{-1} \text{ for some } g \in G\};$$

the stabilizer of x can now also be written as

$$G_x = \{g \in G : x = g \cdot x = gxg^{-1}\}.$$

Definition 4.6. The **center** of a group G is

$$Z(G) = \{g \in G : gx = xg \quad \text{for all} \quad x \in G\}$$

and the **centralizer** of x in G is

$$\begin{aligned} C_G(x) &= \{g \in G : gx = xg\} \\ &= \{g \in G : gxg^{-1} = x\} \end{aligned}$$

It is easy to see from the definition of center that $Z(G)$ is an abelian normal subgroup of G.

The difference between the definitions of a stabilizer and a centralizer of some $x \in G$, is the focus in the definitions; the group acting on the set is in focus in the definition of the stabilizer, while in the centralizer the commutativity of elements on the element x is the important part.

Theorem 4.7. *If $x \in G$, then*

$$\textit{the number of conjugates of } x = [G : C_G(x)].$$

Proof. Define $\varphi : \mathcal{O}(x) \to \{$ the family of all cosets of G_x in $G\}$ by

$$\varphi(gxg^{-1}) = gG_x.$$

Now φ is well defined, as for any $g, h \in G$ if $gxg^{-1} = hxh^{-1}$, then $h^{-1}gxg^{-1}h = x$, meaning $h^{-1}g \in G_x$, and so $gG_x = hG_x$.

For injectivity, assume that $\varphi(gxg^{-1}) = \varphi(hxh^{-1})$ where $g, h \in G$. Then $gG_x = hG_x$, meaning $h^{-1}g \in G_x$, from which we get

$$\begin{aligned} h^{-1}gx(h^{-1}g)^{-1} &= x \\ h^{-1}gx &= xh^{-1}g \\ gxg^{-1} &= hxh^{-1}, \end{aligned}$$

which means that φ is injective.

The map φ is surjective as a coset gG_x is $\varphi(g \cdot x)$; for every gG_x there is some $g \cdot x$ in the conjugacy class of x. Hence φ is a bijection, and

$$|\mathcal{O}(x)| = [G : G_x].$$

□

Theorem 4.8. *Every normal subgroup H of G is a union of conjugacy classes of G.*

Proof. For all $h \in H$ we have $ghg^{-1} \in H$ for all $g \in G$, then

$$\mathcal{O}(h) = \{ghg^{-1} : g \in G\} \subset H.$$

As h was arbitrary, then for all $h \in H$ we have $\bigcup_{h \in H} \mathcal{O}(h) \subset H$. As all h are in $\bigcup_{h \in H} \mathcal{O}(h)$, clearly $H \subset \bigcup_{h \in H} \mathcal{O}(h)$. So $H = \bigcup_{h \in H} \mathcal{O}(h)$. □

Definition 4.9. A *normal series* of a group G is a sequence of subgroups

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = \{1\}$$

with each G_{i+1} a normal subgroup of G_i. A quotient group G_{i+1}/G_i is called a *factor* of the sequence.

A group may have many different normal series with different factors, and not all subgroups in the sequence have to be normal subgroups of G.

Theorem 4.10 (Correspondence Theorem)**.** *Let K be a normal subgroup of G, and let S^* be a subgroup of $G^* = G/K$.*

(i) There is a unique intermediate subgroup S, meaning $K \subset S \subset G$, with $S/K = S^*$;

(ii) If S^* is a normal subgroup of G^*, then S is normal in G;

(iii) $[G^* : S^*] = [G : S]$;

(iv) If T^* is normal in S^*, then T is normal in S and

$$S^*/T^* \cong S/T.$$

Proof. (i) Define $S = \{x \in G \ : \ xK \in S^*\}$. Now clearly $S/K = S^*$ by the definition of S. As the natural map $\pi : G \to G/K$ is a group homomorphism, and as for any group homomorphism, a preimage of a subgroup $S^* \leq G/K$ is also a subgroup ([HR16] page 235). Therefore $S = \pi^{-1}(S/K)$ is a subgroup of G.

(ii) If $g \in G$, and $x \in S$, then

$$gxg^{-1}K = gKxKg^{-1}K = (gK)(xK)(gK)^{-1} \in S^*,$$

as S^* is normal in G^*; therefore $gxg^{-1} \in S$.

(iii)

$$\begin{aligned}[G^* : S^*] &= |G^*|/|S^*| = |G/K|/|S/K| \\ &= (|G|/|K|)/(|S|/|K|) \\ &= |G|/|S| = [G : S].\end{aligned}$$

(iv) T is normal in S by (ii), and

$$S^*/T^* = (S/K)/(T/K) \cong S/T,$$

by the third isomorphism theorem.

□

Now we can move on to solvable groups. By connecting some definitions and theorems from the section above we get the definition of solvable groups:

Definition 4.11 (Solvable group)**.** A group G is called a **solvable group** if it has a normal series with abelian factor groups.

Lemma 4.12. *Every finite abelian group $G \neq \{1\}$ contains a subgroup of prime index.*

Proof. First we show that if G has a composite order rs, then G has a proper subgroup. Let $x \in G$ with $x \neq 1$. If x has order smaller than rs, then $\langle x \rangle$ is a proper subgroup. Otherwise x has order rs, and so $\langle x^r \rangle$ is a proper subgroup.

The proof of the lemma is done by induction on the number k of (not necessarily distinct) prime factors of $|G|$. If $k = 1$, then G has prime order and $\{1\}$ has prime index. If $k > 1$, then by the first paragraph of this proof clearly G has to have a proper subgroup H. This H is necessarily normal as G is abelian, and so the quotient group G/H is defined. By induction G/H has a subgroup S^* of prime index, and the correspondence theorem 4.10 gives a subgroup S of G of prime index. □

Theorem 4.13. *A finite group $G \neq \{1\}$ is solvable if and only if G has a normal series with factor groups of prime order.*

Proof. Assuming G has a normal series with factor groups of prime order, one can recall that groups of prime order are cyclic, resulting in them being abelian. And so G has a normal series with abelian factors, and has to be solvable.

For proving the other direction, we prove it by induction on $|G|$. Assume that $G \neq \{1\}$ is solvable and

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

is a normal series of G with abelian factor groups. We may also assume that $G \neq G_1$. By previous lemma 4.12 G/G_1 must contain some subgroup S^* of prime index. By the correspondence theorem 4.10 there is an intermediate normal subgroup S such that $G \supset S \supset G_1$, for which $S^* = S/G_1$. Then we note that

$$[G : S] = |G| : |S| = (|G| : |G_1|) : (|S| : |G_1|) = [G/G_1 : S^*]$$

where $[G/G_1 : S^*]$ is a prime number, meaning G/S is also of prime order. Now S is a solvable group (as G is solvable) and has the normal series

$$S \supset G_1 \supset \cdots \supset G_n = \{1\},$$

where the factor groups are now abelian; now S/G_1 is abelian as a subgroup of the abelian G/G_1 group. And by induction we find a normal series of S with factor groups of prime order. Continuing this line of thought induction provides a normal series of G with factor groups of prime order. □

Definition 4.14. The **commutator** of elements $a, b \in G$ in a group is

$$[x, y] = xyx^{-1}y^{-1}.$$

The **commutator subgroup** G' of G is the subgroup generated by all the commutators. It is good to note that the product of two commutators may not be a commutator. Note also that G' is a normal subgroup of G, for if $a \in G$, then

$$\begin{aligned} a[x, y]a^{-1} &= axyx^{-1}y^{-1}a^{-1} \\ &= axya^{-1}(ax^{-1}y^{-1}a^{-1}) \\ &= axa^{-1}aya^{-1}(ax^{-1}a^{-1}\, ay^{-1}a^{-1}) \\ &= (axa^{-1})(aya^{-1})((axa^{-1})^{-1}(aya^{-1})^{-1}) \\ &= [axa^{-1}, aya^{-1}]. \end{aligned}$$

Moreover, G/G' is abelian, which follows from the next lemma 4.16.

