The Abel-Ruffini Theorem

The insolvability of the general quintic equation by radicals

Axel Sjöblom
Abstract

This thesis explores the topic of Galois theory at a relatively introductory level with the goal of proving the Abel Ruffini theorem. In the first part algebraic structures are considered: groups, ring, fields, etc. Following this, polynomial rings are introduced and the attention is then turned to finite field-extensions. In the final section of the main text solvable extensions are studied and the Abel-Ruffini theorem is proved. The discussion section gives a brief overview of analytic methods of solving polynomial-equations.

Sammanfattning

Contents

1 Introduction ................................. 7

2 Algebraic structures ....................... 9
   2.1 Groups ...................................... 9
       2.1.1 Basic concepts .......................... 9
       2.1.2 Normal subgroups and quotient groups .......... 13
       2.1.3 Solvability of Groups ................... 16
   2.2 Rings ..................................... 19
       2.2.1 Rings, Ideals and homomorphisms ............. 19
       2.2.2 Integral domains and PIDs ................. 22
   2.3 Linear algebra ............................ 25
       2.3.1 Finite dimensional vector spaces ............ 25
       2.3.2 Linear maps ............................. 28
   2.4 Lattices .................................. 29

3 Polynomial Rings ......................... 31
   3.1 Rings of polynomials .................... 31
   3.2 Polynomials over fields .................. 33
   3.3 Irreducibility criterion .................. 36

4 Field Extensions ......................... 41
   4.1 Field extensions .......................... 41
   4.2 Splitting fields ........................... 43
   4.3 The Galois group .......................... 45
   4.4 Characters ................................. 46

5 Galois extensions ......................... 49
   5.1 Galois extensions .......................... 49
   5.2 The fundamental theorem ................. 51

6 The Abel Ruffini Theorem ................ 53
   6.1 Solvable extensions ...................... 53
   6.2 Roots of unity ............................. 54
   6.3 $S_n$ and $A_n$ ............................. 56
   6.4 Galois group $S_5$ ........................ 59

7 Discussion and further topics .......... 61
   Acknowledgements ............................ 65
   Bibliography ................................ 67
Chapter 1

Introduction

One of the most important problems in mathematics is that of solving equations, not surprisingly, it also happens to be one of the older ones. It is well known that the Babylonians knew how to solve linear and quadratic equations about 4000 years ago ([1], p. 28). Quadratic equations would often appear when solving a pair of equations of the form

\[ x + y = p, \quad xy = q. \]

Which comes up when one wants to find the sides of a rectangle given its circumference and area, and is equivalent to the equation

\[ x^2 - px + q = 0. \]

The solution of which is given by the quadratic formula

\[ x_{1,2} = \frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}. \]

The ancients could solve a few cubic equations, but it would not be until the 1500s that Italian mathematicians would finally give an algebraic solution to the general cubic equation, soon afterwards the general degree 4 equation was cracked by the Italian mathematician Lodovico Ferrari ([1], pp. 255-260). The formulas that solved the degree 3 and 4 equations were similar to the quadratic formula in that it involved the basic arithmetic operations along with nested roots \( n \sqrt{\cdot} \), such a solution is called a solution by radicals. The degree 5 polynomial was more difficult to solve, and try as they might, mathematicians were unable to find a solution formula by radicals as they had done for the lower degree equations.

In 1799 the Italian mathematician Paolo Ruffini published an incomplete proof of what has been called the Abel-Ruffini theorem [2]

**Theorem 6.4. The Abel-Ruffini theorem:** The general degree 5 polynomial over the rational numbers is not solvable by radicals.

Although the proof was incomplete, his use of permutation groups turned out to be the right approach to the problem and feature both in the final proof of the theorem given by the Norwegian mathematician Niels Henrik Abel in 1824 ([1], p. 475), but also in the later theory developed by Galois. Because while Abel had shown that the general degree 5 equation could not be solved by radicals, he had not found a criterion for when a solution by radicals could be obtained.
That problem was solved by the French mathematician Évariste Galois who found a criterion for a polynomial to be solvable by radicals, namely if and only if its Galois group (which will be introduced in Chapter 4) is solvable. Galois’ solution was not only more elegant and gave a stronger result than his predecessors, but the techniques he developed were also crucial for the later development of group theory. The interested reader can refer to [3] for a more detailed history of Galois’ life and the subsequent impact of his work.

In this essay, Galois’ ideas are studied in the modern context of group and field theory to ultimately prove the Abel-Ruffini theorem. The text is almost self-contained and requires little background other than some basic level of mathematical maturity. More in-depth treatments for the various topics can be found in the references.

The overview is as follows: In Chapter 2 the background is laid by studying the algebraic structures that will be of interest to us. For a more thorough introduction to the topic, one can consult [4], and for something more advanced see [5] or [6]. The well-acquainted reader can skip the chapter if he or she wishes. Chapter 3 is dedicated to the topic of polynomial rings and can again be skipped if the reader is familiar with the topic.

Chapters 4 and 5 will cover field extensions and the Galois group, a proof of the fundamental theorem of Galois theory is given for completeness in Chapter 5. In Chapter 6 the Abel-Ruffini theorem will finally be proved. Chapter 7 contains a brief discussion of analytic methods for solving polynomial equations.

For a more complete introduction to Galois theory [7] and [8] are recommended.
Chapter 2

Algebraic structures

As stated in the introduction, the exposition of the subject matter is generally more eloquent if framed in the general context of abstract algebraic structures, and as such the objects in question will have to be defined and studied before moving on.

The main structures that will be used are groups, rings, and fields. Vector spaces and lattices will show up towards the end of the chapter.

2.1 Groups

In this section, groups will first be defined, and subsequently, basic concepts such as group homomorphisms, cosets, and quotient groups are introduced, and classical results such as Lagrange’s theorem and the isomorphism theorems are proven and applied to the topic of solvable groups, which will be essential in the proof of the Abel-Ruffini theorem. Finally, a quick proof of Cauchy’s theorem is given, as it will be used in Chapter 6.

2.1.1 Basic concepts

The idea of group theory is to encode the idea of the symmetries of objects into an abstract algebraic language. After searching for a proper definition for some time, here is what was settled on:

Definition 2.1. A group \((G, \ast)\) is a set \(G\) with a binary operation, that is a map \(\ast : G \times G \to G\), written \((g_1, g_2) \mapsto g_1g_2\), satisfying the following conditions called group axioms:

- \((g_1g_2)g_3 = g_1(g_2g_3)\) (Associativity).
- There exists an element \(e \in G\) such that \(eg = ge = g\) for all \(g \in G\) (Existence of an identity).
- For all \(g \in G\) there exists an element \(h \in G\) such that \(gh = hg = e\) (Existence of inverses).

If the group operation satisfies the extra criterion that \(gh = hg\) for all \(g, h \in G\) then \(G\) is called abelian and the group operation is often written as ‘+’.
Remark: A group will often be written as $G$ instead of $(G,*)$ if the operation has already been specified or is obvious from the context, this is done to save space and time.

As with any abstract object in mathematics, it is useful to see a few examples to get a better understanding of it.

**Example 2.2.** Consider the set $N = \{1, 2, \ldots, n\}$ consisting of all integers from 1 to $n$. Let $(S_n, \circ)$, be the set of all bijections $\phi : N \to N$ with $\circ$ being the composition of functions. Then $S_n$ forms a group under $\circ$. Note that the composition of bijective functions is a bijection, so the operation is well-defined. Since the operation of composing functions is associative, the identity function is a bijection and bijections have inverses, all the axioms for a group are satisfied. An element of the form $a_1 \mapsto a_2 \mapsto \ldots \mapsto a_m \mapsto a_1$ is called a cycle and is written as $(a_1 a_2 \ldots a_m)$.

**Example 2.3.** The integers under addition $(\mathbb{Z}, +)$ form a group since addition is associative, has an identity since $x + 0 = 0 + x = x$, and all numbers have an additive inverse, $x + (-x) = 0$.

Below a few elementary results about groups are stated.

- Uniqueness of identity: If $e, e' \in G$ are identity elements then $e = e'$.
- Uniqueness of inverses: If $b, c \in G$ are inverses of $a \in G$ then $b = c$. We usually write the inverse of $a$ as $a^{-1}$.
- Left cancelation: If $ab = ac$ for $a, b, c \in G$ then $b = c$.
- Right cancelation: If $ba = ca$ for $a, b, c \in G$ then $b = c$.

As a consequence, it is worth noting that no element is fixed by the multiplication of an element that is not the identity since $ab = a = ae$ implies $b = e$ and the same holds for left-multiplication. We also have that $ab = e = aa^{-1}$ implies $b = a^{-1}$, so left and right inverses (other than $a^{-1}$) do not exist either.

An important concept in group theory is that of a subgroup.

**Definition 2.4.** A subgroup $H$ of a group $G$ is a subset of $G$ that is a group in its own right under the group operation of $G$. One writes $H \leq G$.

This means a few things:

1) $H$ is closed under the group operation of $G$.

2) $H$ contains the identity of $G$ (since the identity is the only element that can fix any given element).

3) If $g \in H$ then $g^{-1} \in H$ (since inverses are unique).

It is not hard to check that these conditions are sufficient for $H$ to be a subgroup of $G$, meaning that a necessary and sufficient condition for $H$ to be a subgroup is that it satisfies the above 3 criteria.

**Example 2.5.** Consider the group $\mathbb{Z}$ and the subset $2\mathbb{Z}$ consisting of the even integers. Clearly, $2\mathbb{Z}$ is closed under addition (adding two even numbers results in an even number) and $0 \in 2\mathbb{Z}$ since $0 = 2 \ast 0$, we also have that $-(2n) = 2(-n)$ and hence all elements have inverses, so $2\mathbb{Z} \leq \mathbb{Z}$. 

\[ \square \]
A few facts and definitions relating to subgroups are listed below:

- $G \leq G$.
- If $e \in G$ is the identity then $\{e\} \leq G$.
- If $A, B \leq G$ then $A \cap B \leq G$, actually the intersection of an arbitrary number of subgroups of a group is again a subgroup.
- If $A, B \subseteq G$ the intersection of all subgroups of $G$ containing both $A$ and $B$ is denoted by $A \vee B$.

A subgroup that is neither the identity nor the whole group is called a proper or nontrivial subgroup.

**Example 2.6.** Suppose $H \leq \mathbb{Z}$, then $H = n\mathbb{Z}$ for some integer $n \in \mathbb{Z}$. To see this, note that all subgroups are either the zero group or contain a positive integer. Let $n \in H$ be the smallest positive integer and suppose that $m \in H$ is an arbitrary element. Using the division algorithm one can write $m = kn + r$ where $r < n$ is a non-negative integer, but then $r = m - kn \in H$ since $H$ is a subgroup of $\mathbb{Z}$. But since $n$ is the smallest positive integer in $H$ $n$ must be 0, so $m = kn$ for some $k$, i.e. $H = n\mathbb{Z}$.

One can see that even though $2\mathbb{Z} \leq \mathbb{Z}$ the groups are in a sense ”the same”, $x, y \in 2\mathbb{Z} \Rightarrow x = 2n, y = 2m$ with $n, m \in \mathbb{Z}$, but also $x + y = 2n + 2m = 2(n + m)$ meaning elements of $2\mathbb{Z}$ can be identified with those of $\mathbb{Z}$ by removing the multiple of 2 and we get back the original group of integers. Similarly, by relabeling the elements of $\mathbb{Z}$ by multiplying by 2, one gets the group $2\mathbb{Z}$. This process is formalized using the concept of a group isomorphism, but one should first define the more general concept of a group homomorphism.

**Definition 2.7.** A map $\phi : G \rightarrow G'$ where $G, G'$ are groups is called a group homomorphism if $\phi(gh) = \phi(g)\phi(h)$ for all $g, h \in G$. If $\phi$ is also bijective it is called a group isomorphism.

A few properties of group homomorphisms are stated below If $\phi : G \rightarrow G'$ is a group homomorphism then:

- If $e \in G, e' \in G'$ are identities of $G, G'$ respectively then $\phi(e) = e'$.
- If $g \in G$ then $\phi(g^{-1}) = (\phi(g))^{-1}$.
- $\phi(G) \leq G'$.
- If $H' \leq G'$ then $H = \phi^{-1}(H') \leq G$, in particular the kernel of $\phi$, written $\ker(\phi)$, i.e $\phi^{-1}(\{e\})$ is a subgroup of $G$.
- If $H \leq G$ then $\phi|_H : H \rightarrow G'$ is a group homomorphism.
- If $\phi : G \rightarrow G'$ and $\varphi : G' \rightarrow G''$ are group homomorphisms, then so is $\varphi \circ \phi : G \rightarrow G''$.
- A group homomorphism is injective if and only if $\ker(\phi) = \{e\}$, in which case it is called a monomorphism.
• Surjective group homomorphisms are called epimorphisms.

• Let $G$ be Abelian and $H$ a group, if $\phi : G \to H$ is an epimorphism, then $H$ is also Abelian.

Recall that a bijective group homomorphism is referred to as a group isomorphism, and $G$ is said to be isomorphic to $H$ if there is a group isomorphism $\phi : G \to H$.

Below are again given a few results relating to isomorphisms:

• The identity map $id : G \to G$ is an isomorphism.

• If $\phi : G \to G'$ is an isomorphism, then so is the inverse map $\phi^{-1} : G' \to G$.

• If $\phi : G \to G'$ and $\varphi : G' \to G''$ are group isomorphisms, then so is $\varphi \circ \phi : G \to G''$.

The above facts can be summarised by saying that the notion of two groups being isomorphic is an equivalence relation, written $G \cong H$ if there is an isomorphism $\phi : G \to H$.

**Example 2.8.** Let $G$ be a group and $g \in G$ an element in $G$. The map $\phi_g : G \to G$ given by $\phi_g(x) = gxg^{-1}$ is an isomorphism. It is a homomorphism because $\phi_g(xy) = g(xy)g^{-1} = gxg^{-1}gyg^{-1} = \phi_g(x)\phi_g(y)$, it is injective since $gxg^{-1} = gyg^{-1} \Rightarrow x = y$ (use the cancellation rule twice) and surjective since $\phi_g(g^{-1}xg) = x$ for any $x \in G$. An isomorphism from a group to itself is referred to as a group Automorphism, and the maps $\phi_g$ are known as conjugation maps.

Using this language, the observation of $\mathbb{Z}$ and $2\mathbb{Z}$ being "the same" can be formalized by saying they are isomorphic, and the isomorphism is given by $\phi : \mathbb{Z} \to 2\mathbb{Z}$, $\phi(n) = 2n$, which is easily seen to be an isomorphism.

If $H \leq G$ a left coset of $H$ is a set of the form $gH = \{gh : h \in H\}$ for some $g \in G$, a right coset is defined similarly. There are three things to note here. First of all, the coset $hH$ is the same set as $H$ if $h \in H$, this can be noted as follows: Since $H$ is a group the map $\phi : H \to hH$ given by $\phi(h') = hh'$ is well defined (i.e the image of every element in $H$ lies in $H$), and as a result of the cancelation rule, the map is injective, and since $\phi(h^{-1}h') = h'$ the map is also surjective. Secondly, every element in $G$ is in one coset of $H$. This is because if $g \in G$ then $gH$ contains $g$ as $G$ contains $e$. Finally, a given coset contains no multiple elements since $gh = gh' \Rightarrow h = h'$ This leads to the question of whether the cosets form a partition of $G$, the answer turns out to be in the affirmative.

**Theorem 2.9.** Let $G$ be a group, $H \leq G$ and $g, g' \in G$, then:

1) $gH = g'H$ if and only if $g^{-1}g' \in H$.

2) $gH \cap g'H \neq \emptyset \Rightarrow gH = g'H$.

**Proof.** 1) If $gH = g'H$ then since $g' \in g'H$, $g' = gh$ for some $h \in H$, so $g^{-1}g' \in H$. If $g^{-1}g' \in H$, then $g^{-1}g = h$ so $g' = gh$ for some $h \in H$. Now $g' H = (gh)H = gH$, and the result follows.
2) Suppose that \( gH \cap g'H \neq \emptyset \), then \( gh_1 = g'h_2 \) for some \( h_1, h_2 \in H \). Doing a bit of manipulation the expression turns into \( g^{-1}g' = h_1h_2^{-1} \in H \). This result then follows from the last.