Definition 4.15. The **higher commutator subgroups** are defined inductively:

$$G^{(0)} = G; \qquad G^{(i+1)} = G^{(i)\prime};$$

that is, $G^{(i+1)}$ is the commutator subgroup of $G^{(i)}$.

Lemma 4.16. *If H is a normal subgroup of G, then G/H is abelian if and only if $G' \subset H$.*

Proof. If G/H is abelian, then for all $x, y \in G$

$$xyH = xHyH = yHxH = yxH,$$

so that

$$xyx^{-1}y^{-1}H = H \quad \text{and so} \quad xyx^{-1}y^{-1} \in H.$$

Thus $G' \subset H$. Suppose then that $G' \subset H$; by the third isomorphism theorem 2.18 G/H is a quotient group of the abelian group G/G', and hence it is abelian. □

Lemma 4.17. *A group G is solvable if and only if $G^{(n)} = \{1\}$ for some n.*

Proof. If G is solvable, then there is some normal series

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

with each factor group G_i/G_{i+1} abelian. We will prove by induction on i, that $G_i \supset G^{(i)}$; as then, when $i = n$, we will have $\{1\} = G_n \supset G^{(n)}$, meaning $G^{(n)} = G_n = \{1\}$.

If $i = 0$, then clearly $G_i = G_0 = G = G^{(0)}$. Assume then by induction that $G_i \supset G^{(i)}$. Then $G_i' \supset G^{(i)\prime} = G^{(i+1)}$. But by lemma 4.16 G_i/G_{i+1} being abelian implies $G_{i+1} \supset G_i'$, and so $G_{i+1} \supset G^{(i+1)}$.

Conversely, if $G^{(n)} = \{1\}$, then

$$G = G^{(0)} \supset G^{(1)} \supset \cdots \supset G^{(n)} = \{1\}$$

is a normal series with abelian factor groups since the factor groups are abelian by the previous lemma. Hence G is solvable. □

Theorem 4.18. *If G is a solvable group, then every subgroup H and every quotient group of G is also solvable.*

Proof. It is easy to prove by induction that $H^{(i)} \subset G^{(i)}$ for all i:

When $i = 0$, clearly $H^{(0)} = H \subset G = G^{(0)}$. Assume by induction then $H^{(k)} \subset G^{(k)}$, then clearly

$$H^{(k+1)} = H^{(k)\prime} \subset G^{(k)\prime} = G^{(k+1)}.$$

From there we get $H^{(n)} \subset G^{(n)}$ where now $G^{(n)} = \{1\}$ implies $H^{(n)} = \{1\}$ and so H is solvable.

Let $K = G/N$ be a quotient group (with N being normal) and $\pi : G \to K$ the natural map of G onto K. If $uvu^{-1}v^{-1}$ is a commutator in K, we can choose by surjectivity some $x, y \in G$ with $\pi(x) = xN = u$ and $\pi(y) = yN = v$, then

$$\begin{aligned}\pi(xyx^{-1}y^{-1}) &= (xyx^{-1}y^{-1})N \\ &= xNyNx^{-1}Ny^{-1}N \\ &= xNyN(xN)^{-1}(yN)^{-1} \\ &= uvu^{-1}v^{-1},\end{aligned}$$

therefore $\pi(G') \supset K'$. Then let $x, y \in G$, and we get the same result as above, that $\pi(xyx^{-1}y^{-1}) = xNyN(xN)^{-1}(yN)^{-1} \in K'$. So $\pi(G') \subset K'$.

It is also easy to prove by induction that $\pi(G^{(i)}) = K^{(i)}$. Therefore, if G is solvable, then $G^{(n)} = \{1\}$ for some n and $K^{(n)} = \{1\}$; and so K is solvable. So quotient groups of G are also solvable. □

Theorem 4.19. *Let G be a group with normal subgroup H. If H and G/H are solvable groups, then G is solvable.*

Proof. Let

$$G/H = G^* \supset G_0^* \supset \cdots \supset G_m^* = \{1\}$$

be a normal series of G/H with abelian factor groups. By the correspondence theorem 4.10, from this series we can then define a new series

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = H$$

with each G_i being normal in G_{i-1} and with abelian factor groups. Since H is solvable, there is a normal series

$$H = H_0 \supset H_1 \supset \cdots \supset H_n = \{1\}$$

with abelian factor groups. Combining these two series together we get a normal series of G with abelian factor groups:

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = H = H_0 \supset H_1 \supset \cdots \supset H_n = \{1\}.$$

So G is also solvable. □

4.1.1 Symmetry groups

Next, our focus will be on alternating groups and subgroups of symmetry group S_n. It is assumed that the reader has at least a base level knowledge of symmetry groups and permutations, and the notations that come with them.

Definition 4.20. A **permutation** of a set is a bijection from the set to itself. Let $n > 0$ and $N_n = \{1, 2, \ldots, n\} \subset \mathbb{N}$. All the permutations of the set N_n form the **symmetric group** under composition, denoted by S_n. It has order $n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$.

The symmetric group of some set X can be notated by S_X.

Example 4.21. Let $N_3 = \{1, 2, 3\}$ with the symmetric group S_3, which has $3! = 6$ elements. Now the possible permutations of these elements are

$$(1)(2)(3) = (1), \quad (123), \quad (132), \quad (23), \quad (12) \text{ and } (13).$$

One may also notate the permutations in a 2-line notation, for example elements $(123), (12) \in S_3$ can be written as

$$(123) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \text{and} \quad (12) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Two permutations are said to be *disjoint* if one permutation permutes some elements while the other fixes them and permutes some other elements. For example two permutations $(ab), (cd) \in S_X$, where $X = \{a, b, c, d\}$, clearly permute different elements of X. One can also notice that disjoint permutations commute, meaning $(ab)(cd) = (cd)(ab)$.

Any permutation can be written as a product of 2-cycles (sometimes referred to as *transpositions*), for example, the element (123) in S_3 can be written as $(12)(23)$. A permutation is said to be *even* if the amount of 2-cycles in this product of transpositions is even, and *odd* if it is odd. The property of evenness or oddness is called *parity*:

Definition 4.22. Suppose that $\sigma \in S_n$ is composed (or can be notated as a composition) of t transpositions. Then the *parity* of σ is

$$sgn(\sigma) = (-1)^t = \begin{cases} 1, & \text{when } \sigma \text{ is even} \\ -1, & \text{when } \sigma \text{ is odd.} \end{cases}$$

Theorem 4.23. *JH s. 26, lause 3.3*

For all $\alpha, \beta \in S_n$

$$sgn(\alpha\beta) = sgn(\alpha)sgn(\beta),$$

meaning the mapping $sgn : S_n \to (\{-1, 1\}, \cdot)$ is a group homomorphism.

Proof of this can be found in [Rot15].

Definition 4.24. The kernel of the parity mapping

$$\ker(sgn) = \{\sigma \in S_n : \sigma \text{ is even}\}$$

is called the *alternating group* and is notated by A_n. It consists of all even permutations and has order $\frac{1}{2}n!$.

Example 4.25. The alternating group A_3 consists of the elements

$$(1), \quad (123) \text{ and } (132).$$

Definition 4.26. Two permutations $\sigma, \tau \in S_n$ are said to be *conjugates* if there exists $\upsilon \in S_n$ with $\tau = \upsilon\sigma\upsilon^{-1}$.

Permutations also have *conjugacy classes*, a set consisting of all the conjugates of the given permutation. When dealing with multiple groups and their similar permutations, say the permutation (1) of a group G or a group H, we may denote the conjugacy classes of (1) of each group by ${}^{G}(1)$ and ${}^{H}(1)$.

Example 4.27. The alternating group A_3 has three conjugacy classes:

$$\{(1)\}, \quad \{(12), (13), (23)\}, \quad \{(123), (132)\}.$$

The classes consist of 1-cycles of the form (a), 2-cycles of the form (ab) and 3-cycles of the form (abc).

Lemma 4.28. *The alternating group A_n is generated by the 3-cycles.*

Proof. If $\alpha \in A_n$, then $\alpha = \tau_1 \cdots \tau_m$, where each τ_i is a transposition (a cycle of two elements), and m is even. Then

$$\alpha = (\tau_1\tau_2)(\tau_3\tau_4)\cdots(\tau_{m-1}\tau_m).$$

If two sequent transpositions τ_{2k-1} and τ_{2k} are *not* disjoint, meaning $\tau_{2k-1}\tau_{2k} = (ab)(ac)$ for some $a, b, c \in \{1, 2, 3, 4, 5\}$, then their product is a 3-cycle; $\tau_{2k-1}\tau_{2k} = (ab)(ac) = (acb)$. And if they are disjoint, then

$$\tau_{2k-1}\tau_{2k} = (ab)(cd) = (ab)(bc)(bc)(cd) = (bca)(cbd),$$

the permutation consisting of 3-cycles. Hence α is a product of 3-cycles.

□

Lemma 4.29. *If $\gamma = (i_0, i_1, \ldots, i_{k-1})$ is a k-cycle in S_n and $\alpha \in S_n$, then $\alpha\gamma\alpha^{-1}$ is also a k-cycle; indeed*

$$\alpha\gamma\alpha^{-1} = (\alpha i_0, \alpha i_1, \ldots, \alpha i_{k-1}).$$

Conversely, if $\gamma' = (i'_0, i'_1, \ldots, i'_{k-1})$ is another k-cycle, then there exists $\alpha \in S_n$, with $\gamma' = \alpha\gamma\alpha^{-1}$.

Proof. If $0 \leq l \leq n$ and $l \neq \alpha i_j$, where $0 \leq j \leq k-1$, then $\alpha^{-1}l \neq i_j$ and so $\gamma(\alpha^{-1}l) = \alpha^{-1}l$; therefore

$$\alpha\gamma\alpha^{-1} : \ l \ \mapsto \ \alpha^{-1}l \ \mapsto \ \alpha^{-1}l \ \mapsto \ l,$$

meaning $\alpha\gamma\alpha^{-1}$ fixes l.

If $l = \alpha i_j$, then

$$\alpha\gamma\alpha^{-1} : \ l \ = \ \alpha i_j \ \mapsto \ i_j \ \mapsto \ i_{j+1} \ \mapsto \ \alpha i_{j+1}.$$

Note that the subscripts are $\bmod k$. Therefore $\alpha\gamma\alpha^{-1}$ and $(\alpha i_0, \alpha i_1, \ldots, \alpha i_{k-1})$ are equal.

For the given γ and γ', choose a permutation α with $\alpha i_j = i'_j$ for all j. Then the first part of the proof shows that $\gamma' = \alpha\gamma\alpha^{-1}$. □

The conjugacy classes of S_5 and A_5 and the orders of each class are given in the tables 4.1 and 4.2. We will be needing these conjugacy classes in some of the following theorems. The tables and more can be found in [Rot95].

Lemma 4.30. *(i) There are 20 3-cycles in S_5, and they are all conjugate in S_5.*

(ii) All 3-cycles are conjugate in A_5.

Proof. (i) The number of each conjugacy class in S_5 is seen in the table 4.1. The conjugacy of any two 3-cycles follows from lemma 4.29 directly, so the only 3-cycles are in the conjugacy class ${}^{S_5}(123)$; there are 20 3-cycles in S_5.

(ii) If $\alpha = (123) \in A_5$, and $C_S(\alpha)$ and $C_A(\alpha)$ are the centralizers of α in S_5 and A_5 respectively, then by theorem 4.7 $[S_5 : C_S(\alpha)]$ is the number of conjugates of α, in this case 20 as seen in the table 4.1, therefore $|C_S(\alpha)| = |S_5| : 20 = 6$. In fact, all the six elements that commute with α are

$$1, \quad \alpha, \quad \alpha^2, \quad (45), \quad (45)\alpha, \quad (45)\alpha^2.$$

Only the first three are even permutations, meaning $|C_A(\alpha)| = 3$. Then by theorem 4.7 again and Lagrange's theorem (2.14), the number of conjugates of α in A_5 is

$$[A_5 : C_A(\alpha)] = |A_5| : |C_A(\alpha)| = 60/3 = 20 = [S_5 : C_S(\alpha)].$$

Therefore all 3-cycles are conjugates to one another in A_5. □

Theorem 4.31. *A_5 is simple, meaning its only normal subgroups are A_5 and $\{1\}$.*

Proof. Suppose $H \neq \{1\}$ is a normal subgroup of A_5 and that $\sigma \in H$. Then every conjugate of σ in A_5 also lies in H. Particularly if H contains a 3-cycle, then by previous lemma 4.30 it contains all 3-cycles, but then $H = A_5$ by lemma 4.28.