As a result of Theorem 2.9, the cosets end up forming a partition of \( G \), if \( G \) is a finite group (i.e. \( G \) is finite as a set) then the result known as Lagrange’s theorem follows.

**Theorem 2.10. Lagrange’s Theorem:** Let \( G \) be a finite group and \( H \leq G \), then \( \frac{|G|}{|H|} \) is an integer, i.e \( |H| \) divides \( |G| \).

**Proof.** Since the cosets of \( H \) form a partition of \( G \), the result follows from the fact that all cosets of \( H \) have the same number of elements, that is \( |H| \). To see this, note that the map \( \phi : H \to gH \) given by \( \phi(h) = gh \) is a bijective map. It is surjective from the way that \( gH \) is defined, and injectivity follows from the cancellation rule. As a result, \( G \) is partitioned into a finite collection of disjoint subsets of the size \( |H| \), i.e. \( |H| \) divides \( |G| \).

**Corollary 2.10.1.** If a group \( G \) is of prime order, that is \( |G| = p \) where \( p \) is prime, then the only subgroups of \( G \) are \( \{e\} \) and \( G \) itself.

**Proof.** Since the order of any subgroup divides the order of \( G \), and the order of \( G \) is prime, the order of any subgroup is either 1 or \( |G| \). In the first case, the group is \( \{e\} \), since any subgroup of \( G \) contains the identity, and in the second case the group is the whole of \( G \).

Lagrange’s theorem is useful for classifying finite groups, but that is not the purpose of the paper in question, and hence the result is mentioned in passing.

### 2.1.2 Normal subgroups and quotient groups

Consider the automorphisms \( \phi_g \) discussed in Example 2.9, if \( H \leq G \) a natural question might be to ask whether \( \phi_g \) is also an automorphism of \( H \), i.e if \( H \) is mapped to itself (note that if \( \phi_g(H) \leq H \) for every \( g \in G \), then \( \phi_g(\phi_g^{-1}(x)) = x \) which is in \( H \), so the map is onto \( H \)). If \( g \in H \) then this is straightforward, but does it hold for every \( g \in G \)? Suppose for a second that it did, then since the maps \( \phi_g \) are defined by \( \phi_g(x) = gxg^{-1} \) the result is that \( gh_1g^{-1} = h_2 \), and hence \( gh_1 = h_2g \) for \( g \in G \) and \( h_1, h_2 \in H \). As a result \( gH = Hg \) since the same procedure can be applied to \( \phi_g^{-1} \). This leads to the following definition:

**Definition 2.11.** A group that is closed under all the maps \( \phi_g \) for \( g \in G \) is called a normal subgroup of \( G \).

**Theorem 2.12.** Let \( G \) be a group and \( H \leq G \), then \( H \) is normal if and only if \( gH = Hg \) for all \( g \in G \).

**Proof.** The first part has already been proven, so suppose now that \( gH = Hg \) for all \( g \in G \), then \( gh = h'g \) for all \( h_1, h_2 \in H \), and hence \( ghg^{-1} = h' \in H \), i.e \( H \) is normal.

If \( N \) is a normal subgroup of \( G \), it is written as \( N \triangleleft G \). Below a few facts relating to normal subgroups are listed:
2.1. GROUPS

• \( \{e\} \triangleleft G \) and \( G \triangleleft G \).

• If \( G \) is abelian and \( H \leq G \), then \( H \triangleleft G \).

• If \( N \leq H \leq G \) and \( N \triangleleft G \) then \( N \triangleleft H \).

• For any homomorphism \( \phi : G \to G' \), \( \ker(\phi) \triangleleft G \).

• If \( H \) is a finite subgroup of \( G \) and \( |G| \mid |H| \) then \( H \) is a normal subgroup of \( G \).

Normal subgroups allow for the notion of a quotient group, the idea is to define an operation on the collection of cosets of the normal subgroup which makes it into a group. If \( A, B \subseteq G \) then the product of \( A \) and \( B \), written \( AB \) is defined to be the set \( \{ab : a \in A, b \in B\} \), if \( N \) is a normal subgroup then \( g_1 Ng_2N = \{g_1n_1g_2n_2 : n_1, n_2 \in N\} \), but since \( N \) is normal one has \( n_1g_2 = g_2n' \) and hence \( g_1n_1g_2n_2 = g_1g_2n_2 = g_1g_2n \in (g_1g_2)N \). It is also obviously true that \((g_1g_2)N \subseteq g_1Ng_2N\) since one can take \( g_1g_2n = (g_1e)(g_2n) \). This means that the product of two cosets of a normal subgroup satisfies \( g_1Ng_2N = (g_1g_2)N \). It does not matter which representative of the coset is chosen, so the operation is well-defined. It is not hard to see that the cosets form a group under coset multiplication.

**Definition 2.13.** Let \( G \) be a group and \( N \triangleleft G \), then the quotient group of \( G \) by \( N \), written \( G/N \), is defined to be the collection of cosets of \( N \) under coset multiplication given by \( (gN)(g'N) = gg'N \)

A few results about quotient groups are stated below:

• If \( G \) is a group and \( N \triangleleft G \) the map \( \rho : G \to G/N \) defined by \( \rho(g) = gN \) is a group homomorphism.

• If \( G \) is a group then \( G/\{e\} \cong G \).

• If \( G \) is a group then \( G/G \cong \{e\} \).

The map \( \rho : G \to G/N \) defined by \( \rho(g) = gN \) is a group homomorphism with kernel \( N \), this means that normal subgroups are exactly the subgroups that are kernels of some group homomorphism of \( G \).

**Theorem 2.14. The first isomorphism theorem:** Let \( f : G \to G' \) be a group homomorphism, \( N \subseteq \ker(f) \) a normal subgroup of \( G \), and \( \rho : G \to G/N \) is the projection map. Then there exists a unique group homomorphism \( \tilde{f} : G/N \to G' \) such that \( f = \tilde{f} \circ \rho \), if in addition, \( N = \ker(f) \) then \( \tilde{f} \) is an isomorphism onto its image.

**Proof.** Consider the map \( \tilde{f} : G/N \to G' \) given by \( \tilde{f}(gN) = f(g) \). The map is well defined since if \( gN = g'N \) then \( g' = gn \) for some \( n \in N \), meaning \( \tilde{f}(g) = \tilde{f}(g') \) and \( \tilde{f} \) can be seen to be a group homomorphism since \( \tilde{f}(g_1g_2N) = f(g_1)f(g_2) = \tilde{f}(g_1N)\tilde{f}(g_2N) \). If \( N = \ker(f) \) then \( \tilde{f} \) is injective since \( f(gN) = e \) means \( f(g) = e \) and hence \( g \in \ker(f) = N \), meaning \( gN = N \). It follows that \( \tilde{f} \) is an isomorphism onto its image. \( \square \)

The theorem is called the first isomorphism theorem because there are other isomorphism theorems relating to quotient groups, but all of them turn out to be a consequence of the first. The isomorphism theorems will be returned to shortly, but first, there will be a brief overview of cyclic groups.
Example 2.15. Consider the group \( \mathbb{Z} \) of integers, according to Example 1.4 the nontrivial subgroups of the integers are exactly the groups \( n\mathbb{Z} \) for \( n \in \mathbb{Z} \), since \( \mathbb{Z} \) is abelian one can form the quotient group \( \mathbb{Z}/n\mathbb{Z} \). It consists of the cosets \( n\mathbb{Z}, 1+n\mathbb{Z}, ..., (n-1)+n\mathbb{Z} \) since any \( m \in \mathbb{Z} \) can be divided by \( n \) to give \( m = kn + r \) for some positive \( r < n \), and as a result the coset \( m + n\mathbb{Z} \) is one of the cosets above. The group \( \mathbb{Z}/n\mathbb{Z} \) will often be written as \( \mathbb{Z}/n \).

The projection map \( \rho : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \) given by \( \rho(m) = m + n\mathbb{Z} \) makes it clear that \( 1 + n\mathbb{Z} \) is a generator of the group \( \mathbb{Z}/n\mathbb{Z} \), i.e one can obtain every element of the group by repeatedly applying the addition operation with \( 1 + n\mathbb{Z} \) to obtain any element. This leads to the following definition:

Definition 2.16. A group \( G \) is called cyclic if it is generated by one element, that is if \( G = \langle a \rangle = \{a^n : n \in \mathbb{Z} \} \) for some \( a \in G \).

If \( G \) is cyclic and \( a \in G \) is a generator then consider the unique homomorphism \( f : \mathbb{Z} \to G \) mapping 1 to \( a \). If \( \ker(f) \) trivial the first isomorphism theorem yields that \( G \cong \mathbb{Z} \), and if it is the whole of \( \mathbb{Z} \) then \( G \cong \{e\} \). Finally, in the case where the kernel is a nontrivial subgroup one obtains \( \ker(f) = n\mathbb{Z} \) and hence \( G \cong \mathbb{Z}/n\mathbb{Z} \).

Below a few results about cyclic groups are stated:

- Every subgroup of a cyclic group is cyclic.
- If \( G \) is cyclic with \( |G| = n \) and \( d|n \), there is exactly one subgroup \( H \leq G \) with \( |H| = d \).
- If \( G \) is a cyclic group with \( |G| = n \) then there are exactly \( \phi(n) \) generators where \( \phi \) is Euler’s totient function.

Another important result that will be used later on is now stated:

Theorem 2.17. Let \( G \) be a finite group of order \( n \), then \( G \) is cyclic if and only if there is at most one cyclic subgroup of order \( d \) for \( d|n \).

Proof. The ”only if” implication is one of the items listed above. Now suppose there is at most one cyclic subgroup of order \( d \) for every divisor of \( n \). Because the order of a subgroup of \( G \) divides \( n \), every element generates one of the said subgroups. Now define \( S_d \) to be the set of all the generators of the cyclic subgroup of order \( d \), then \( G = \bigcup_{d|n} S_d \) and hence \( |G| = \bigcup_{d|n} |S_d| = \sum_{d|n} |S_d| \). Now since there are exactly \( \phi(d) \) generators of a cyclic group of order \( d \), one gets \( \sum_{d|n} |S_d| \leq \sum_{d|n} \phi(d) = n \), and this is an equality only if there is a cyclic subgroup of order \( d \) for every divisor \( d|n \). In particular, it holds if \( d = n \), and hence \( G \) is cyclic.

As already stated there are multiple isomorphism theorems of groups. These will be useful when studying solvable groups, so they will be listed and their proofs are given below:

Theorem 2.18. The second isomorphism theorem: Let \( N \triangleleft H \triangleleft G \) and \( N \triangleleft G \), then \( G/H \cong (G/N)/(H/N) \). 

15
2.1. GROUPS

CHAPTER 2. ALGEBRAIC STRUCTURES

Proof. Consider the map \( \phi : G/N \to G/H \) given by \( \phi(gN) = gH \), first of all this map is well defined since if \( gN = g'N \) then \( gH = g'H \) because \( g' = gn \) for some \( n \in N \), but \( N \leq H \), so \( gH = g'H \). Now the map is a homomorphism because \( \phi(g_1g_2N) = g_1g_2H = g_1g_2H = \phi(g_1N)\phi(g_2N) \), and the kernel are the cosets \( gN \) such that \( g \in H \), which is exactly the quotient group \( H/N \). The result follows from the first isomorphism theorem. \( \square \)

Theorem 2.19. The third isomorphism theorem: Let \( f : G \to G' \) be an epimorphism and \( H' \triangleleft G' \), then \( f^{-1}(H') = H \triangleleft G \) and \( G/H \cong G'/H' \).

Proof. Consider the map \( \phi : G \to G'/H' \) given by \( \phi = \rho \circ f \), it is an epimorphism since it is the composition of two epimorphisms, it has kernel being the elements in \( G \) that map to \( H' \) under \( f \), i.e \( \ker(\phi) = f^{-1}(H') = H \), therefore the first isomorphism theorem yields \( G/H \cong G'/H' \). \( \square \)

Theorem 2.20. The fourth isomorphism theorem: Let \( H \leq G \) and \( N \triangleleft G \), then \( HN \) is a group and \( HN/N \cong \frac{H}{HN} \).

Proof. \( HN \) is a group because if \( h_1n_1, h_2n_2 \in HN \) then \( h_1n_1h_2n_2 = h_1h_2^{-1}n_1h_2n_2 \in HN \) since \( N \) is normal, the identity is also in \( HN \) since both \( H \) and \( N \) are subgroups.

Finally, \( (hn)^{-1} = n^{-1}h^{-1} = h^{-1}n' \in HN \) since \( N \) is normal. Now consider the map \( \phi : H \to HN/N \) given by \( \phi(h) = hN \). This is an epimorphism since it is a homomorphism, and \( (hn)N = hN \) so it is surjective. Now the kernel of \( \phi \) is exactly \( H \cap N \) since \( \phi(h) = N \) if and only if \( h \in N \). The first isomorphism theorem then again yields \( \frac{H}{HN} \cong HN/N \). \( \square \)

2.1.3 Solvability of Groups

Suppose that \( G \) is a group and \( N \triangleleft G \), is there any particular property of \( N \) that guarantees that \( G/N \) is abelian? This might not seem like a particularly interesting question, but determining if quotient groups are abelian will be essential in the study of Galois groups.

Theorem 2.21. Let \( G \) be a group and \( N \triangleleft G \), the group \( G/N \) is abelian if and only if for all \( g, h \in G \) the commutator of \( g \) and \( h \), \( ghg^{-1}h^{-1} \), is in \( N \).

Proof. Suppose that \( G/N \) is abelian, then for all \( g, h \in G \) \( (gh)N = (hg)N \), i.e \( gh(hg)^{-1} = gh^{-1}h^{-1} \in N \). Conversely, if \( ghg^{-1}h^{-1} \in N \) for all \( g, h \in G \), then \( ghg^{-1}h^{-1} = n \Rightarrow gh = nhg \Rightarrow gh = hgn' \) (using the fact that \( N \triangleleft G \)) so \( ghN = hN \) and \( G/N \) is an abelian group. \( \square \)

Definition 2.22. A group \( G \) is called solvable if there exists a tower of normal subgroups \( \{ e \} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_{n-1} \triangleleft G_n = G \) such that the quotient groups \( G_{i+1}/G_i \) are all abelian.

This might seem like an odd property to define, but it turns out to be exactly what is needed to prove the insolvability of the quintic by radicals. More precisely, a polynomial turns out to be solvable by radicals if and only if its Galois group is solvable.

Example 2.23. Let \( G \) be an abelian group, then \( G \) is solvable as one can take the tower \( \{ e \} \triangleleft G \) which satisfies all the relevant properties. \( \square \)
Example 2.24. The symmetric groups: The group $S_2$ is solvable since it only has two elements and is hence isomorphic to $\mathbb{Z}/2\mathbb{Z}$. $S_3$ is also solvable, as can be seen by the following tower: $\{e\} \triangleleft (123) \triangleleft S_3$, where (123) is the group generated by the cycle $1 \to 2 \to 3 \to 1$ which is an abelian group, since $S_3$ has $3! = 6$ elements and (123) has 3 elements it follows that $(123) \triangleleft S_3$ and the quotient group $S_3/(123)$ has two elements and is hence abelian, so $S_3$ is also solvable. One can similarly prove that $S_4$ is a solvable group, although it takes a bit more work. Is $S_5$ also solvable? The answer turns out to be no, and this is exactly why fifth-degree polynomials are in general not solvable.

Below a few results about solvable groups will be proved, they end up using the isomorphism theorems from earlier and will be very useful later on.

Theorem 2.25. Let $G$ be a group and $N \triangleleft G$ and $G/N$ be solvable groups, then $G$ is also a solvable group.