Let $\sigma \in H$, $\sigma \neq 1$. We want to look at all the possible cycle structures σ could have in A_5. So, using examples, σ could be of the type (123), (12)(34) or (12345). If $\sigma = (123)$, then $H = A_5$ by above explanation. If $\sigma = (12)(34)$, define $\tau = (12)(35) \in A_5$. As H is normal $\tau\sigma\tau^{-1}$ has to also be in H. We want to show that $\tau\sigma\tau^{-1}\sigma^{-1}$ as a product of two elements of H (and therefore as an element of H) is a 3-cycle. Showing each step: we have $\sigma^{-1} = \sigma$ and $\tau^{-1} = \tau$, so now

$$\begin{aligned}\sigma\tau^{-1} &= \begin{pmatrix}1&2&3&4&5\\2&1&4&3&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&1&5&4&3\end{pmatrix}\\ &= (354),\end{aligned}$$

then

$$\begin{aligned}\tau\sigma\tau^{-1} &= \begin{pmatrix}1&2&3&4&5\\2&1&5&4&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\1&2&5&3&4\end{pmatrix}\\ &= (12)(45),\end{aligned}$$

and then calculating $\tau\sigma\tau^{-1}\sigma^{-1} \in H$ we get

$$\begin{aligned}\tau\sigma\tau^{-1}\sigma^{-1} &= \begin{pmatrix}1&2&3&4&5\\2&1&3&5&4\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&1&4&3&5\end{pmatrix}\\ &= (354),\end{aligned}$$

leading to $H = A_5$ as shown before. Then suppose $\sigma = (12345)$, and define $\tau = (132) \in A_5$. Their inverses are $\sigma^{-1} = (15432)$ and $\tau^{-1} = (123)$. Then

$$\begin{aligned}\sigma\tau^{-1} &= \begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix}\\ &= (13245),\end{aligned}$$

and so

$$\begin{aligned}\tau\sigma\tau^{-1} &= \begin{pmatrix}1&2&3&4&5\\3&1&2&4&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\end{pmatrix}\\ &= (12453)\end{aligned}$$

Table 4.1: Conjugacy classes of S_5

Class representative	Number	Order	Parity
(1)	1	1	Even
(12)	$10 = (5 \cdot 4)/2$	2	Odd
(123)	$20 = (5 \cdot 4 \cdot 3)/2$	3	Even
(1234)	$30 = (5 \cdot 4 \cdot 3 \cdot 2)/4$	4	Odd
(12345)	$24 = 5!/5$	5	Even
(12)(34)	$15 = \frac{1}{2}(\frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2}{2})$	2	Even
(123)(45)	$20 = \frac{5 \cdot 4 \cdot 3}{3} \cdot \frac{2 \cdot 1}{2}$	6	Odd

Table 4.2: Conjugacy classes of A_5

Class representative	Number	Order	Parity
(1)	1	1	Even
(123)	$20 = (5 \cdot 4 \cdot 3)/2$	3	Even
(12345)	$24 = 5!/5$	5	Even
(12)(34)	$15 = \frac{1}{2}(\frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2}{2})$	2	Even

from where we get

$$H \ni \tau\sigma\tau^{-1}\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix} = (134)$$

In each case, H must contain a 3-cycle, so $H = A_5$. Therefore A_5 contains no proper normal subgroup that is non trivial, and hence it is simple.

□

Theorem 4.32. *The only normal subgroups of S_5 are $\{1\}$, A_5 and S_5 itself.*

Proof. Clearly $\{1\}$ and S_5 itself are normal subgroups of S_5. Now we will use the group homomorphism $sgn\colon S_n \to \{\pm 1\}$, defined by $sgn(\sigma) = (-1)^t$, where t is the amount of transpositions in the decomposition of σ. Then as A_n is the kernel of this homomorphism as a group of all even permutations in S_5, it means A_n is a normal subgroup of S_n.

Let $H \neq \{1\}$ be a normal subgroup of S_5. Using the table 4.1 of the conjugacy classes of S_5, we now have that H would consist of $\{1\}$ and at least one other conjugacy class by theorem 4.8. As a normal subgroup, its order would have to be a divisor of the order of S_n, which is 120. The only possible combinations of the orders are $1 + 15 + 24 = 40$ (of classes of $\{1\}$, (12)(34) and (12345)), and $1 + 15 + 20 + 24 = 60$, which is the order of A_5.

If the order of H is 60, then $H = A_5$. If the order is 40, then H consists of permutations of the forms (1), (12)(34) and (12345) and their products. But as for example

$$\big((12)(34)\big)(12345) = \begin{pmatrix}1&2&3&4&5\\2&1&4&3&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\1&4&3&5&2\end{pmatrix} = (245)$$

then H must include (245), meaning H contains all 3-cycles as they are all conjugates to one another. Then the intersection $H \cap A_5$ is non-trivial as they have common elements. Then the intersection of a subgroup $H \leq S_5$ and a normal subgroup $A_5 \leq S_5$ is a normal subgroup of A_5 by theorem 4.1. But as A_5 is simple it then has to be that $H = A_5$.

□

4.1.2 S_n and solvability

We can now apply our definition of solvability and its qualities to symmetry groups.

Theorem 4.33. *S_n is solvable for $n \leq 4$ and is not solvable for $n \geq 5$.*

Proof. It suffices to show that S_4 is solvable by theorem 4.18 and with the knowledge that if $m < n$, then S_m is isomorphic to some subgroup of S_n; if S_4 is solvable, then all S_m with $m < 4$ are isomorphic to some solvable subgroup of S_4, making them solvable too. We will show that S_5 is not solvable by theorem 4.18.

S_4 is solvable: Now define $V \subset A_4$ as the *four group* that consists of the elements (1), (12)(34), (13)(24), and (14)(23). It is a normal subgroup of S_4 (and A_4), as it is a union of conjugacy classes ${}^{S_4}(1)$ and ${}^{S_4}(12)(34)$. Let $W \subset V$ be any subgroup of V of order 2. Now as V is abelian since all its elements are products of disjoint transpositions, then W has to be a normal subgroup of V. We now have a normal series:

$$\{1\} \leq W \leq V \leq A_4 \leq S_4.$$

Now the orders of the factor groups are

$$\begin{aligned} |S_4| : |A_4| &= 24/12 = 2, \\ |A_4| : |V| &= 12/4 = 3, \\ |V| : |W| &= 4/2 = 2, \quad \text{and} \\ |W| : |\{1\}| &= 2/1 = 2, \end{aligned}$$

all of which are of prime order, so by lemma 3.2 the factor groups are cyclic, and therefore abelian.

S_5 not solvable: If S_5 was solvable, then A_5 would also be solvable. By theorem 4.32 we know that A_5 and $\{1\}$ are the only normal subgroups of S_5 and by theorem 4.31

that A_5 is simple. The only normal series of A_5 is $\{1\} \leq A_5$, and its only factor group is a nonabelian group $A_5/\{1\} \cong A_5$. Therefore A_5 is not solvable, meaning S_5 can not be solvable.

□

With the following theorems we can connect groups of order n to symmetry groups S_n. This way if we know that a symmetry group S_n is solvable we can prove that an isomorphic group, or a group isomorphic to a subgroup of S_n, is also solvable.

Theorem 4.34 (Cayley)**.** *Every group G of order n is isomorphic to a subgroup of S_n.*

Proof. Let $g \in G$ and define $\lambda_g \colon G \to G$ by $x \mapsto gx$. Denote the set of all permutations of G by S_G. The map λ_g is now a bijection as it has an inverse $\lambda_{g^{-1}} \colon x \mapsto g^{-1}x$, and so $\lambda_g \in S_G$.

Now $S_G \cong S_n$, as we can define an isomorphism such that for $\alpha \in S_G$ we have $\alpha \mapsto \theta\alpha\theta^{-1}$, where $\theta(g_i) = i$ for $g_i \in G$.

Then define $\lambda \colon G \to S_G$ by $a \mapsto \lambda_a$. The aim is to prove that this is also an isomorphism. Now

$$\lambda_a(\lambda_b(x)) = \lambda_a(b(x)) = a(bx) = (ab)x = \lambda_{ab}(x),$$

where we get that $\lambda_a\lambda_b = \lambda_{ab}$, so λ is a group homomorphism. Clearly if $a \neq b$ for any $a, b \in G$ then $\lambda_a \neq \lambda_b$, as for example $\lambda_a(1) = a \neq b = \lambda_b(1)$, so λ is injective.

Thus we now have that G is isomorphic to some subgroup of S_G and $S_G \cong S_n$, so the group G is isomorphic to some subgroup of S_n. □

Here is a theorem that was mentioned but not proved in the first introductory section about Galois groups. With this theorem and the one above we can connect Galois groups to symmetry groups.

Theorem 4.35. *If $f(x) \in F[x]$ has n distinct roots in its splitting field E, then $Gal(E/F)$ is isomorphic to a subgroup of the symmetry group S_n, and so its order is a divisor of $n!$.*

Proof. Let $X = \{\alpha_1, \dots \alpha_n\}$ be the set of all the roots of $f(x)$ in E. Define the map $\varphi : \mathrm{Gal}(E/F) \to S_X$, by $\sigma \mapsto \sigma|X$. By lemma 2.83 we have that if $\sigma \in \mathrm{Gal}(E/F)$, then $\sigma(X) = X$, so all σ permute X. Now φ is clearly a homomorphism, as

$$\sigma|X(\alpha_i\alpha_j) = \sigma(\alpha_i\alpha_j) = \sigma(\alpha_i)\sigma(\alpha_j) = \sigma|X(\alpha_i)\sigma|X(\alpha_j).$$

The image of φ is a subgroup of $S_X \cong S_n$, and the kernel of φ is the set of all the $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma|X = 1_X$. By theorem 2.84 we get that $\ker\varphi = \{1\}$, and therefore by theorem 2.15 the mapping φ has to be injective.

So now $\mathrm{Gal}(E/F) \cong S_X$. Finally $S_X \cong S_n$. The order of $\mathrm{Gal}(E/F)$ being a divisor of $n!$ is easily proved using Lagrange's theorem (2.14) and the above isomorphisms. □

4.2 Solvability by radicals

In terms of field extensions one can define solvability a little differently from group theory. Instead of looking at normal series of a group, we will be looking at *radical extensions* and their towers, and applying our knowledge of polynomials, introduced in chapter 3.

Definition 4.36. A field extension B/F is a **pure extension of type** m if $B = F(\alpha)$, where $\alpha^m \in F$ for some positive integer m.

Definition 4.37. A tower of fields $F = B_0 \subset B_1 \subset \cdots \subset B_t$ is a **radical tower** if each B_{i+1}/B_i is a pure extension. In this case, we call B_t/F a **radical extension** of F.

Theorem 4.38. *If E/F is a radical extension over F, then there is a radical tower*

$$F = B_0 \subset B_1 \subset \cdots \subset B_t,$$

with each B_{i+1}/B_i a pure extension of prime type.

Proof. Let E/F be a radical extension and let $F = B_0 \subset \cdots \subset B_t$ be a radical tower for which $B_{i+1} = B_i(\alpha_i)$ where $\alpha_i^{m_i} \in B_i$. If all m_i are primes the result follows right away.

Assume $m = m_1$ is not a prime and notate $\alpha = \alpha_1$. Then $B_1 = B_0(\alpha) = F(\alpha)$ and $\alpha^m \in F$. Without loss of generality suppose $m = pn$ where p is a prime. Then there is a tower of fields

$$B_0 = F \subset F(\alpha^n) \subset F(\alpha) = B_1.$$

Now $F(\alpha^n)/F$ is a simple extension of type p because $(\alpha^n)^p = \alpha^m \in F$, so it is a pure extension of prime type. And $F(\alpha)/F(\alpha^n)$ is a simple extension of type n because $F(\alpha) = F(\alpha^n)(\alpha)$ and $\alpha^n \in F(\alpha^n)$. As m consists of finitely many primes we can repeat this process for n and the integers and primes it consists of, until we get a radical tower between B_0 and B_1 with all the extensions between being of prime type. This results in a radical tower from F to B_t with each extension being a pure extension of prime type. □

Theorem 4.39. *Let $F \subset B \subset E$, and B/F be a finite extension. Then there is an extension K/B so that K/F is a splitting field of some polynomial $f(x) \in F[x]$.*

Proof. By theorem 2.71 we know that since B/F is finite, then it is also algebraic. So there are elements $\alpha_1, \ldots, \alpha_n$ with $B = F(\alpha_1, \ldots, \alpha_n)$. Let $p_i(x) \in F[x]$ be the minimal polynomials of α_i and define $f(x) = p_1(x) \cdots p_n(x)$. Now all p_i are monic and irreducible for all i, and all α_i are algebraic and $\alpha_i \in B$, then B contains all roots of $f(x)$ that are not in F.

Let $\beta_{i,1}, \ldots, \beta_{i,m_i} \in E - B$ be all the other roots of the polynomial $p_i(x)$ algebraic over F but not contained in B, where the integer $m_i \leq \deg(p_i) - 1$. Extending the field B by these elements we can denote

$$\begin{aligned} K &= B(\beta_{1,1}, \ldots \beta_{1,m_1}, \ldots, \beta_{n,1}, \ldots, \beta_{n,m_n}) \\ &= F(\alpha_1, \ldots, \alpha_n)(\beta_{1,1}, \ldots, \beta_{1,m_1}, \ldots, \beta_{n,1}, \ldots, \beta_{n,m_n}). \end{aligned}$$

As the extension K/F contains all roots of $f(x)$, K is a splitting field of $f(x)$. □

The following two theorems have the same premise as the previous. For both of them, let $F \subset B \subset E$, and B/F be a finite extension.

Theorem 4.40. *Any splitting field K/F containing B (as in theorem 4.39) has the form $K = B_1 \vee \cdots \vee B_r$, where each B_i is isomorphic to B via an isomorphism which fixes F.*

Proof. Let $f(x) \in F[x]$ be a polynomial that has K as its splitting field. As B/F is defined to be finite in 4.39, then it is algebraic; let $\alpha_1, \ldots, \alpha_n$ be the algebraic roots of $f(x)$, then we may notate $B = F(\alpha_1, \ldots, \alpha_n)$. From the proof of the previous theorem 4.39 we also know that

$$K = B(\beta_1, \ldots, \beta_m) = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m),$$

where $\beta_1, \ldots, \beta_m$ are roots of the polynomial $f(x)$ that are algebraic over F (but not found in B).

Let $\mathrm{Gal}(K/F) = \{\sigma_1, \ldots, \sigma_r\}$. Define $B_i = \sigma_i(B)$ where $\sigma_i \in \mathrm{Gal}(K/F)$. Now all σ_i fix F and map all β_t and α_k to some elements in $\{\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m\}$ as $\mathrm{Gal}(K/F)$ acts transitively on these elements by theorem 2.92. Then

$$B_i = \sigma_i(B) = F(\sigma_i(\alpha_1), \ldots, \sigma_i(\alpha_n)),$$

where some of the elements $\{\alpha_1, \ldots, \alpha_n\}$ may map to some of the elements $\{\beta_1, \ldots, \beta_m\}$.