Proof. Consider the projection map $\rho : G \to G/N$, this is an epimorphism. Since $G/N$ is solvable there is a tower $\{e\} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G/N$. Taking the preimage of this tower under $\rho$ one ends up with a tower that starts at $N$ and ends up at $G$. Denote $\rho^{-1}(G_i)$ by $H_i$, the Morphism $\rho|_{H_i} : H_i \to G_i$ is then also an epimorphism, and since $G_i \triangleleft G_i$, the third isomorphism theorem gives that $H_{i-1} \triangleleft H_i$, and that $H_i/H_{i-1} \cong G_i/G_{i-1}$ which is abelian. So there is then a tower $N \triangleleft H_1 \triangleleft \ldots \triangleleft H_n = G$ such that the quotient groups $H_{i+1}/H_i$ are all abelian. Since $N$ is also solvable, the result follows by amalgamating the tower from $\{e\}$ to $N$ and the tower from $N$ to $G$.

Theorem 2.26. Let $G$ be a solvable group, if $H \trianglelefteq G$ then $H$ is also solvable.

Proof. Consider the sequence $\{e\} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_{n-1} \triangleleft G_n = G$ where $G_{i+1}/G_i$ is abelian. Since $H \trianglelefteq G$ consider $H_i = H \cap G_i$. $H_i \triangleleft H_{i+1}$ if $g \in H_{i+1}$ and $h \in H_i$ then $ghg^{-1} \in H_i$ since $h, g \in H$ so $ghg^{-1} \in H$ and since $G_i \triangleleft G_{i+1}$, $ghg^{-1} \in G_i$, so $ghg^{-1} \in G_i \cap H = H_i$. Now consider the map $\phi : H_{i+1} \to G_{i+1}/G_i$ given by $\phi(h) = hG_i$, this is clearly a homomorphism and it has kernel $G_i \cap H = H_i$, so $H_{i+1}/H_i$ is isomorphic to a subgroup of $G_{i+1}/G_i$ and is hence abelian, so $H$ is solvable.

Theorem 2.27. Let $G$ be a solvable group and $f : G \to G'$ a surjective homomorphism, then $G'$ is solvable.

Proof. Suppose that $\{e\} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_{n-1} \triangleleft G_n = G$ is a sequence such that $G_{i+1}/G_i$ is abelian for $i = 0, 1, \ldots, n-1$. Consider now $f(H_i) = H'_i$, $f(\{e\}) = \{e\}$ and $H'_n = f(G) = G'$. Now $H'_i \triangleleft H'_{i+1}$ because if $g' \in H'_{i+1}$, $h' \in H'_i$ then $g' = f(g), g \in G_{i+1}$ and $h' = f(h), h \in G_i$ so $g'h'g'^{-1} = f(g)f(h)f(g'^{-1}) = f(g)f(h)f(g^{-1}) = f(ghg^{-1})$, but $ghg^{-1} \in G_i$, so $f(ghg^{-1}) \in H_i$. Now consider the map $\phi : G_{i+1} \to H_{i+1}/H_i$ given by $\phi = \rho \circ f$ where $\rho$ is the projection from $H_{i+1}$ onto $H_{i+1}/H_i$, $G_i \cong \ker(\phi)$ since $f(G_i) = H_i$, so there is a well defined epimorphism $\varphi : G_{i+1}/G_i \to H_{i+1}/H_i$. Then $H_{i+1}/H_i$ is abelian, and hence $G'$ is solvable.

Corollary 2.27.1. If $G$ is a solvable group and $N \triangleleft G$, then $G/N$ is a solvable group.

Proof. Use Theorem 2.27 with $f : G \to G/N$ being the projection onto cosets.
There is one final result from finite group theory which will be used, namely Cauchy’s theorem.

**Theorem 2.28. Cauchy’s:** Let $G$ be a finite group such that a prime $p$ divides the order of $G$, then $G$ has an element of order $p$.

**Proof.** Consider the map $\phi : G^p \to G$ given by $\phi(g_1, g_2, ..., g_p) = g_1g_2...g_p$. Consider now $\phi(g_1, g_2, ..., g_p) = g_1g_2...g_p = 1$. This equation has $|G|^{p-1}$ solutions since one can choose any elements for the first $p-1$ terms and one is forced to pick the inverse for the last term. Consider now the action of $\mathbb{Z}_p$ on $G^p$ which cycles through the elements (i.e $n \ast (g_1, g_2, ..., g_p) = (g_{n+1}, g_{n+2}, ..., g_{n+p})$ where the subscripts are taken modulo $p$. Since $\mathbb{Z}_p$ has prime order, the subgroup which fixes any given element in $G^p$ is either trivial or the whole of $\mathbb{Z}_p$, in which case all elements in the p-tuple are the same. Now note that if $\phi(g_1, g_2, ..., g_p) = 1$ then the action of $\mathbb{Z}_p$ preserves the image (multiply by $g_1^{-1}$ on the left and $g_1$ on the right). As such the solutions can be grouped into sets of $p$ under their orbits, except for the cases of all elements being equal, in which case there is only one solution. So $|G|^{p-1} = np + |\{g \in G : g^p = 1\}|$, and since $1^p = 1$, $\{g \in G : g^p = 1\}$ has at least one element and both sides are divisible by $p$, there are $mp$ elements with $x^p = 1$, and hence there are some elements in $G$ with order $p$. \qed

This covers most of the results relating to groups that will be used in later sections.
2.2 Rings

In this section, some basic results relating to rings, particularly commutative rings will be given. The importance of rings is because the familiar number systems are rings, and polynomials (which will be studied more deeply in Chapter 3) naturally have a ring structure. Principal ideal domains will be of particular interest as polynomials over fields (see Definition 2.40) turn out to be principal ideal domains.

2.2.1 Rings, Ideals and homomorphisms.

Recall that \( \mathbb{Z} \) under addition forms a group, but as should be well known, other operations can be applied to integers, specifically multiplication. This leads to the definition of a ring.

Definition 2.29. A ring \( (R, +, \cdot) \) is a set \( R \) with two binary operations \( + \) and \( \cdot \), called addition, written \( (a, b) \mapsto a + b \), and \( \cdot \) called multiplication, \( (a, b) \mapsto ab \), such that \( R \) is an abelian group under \( + \) and multiplication satisfies the following rules:

- \( a(bc) = (ab)c \) for all \( a, b, c \in R \).
- \( a(b + c) = ab + ac \) for all \( a, b, c \in R \).
- \( (a + b)c = ac + bc \) for all \( a, b, c \in R \).

If multiplication is commutative, that is \( ab = ba \) for all \( a, b \in R \) then \( R \) is called a commutative ring, and if there is an element \( 1 \in R \) such that \( 1a = a1 = a \) for all \( a \in R \) then \( R \) is said to be a ring with identity. Most rings that will be considered in this paper will be commutative rings with identity.

Example 2.30. Consider the integers under addition and multiplication. This is a ring since it is an abelian group under addition, multiplication is associative, and it satisfies the distributive properties. The integers also have two other properties, namely that multiplication is commutative and that there is an element \( 1 \in \mathbb{Z} \) so that \( a1 = 1a = a \) for all \( a \in \mathbb{Z} \). Such an element is called a multiplicative identity.

If \( R \) is a ring with identity then it is not hard to see that the set of invertible elements in \( R \) form a group under multiplication, a few properties of invertible elements are given below:
• The identity is invertible.

• The inverses of invertible elements are unique, one writes the inverse of \( a \) as \( a^{-1} \).

• If \( a \) is invertible and \( x, y \in R \) are arbitrary elements such that \( ax = ay \) or \( xa = ya \) then \( x = y \).

• The group of invertible elements in a ring \( R \) is written as \( R^* \) and its elements are called units of the ring.

It is worth noting that not all rings have identities, the most obvious counterexample is the ring of even integers \( 2\mathbb{Z} \) which also forms a ring under the usual addition and multiplication.

**Definition 2.31.** Let \( R \) be a ring and \( S \subseteq R \) such that \( S \) is a ring in its own right, then \( S \) is called a subring of \( R \).

Similarly to the situation with subgroups, a subset of a ring only needs to satisfy a few properties to be a subring (closure under both operations, the inclusion of 0, and the inclusion of additive inverses), but unlike groups, a subring can have drastically different properties. For instance, a subring of a ring with identity need not be a ring with identity. Weirder still, even if the subring \( S \subseteq R \) does have an identity it might not be the same element as the identity of \( R \). Below a few properties of subrings are stated:

• If \( R \) is a ring, then \( \{0\} \) and \( R \) are subrings.

• If \( R \) is a ring, the intersection of an arbitrary number of subrings of \( R \) is again a subring of \( R \).

**Definition 2.32.** Let \( R \) and \( S \) be rings, a map \( \phi : R \to S \) is called a ring homomorphism if \( \phi(a + b) = \phi(a) + \phi(b) \) and \( \phi(ab) = \phi(a)\phi(b) \).

Like in the case of groups, a ring homomorphism is called an epimorphism if it is surjective, a monomorphism if it is injective, and an isomorphism if it is bijective. If \( \phi : R \to S \) is a ring homomorphism it satisfies:

• \( \phi(0) = 0 \).

• \( \phi(-x) = -\phi(x) \).

• \( \phi(R) \) is a subring of \( S \).

• If \( S' \) is a subring of \( S \) then \( \phi^{-1}(S') \) is a subring of \( R \).

• If \( R \) is a ring with identity then \( \phi(1) \) serves as an identity for the subring \( \phi(R) \).

• If \( a \in R \) is an invertible element in \( R \), the \( \phi(a) \) is invertible in \( \phi(R) \) with inverse \( \phi(a^{-1}) \).

• A ring homomorphism is injective if and only if \( \ker(\phi) = \{0\} \).
If $\phi : R \rightarrow S$ is a ring homomorphism then the subring $\phi^{-1}(\{0\})$ is a subring of $R$ called the kernel of $\phi$ or $\ker(\phi)$. Other than being a subring, it has the property that if $a \in R$ and $b \in \ker(\phi)$ then $ab, ba \in \ker(\phi)$, i.e. it has the property of closure under the multiplication of any element in $R$. Such a subring is called an ideal of a ring, that is:

**Definition 2.33.** A subring $I \subseteq R$ is called a left ideal if for any $x \in R$ and $y \in I$ $xy \in I$, a similar definition is given for a right ideal. A subring that is both a right and a left ideal is simply called an ideal.

Almost all the rings in this text will be commutative, so any left or right ideal will be ideals, but the terminology can be useful to know either way. Below a few examples of ideals are given:

- If $R$ is a ring then $R$ and $\{0\}$ are ideals.
- If $\phi : R \rightarrow S$ is a ring homomorphism and $I \subseteq S$ is an ideal, then $\phi^{-1}(I)$ is an ideal.
- If $R$ is a commutative ring with identity and $a \in R$ then $\langle a \rangle = \{xa : x \in R\}$ is an ideal called a principal ideal.
- If $R$ is a commutative ring with identity and $I$, and $K$ are ideals, then $I + K$, that is all elements of the form $r + k$ for $r \in I$, $k \in K$ is an ideal.
- The intersection of an arbitrary number of ideals is again an ideal.

It is worth noting that if $I \subseteq R$ is an ideal that contains the multiplicative identity, then $I = R$, this follows since $I$ is closed under the multiplication of any element in $R$.

Let $R$ be a ring and $I$ an ideal, since $R$ is an abelian group under addition, one can form cosets of the form $a + I$ for $a \in R$, and like before the sum of two cosets is a well-defined notion, that is $(a + I) + (b + I) = (a + b) + I$ and one can also form the product of two cosets: $(a + I)(b + I) = ab + I$. To see that this is a well-defined notion, suppose that $a' + I$ and $b' + I$ are two other representatives for $a + I$ and $b + I$, that means $a' = a + r, b' = b + s$ for $r, s \in I$, so $(a' + I)(b' + I) = a'b' + I = (a + r)(b + s) + I = (ab + as + rb + rs) + I = ab + I$ because $I$ is an ideal so multiplication absorbs into $I$. With the operations defined above, the cosets $a + I$ form a ring with the operations of coset addition and coset multiplication.

**Definition 2.34.** Let $R$ be a ring and $I \subseteq R$ an ideal, then the collection of cosets of $I$ forms a ring under coset addition and multiplication, called the quotient ring of $R$ over $I$, written $R/I$. The map $\rho : R \rightarrow R/I$ given by $\rho(a) = a + I$ is a ring homomorphism with kernel $I$ called the projection onto cosets.

Same as with groups, there is an isomorphism theorem for quotient rings.

**Theorem 2.35.** Let $f : R \rightarrow S$ be a ring homomorphism with kernel $I$, then there is a unique ring monomorphism $\hat{f} : R/I \rightarrow S$ such that $f = \hat{f} \circ \rho$.
Proof. Define \( \hat{f}(a + I) = f(a) \), this is a well-defined map since any other representative would be of the form \( a + r \) for \( r \in I \) It is also obviously unique since \( \hat{f}(a + I) = f(a) \) is a requirement. It can easily be seen to be a ring homomorphism and \( \hat{f}(a + I) = 0 \Rightarrow f(a) = 0 \Rightarrow a \in I \), so it is injective, and \( \hat{f} \circ \rho = f \). The result follows.

The fact that the projection map is a ring homomorphism means in particular that the quotient of a commutative ring by an ideal is again a commutative ring and that the quotient of a ring with identity again has an identity, namely \( \rho(1) = 1 + I \).

Example 2.36. Consider the ring \( \mathbb{Z} \) and the ideal \( I = \langle n \rangle = n\mathbb{Z} \), the quotient \( R/I \) is then formed by the cosets \( 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n - 1) + n\mathbb{Z} \), which as already shown are distinct cosets, then the quotient group \( \mathbb{Z}/n\mathbb{Z} \) also has a ring structure, with \( (a + n\mathbb{Z})(b + n\mathbb{Z}) = ab + n\mathbb{Z} \), and \( 1 + n\mathbb{Z} \) being an identity.

2.2.2 Integral domains and PIDs

Let \( R \) be a ring, a zero divisor is an element \( 0 \neq a \in R \) such that there is a non-zero \( b \in R \) with \( ab = 0 \) or \( ba = 0 \). For example, if \( n = mr \) is a composite number, then \( (m + n\mathbb{Z})(r + n\mathbb{Z}) = mr + n\mathbb{Z} = n\mathbb{Z} = 0 \), so \( m + n\mathbb{Z} \) and \( r + n\mathbb{Z} \) are zero divisors in \( R \). If \( x \in R \) is invertible with inverse \( y \), then \( x \) is not a zero divisor, since \( ax = 0 \Rightarrow (ax)x^{-1} = a(xx^{-1}) = a = 0 \), and vice versa for right multiplication.

Definition 2.37. A commutative ring with identity that has no zero divisors is called an integral domain.

Example 2.38. Let \( R \) be a commutative ring with identity and \( E \) be an integral domain. If \( \phi : R \rightarrow E \) is a non-zero ring homomorphism, then \( \phi(1) = 1 \). This is quite easy to see, using the multiplicative property one has \( \phi(1) = \phi(1^2) = \phi(1)\phi(1) \Rightarrow \phi(1)(\phi(1) - 1) = 0 \). Since \( E \) is an integral domain, one of the factors has to be zero, but \( \phi(1) \) being zero would mean \( \phi(x) = \phi(x \cdot 1) = \phi(x)\phi(1) = 0 \) for all \( x \in R \). It follows that \( \phi(1) = 1 \).

The most obvious example of an integral domain is the integers, but others will be important later.

Definition 2.39. Let \( R \) be an integral domain and consider the group homomorphisms \( \phi_a : \mathbb{Z} \rightarrow R \) given by \( \phi_a(1) = a \) and \( \phi_i(n) = na = (1 + \ldots + 1)a \). The characteristic of \( R \), written \( \text{char}R \) is defined to be the smallest positive generator of \( \ker(\phi_a) \) as a ranges trough \( R \) (recall that all subgroups of \( \mathbb{Z} \) are of the form \( n\mathbb{Z} \)).

Integral domains satisfy the following:

- A commutative ring with identity \( R \) is an integral domain if and only if for all \( a \in R/\{0\} \), \( ab = ac \Rightarrow b = c \).
- If \( \phi : R \rightarrow S \) is a ring homomorphism where \( S \) is an integral domain and \( R \) a ring with identity, then \( \phi(1) = 1 \).
- The characteristic of an integral domain is either 0 or a prime number.
As mentioned in the discussion following example 2.37, invertible elements are not zero divisors. A consequence is that if every non-zero element is invertible, then the ring is an integral domain (provided it is commutative).

**Definition 2.40.** A commutative ring with identity in which every non-zero element is invertible is called a field.

Below a few examples of fields along with some properties are listed.

- The rational numbers $\mathbb{Q}$ under addition and multiplication is a field.
- The real numbers $\mathbb{R}$ under addition and multiplication is a field.
- The complex numbers $\mathbb{C}$ under addition and multiplication is a field.
- The integers modulo $p$, $\mathbb{Z}_p$ for $p$ prime are fields.
- All non-zero ring homomorphisms between fields are monomorphisms.

To see that the last result holds note that if $\phi : E \rightarrow F$ is a ring morphism between fields and $\phi(x) = 0$ for some $x \neq 0$ in $E$, then if $a \in E$, $a = ae = a(x^{-1})x = (ax^{-1})x$, and $\phi(a) = \phi(ax^{-1})\phi(x) = 0$. The result follows.

**Example 2.41.** Let $\mathbb{Z}$ be the ring of integers. Recall from the section on groups that every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. This means that in particular every subring, and indeed every ideal of $\mathbb{Z}$ is of the form $\langle n \rangle$.

An integral domain with this type of property is called a principle ideal domain:

**Definition 2.42.** An integral domain in which every ideal is a principle ideal is called a principal ideal domain (PID)

Let $R$ be a commutative ring with identity, and $a, b \in R$. An element $x \in R$ is said to be a common divisor of $x, y$ if $a = xr, y = xs$ for some $r, s \in R$.

**Definition 2.43.** A common divisor $x$ of $a, b$ is called a greatest common divisor of $a$ and $b$, written $\gcd(a, b)$, if $d$ is a common divisor of $a$ and $b$ means that $d$ divides $x$, that is $x = dr$ for some $r \in R$.

It is worth noting that greatest common divisors are in general not unique. The most obvious case of this is the fact that $-a$ is a factor of $a$, so if $d$ is a greatest common divisor of $a$ and $b$, then $-d = (-1)d$, so $-d$ is also a greatest common divisor.

**Theorem 2.44.** Bezout’s identity: Let $R$ be a PID and $a, b \in R$ be two elements, then there are elements $c, d \in R$ such that $ac + bd = x$ where $x$ is the gcd of $a$ and $b$.

**Proof.** Consider the set $I = \{ac + bd : c, d \in R\}$, this is an ideal, and since $R$ is a PID, that means $I = \langle y \rangle$ for some $y \in R$. Since both $a$ and $b$ are in $I$, it follows that $y$ is a common divisor of $a$ and $b$. Now let $s$ be a common divisor of $a$ and $b$, since $I = \langle y \rangle$, it follows that there are $c, d \in R$ such that $ac + bd = y$, but since $s$ is a common factor of $a$ and $b$, $s$ is then a factor of $y$, meaning $y$ is a greatest common divisor of $a$ and $b$.
Example 2.45. The ring of integers \( \mathbb{Z} \) is a PID, so Bezout’s identity holds. If \( p \) is a prime number and \( p \) divides the product \( ab \), then it turns out that \( p \) divides \( a \) or \( b \). Suppose WLOG that \( p \) does not divide \( a \), then \( a \) and \( p \) are relatively prime. Bezout’s identity then gives integers \( x, y \) so \( ax + py = 1 \). Multiplying by \( b \) one gets \( (ab)x + p(by) = b \), but since \( p \) divides \( ab \), \( p \) must now divide \( b \). This proves the result. Suppose conversely that \( p \) is an integer such that if \( p \) divides \( ab \), then \( p \) divides \( a \) or \( b \). This means that if \( p = cd \) for some integers \( c, d \), then \( p \) divides \( c \) or \( d \), meaning one of them has to be \( p \) or \(-p \).

Example 2.45 allows one to generalize the notion of a prime to an arbitrary ring with identity.

Definition 2.46. Let \( R \) be a commutative ring with identity, \( p \in R \) is said to be prime if it is a non-zero, non-unit such that if \( p \) divides the product \( ab \), then \( p \) divides \( a \) or \( p \) divides \( b \).

An ideal \( I \subseteq R \) is said to be a prime ideal if \( I \neq R \) and whenever \( a, b \in R \) satisfy \( ab \in I \), then either \( a \in I \) or \( b \in I \).

Theorem 2.47. Let \( R \) be a commutative ring with identity and \( p \in R \), the ideal \( I = \langle p \rangle \) is a prime ideal if and only if \( p \) is prime in \( R \).

Proof. Suppose \( p \) is prime and \( ab \in I = \langle p \rangle \). It follows that \( ab = px \) for some \( x \in R \). As a result, \( p \) divides \( ab \) and hence \( p \) divides either \( a \) or \( b \), which means \( a \in I \) or \( b \in I \). Now if \( I = \langle p \rangle \) is a prime ideal, then \( ab = px \Rightarrow a \in I \) or \( b \in I \). A result is that if \( p \) divides \( ab \), then \( p \) divides \( a \) or \( b \). □

Theorem 2.48. Let \( R \) be a commutative ring with identity and \( I \subseteq R \) an ideal. The quotient ring \( R/I \) is an integral domain if and only if \( I \) is a prime ideal.

Proof. Suppose that \( I \) is a prime ideal and that \( (a + I)(b + I) = I \), that is \( ab \in I \). Since \( I \) is a prime ideal, this means that \( a \) or \( b \) is in \( I \), i.e. one of the cosets \( a + I \), \( b + I \) is the zero coset. It follows that \( R/I \) is an integral domain. Now suppose that \( R/I \) is an integral domain, then \( (a + I)(b + I) = I \) if and only if \( a \in I \) or \( b \in I \), this means that \( ab \in I \) if and only if \( a \in I \) or \( b \in I \). So \( I \) is a prime ideal. □

Example 2.49. As was shown above, the ideals \( \langle p \rangle \) in \( \mathbb{Z} \) are prime ideals for \( p \) prime. Another important property of the ideals \( \langle p \rangle \) is that it is not contained in another proper ideal. That is to say, if \( \langle p \rangle \subseteq I \) is an ideal, then \( I = \langle p \rangle \) or \( I = R \). This is quite easy to see. Since \( \mathbb{Z} \) is a PID, \( I = \langle q \rangle \) for some \( q \in \mathbb{Z} \). So \( \langle p \rangle \subseteq \langle q \rangle \), meaning \( p = aq \) for some \( a \in R \). Since \( p \) is prime, it follows that \( p \) divides \( a \) or \( q \). If \( p \) divides \( a \), one gets \( p = aq = (px)q = p(xq) \), meaning \( xq = 1 \) since \( \mathbb{Z} \) is an integral domain. As a result, \( q \) is invertible, and \( I = R \). If \( p \) divides \( q \) one gets \( p = aq = a(py) = p(ay) \), meaning \( p = aq \) where \( a \) is invertible, and hence \( I = \langle p \rangle \). That is to say, \( \langle p \rangle \) is not contained in a larger proper ideal. □

This leads to the following definition:

Definition 2.50. Let \( R \) be a ring with and \( I \subseteq R \) be an ideal. \( I \) is said to be a maximal ideal if it is not contained in a larger proper ideal.

Theorem 2.51. Let \( R \) be a PID and \( I \) a prime ideal, then \( I \) is a maximal ideal.
Proof. The proof is given by making minimal modifications to the argument in Example 2.49.  

**Theorem 2.52.** Let $R$ be a commutative ring with identity and $I \subseteq R$ be an ideal, then $R/I$ is a field if and only if $I$ is a maximal ideal.

**Proof.** Suppose that $I$ is a maximal ideal and consider any coset $a + I$ in $R/I$ such that $a \notin I$. Consider now the set $I + \langle a \rangle$. This is an ideal and $I$ is a proper subset, since $I$ is a maximal ideal this means that $I + \langle a \rangle = R$. As a result, any element in $R$, including the multiplicative identity $1$, can be written as $ax + y$ for some $x \in R$ and $y \in I$. Hence there is an $x \in R$ such that $ax \in 1 + I$ and $(a + I)(x + I) = 1 + I$, so every non-zero element is invertible, and $R/I$ is a field. Conversely, if $R/I$ is a field and $I$ is an ideal, then for any $a \in J/I$ there is a $b \notin I$ such that $ab \in 1 + I$. Since $J$ is an ideal, $ab \in J$, and since $ab = 1 + k, k \in I$, it follows that $1 \in J$, and $J = R$, i.e $I$ is a maximal ideal. 

**Corollary 2.52.1.** Every maximal ideal in a commutative ring with identity is a prime ideal.

**Proof.** Suppose $I \subseteq R$ is a maximal ideal, then $R/I$ is a field, and hence an integral domain, by Theorem 2.48 it follows that $I$ is a prime ideal.

**2.3 Linear algebra**

It was noted at the beginning of the last section that if $K$ and $L$ are fields (or rings for that matter) the product $K \times K$ is a ring. However, the operation of multiplication does not behave very well, since for instance $(x, 0)$ lacks an inverse for any $x \in K$. However, if the operation of multiplication is replaced by a related notion, an important structure is obtained, namely that of a vector space.

**2.3.1 Finite dimensional vector spaces**

**Definition 2.53.** Let $K$ be a field. A vector space over $K$ is defined to be a set $V$ with two operations $+: V \times V \to V$ and $*: K \times V \to V$ ($*(a, \alpha)$ will be written as $a\alpha$) such that the following holds:

- $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ for all $\alpha, \beta, \gamma \in V$.
- $\alpha + \beta = \beta + \alpha$ for all $\alpha, \beta \in V$.
- There is an element $0 \in V$ such that $0 + \alpha = \alpha$ for all $\alpha \in V$.
- For each $\alpha \in V$ there is an element $\beta \in V$ such that $\alpha + \beta = 0$.
- If $a, b \in K$ and $\alpha \in V$, then $(ab)\alpha = a(b\alpha)$.
- For $\alpha, \beta \in V$ and $x \in K$ $x(\alpha + \beta) = x\alpha + x\beta$.
- For $\alpha \in V$ and $x, y \in K$, $(x + y)\alpha = x\alpha + y\alpha$.
- If $1 \in K$ is the multiplicative identity in $K$ and $\alpha \in V$, then $1\alpha = \alpha$. 

25
If $V$ is a vector space and $W \subseteq V$ is a vector space under the same operations of vector addition and scalar multiplication $W$ is said to be a vector subspace of $V$. It is easy to check that this holds exactly when $W$ is closed under both operations, contains $0$, and contains an additive inverse to any element.

A few properties of vector spaces are stated below:

- The additive identity is unique.
- Additive inverses are unique and $-\alpha = (-1)\alpha$, i.e the additive inverse of $\alpha$ is $(-1)\alpha$.
- $0'\alpha = 0$ where $0'$ is the additive identity of $K$, $\alpha \in V$ is arbitrary and $0$ is the additive identity of $V$.
- $x0 = 0$ where $0$ is the additive identity in $V$ and $x \in K$ is arbitrary.
- The order of addition does not matter, i.e if $\alpha_1, \alpha_2, ..., \alpha_n$ are vectors in $V$ then it does not matter how the parentheses in $\alpha_1 + \alpha_2 + ... + \alpha_n$ are put.
- If $F \subseteq E$ is a subfield of $E$, then $E$ forms a vector space over $F$.

**Example 2.54.** Let $K$ be a field and consider $K^n$, i.e the set of all $n$-tuples of elements in $K$. This has a natural vector space structure given by pointwise addition and scalar multiplication, that is $(a_1, a_2, ..., a_n) + (b_1, b_2, ..., b_n) = (a_1 + b_1, a_2 + b_2, ..., a_n + b_n)$ and $x(a_1, a_2, ..., a_n) = (xa_1, xa_2, ..., xan)$.\[\square\]

This vector space has an additional property, namely that any element in it can be written in the form $a_1(1, 0, ..., 0) + a_2(0, 1, ..., 0) + ... + a_n(0, 0, ..., 1)$, and in a unique way. This leads to the following definition. An expression like the one above (i.e a finite sum of scaled vectors) is called a linear combination of the vectors $\{(1, 0, ..., 0), (0, 1, ..., 0), ..., (0, 0, ..., 1)\}$.

**Definition 2.55.** Let $X \subseteq V$ be a set of vectors. The span of $X$, written $\text{Span}(X)$, is defined to be all linear combinations of vectors in $X$, $X$ is said to span $V$ if $V = \text{Span}(X)$. If $V$ is spanned by some finite set of vectors, the vector space is said to be finite-dimensional.

**Theorem 2.56.** If $X \subseteq V$ is a nonempty set of vectors, $\text{Span}(X)$ is a subspace of $V$.

**Proof.** Since $X$ is nonempty, pick $v \in X$, then $0 = 0v \in \text{Span}(X)$. If $v_1, v_2 \in \text{Span}(X)$, then $v_1 = a_1\alpha_1 + a_2\alpha_2 + ... + a_n\alpha_n$ and $v_2 = b_1\beta_1 + b_2\beta_2 + ... + b_m\beta_m$ and hence $xv_1 = x(a_1\alpha_1 + x_2\alpha_2 + ... + x_n\alpha_n)$, $v_1 + v_2 = a_1\alpha_1 + a_2\alpha_2 + ... + a_n\alpha_n + b_1\beta_1 + b_2\beta_2 + ... + b_m\beta_m \in \text{Span}(X)$. Finally, if $v \in \text{Span}(X)$ then $-v = (-1)v \in \text{Span}(X)$.\[\square\]

A set of vectors $X \subseteq V$ is said to be linearly independent if $a_1e_1 + a_2e_2 + ... + a_ne_n = 0 \Rightarrow a_i = 0, i = 1, 2, ..., n$ for any finite collection of distinct vectors $e_i \in X$, $i = 1, 2, ..., n$.

**Theorem 2.57.** If $X = \{e_1, ..., e_n\}$ is a finite and linearly independent set of vectors and $v \in \text{Span}(X)$, then $v$ can be written as a linear combination of elements in $X$ in a unique way.
Proof. Let \( v \in \text{Span}(X) \). If \( v = a_1e_1 + \ldots + a_ne_n = b_1e_1 + \ldots + b_ne_n \) then \( 0 = a_1e_1 + \ldots + a_ne_n - (b_1e_1 + \ldots + b_ne_n) = (a_1 - b_1)e_1 + \ldots + (a_n - b_n)e_n \), and since \( X \) is linearly independent this means that \( (a_i - b_i) = 0 \Rightarrow a_i = b_i, i = 1, \ldots, n \). \( \square \)

**Definition 2.58.** Let \( V \) be a finite-dimensional vector space over a field \( K \), a set \( X \subseteq V \) that is both linearly independent and spans \( V \) is called a basis for \( V \), and the vectors in \( X \) are called basis vectors.

**Theorem 2.59.** Let \( X \) be a linearly dependent set of vectors, then one can remove some vectors from \( X \) and obtain a list \( Y \) with the same span.

**Proof.** Since \( X \) is a linearly dependent set of vectors there are some \( \{e_1, e_2, \ldots, e_n\} \subseteq X \) and constants \( a_1, a_2, \ldots, a_n \) in \( K \) not all 0 such that \( a_1e_1 + a_2e_2 + \ldots + a_ne_n = 0 \), if \( j \) is the largest index such that \( a_j \neq 0 \), then \( a_1e_1 + a_2e_2 + \cdots + a_{j-1}e_{j-1} + a_je_j = 0 \) \( \Rightarrow e_j = -\frac{1}{a_j}(a_1e_1 + \cdots + a_{j-1}e_{j-1}) \). So if one removes \( e_j \), one ends up with the same span. \( \square \)

**Corollary 2.59.1.** Let \( V \) be a finite-dimensional vector space, then every finite linearly independent set of vectors can be extended to a basis.