Now B_i is clearly an extension of F. Both B_i and B have the same amount of elements, and as all σ_i are automorphisms of K fixing F and for each α_k in B there is some element $\sigma_i(\alpha_k) \in B_i$ and vice versa, it is easy to see that σ_i makes B and B_i isomorphic.

Now the intersection of all the subfields containing all B_i is $B_1 \vee \cdots \vee B_r$. By theorem 2.104 we can write

$$\begin{aligned} B_1 \vee \cdots \vee B_r &= F(\sigma_1(\alpha_1), \ldots, \sigma_1(\alpha_n)) \vee \cdots \vee F(\sigma_r(\alpha_1), \ldots, \sigma_r(\alpha_n)) \\ &= F(\sigma_1(\alpha_1), \ldots, \sigma_1(\alpha_n), \ldots, \sigma_r(\alpha_1), \ldots, \sigma_r(\alpha_n)) \end{aligned}$$

where some of the elements $\sigma_i(\alpha_k)$ and $\sigma_j(\alpha_l)$, where $i \neq j$, may be equal.

By theorem 2.92 we know that for any roots $\alpha_k \in \{\alpha_1, \ldots, \alpha_n\}$ and $\beta_t \in \{\beta_1, \ldots, \beta_m\}$ of $f(x)$ there is some automorphism $\sigma_j \in \mathrm{Gal}(K/F)$ that gives $\sigma_j(\alpha_k) = \beta_t$. This means that for all $\beta_t \in \{\beta_1, \ldots, \beta_m\}$ there is some $\sigma_j \in \mathrm{Gal}(K/F)$ for which $\beta_t \in B_j = \sigma_j(B)$. So all $\beta_1, \ldots, \beta_m$ are in $B_1 \vee \cdots \vee B_r$. As $id \in \mathrm{Gal}(K/F)$, clearly $id(B) = B$ gives us that all $\alpha_1, \ldots, \alpha_n$ are also in $B_1 \vee \cdots \vee B_r$. And clearly as all B_i are extensions of F, we have that $F \subset B_1 \vee \cdots \vee B_r$. So all elements in K are found in $B_1 \vee \cdots \vee B_r$, meaning $K \subset B_1 \vee \cdots \vee B_r$. And by definition of B_i, all elements of $B_1 \vee \cdots \vee B_r$ are found in K. □

Definition 4.41. If $f(x) \in F[x]$, then $f(x)$ is **solvable by radicals over** F if there is a radical extension B/F which contains a splitting field E of $f(x)$ over F.

Theorem 4.42. *Any splitting field K/F like in theorem 4.39 containing a radical extension R_t/F is itself a radical extension.*

Additionally, in the definition of solvable by radicals one can assume that the last field R_t is a splitting field of some polynomial over F.

Proof. Let K/F be a splitting field of some polynomial(s) in $F[x]$, meaning the polynomial(s) split into linear factors over K.

A field extension over F is a radical extension, if the extension is constructed by adjoining to it elements $a_1, \ldots, a_k$ for which $a_i^{n_i} \in F$ for some $n_i \in \mathbb{N}$. In other words, here a radical extension R_t/F contained in K/F consists of F and elements of the form $\sqrt[n_i]{a_i}$. Now the element $\sqrt[n_i]{a_i}$ is a root of the polynomial $x^{n_i} - a_i$, so by theorem 4.39 the radical extension R_t/F can be constructed by adjoining roots of these types of polynomials. So we can write the extension as $R_t = F(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k})$, where $a_i \in F$ and $n_i \in \mathbb{N}$.

As we have $R_t/F \subset K/F$, the field K contains all elements of R_t including the roots $\sqrt[n_i]{a_i}$ of the polynomials $x^{n_i} - a_i$. The field K of course also contains F and the roots of the polynomial(s) that split over K.

We want to show that K is a radical extension of F. We can show this by showing that K can be constructed by adjoining roots of polynomials of the form $x^n - b$, where $b \in F$.

Now K contains all roots of some $f(x) \in F[x]$ that splits over K. Each of these roots can be expressed in terms of the radical elements already in K, meaning some of the elements of R_t and possibly other roots. In other words, any element in K can be expressed as a combination of the radical elements $\sqrt[n_i]{a_i}$, and the roots of the polynomial $f(x)$. Therefore all of K can be constructed by adjoining these roots in terms of radicals. Thus K/F is a radical extension.

And lastly, in the definition of solvable by radicals (definition 4.41) we can assume that the last field R_t of a radical tower is a splitting field of some polynomial over F, as, by above proof, any splitting field containing a radical extension is itself a radical extension. □

In the above proof Chris Trentman's solution [Tre21] to a problem from Rotman (2001) was used as an aid.

Here are two examples from Allenby's (1991) book with more elaborate explanations to illustrate the definition of solvability by radicals:

Example 4.43. Let $F = \mathbb{Q}$ and $r = \sqrt{2}$. Set $B = \mathbb{Q}(r) \subset \mathbb{R}$, meaning B is a simple extension field of F. The polynomial $f(x) = x^2 - 2 \in F[x]$ has the roots $\sqrt{2}$ and $-\sqrt{2}$ and splits over $\mathbb{R}$, and its splitting field is B.

Thus B/F is a pure extension of type 2, and B is the splitting field of $f(x)$ over F. Therefore $f(x)$ is solvable by radicals over F.

Example 4.44. Let $F = \mathbb{Q}$ and $r = \sqrt[3]{2}$, the real cube root of 2. Setting $B_1 = \mathbb{Q}(r)$ and $B_2 = B_1(\omega) \subset \mathbb{C}$ where $\omega = e^{2\pi i/3}$ is a cube root of unity, we now have a radical tower $F \subset B_1 \subset B_2$.

The polynomial $f(x) = x^3 - 2 \in F[x]$ has three roots, $r = \sqrt[3]{2}$, $r\omega$ and $r\omega^2$. This polynomial splits over $\mathbb{C}$, and its splitting field is now $B_2 = \mathbb{Q}(r, \omega)$. Thus B_2/F is a pure extension of type 3, containing the splitting field B_2 of $f(x)$, and so $f(x)$ is solvable by radicals over F.

Lemma 4.45. *Let F be a field of characteristic 0, let $f(x) \in F[x]$ be solvable by radicals, and let E be a splitting field of $f(x)$ over F.*

(i) There is a radical tower

$$F = R_0 \subset R_1 \subset \cdots \subset R_t$$

with $E \subset R_t$ with R_t being a splitting field of some polynomial over F, and with each R_i/R_{i-1} is a pure extension of prime type p_i.

(ii) If R_t/F is a radical extension as in part (i), and if F contains the p_ith roots of unity for all i, then Gal(E/F) is a solvable group.

Proof. (i) As f is solvable by radicals, there is a radical tower

$$F = B_0 \subset B_1 \subset \cdots \subset B_l$$

with $E \subset B_l$. By theorem 4.39 there is an extension K/B_l which is a splitting field of some polynomial over F. And by theorem 4.42 K/F is itself also a radical extension, so we now have a tower $E \subset B_l \subset K$. By theorem 4.38 a radical tower from F to K can be refined so that each extension in the tower is a pure extension of prime type.