**Proof.** Let \( X \) be a finite linearly independent set of vectors. Since \( V \) is finite-dimensional there is some finite spanning set \( Y \) of \( V \), consider \( X \cup Y \), this is a linearly dependent spanning set. By Theorem 2.59 vectors can be removed one at a time while maintaining the span. Since \( X \) is linearly independent, this can be done while only removing vectors from \( Y \), because in any linear combination that gives the zero vector, at least one non-zero coefficient has to come from \( Y \). This process can be continued until the list is linearly independent. \( \square \)

**Corollary 2.59.2.** Every finite dimensional vector space \( V \) has a basis

**Proof.** Let \( X = \{e_1, \ldots, e_n\} \) be a spanning set of \( V \). If \( X \) is independent, the result is trivial. If not, then the list can be reduced by Theorem 2.59 until it is linearly independent. The result follows. \( \square \)

**Theorem 2.60.** Let \( X = \{e_1, e_2, \ldots, e_n\} \) be a finite spanning set of \( V \) and \( Y \) linearly independent, then the cardinality of \( X \) is greater than or equal to the cardinality of \( Y \)

**Proof.** Let \( v_1 \in Y \), since \( X \) is a spanning set of \( V \), one can write \( v_1 = a_1e_1 + \ldots + a_ne_n \) for some coefficients \( a_i \in K \), now let \( j \) be the largest integer such that \( a_j \neq 0 \), then \( v_1 = a_1e_1 + \ldots + a_je_j \Rightarrow e_j = \frac{1}{a_j}(v - a_1e_1 - \cdots - a_{j-1}e_{j-1}) \). Meaning if one replaces \( e_j \) with \( v_1 \), then the span remains the same.

Now work by induction, suppose that \( m-1 \) vectors in \( X \) have been replaced by vectors in \( Y \) while keeping the span the same, then any remaining element in \( Y \) is still in the span of the vectors of the modified list. So now pick a new \( v_m \in Y \), then since the modified list still spans \( V \), one gets \( v_m = a_1v_1 + \ldots + a_{m-1}v_{m-1} + c_1e_1 + \ldots + c_k e_k \) for some integer \( k \). Since the set \( v_1, v_2, \ldots, v_{m-1}, v_m \) is linearly independent, at least one of the \( c_i \) has to be non-zero since otherwise one would get \( a_1v_1 + \ldots + a_{m-1}v_{m-1} - v_m = 0 \), and since the coefficient of \( v_m = 1 \neq 0 \), this would be a contradiction. Suppose then that \( j \) is the largest integer such that \( c_j \neq 0 \), then \( e_j = \frac{1}{c_j}(v_m - a_1v_1 - \cdots - a_{m-1}e_{m-1} - c_1e_1 - \cdots - c_{j-1}e_{j-1}) \), so one more vector can be changed without
affecting the span. If the cardinality of the set \( Y \) were larger than that of \( X \), then one could replace every vector in \( X \) with one in \( Y \) in this fashion and still have vectors remaining in \( Y \). This is impossible, as the resulting set would both span \( V \) and be independent, but adding a vector to a spanning set makes it linearly dependent, and the result follows.

**Corollary 2.60.1.** If \( V \) is a finite-dimensional vector space, then every basis has the same number of elements.

*Proof.* Since \( V \) is finite-dimensional, Theorem 2.60 guarantees that any linearly independent set of vectors is finite. Now let \( X = \{ e_1, e_2, ..., e_n \} \) and \( Y = \{ u_1, u_2, ..., u_m \} \) be two bases of \( V \). Since \( X \) is a spanning set and \( Y \) is independent \( m \leq n \), but similarly, \( Y \) is spanning and \( X \) is independent, so \( n \leq m \). It follows that \( m = n \) and all bases have the same size. 

**Definition 2.61.** Let \( V \) be a finite-dimensional vector space, the number of vectors in any basis is called the dimension of \( V \), written \( \dim V \).

**Corollary 2.61.1.** Let \( V \) be a finite-dimensional vector space over a field \( K \) and \( U \subseteq V \) be a subspace, then \( \dim U \leq \dim V \)

*Proof.* Since \( V \) is finite-dimensional, there is some finite basis set of \( V \), say \( X \). Since \( U \) is a subspace of \( V \), it follows that any linearly independent set of vectors in \( U \) would have a smaller size than the dimension of \( V \). If \( U \) were not finite-dimensional, then one could pick a vector \( u_1 \in U \) and inductively choose \( u_n \in U \) which is not in the span of the previous vectors. Since \( V \) is finite-dimensional, this would eventually lead to a list of linearly independent vectors that have a larger size than \( \dim V \), which is a contradiction. This proves the whole result since the collection of linearly independent vectors generated can not be larger than \( \dim V \).

**Example 2.62.** Consider again the space \( K^n \) for some field \( K \). The vectors \( e_1 = (1, 0, ..., 0), e_2 = (0, 1, ..., 0), ..., e_n = (0, 0, ..., 1) \) form a basis for \( K^n \) since they are clearly linearly independent and span \( K^n \), that means that \( \dim K^n = n \).

### 2.3.2 Linear maps

**Definition 2.63.** Let \( V \) and \( W \) be vector spaces over the field \( K \). A map \( T : V \rightarrow W \) is called a linear map if

- \( T(\alpha + \beta) = T(\alpha) + T(\beta) \) for all \( \alpha, \beta \in V \).
- \( T(x\alpha) = xT(\alpha) \) for all \( x \in K \) and \( \alpha \in V \).

The set of all linear maps from \( V \) to \( W \) is written as \( \text{Hom}(V, W) \)

Below some facts about linear maps are stated:

- The identity map \( \text{id} : V \rightarrow V \) is a linear map.
- \( \text{Hom}(V, W) \) forms a vector space over \( K \) with the natural operations given by \( (T + S)(v) = T(v) + S(v) \) and \( (aT)(v) = a(T(v)) \).
- If \( T \in \text{Hom}(V, W) \) and \( S \in \text{Hom}(W, U) \) then \( S \circ T \in \text{Hom}(V, U) \).
• If $T : V \to W$ is a bijective linear map, then the inverse $T^{-1} : W \to V$ is also a bijective linear map, such maps are called linear isomorphisms.

• If $T \in \text{hom}(V, W)$ then $T(V) \subseteq W$ is a subspace of $W$.

• If $T \in \text{hom}(V, W)$ and $U \subseteq W$ is a subspace, then $T^{-1}(U)$ is a subspace of $V$.

In particular, the kernel of a linear map (defined as $T^{-1}(\{0\})$) is a subspace. This leads to the last important theorem that will be used, the rank nullity theorem:

**Theorem 2.64. The rank nullity theorem:** Let $V$ and $W$ be finite dimensional vector spaces over the field $K$ and $T \in \text{Hom}(V, W)$. Then $\dim V = \dim(\ker(T)) + \dim(T(V))$.

**Proof.** Since $V$ is finite-dimensional, so is the subspace $\ker(T)$. This means that there is a basis $\{e_1, e_2, ..., e_m\}$ of $\ker(T)$ that can be extended to a basis of $V \{e_1, e_2, ..., e_m, v_1, ..., v_k\}$. Now any vector in $T(V)$ can be written as a linear combination of $T(v_1), T(v_2), ..., T(v_k)$ since any $v \in V$ can be written as $a_1e_1 + ... + a_m e_m + b_1 v_1 + ... + b_k v_k$, and the first $m$ vectors are mapped to the 0 vector in $W$. Now to show that the vectors are linearly independent. Now $a_1T(v_1) + a_2T(v_2) + ... + a_k T(v_k) = 0 \Rightarrow T(a_1 v_1 + a_2 v_2 + ... + a_k v_k) = 0 \Rightarrow a_1 v_1 + a_2 v_2 + ... + a_k v_k \in \ker(T)$. But that would mean there was some linear combination of the basis vectors $\{e_1, e_2, ..., e_m, v_1, ..., v_k\}$ that was zero, meaning all of the coefficients are zero, and the result is proved. \(\square\)

### 2.4 Lattices

**Definition 2.65.** A partially ordered set (Poset) is a set $X$ with a partial ordering, that is to say, a relation $\leq$ on $X$ such that:

- $x \leq x$ for all $x \in X$.
- $x \leq y$ and $y \leq z \Rightarrow x \leq z$.
- $x \leq y$ and $y \leq x$ implies that $x = y$.

If $x, y \in X$ then a lower bound of $x$ and $y$ is an element $d \in X$ such that $d \leq x$ and $d \leq y$. If $c$ satisfies $x \leq c$ and $y \leq c$ then $c$ is known as an upper bound of $x$ and $y$.

**Example 2.66.** Let $X$ be a set and $P(X)$ be the collection of all subsets of $X$. The relation $\subseteq$ gives a partial ordering on $P(X)$ since for any subset $A$ of $X$ has $A \subseteq A$, if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$, finally if $A \subseteq B$ and $B \subseteq A$ then $A = B$. \(\square\)

The poset discussed above has another property, namely that if $A$ and $B$ are subsets of $X$ then there is a greatest lower bound of $A$ and $B$, written $C = A \cap B$, such that $C$ is a lower bound of $A$ and $B$, and if $D$ is a lower bound of $A$ and $B$, then $D \leq C$, namely $A \cap B$. By the same token, there is a least upper bound on any two subsets, written $C = A \cup B$, such that $C$ is an upper bound of $A$ and $B$, and if $D$ is an upper bound of $A$ and $B$, then $C \leq D$. The least upper bound is of course $A \cup B$.

**Definition 2.67.** A lattice $L$ is a poset such that every two elements $x, y \in L$ has a least upper bound, written $x \vee y$, and a greatest lower bound $x \wedge y$. 

29
Example 2.68. Let $G$ be a group and consider the collection of all subgroups of $G$ with the relation of subgroup inclusion $\leq$. $L$ is a poset since it is just a subcollection of all subsets of $G$. If $H, K \leq G$ then $H \cap K$ is the greatest lower bound, since the intersection of any subgroups is again a group, and any subgroup $C \leq G$ that is contained in both $H$ and $K$ is contained in their intersection. The least upper bound of $H, K$, $H \lor K$, is defined to be the intersection of all subgroups of $G$ containing both $H$ and $K$. This is obviously a subgroup of $G$, and any group that contains both $G$ and $H$ also contains $H \lor K$, meaning it is indeed a least upper bound.

Example 2.69. Let $E$ be a field and consider the collection of all subfields of $E$ under inclusion. It is a poset, and since the intersection of two fields is again a field, it is clear that the greatest lower bound of two subfields always exists. The least upper bound of two subfields $L, K$ can be taken to be the intersection of all fields containing both $L$ and $K$.

Definition 2.70. Let $L$ and $M$ be two lattices and $\phi : L \to M$ be a map. If $\phi(x \lor y) = \phi(x) \lor \phi(y)$ and $\phi(x \land y) = \phi(x) \land \phi(y)$, $\phi$ is called an order preserving lattice isomorphism, and if $\phi(x \land y) = \phi(x) \lor \phi(y)$ and $\phi(x \lor y) = \phi(x) \land \phi(y)$ it is called an order reversing lattice morphism.

Below a few facts about lattice morphisms are stated:

- If $\phi$ is bijective it is called a lattice isomorphism, and the inverse is order-preserving/reversing if $\phi$ is order-preserving/reversing.

- A bijection $\phi : L \to L'$ between lattices is an order-preserving/reversing lattice isomorphism if and only if $x \leq y \Rightarrow \phi(x) \leq \phi(y) / \phi(y) \leq \phi(x)$. 

Chapter 3

Polynomial Rings

In this chapter, the topic of polynomial rings will be studied. First, the concept of a polynomial ring is introduced, along with basic concepts like polynomial degree and irreducibility. Following this, polynomial rings over fields are studied. Finally, the topic of irreducibility is studied more in-depth, and various methods for testing whether a polynomial is irreducible are devised.

3.1 Rings of polynomials

Definition 3.1. Let R be a commutative ring, the ring of polynomials over R, written \( R[x] \) consists of expressions of the form

\[
a_0 + a_1 x + ... + a_n x^n.
\]

where \( x \) is said to be an indeterminate and \( a_i \in R \) for \( i = 0, 1, ..., n \). \( R[x] \) is a ring with the operation of addition given by

\[
\sum_{m=0}^{n} a_m x^m + \sum_{m=0}^{n} b_m x^m = \sum_{m=0}^{n} (a_m + b_m) x^m.
\]

and multiplication is given by

\[
(a_0 + a_1 x + ... + a_n x^n)(b_0 + b_1 x + ... + b_m x^m) = c_0 + c_1 x + ... + c_{n+m} x^{n+m}.
\]

Where

\[
\sum_{i+j=k} a_i b_j.
\]

The exponent to the indeterminate with the highest non-zero coefficient is called the degree of the polynomial. Polynomials of degree greater than zero are said to be of positive degree.

Remark: The 0 polynomial is said to be of degree \(-\infty\) for reasons that will become clear later on.

Checking that \( R[x] \) is a ring is straightforward, if a bit tedious. If \( R \) has an identity then \( R[x] \) also has an identity (namely 1). The Ring \( R[x] \) comes with a ring monomorphism \( i: R \to R[x] \), \( i(a) = a \), that is to say injecting the ring into the
order 0 (and $-\infty$) polynomials.

It is at this stage perhaps worth noting that the polynomial ring $R[x]$ is not the same as the ring of polynomial functions, that is functions $f : R \to R$ of the form

$$\alpha \mapsto a_0 + a_1 \alpha + \ldots + a_n \alpha^n.$$ 

For instance consider the polynomial $p(x) = x^2 - x$ in $\mathbb{Z}_2[x]$. As a function, $p(x)$ is the zero function (as can be easily checked), but as a polynomial, it is not 0.

Consider the map $\phi : R[x] \to R^R$, where $R^R$ is the ring of functions from $R$ to itself given by

$$\phi(p(x))(a) = p(a).$$

This can easily be seen to be a ring homomorphism. The image consists of all functions $R \to R$ that can be written as polynomials, and the kernel consists of all polynomials that are zero as functions. If $R$ is a finite ring it is guaranteed that some non-zero polynomial produces the zero function (there are finitely many functions from a finite set to itself, but infinitely many polynomials, the result is obtained by subtracting two different polynomials that define the same function).

**Example 3.2.** How does the notion of degree behave under the ring operations? It is clear that $\deg(p(x) + q(x)) \leq \max(\deg(p(x)), \deg(q(x)))$, and if the degrees of the polynomials are different it is indeed equal to the maximum. The product is a bit different. If the Leading coefficient of one of the polynomials is not a zero divisor, then $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$ In particular, if the leading coefficient of either $p(x)$ or $q(x)$ have leading coefficient 1 this property holds.

This also explains why the zero polynomial is defined to have degree $-\infty$, namely so that the relation $\deg(p(x)q(x)) \leq \deg(p(x)) + \deg(q(x))$ always hold.

From Example 3.2 one gets

**Theorem 3.3.** Let $R$ be an integral domain, then $R[x]$ is also an integral domain, and $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$ for any $p(x), q(x) \in R[x]$.

**Proof.** The proof follows from Example 3.2. \qed

**Corollary 3.3.1.** If $R$ is an integral domain, polynomials of positive degree are not invertible.

**Proof.** If $p(x)$ is of positive degree and $q(x) \in R[x]$ then

$$\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)).$$

Which is either positive or $-\infty$. \qed

**Definition 3.4.** A polynomial in $R[x]$ is said to be irreducible if it can not be factored into two or more non-invertible factors, that is to say $a(x)$ is irreducible if

$$a(x) \neq p(x)q(x)$$

for any $p(x)$ and $q(x)$ that are not invertible.

**Theorem 3.5.** Let $R$ be an integral domain and $p(x) \in R[x]$ a prime polynomial, then $p(x)$ is irreducible.
Proof. Suppose \( p(x) = q(x)r(x) \) then \( p(x) \) has to divide one of the polynomials \( q(x), r(x) \), say, \( q(x) = p(x)f(x) \). Then \( p(x) = p(x)(f(x)r(x)) \), meaning \( f(x)r(x) = 1 \) since \( R[x] \) is an integral domain. Hence \( r(x) \) is invertible and \( p(x) \) is irreducible. \( \square \)

If one chooses to work over fields, the notion of irreducibility only needs to be considered for monic polynomials as the leading coefficient can be factored out and is an invertible element.