(ii) Suppose (i) holds and that F contains the p_ith roots of unity for all i.

Let $F = R_0 \subset R_1 \subset \cdots \subset R_t$ be a radical tower as in part (i), and define

$$G_i = \mathrm{Gal}(R_t/R_i).$$

Since F contains the p_ith roots of unity let each R_i be a splitting field of a polynomial over R_{i-1}. Then the hypothesis of theorem 2.91 holds, giving us a normal series

$$\mathrm{Gal}(R_t/F) = G_0 \supset G_1 \supset \cdots \supset G_t = \{1\}.$$

By the same theorem the factor groups $\mathrm{Gal}(R_t/R_{i-1})/\mathrm{Gal}(R_t/R_i)$ of this normal series are isomorphic to $\mathrm{Gal}(R_i/R_{i-1})$, and these last groups are cyclic of prime order, by corollary 3.10. So $\mathrm{Gal}(R_t/F)$ is a solvable group.

Applying theorem 2.91 again but now to the tower of fields

$$F \subset E \subset R_t,$$

we see that $\mathrm{Gal}(E/F)$ is a quotient group of the solvable group $\mathrm{Gal}(R_t/F)$, and so it too is solvable by theorem 4.18.

□

Theorem 4.46. *Let $f(x) \in F[x]$ be solvable by radicals over a field F of characteristic 0, and let E/F be its splitting field. Then Gal(E/F) is a solvable group.*

Proof. By hypothesis there is a radical tower

$$F = R_0 \subset R_1 \subset \cdots \subset R_t,$$

with $E \subset R_t$, and where all R_i/R_{i-1} are pure extensions. By lemma 4.45(i) we may assume that the R_i/R_{i-1} are of prime type p_i, and that R_t/F is a splitting field of some polynomial $h(x) \in F[x]$. Let m be the least common multiple of all the p_i's and let ω be a primitive nth root of unity. Let $R' = R_t(\omega) \supset R_t$. The above tower can be lengthened by R', and then refined so that each pure extension in it has prime type. Note that R' is now a splitting field of $(x^m - 1)h(x) \in F[x]$.

Construct a new tower by adjoining ω first:

$$F = R_0 \subset F(\omega) \subset R_1(\omega) \subset \cdots \subset R_t(\omega) = R'.$$

Each extension in this tower is pure and E, the splitting field of $f(x)$, is contained in R'. As $F(\omega)/F$ is a splitting field, then by theorem 2.91 $\mathrm{Gal}(R'/F(\omega))$ is a normal subgroup of $\mathrm{Gal}(R'/F)$, and

$$\mathrm{Gal}(R'/F)/\mathrm{Gal}(R'/F(\omega)) \cong \mathrm{Gal}(F(\omega)/F).$$

Now $\mathrm{Gal}(F(\omega)/F)$ is abelian by theorem 3.8, and therefore solvable. It means that $\mathrm{Gal}(R'/F)/\mathrm{Gal}(R'/F(\omega))$ is also abelian and therefore solvable through the isomorphism.

Each extension in the tower

$$F(\omega) \subset R_1(\omega) \subset \cdots \subset R_t(\omega) = R'$$

is a pure extension of prime type. And with the way we chose m and ω primitive root, $F(\omega)$ now contains the necessary roots of unity, so by theorem 4.45 $\mathrm{Gal}(R'/F(\omega))$ is solvable. As it is a solvable normal subgroup of $\mathrm{Gal}(R'/F)$, and as their quotient is also solvable, it means that $\mathrm{Gal}(R'/F)$ itself must be solvable by theorem 4.19. Lastly, with the theorem 2.91 we get that $\mathrm{Gal}(E/F)$ is isomorphic to a quotient group of the solvable group $\mathrm{Gal}(R'/F)$, meaning it is also solvable by theorem 4.18. □

4.3 Abel-Ruffini theorem

The definitions of solvability when it comes to groups and fields are vastly different. But with Galois theory we can connect group theory and field theory, and be able to use these different definitions together. And in the case of this thesis, using both the definition of solvability by radicals and connecting it to Galois groups and symmetry groups, we can show that polynomials of nth degree, $n \geq 5$, are not solvable with a general solution formula.

This version of the below theorem is from [Häs14].

Theorem 4.47 (Abel-Ruffini)**.** *Let F be a field, with characteristic zero. If $n \geq 5$, then polynomials of nth degree with coefficients in F do not have a general solution formula.*

Proof. Let $f(X) \in F[X]$ be a general nth degree polynomial with n roots $a_1, \ldots, a_n$. Using symmetric polynomials introduced in section 3.2.4 we can express the general nth degree polynomial in the form

$$\begin{aligned} f(X) &= (X - a_1)(X - a_2)\cdots(X - a_n) \\ &= X^n + s_{n-1}X^{n-1} + \cdots + s_1 + s_0, \end{aligned}$$

where every s_i is an elementary symmetric polynomial consisting of the roots $a_1, \ldots, a_n$. Here these polynomials are

$$\begin{aligned} s_{n-1} &= -(a_1 + \cdots + a_n), \\ s_{n-2} &= a_1a_2 + a_1a_3 + \cdots + a_2a_3 + \ldots a_{n-1}a_n \\ &\vdots \\ s_0 &= (-1)^n a_1 \cdots a_n. \end{aligned}$$

The coefficients s_i of $f(X)$ are now from the field $B = F(s_1, \ldots, s_n) \subset F(a_1, \ldots, a_n)$. Let us denote the latter extension field of F adjoined with the roots of $f(x)$ by $E = F(a_1, \ldots, a_n)$. Now the elements of $\mathrm{Gal}(E/B)$ are defined by how they permute the a_i, as by theorem 4.35 $\mathrm{Gal}(E/B)$ is isomorphic with some subgroup of a symmetric group S_n.

But as any permutation of the n unknown elements fixes every symmetric polynomial s_i, then $\mathrm{Gal}(E/B) \cong S_n$. As S_n is not solvable when $n \geq 5$, then by theorem 4.46 $f(X)$ can not be solvable by radicals. □

Clearly, as by theorem 4.33 all S_n are solvable for all $n \leq 4$, we have that the above $\mathrm{Gal}(E/B) \cong S_n$ is solvable. Therefore polynomials of fourth degree or lower can be solvable by radicals and there is a solution formula for those polynomials. This was shown in chapter 3 before we introduced solvability in Galois theory.

Chapter 5

History

The short life of Évariste Galois

Due to foolishness and carelessness of others, and the mathematician's own arrogance, Évariste Galois's (1811 − 1832) works were either lost or abandoned one after another, and failures and bad luck led him to his early death. Galois lived his whole life in France during chaotic and politically tense times of the early 1800s, and sadly died at the age of twenty in a duel right after getting out of prison ([Liv05], p.128).

He was not very interested in any school subjects once he entered school, but when his then teacher introduced the book of Adrien-Marie Legendre (1752−1833) on geometry, the boy was consumed by mathematics ([Bel63], p.360). He started reading other books and the academic papers of his time, including some of Joseph-Louis Lagrange (1736 − 1813) and Niels Henrik Abel (1802 − 1829), and writing his own proofs and short articles. He contributed to number theory and outlined theorems on elliptic functions and integrals in his publications and abstracts ([All91], p.275).