**Example 3.6.** Let \( S \) be a commutative ring with identity and \( R \subseteq S \) be a subring that is also commutative with identity. If \( a \in S \) there is a ring homomorphism \( \phi : R[x] \to S \) defined by \( \phi(p(x)) = p(a) \), that is to say, one replaces \( x \) by \( a \). This is a ring homomorphism, and the polynomials in the kernel of \( \phi \) are said to have \( a \) as a root. \( \square \)

**Theorem 3.7.** Let \( R \) be a commutative ring and \( p(x) \in R[x] \), then \( p(x) \) has root \( a \in R \) if and only if \( x - a \) is a factor of \( p(x) \).

**Proof.** If \( p(x) = (x - a)q(x) \) for some polynomial \( q(x) \in F[x] \) then \( p(a) = 0 \). Conversely, if \( p(a) = 0 \) then consider \( p(x) = a_0 + a_1x + ... + a_nx^n = p(x) - p(a) = a_1(x - a) + ...a_n(x^n - a^n) \). The factors \( x^m - a^m \) can be written as \( x^m - a^m = (x - a)(x^{m-1} + x^{m-2}a + ... + xa^{m-2} + a^{m-1} \) as can readily be checked, meaning \( x - a \) is a factor of \( p(x) \). \( \square \)

**Corollary 3.7.1.** Let \( R \) be an integral domain and \( p(x) \in R[x] \) be a degree \( n \) polynomial for \( n \geq 0 \), then \( p(x) \) has at most \( n \) roots in \( R \).

**Proof.** The proof follows by induction from Theorem 3.8. \( \square \)

**Corollary 3.7.2.** Let \( R \) be an infinite integral domain, then the map \( \phi : R[x] \to R^R \) given by \( \phi(p(x))(a) = p(a) \).

is a monomorphism

**Proof.** Let \( p(x) \) be a polynomial of degree \( n > 0 \) (the degree 0 case is trivial), then \( p(x) \) has at most \( n \) roots in \( R \), meaning \( \phi(p(x)) \) is not the zero function, as such \( \ker(\phi) \) is trivial and \( \phi \) a monomorphism. \( \square \)

### 3.2 Polynomials over fields

Based on Example 3.7, a natural question to ask is if \( R[x] \) is a PID. Since if it is, every polynomial \( p(x) \in R[x] \) with \( a \in S \), with \( R \subseteq S \) a subring, that has \( a \) as a root is a multiple of some polynomial \( q(x) \in R[x] \). It was already noted that if \( R \) is an integral domain then so is \( R[x] \), it turns out that \( R \) being a field is all that is required for it to be a principle ideal domain, and more than that. The result that gives polynomials over fields good properties is the following:

**Theorem 3.8. Division algorithm:** Let \( F \) be a field and \( a(x), p(x) \in F[x] \) be non-zero polynomials. There are then polynomials \( q(x), r(x) \in F[x] \) with \( \deg(r(x)) < \deg(p(x)) \) such that \( a(x) = p(x)q(x) + r(x) \), the polynomials \( p(x) \) and \( r(x) \) are also unique.
Proof. First of all, if \( p(x) = c \) is a degree 0 polynomial, then the result holds since \( a(x) = c(c^{-1}(a(x))) + 0 \). The rest of the proof is done by induction on the degree of \( a(x) \) while keeping \( p(x) \) fixed. If \( \deg(a(x)) = 0 \), that is to say that \( a(x) = a \) for some \( a \in F \), if \( p(x) \) is of higher degree then choose \( r(x) = a(x) \). Now suppose it works for polynomials \( a(x) \) of degree less than \( n \) and pick a polynomial \( a(x) \) of degree equal to \( n \)

\[
a(x) = a_0 + a_1 x + ... + a_n x^n.
\]

If \( \deg(p(x)) > \deg(a(x)) \) then pick \( r(x) = a(x) \) and \( q(x) = 0 \). If not, then \( p(x) = b_0 + b_1 x + ... + b_m x^m \) for \( m < n \) and one can multiply \( p(x) \) by \( \frac{a_n}{b_m} x^{n-m} \) and by subtracting from \( a(x) \) one gets a polynomial of degree (at most) \( n - 1 \). So by induction, \( \hat{a}(x) = a(x) - \frac{a_n}{b_m} x^{n-m} p(x) \) is then a polynomial on which one can find \( q(x) \) and \( r(x) \) with \( \deg(r(x)) < \deg(p(x)) \) such that

\[
\hat{a}(x) = p(x)q(x) + r(x).
\]

and

\[
a(x) - \frac{a_n}{b_m} x^{n-m} p(x) = p(x)q(x) + r(x) \Rightarrow a(x) = \left( \frac{a_n}{b_m} x^{n-m} + q(x) \right) p(x) + r(x).
\]

Since this holds for any choice of \( p(x) \), the existence follows. Now to show uniqueness. Suppose

\[
a(x) = p(x)q(x) + r(x) = p(x)q'(x) + r'(x).
\]

Then

\[
p(x)(q(x) - q'(x)) = r'(x) - r(x).
\]

But \( \deg(r(x)), \deg(r'(x)) < \deg(p(x)) \), so \( q(x) - q'(x) = 0 \Rightarrow q(x) = q'(x) \) and hence \( r(x) = r'(x) \).

\[\Box\]

**Theorem 3.9.** Let \( F \) be a field, then \( F[x] \) is a PID.

**Proof.** Suppose that \( I \subseteq F[x] \) is an ideal. Pick a non-zero monic polynomial of lowest degree \( p(x) \in I \). Such a polynomial is unique since if \( q(x) \) were another, then \( p(x) - q(x) \) is a non-zero polynomial of lower degree in \( I \), and multiplying by a suitable element in \( F \) one obtains a monic polynomial of lower degree in \( I \). Now let \( b(x) \) be any polynomial in \( I \), using the division algorithm one obtains

\[
b(x) = p(x)q(x) + r(x).
\]

For some \( r(x) \) of degree less than that of \( p(x) \). Because \( p(x) \in I \) it follows that \( r(x) = b(x) - p(x)q(x) \) is also in \( I \) since it is an ideal, but the degree of \( r(x) \) is less than that of \( p(x) \), and hence it must be 0. Therefore \( I = \langle p(x) \rangle \) and \( F[x] \) is a PID. \[\Box\]

Now let \( E \) be a field and \( F \) be a subfield \( F \subseteq E \). Consider \( f(x) \in F[x] \) with a root \( a \in E \). It follows from the fact that \( F[x] \) is a PID that \( f(x) \) is a multiple of some monic polynomial \( p(x) \) with root \( a \). That is to say, every polynomial with root \( a \) in \( F[x] \) is a multiple of \( p(x) \). This leads to the following definition:

**Definition 3.10.** Let \( F \subseteq E \) be two fields and \( \alpha \in E \) be the root of some polynomial \( f(x) \in F[x] \). \( \alpha \) is called algebraic over \( F \), and a monic polynomial \( p(x) \in F[x] \) of lowest degree with \( \alpha \) as root is called a minimal polynomial of \( \alpha \).
Theorem 3.11. Let \( E \) be a field and \( F \subseteq E \) a subfield. If \( \alpha \) is algebraic over \( F \) then there exists a unique minimal polynomial \( p(x) \in F[x] \) of \( \alpha \) which is irreducible. In addition, every polynomial over \( F \) with \( \alpha \) as root has \( p(x) \) as a factor.

Proof. The set \( I = \{ a(x) \in F[x] : a(\alpha) = 0 \} \) is an ideal, and since \( F[x] \) is a PID it follows that \( I = \langle p(x) \rangle \) for some polynomial \( p(x) \in F[x] \). One can choose this \( p(x) \) to be monic, this \( p(x) \) is the minimal polynomial of \( \alpha \).

To see this note that every polynomial with \( \alpha \) as root has \( p(x) \) as a factor, and hence no monic polynomial of the same or lower degree can have \( \alpha \) as a root (other than 0 of course). To see that \( p(x) \) is irreducible, suppose \( p(x) = a(x)b(x) \) for some polynomials \( a(x), b(x) \) of positive degree, then either \( a(x) \) or \( b(x) \) has \( \alpha \) as a root, a clear contradiction of the fact that \( p(x) \) is the minimal polynomial of \( \alpha \). \( \square \)

Theorem 3.12. Let \( E \) be a field and \( F \subseteq E \) a subfield. If \( \alpha \in E \) is algebraic over \( F \) and \( p(x) \) is a monic, irreducible polynomial with \( \alpha \) as root then \( p(x) \) is the minimal polynomial of \( \alpha \) over \( F \).

Proof. Recall that \( I = \{ a(x) \in F[x] : a(\alpha) = 0 \} \) is an ideal, and since \( F[x] \) is a PID, \( I = \langle p(x) \rangle \) for some monic \( q(x) \in F[x] \). By definition \( p(x) \) has to be in \( I \), meaning \( p(x) = a(x)q(x) \), but since \( p(x) \) is irreducible \( a(x) \) is of degree 0, and \( p(x) = aq(x) \), but both \( q(x) \) and \( p(x) \) are monic, meaning \( a = 1 \) and \( p(x) = q(x) \), the result follows. \( \square \)

Example 3.13. Suppose that \( p(x) \) is an irreducible polynomial over a field \( F \). Since \( F[x] \) is a PID Bezout’s identity holds, meaning \( p(x) \) is prime in \( F[x] \), since if \( p(x) \) divides \( a(x)b(x) \) and say it does not divide \( a(x) \), then their gcd is 1 since \( p(x) \) is irreducible. As a result one has \( q(x) \) and \( c(x) \) so \( p(x)q(x) + a(x)c(x) = 1 \), and hence \( \text{gcd}(p(x),q(x)b(x)) = (a(x)b(x))c(x) = b(x) \), meaning \( p \) divides \( b(x) \).

One obtains:

Theorem 3.14. Let \( f(x) \in F[x] \) be a polynomial over the field \( F \). There exists a factorization \( f(x) = p_1(x)p_2(x)\ldots p_n(x) \) intro irreducible factors such that if \( q_1(x)q_2(x)\ldots q_m(x) \) is another factorization into irreducible polynomials, then \( m = n \) and \( q_i(x) = cp_j(x) \) for all \( i \) and some \( j \) with \( c \in F \).

Proof. For existence note that if \( f(x) \) cannot be factored into lower order terms, then it is irreducible, and if it can, then an inductive argument finishes the proof. Insofar as uniqueness goes, suppose that

\[
  f(x) = p_1(x)p_2(x)\ldots p_n(x) = q_1(x)q_2(x)\ldots q_m(x).
\]

For all \( i \), \( p_i(x) \) divides \( f(x) \) and is a prime polynomial, it follows that \( p_i(x) \) divides one of the \( q_j(x) \), and since they are also irreducible, \( p_i(x) = cq_j(x) \) for some \( c \in F \), the result follows by induction. \( \square \)

This means that the principle ideals generated by an irreducible polynomial are prime ideals, but even more is true.

Theorem 3.15. Let \( F \) be a field and \( p(x) \in F[x] \) be a polynomial, then the ideal \( \langle p(x) \rangle \) is a maximal ideal if and only if \( p(x) \) is irreducible.
Proof. Let \( p(x) \) be irreducible and suppose that \( \langle p(x) \rangle \subseteq I \) where \( I \) is an ideal, and let \( q(x) \in I/\langle p(x) \rangle \). Since \( p \) is irreducible and \( p \) does not divide \( q \), one gets that their greatest common divisor is 1. Bezout’s identity yields: \( a(x)p(x) + b(x)q(x) = 1 \), hence 1 is contained in \( I \) and \( I = F[x] \). Now if \( \langle p(x) \rangle \) is an ideal where \( p(x) = a(x)b(x) \) for non-invertible \( a(x) \) and \( b(x) \), then \( \langle a(x) \rangle \) and \( \langle b(x) \rangle \) are proper subsets of \( \langle p(x) \rangle \), meaning a maximal principle ideal is generated by an irreducible polynomial.

\[ \square \]

Recall now that the quotient of a commutative ring with identity by a maximal ideal is a field, from this one gets the following corollary:

**Corollary 3.15.1.** Let \( F[x] \) be a polynomial ring over a field and \( p(x) \in F[x] \) be an irreducible polynomial of order \( n \). Then \( F[x]/\langle p(x) \rangle \) is a field and a vector space over \( F \) of dimension \( n \), a basis is given by the cosets \( x^m + \langle p(x) \rangle \) for \( m = 0, 1, \ldots, n - 1 \).

**Proof.** Since \( \langle p(x) \rangle \) is a maximal ideal it follows from Theorem 2.52 that \( F[x]/\langle p(x) \rangle \) is a field. By injecting \( F \) into \( F[x] \) and then following with \( \rho \), it is also clear that \( F \) is a subfield of \( F[x]/\langle p(x) \rangle \). As such, it is a vector space over \( F \). Moreover, the cosets \( x^m + \langle p(x) \rangle \) spans the space, as any polynomial \( f(x) \) can be divided by \( p(x) \) and one gets

\[ f(x) = p(x)q(x) + r(x). \]

For some polynomial \( r(x) \) of lower degree than \( p(x) \). The set is also linearly independent, as the lowest degree non-zero polynomial which is in \( \langle p(x) \rangle \) is of degree \( n \), and hence no non-trivial combination \( a_0 + a_1x + \ldots + a_{n-1}x^{n-1} \) can be in \( \langle p(x) \rangle \). \( \square \)

**Example 3.16.** Let \( R \) be an integral domain and \( p(x) \in R[x] \) be a degree 2 or 3 polynomial without any roots in \( R \). If \( p(x) = a(x)b(x) \) for polynomials of non-zero degree \( a(x) \) and \( b(x) \) it follows that at least one of them are of degree 1 since \( a + b = 2 \) for \( a, b \in Z^+ \) implies that \( a = b = 1 \), and \( a + b = 3 \) gives \( a = 1, b = 2 \) or \( a = 2, b = 1 \). Either way this means that \( p(x) \) has a root in \( R \). So if \( R \) is an integral domain, then the statements that a degree 2 or 3 polynomial can be factored into two polynomials of positive degrees is equivalent to \( p(x) \) having a root in \( R \). \( \square \)

Note that the above implies that if \( F \) is a field, then a polynomial of degree 2 or 3 is irreducible over \( F \) if and only if it has no roots in \( F \). This section finishes by giving an example that will be generalized in Chapter 4.

**Example 3.17.** Consider the polynomial \( p(x) = x^2 - 2 \in \mathbb{Q}[x] \). Since degree two polynomials over a field \( F \) are irreducible if and only if they lack a root in \( F \), this means that \( p(x) \) is irreducible. Consider now the homomorphism \( \phi : \mathbb{Q}[x] \to \mathbb{R} \) given by \( \phi(a(x)) = a(\sqrt{2}) \). The image of this map is all the polynomials in \( \sqrt{2} \) over \( \mathbb{Q} \), written \( Q(\sqrt{2}) \), and by the isomorphism theorem for rings (Theorem 2.35) one has that \( \mathbb{Q}[x]/\ker(\phi) \cong Q(\sqrt{2}) \). But recall that \( \mathbb{Q}[x] \) is a PID, and hence \( \ker(\phi) = \langle q(x) \rangle \) for some monic \( q(x) \in \mathbb{Q}[x] \). Since \( p(x) \) is an irreducible monic polynomial in \( \ker(\phi) \), then \( q(x) = p(x) \) and \( \mathbb{Q}[x]/\langle p(x) \rangle \cong Q(\sqrt{2}) \). \( \square \)

### 3.3 Irreducibility criterion

Since irreducible polynomials are quite important in the study of Galois theory, it would be nice to have a few criteria for determining if a given polynomial is irreducible. From here on out all rings are assumed to be integral domains.
Example 3.18. Suppose that $\phi: R \to S$ is ring morphism, there is then an induced morphism of polynomial rings given by $\phi': R[x] \to S[x]$, $\phi'(a_0 + a_1x + \ldots + a_nx^n = \phi(a_0) + \phi(a_1)x + \ldots + \phi(a_n)x^n$.

Theorem 3.19. Let $\phi: R \to S$ be a ring homomorphism and $\phi': R[x] \to S[x]$ the induced morphism of polynomial rings

1) If $\phi$ is a monomorphism so is $\phi'$ and $\deg(p(x)) = \deg(\phi'(p(x)))$.

2) If $\phi$ is an epimorphism so is $\phi'$.

3) If $\phi$ is an isomorphism so is $\phi'$ and $\phi'$ maps irreducible polynomials to irreducible polynomials.

Proof.
1) If $\phi$ is a monomorphism and $\phi'(p(x)) = 0$ then all the coefficients of $p(x)$ are zero, meaning $\ker(\phi') = \{0\}$ and $\phi'$ is a monomorphism, it is easy to see that the degree is also preserved.

2) Let $p(x) = a_0 + a_1x + \ldots + a_nx^n$ be a polynomial in $S[x]$. Since $\phi$ is surjective, there are $b_0, b_1, \ldots, b_n \in R$ such that $\phi(b_i) = a_i$. Now define

$$q(x) = b_0 + b_1x + \ldots + b_nx^n.$$ Then $\phi'(q(x)) = p(x)$, meaning $\phi'$ is surjective.

3) $\phi'$ being an isomorphism follows from 1) and 2). Now suppose that $p(x) \in R[x]$ is irreducible and $\phi'(p(x)) = a(x)b(x)$ where $a(x)$ or $b(x)$ are not invertible. Since $\phi'$ is an isomorphism, it follows that $p(x) = (\phi')^{-1}(a(x))\phi'^{-1}(b(x))$, which contradicts the assumption that $p(x)$ is irreducible.

Returning to the topic of finding irreducibility criterion, the following result is very useful.

Theorem 3.20. Let $R$ be an integral domain and $F$ be a field. If $\phi: R \to F$ is a ring homomorphism and $p(x) \in R[x]$. If $\phi'(p(x))$ is an irreducible polynomial of the same degree as $p(x)$, then $p(x)$ cannot be written as a product of polynomials in $R[x]$ each of degree less than $p(x)$

Proof. Suppose that $p(x) = f(x)g(x)$ where both $f(x)$ and $g(x)$ have degrees less than that of $p$. Then $\phi'(p(x)) = \phi'(f(x))\phi'(g(x))$, but since $\phi'(p(x))$ is irreducible this means that one of the polynomials, say $\phi'(f(x))$, is of degree 0. Since $\phi'$ does not increase the degree of any polynomials, and $\phi'(p(x))$ has the same degree as $p(x)$ by assumption. As such, a contradiction is reached, since

$$\deg(p) = \deg(\phi'(p)) = \deg(\phi'(f)) + \deg(\phi'(g)) = \deg(\phi'(g)) \leq \deg(g) < \deg(p).$$

Example 3.21. Consider $p(x) = 8x^3 - 6x - 1 \in \mathbb{Z}[x]$. It is not at all obvious that this polynomial is irreducible, but consider the map projection map $\phi: \mathbb{Z} \to \mathbb{Z}_5$. The resulting polynomial $3x^3 - x - 1 \in \mathbb{Z}_5$ can be seen to lack roots, and hence it is irreducible as the polynomial is of degree 3. Hence $p(x)$ is irreducible.
3.3. IRREDUCIBILITY CRITERION  \hspace{1cm} \text{CHAPTER 3. POLYNOMIAL RINGS}

Theorem 3.20 is a very nice result, but it is often insufficient on its own.
Suppose \( p(x) \in \mathbb{Q}[x] \), then \( p(x) = \frac{a_n x^n + \cdots + a_0}{b_n} \). Multiplying by \( b_0 b_1 \cdots b_n \), one obtains \( c_0 + c_1 x + \cdots + c_n x^n \) with \( c_i \in \mathbb{Z} \). From here, factor out the greatest common divisor of all the coefficients and obtain a polynomial \( p'(x) \) whose coefficients have greatest common divisor equal to 1. One also obtains that \( a p(x) = b p'(x) \Rightarrow p(x) = \frac{b}{a} p'(x) \).

**Definition 3.22.** A polynomial \( p(x) \in \mathbb{Z}[x] \) whose coefficients have greatest common divisor equal to 1 is called a primitive polynomial.

Using this language, any polynomial \( p(x) \in \mathbb{Q}[x] \) can be written as \( q p'(x) \) where \( q \in \mathbb{Q} \) and \( p'(x) \in \mathbb{Z}[x] \) is a primitive polynomial.

**Theorem 3.23.** The product of two primitive polynomials is a primitive polynomial.

*Proof.* Let \( a(x), b(x) \in \mathbb{Z}[x] \) be primitive and consider the product \( f(x) = a(x) b(x) \). If \( f(x) \) were not primitive, there would be some prime number \( p \) that divided all the coefficients of \( a(x) b(x) \). Under the projection \( \rho : \mathbb{Z} \rightarrow \mathbb{Z}_p \), one gets \( 0 = \rho'(f(x)) = \rho'(a(x)) \rho'(b(x)) \), but \( a(x) \) and \( b(x) \) are primitive, meaning their images can not be zero under \( \rho' \), and since \( \mathbb{Z}_p[x] \) is an integral domain, a contradiction has been reached, and hence \( f(x) \) has to be primitive.

As already noted, every polynomial in \( \mathbb{Q}[x] \) can be written in the form \( q p(x) \) where \( q \in \mathbb{Q} \) and \( p(x) \in \mathbb{Z}[x] \) is a primitive polynomial, it turns out that this factorisation will also be unique.

**Theorem 3.24.** Let \( f(x) \in \mathbb{Q}[x] \), there is a unique \( q \in \mathbb{Q} \) and a unique primitive \( p(x) \in \mathbb{Z}[x] \) such that \( f(x) = q p(x) \).

*Proof.* Existence has already been shown, so now suppose that \( f(x) = q p(x) = e g(x) \) where \( p(x), g(x) \) are primitive. Then \( p(x) = \frac{c}{q} g(x) \), writing \( \frac{c}{q} = \frac{c}{d} \) in lowest terms with \( c, d \in \mathbb{Z} \), one gets \( p(x) = \frac{c}{d} g(x) \). This implies that \( d p(x) = c g(x) \), but \( \gcd(c, d) = 1 \), so every coefficient of \( g(x) \) has \( d \) as a factor, and every coefficient of \( p(x) \) has \( c \) as factor. Since \( p(x) \) and \( g(x) \) are primitive, this means \( c = d = 1 \), and the result follows.

**Corollary 3.24.1.** If \( f(x) \in \mathbb{Z}[x] \), then if \( p(x) \in \mathbb{Z} \) is a primitive polynomial and \( q \in \mathbb{Q} \) is a rational number such that \( f(x) = q p(x) \), then \( q \in \mathbb{Z} \).

*Proof.* One can begin by factoring out the greatest common divisor of all coefficients of \( f(x) \), \( d \), to obtain \( f(x) = d p(x) \) with \( p(x) \) primitive. Since the coefficients and primitive polynomials are unique, the result follows.

This implies that if \( f(x), g(x) \in \mathbb{Q}[x] \), and \( a, b \in \mathbb{Q} \), \( p(x), q(x) \in \mathbb{Z}[x] \) are primitive so that \( f(x) = a p(x) \), \( g(x) = b q(x) \) then \( f(x) g(x) = a b p(x) q(x) \), and since the product of two primitive polynomials is primitive, then \( p(x) q(x) \) is primitive. From this follows Gauss’ lemma:

**Theorem 3.25.** If \( p(x) \in \mathbb{Z}[x] \) is not the product of two polynomials in \( \mathbb{Z}[x] \), then it is irreducible in \( \mathbb{Q}[x] \).
CHAPTER 3. POLYNOMIAL RINGS 3.3. IRREDUCIBILITY CRITERION

Proof. Suppose that \( p(x) \) is reducible in \( Q[x] \), write it as \( p(x) = f(x)g(x) \) for \( f(x), g(x) \in Q[x] \). One can then write \( f(x) = ca(x) \), \( g(x) = db(x) \) for primitive \( a(x), b(x) \in Z[x] \) and \( c, d \in Q \). Subsequently \( p(x) = (cd)a(x)b(x) \). Since \( p(x) \in Z[x] \) \( cd \) must be an integer, and hence \( p(x) \) can be factored in \( Z[x] \). 

This finally leads to the classical result known as Eisenstein’s criterion:

**Theorem 3.26. Eisenstein’s criterion:** Let \( p(x) = a_0 + a_1x + ... + a_nx^n \in Z[x] \) be a polynomial such that a prime \( p \) divides all coefficients of \( p(x) \) except for \( a_n \) and \( p^2 \) does not divide \( p_0 \). \( p(x) \) is then irreducible over \( Q[x] \).

Proof. By Gauss’ lemma one need only check for factorisation over \( Z[x] \). Suppose that \( p(x) = f(x)g(x) \) for polynomials \( f(x), g(x) \in Z[x] \) of positive degree. One can write

\[
f(x) = b_0 + b_1x + ... + b_mx^m.
\]

And

\[
g(x) = c_0 + c_1 + ... + c_kx^k.
\]

Where \( m + k = n \). Then \( b_0c_0 = a_0 \), and since \( p \) divides \( a_0 \) but \( p^2 \) does not, it follows that \( p \) divides exactly one of \( b_0, c_0 \), say for the sake of argument that it divides \( b_0 \). Now

\[
p(x) = (b_0 + b_1x + ... + b_mx^m)(c_0 + c_1x + ... + c_kx^k) = a_0 + a_1x + ... + a_nx^n.
\]

By comparing coefficients one notices that \( a_i = \sum_{j=i} b_jc_j \), by induction one can show that \( p \) divides \( b_i \) for all \( i \). Suppose that \( p \) divides \( b_j \) for all \( j < i \) and that \( i \leq m \), then

\[
b_ic_0 + b_{i-1}c_1 + ... = a_i.
\]

By subtracting all the terms on the right side except the first one has

\[
a_i - b_{i-1}c_1 - ... = b_ic_0.
\]

Since \( p \) divides \( a_i \) and every \( b_j \) for \( j < i \), \( p \) divides \( b_ic_0 \). Since \( p \) does not divide \( c_0 \), it follows that \( p \) divides \( b_i \). By induction \( p \) divides all coefficients of \( f(x) \), but this is impossible since \( p \) does not divide \( a_n \). It follows that \( p(x) \) cannot be factored in \( Z[x] \), and hence is irreducible in \( Q[x] \) by Gauss’ lemma.

**Example 3.27.** Consider the polynomial \( p(x) = x^5 - 6x - 2 \). This polynomial is irreducible by Eisenstein’s criterion, which would take a lot of work to prove without it. 

**Definition 3.28.** Let \( p(x) = a_0 + a_1x + ... + a_nx^n \in F[x] \) be a polynomial over a field \( F \). The derivative of \( p(x) \), \( p'(x) \) is then defined as \( p'(x) = a_1 + ... + na_nx^{n-1} \).

The derivative can be checked to satisfy \( (f(x) + g(x))' = f'(x) + g'(x) \) and \( (f(x)g(x))' = f'(x)g(x) + f(x)g'(x) \). The derivative will turn out to be a useful tool in Chapter 4.
Chapter 4

Field Extensions

In this chapter, the concept of a field extension is properly introduced. Following this introduction, splitting fields are studied, then the Galois group of a field extension is defined, and finally, characters will be discussed.

4.1 Field extensions

Definition 4.1. Let E be a field and F be a subfield of E. E is said to be a field extension of F, and one writes $E/F$. E can be thought of as a vector space over F and the dimension of $E/F$ is written as $[E:F]$.

Example 4.2. Consider a field F and an irreducible $p(x) \in F[x]$, by Corollary 3.4.1 $E = F[x]/\langle p(x) \rangle$ is a field extension of F and $[E:F] = n$.

Theorem 4.3. Tower law: Let $K \subseteq F \subseteq E$ where $E/F$ and $F/K$ are finite field extensions, then $E/K$ is finite and $[E:K] = [E:F][F:K]$.

Proof. Let $x_1, x_2, ..., x_n$ be a basis for $E/F$ and $y_1, y_2, ..., y_m$ for $F/K$. Then $x_i y_j$ as $i$ and $j$ ranges over $1, ..., n$ and $1, ..., m$ respectively is a basis for $E/K$. To see this, note that any $\alpha \in K$ can be written as

$$\alpha = a_1 x_1 + a_2 x_2 + ... + a_n x_n = (c_{11}y_1 + ... + c_{1m}y_m)x_1 + (c_{21}y_1 + ... + c_{2m}y_m)x_2 + ... + (c_{n1}y_1 + ... + c_{nm}y_m)x_n.$$  

This means it is in the span of the vectors above. Insofar as linear independence goes, note that

$$\sum_{i,j} a_{ij} x_i y_j = 0 \Rightarrow \sum_{i} (\sum_{j} a_{ij} y_j) x_j = 0.$$  

$$\Rightarrow \sum_{j} a_{i,j} y_j = 0.$$  

Holds all i, but then $a_{ij} = 0$ for all i,j. The result follows.

Definition 4.4. Let $F \subseteq E$ be fields and $X \subseteq E$. The field $F(X)$ is defined to be the smallest subfield of $E$ containing $F$ and $X$, $X$ is said to generate $E$. An extension generated by a single element $\alpha$ is written $F(\alpha)$ and is called a simple extension. If $X = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ one writes $F(X) = F(\alpha_1, \alpha_2, ..., \alpha_n)$ and one says the extension is finitely generated.
From this one can see that \( E = F[x]/\langle p(x) \rangle \) is a simple extension of \( F \) since \( x \) generates it. If \( E/F \) is a field extension and \( \alpha \in E \) is the root of some polynomial \( p(x) \in F[x] \), then \( \alpha \) is said to be algebraic over \( F \). If \( \alpha \) is not algebraic over \( F \) it is said to be transcendental.

**Example 4.5.** Let \( E/F \) be a field extension and \( \alpha \in E \) be algebraic. From Chapter 3 it follows that there is a minimal polynomial of \( \alpha \), \( p(x) \in F[x] \). The homomorphism \( \phi : F[x] \rightarrow F(\alpha) \) given by \( f(x) \mapsto f(\alpha) \) induces a monomorphism \( \phi : F[x]/\langle p(x) \rangle \rightarrow F(\alpha) \). Since the image of \( \alpha \) is a field, it follows that the map is an isomorphism (recall that \( F(\alpha) \) is the smallest subfield of \( E \) containing \( F \) and \( \alpha \), and any such field must contain all polynomials in \( \alpha \)).

A field extension \( E/F \) is said to be algebraic if every element in \( E \) is algebraic over \( F \).

**Theorem 4.6.** A field extension \( E/F \) is finite if and only if it is algebraic and finitely generated.

**Proof.** Let \( E/F \) be a finite field extension. Pick a basis \( e_1, ..., e_n \) for \( E \). \( E = F(e_1, ..., e_n) \) so \( E \) is finitely generated, now let \( \alpha \in E \) be any element and consider the list

\[ 1, \alpha, \alpha^2, ..., \alpha^n. \]

Since \( [E:F] = n \) the list above is linearly independent, which means there is some nontrivial linear combination

\[ a_0 + a_1 \alpha + a_2 \alpha^2 + ... + a_n \alpha^n = 0, \]

meaning \( \alpha \) is a root of

\[ p(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n. \]

It follows that the extension algebraic.

Conversely, suppose that \( E/F \) is algebraic and finitely generated. One has that

\[ [F(\alpha_1, ..., \alpha_i) : F(\alpha_1, ..., \alpha_{i-1})] \] is finite since \( \alpha \) is algebraic over \( F \), and hence over \( F(\alpha_1, ..., \alpha_{i-1}) \). Inductively by the tower law one has:

\[ [F(\alpha_1, ..., \alpha_n) : F] = [F(\alpha_1, ..., \alpha_n) : F(\alpha_1, ..., \alpha_{n-1})] [F(\alpha_1) : F], \]

all of which are finite, and hence \( E/F \) is finite.