He did not get much recognition during his life time. He applied to the French École Polytechnique twice, but he was rejected both times ([Bel63], p.365). The solutions to questions asked of him in the examinations came very easily to him, but he had had always difficulties relaying his thoughts and ideas to others ([Bel63], p.361). Due to either having not prepared for the exams or the problems with the oral examination, he was denied each time.

He wrote many articles during his life time in different topics in mathematics and some were even published. But each time he tried to publish or submit his work on groups and early concepts of Galois theory to a competition, his manuscripts kept being lost by someone in the institutions he submitted them to ([Liv05], p.135). His anger at the injustices in his life and life in general made him get politically involved, which eventually led him into prison. It is not quite clear how or why, but while Galois was in prison he

was challenged to a duel, to be fought the day he gets out of prison. There are many theories on how this happened, but one popular one was that he fell in and out of love with a woman at an off-site hospital he was transferred to while in prison ([Liv05], p.155) which led to problems for him.

During his final night in prison, knowing he was likely to die in the duel, he wrote letters to his friends and comrades. In a letter to his friend Auguste Chavalier he included a 60 page draft of his lost work and asked him to send it forward to mathematicians he looked up to, Carl Gustav Jacob Jacobi ($1804-1851$) and Johann Carl Friedrich Gauss ($1777-1855$) ([Liv05], p.159). This long draft later came to be known as Galois theory.

After Galois's death in the duel, his brother and Chavalier collected all the papers and catalogued everything, and took them to Joseph Liouville ($1809-1882$) ([Liv05], p.169). It was a difficult read to say the least, but, fortunately, Liouville took the text in well. Liouville published some of Galois's writings and his own comments in the Journal de Mathématiques pures et appliquées 14 years after Galois's death. He wrote to the Academy in 1843, enthusiastic about Évariste Galois's "precise and profound solution of this beautiful theorem" ([Liv05], p. 170). He gave his own explanations of Évariste's ideas and clarified some points, and shortened the text for easier reading.

Recognition for Galois soon followed. Jacobi, whom Galois admired, contacted Galois's brother and tried to find more of the late Galois's work ([Liv05], p.170). Galois's theory began to be taught at least as early as 1856, about ten years after Liouville's writings, in advanced algebra courses in France and Germany.

Polynomials and Galois Theory

The general solution formulas for quadratic, cubic and quartic polynomials were found much earlier than the fact that that quintics do not have such formula. It took many years of wondering and attempts before any results were made.

Earliest findings of linear polynomials being solved were found in a papyrus in ancient Egypt ([Liv05], p.66), and the quadratic solution formula was already well known from Babylonian times ([Liv05], p.100). Centuries later Scipione del Ferro ($1465-1526$), Nicolo Tartaglia (1499 or $1500-1557$), and Gerolamo Cardano ($1501-1576$) invented the general solution formula for cubics, and Lodovico de Ferrari ($1522-1565$) found the one for quartics. And then, for over two hundred years no one was able to prove whether the quintics had a general solution formula.

Lagrange tried and failed with his attempts to prove that quintics *had* a general solution formula, and came to the conclusion that no such formula likely exists ([Liv05], p. 98). He tried to continue his attempts by using permutations, but to no avail, he never got a result.

Many tried proving the existence of a solution formula, and it was not until Paolo

Ruffini ($1762 - 1822$) that some progress was made. He attempted to prove that no such general solution formula exists for quintics. But, in his proof there was still a problem. He had made an assumption that he did not prove, which lead to a question whether the whole proof itself stands ([Liv05], p.103). His theorem was left without a proof.

Some time later Abel, who had a similarly short and miserable life as Galois, was able to prove what Ruffini had almost done, that fifth degree polynomials were not solvable by radicals ([Liv05], p. 112). He proved it by assuming that they are solvable by radicals, and coming to a contradiction with that assumption. And he had done it all not knowing of Ruffini's work.

Later on this theorem and its proof about quintics not being solvable by radicals came to be known as the Abel-Ruffini theorem.

While Abel had shown that there was no general solution formula for fifth degree equations, that left people with the question, "does a *given* fifth-degree equation have a solution formula?" ([Liv05], p. 134). Galois was able to answer that with his theory, connecting polynomials to Galois groups and determining if the groups are solvable.

Galois introduced the concept of groups, which had already been a known but undefined concept in mathematics for a long time ([HR16], p. 53). His definition of groups is different from the modern definition too, but he used similar tools such as cosets and normal subgroups in his work ([HR16], p. 75). Therefore, his results are considered the beginning of group theory.

In forming group theory, he also formulated a new branch of algebra, now known as Galois theory. He chose as his starting point the theory of equations and permutations at the point Lagrange had reached ([Liv05], p. 134). Galois developed *Galois groups* that could be associated with each equation, and proved how the properties of this group determine whether an equation can be solved by a formula or not.

Closing words

Galois's brilliant use of group theory and invention of Galois theory have had fundamental significance for the whole of mathematics. He had found the final correct solution to the puzzle of the solvability of equations that had been plaguing mathematicians, and had provided the basis for Galois theory and had expanded the understanding of algebra. Without his work many theories and problems might have stayed mysteries for a long time.

Bibliography

[All91] R.B.J.T. Allenby. *Rings, Fields and groups. An Introduction to Abstract Algebra.* 2nd ed. Edward Arnold, 1991.

[Bel63] E. T. Bell. *Matematiikan miehiä.* Finnish. Trans. English by Helka and Klaus Vala. Werner Söderström Osakeyhtiö, 1963.

[Fra03] John B. Fraleigh. *A First Course in Abstract Algebra.* 7th ed. Dorling Kindersley and Pearson education, 2003.

[Häs14] Jokke Häsä. *Lecture notes from Algebra II course.* 2014.

[HR16] Jokke Häsä and Johanna Rämö. *Johdatus abstraktiin algebraan.* Gaudeamus, 2016.

[Jac85] Nathan Jacobson. *Basic Algebra I.* 2nd ed. Dover Publications, 1985.

[Liv05] Mario Livio. *Yhtälö, jota ei voinut ratkaista. Miten Matematiikka paljasti symmetrian kielen.* Finnish. Trans. English by Kimmo Pietiläinen. Terra Cognita, 2005.

[OR13] Lotta Oinonen and Johanna Rämö. *Johdatus lineaarialgebraan Osa II.* Finnish. 2013.

[Rot95] Joseph Rotman. *An Introduction to the Theory of Groups, part 148.* Graduate Texts in Mathematics series. Springer, 1995.

[Rot01] Joseph Rotman. *Galois Theory.* 2nd ed. Springer, 2001.

[Rot15] Joseph Rotman. *Advanced Modern Algebra, Part 1.* 3rd ed. Vol. 165. American Mathematical Society, 2015.

[Tre21] Chris Trentman. *Problem 85, Chapter 13, Galois Theory.* 2021. URL: `https://www.numerade.com/questions/using-exercise-84-prove-that-any-splitting-field-k-f-containing-a-radical-extension-r_t-f-as-in-exer/`.