**Corollary 4.6.1.** Let \( E/F \) be a field extension with \( E = F(\alpha_1, ..., \alpha_n) \) where the \( \alpha_i \) are algebraic over \( F \). Then \( E \) is an algebraic, and in fact, a finite extension.

**Proof.** Denote \( F_i = F(\alpha_1, ..., \alpha_i) \). It is clear that \( F_{i+1}/F_i \) is a finite extension (since \( [F_{i+1} : F_i] < [F(\alpha_{i+1}) : F] \), by induction and the tower law it follows that \( [F_n : F] \) is finite, and hence algebraic.

Now let \( E/F \) be a field extension and \( \alpha, \beta \in E \) be algebraic. One has that \( F \subseteq F(\alpha) \subseteq F(\alpha, \beta) \), since \( [F(\alpha, \beta) : F(\alpha)] < \infty \) and \( [F(\alpha) : F] < \infty \), \( [F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)] [F(\alpha) : F] < \infty \). Since the extension is finite, by Theorem 4.5 every algebraic combination of \( \alpha \) and \( \beta \) is algebraic over \( F \). In particular, this means that if \( E/F \) is a field extension then all elements \( \alpha \in E \) that are algebraic over \( F \) form a field called the algebraic closure of \( F \) in \( E \).

**Theorem 4.7.** Let \( E/F \) be a field extension and \( \alpha \) be a root of \( p(x) = a_0 + a_1 x + ... + a_n x^n \) where \( a_i \) are algebraic for \( i = 0, 1, ..., n \), then \( \alpha \) is algebraic over \( F \).

**Proof.** Consider the tower \( F \subseteq F(a_0) \subseteq ... \subseteq F(a_0, ..., a_n) \subseteq F(a_0, ..., a_n, \alpha) \). Each extension is finite, and hence \( [F(a_0, ..., a_n, \alpha) : F] \) is finite and \( \alpha \) is algebraic.
4.2 Splitting fields

Definition 4.8. Let $F$ be a field and $p(x) \in F[x]$ be a polynomial, $p(x)$ is said to split in an extension $E/F$ if it can be written as a product of linear factors in $E[x]$. If $p(x)$ splits in an extension $E/F$ and is generated by the roots of $E$, it is called a splitting field of $p(x)$.

Theorem 4.9. Let $F$ be a field and $p(x) \in F[x]$, there is then a splitting field of $p(x)$.

Proof. First one shows that there is a field in which $p(x)$ splits, the proof is done by induction on the degree of $p(x)$. If $\deg(p(x)) = 1$ then $F$ is a field in which $p(x)$ splits. Now suppose that for each polynomial $p(x) \in F[x]$ of degree less than $n$ there is a field $E$ that contains all roots of $p(x)$ and let $f(x) \in F[x]$ be a degree $n$ polynomial. Write

$$f(x) = g(x)h(x)$$

For an irreducible $g(x)$. In $E = F[x]/\langle g(x) \rangle$ $f(x)$ has a root and hence $f(x) = (x - \alpha)b(x)$ for some polynomial of lower degree $b(x)$. By induction, there is a field extension of $E$ containing all the roots of $b(x)$, and hence there is a field extension $K/F$ containing all the roots of $g(x)$, and the induction is completed. Since there is a field extension $E$ within which $p(x)$ splits, one can then consider $K = F(\alpha_1, \ldots, \alpha_n)$ where the $\alpha_i$ are the roots of $p(x)$, this is a splitting field of $p(x)$ over $F$. \qed

So every polynomial has a splitting field, but is this field unique? The answer turns out to be in the affirmative, and in fact, more is true, which will be shown in a few steps below.

Theorem 4.10. Let $\phi : F \to F'$ be a field isomorphism and $\phi' : F[x] \to F'[x]$ be the induced isomorphism on polynomial rings. Let $p(x) \in F[x]$ be irreducible and $p'(x) = \phi'(p(x))$ be the corresponding irreducible polynomial in $F'[x]$. If $\alpha \in E$ is a root of $p(x)$ in some extension field $E/F$ and $\beta \in E'$ a root of $p'(x)$ for an extension $E'/F'$, then there is a unique isomorphism $\hat{\phi} : F(\alpha) \to F'(\beta)$ extending $\phi$ and mapping $\alpha$ to $\beta$.

Proof. Consider the isomorphisms described in Example 4.5

$$f : F[x]/\langle p(x) \rangle \to F(\alpha).$$

$$g : F'[x]/\langle p'(x) \rangle \to F'(\beta).$$

The map $\rho' \circ \phi' : F[x] \to F'[x]/\langle p'(x) \rangle$ has kernel $\langle p(x) \rangle$ as can readily be checked, hence there is an induced isomorphism $\sigma : F[x]/\langle p(x) \rangle \to F'[x]/\langle p'(x) \rangle$. Then $\hat{\phi} = g \circ \sigma \circ f^{-1}$ is an isomorphism $\hat{\phi} : F(\alpha) \to F'(\beta)$ which extends $\phi$. This isomorphism is unique since any such map fixing $F$ is determined by the image of $\alpha$. \qed

Definition 4.11. Let $f(x) \in F[x]$ be a polynomial and $p_1(x)p_2(x)\ldots p_n(x) = f(x)$ be a factorization of $f(x)$ into irreducibles, $f(x)$ is said to be a separable polynomial if each $p_i(x)$ does not have any repeated roots (where $\alpha$ is a repeated root of $p_i(x)$ if $p_i(x) = (x - \alpha)^2g(x)$) in any field extension of $F$. 

43
Theorem 4.12. Let \( p(x) \in F[x] \) be a polynomial over the field \( F \), \( p(x) \) is separable if and only if the greatest common divisor of \( p(x) \) and its derivative \( p'(x) \) is 1.

Proof. Suppose there was a field extension \( E/F \) such that \( p(x) \) has a multiple root \( \alpha \in E \). Then

\[
p(x) = (x - \alpha)^2 g(x).
\]

\[
p'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x).
\]

Hence both \( p(x) \) and \( p'(x) \) has \( \alpha \) as root. Since every polynomial over \( F \) with \( \alpha \) as root has the minimal polynomial \( q(x) \) as a factor, both \( p(x) \) and \( p'(x) \) have \( q(x) \) as a factor. Suppose conversely that \( p(x) = a(x)b(x) \) and \( p'(x) = a(x)c(x) \) where \( a(x) \) is a polynomial of positive degree, then there is some field extension \( E/F \) in which \( a(x) \) has a root, say \( \alpha \), it follows that

\[
p(x) = (x - \alpha)h(x).
\]

\[
p'(x) = (x - \alpha)g(x).
\]

Then

\[
p'(x) = (x - \alpha)h'(x) + h(x) = (x - \alpha)g(x).
\]

So \( h(x) \) also has \( \alpha \) as a root and \( \alpha \) is hence a multiple root of \( p(x) \).

Definition 4.13. A field \( F \) is called perfect if all irreducible polynomials over \( F \) have no multiple roots, i.e. all polynomials in \( F[x] \) are separable.

Theorem 4.14. An irreducible polynomial \( p(x) \in F[x] \) is separable if and only if \( p'(x) = 0 \)

Proof. If \( p(x) \) has multiple roots, then \( p'(x) \) and \( p(x) \) have a common factor \( q(x) \) of positive degree. But since \( p(x) \) is irreducible this means that \( q(x) = cp(x) \) for some non-zero \( c \in F \), and since \( p'(x) \) has a lower degree than \( p(x) \), this means that \( p'(x) \) must be zero. Now suppose that \( p'(x) = 0 \), then \( p(x) \) and \( p'(x) \) have a common factor \( p(x) \), meaning \( p(x) \) has multiple roots by Theorem 4.11.

Corollary 4.14.1. Let \( F \) be a field of characteristic 0, then \( F \) is perfect.

Proof. Let \( a_0 + a_1 x + ... + a_n x^n = p(x) \in F[x] \) be irreducible and of order \( n > 0 \). Then \( p'(x) = a_1 + ... + n a_n x^{n-1} \), but since \( char F \neq 0 \), \( p'(x) \neq 0 \). From this it follows that \( p(x) \) is irreducible.

Now let us return to the topic of splitting fields.

Theorem 4.15. Let \( \phi : F \to F' \) be an isomorphism of fields and \( \phi' : F[x] \to F'[x] \) be the induced map on polynomial rings. If \( f(x) \in F[x] \) and \( g(x) = \phi'(f(x)) \) the corresponding polynomial in \( F'[x] \), and \( E \) is a splitting field of \( f(x) \) over \( F \), and \( E' \) a splitting field of \( g(x) \) over \( F' \) then:

1) There is an isomorphism \( \hat{\phi} : E \to E' \) extending \( \phi \).

2) If \( f(x) \) is separable, then \( \phi \) has exactly \( [E:F] \) extensions \( \hat{\phi} \).

This yields the uniqueness of splitting fields up to isomorphism by taking \( \phi : F \to F \) to be the identity map.
Proof.
1) The proof is done by induction on \([E : F]\). If \([E : F] = 1\) then \(E = F\) and hence \(f(x)\) splits over \(F\), but then \(g(x) = \phi'(f(x))\) splits over \(F'\) meaning \(E' = F'\). The extension \(\hat{\phi} = \phi\) can then be chosen, and it is trivial to verify that it is unique.

The result follows for \([E : F] = 1\). Now suppose that it holds for fields so that \([E : F] < n\) and let \([E : F] = n\). Factor \(f(x)\) into irreducibles

\[
f(x) = p_1(x)p_2(x)...p_n(x).
\]

Take one of the \(p_i(x)\) that are of degree greater than one and pick a root \(\alpha\) of \(p_i(x)\) in \(E\) and a root of \(\phi'(p_i(x))\), say \(\beta\). By Theorem 4.9 there is a map extending \(\phi\)

\[
\hat{\phi} : F(\alpha) \to F'(\beta)
\]

Now \([E : F(\alpha)] = \frac{[E : F]}{[F(\alpha) : F]} < [E : F]\), and since \(E\) is still a splitting field of \(f(x)\) over \(F(\alpha)\) and \(E'\) of \(g(x)\) over \(F'(\beta)\), it follows by induction that there is an extension \(\hat{\phi} : E \to E'\) which extends \(\hat{\phi}\) and hence \(\phi\).

2) This is also done by induction on \([E : F]\). If \([E : F] = 1\), then it was already shown that there is a unique extension of \(\phi\), namely \(\phi\) itself. Now if \([E : F] > 1\), then factor \(f(x) = p(x)g(x)\) where \(p(x) \in F[x]\) is irreducible of degree \(d > 1\). Pick any root \(\alpha\) of \(p(x)\) and consider the extension

\[
\hat{\phi} : E \to E'.
\]

Then \(\beta = \hat{\phi}(\alpha)\) is a root of \(\phi'(p(x)) = p'(x)\). Since \(g(x)\) is separable, there are exactly \(d\) roots of \(p'(x)\) to choose from, hence there are exactly \(d\) isomorphisms \(\hat{\phi} : F(\alpha) \to F'(\beta)\) extending \(\phi\), one for each root \(\beta\) of \(p'(x)\). Now \(E\) is a splitting field of \(f(x)\) over \(F(\alpha)\) and \([E : F(\alpha)] = [E : F]/d\), by induction there are exactly \([E : F]/d\) extensions of any given \(\phi\), meaning there are a total of \([E : F] = [E : F(\alpha)] \cdot d\) extensions of \(\phi\) because restricting to \(F(\alpha)\) gives one of the isomorphisms in question. \(\Box\)

4.3 The Galois group

Definition 4.16. Let \(F\) be a field, an isomorphism \(\phi : F \to F\) is called an automorphism of \(F\). If \(E/F\) is a field extension of \(F\), then an automorphism \(\phi\) of \(E\) is said to fix \(F\) point-wise if \(\phi(x) = x\) for all \(x \in F\).

It is clear that the automorphisms of a Field form a group under composition, and that the automorphisms of \(E\) fixing \(F\) pointwise form a subgroup is not hard to verify either, but why might automorphism groups be interesting? The next result gives a hint.

Theorem 4.17. Let \(E/F\) be a field extension and \(f(x) \in F[x]\). If \(\phi\) is an automorphism of \(E\) fixing \(F\) point-wise and \(\alpha \in E\) is a root of \(f(x)\), then \(\phi(\alpha)\) is a root of \(f(x)\).

Proof. Consider the polynomial

\[
f(x) = a_0 + a_1x + ... + a_nx^n.
\]
4.4 CHARACTERS CHAPTER 4. FIELD EXTENSIONS

With root \( \alpha \), so

\[
a_0 + a_1\alpha + ... + a_n\alpha^n = 0.
\]

Then

\[
0 = \phi(a_0 + a_1\alpha + ... + a_n\alpha^n) = a_0 + a_1\phi(\alpha) + ... + a_n\phi(\alpha)^n.
\]

Hence \( \phi(\alpha) \) is a root of \( f(x) \).

**Definition 4.18.** Let \( E/F \) be a field extension of \( F \), the group of automorphisms of \( E \) fixing \( F \) pointwise is called the Galois group of \( E/F \), written as \( G(E/F) \). If \( f(x) \in F[x] \) and \( E \) is a splitting field, then the Galois group of \( f(x) \) is the Galois group \( G(E/F) \).

It follows from Theorem 4.15 that the Galois group of a separable polynomial of order \( n \) is a subgroup of \( S_n \).

**Example 4.19.** From Theorem 4.13 one has that \( G(E/F) \) where \( E \) is a splitting field of a separable polynomial has order \( [E:F] \).

Now let’s turn to intermediate field extensions:

**Theorem 4.20.** Let \( F \subseteq B \subseteq E \) with \( B/F \) a splitting field of some \( f(x) \in F[x] \). If \( \sigma \in G(E/F) \) then \( \sigma|_B \in G(B/F) \).

**Proof.** \( B \) is a splitting field of

\[
f(x) = a_0 + a_1x + ... + a_nx^n.
\]

It follows that \( B = F(\alpha_1, ..., \alpha_n) \) where \( \alpha_i \) are roots of \( f(x) \). Then

\[
a_0 + a_1\alpha + ... + a_n\alpha^n = 0 \Rightarrow a_0 + a_1\sigma(\alpha) + ... + a_n\sigma(\alpha)^n = 0.
\]

So \( \alpha \) is mapped to another root of \( f(x) \), meaning \( B \) maps to itself. \( \sigma|_B \) is evidently injective, to see it is also surjective note that \( \sigma|_B \) can be thought of as a linear map of \( B/F \), and by the Rank-Nullity theorem, any injective linear map from a vector space to itself is also surjective.

**Theorem 4.21.** Let \( F \subseteq B \subseteq E \) with \( B/F \) a splitting field of some \( f(x) \in F[x] \) and \( E/F \) the splitting field of some \( g(x) \in F[x] \). Then \( G(E/B) \triangleleft G(E/F) \) and \( G(E/F)/G(E/B) \cong G(B/F) \).

**Proof.** Let \( \phi : G(E/F) \to G(B/F) \) be defined by \( \phi(\sigma) = \sigma|_B \), by Theorem 4.18 this is well defined, and it can easily be seen to be a homomorphism. The kernel of \( \phi \) consists exactly of the automorphisms of \( E \) that fix \( B \), i.e. \( G(E/B) \). It is surjective since any automorphism of \( B \) can be extended to an automorphism of \( E \) (\( E \) is a splitting field over \( F \) and hence over \( B \)).

**4.4 Characters**

**Definition 4.22.** Let \( G \) be a group and \( E \) be a field, a character of \( G \) in \( E \) is a homomorphism \( \sigma : G \to E^* = E/\{0\} \), i.e. the multiplicative group of non-zero elements in \( E \).
Example 4.23. Let $\sigma : E \to E$ be an automorphism of $E$, then $\sigma|_E^*$ is a character since $\sigma(xy) = \sigma(x)\sigma(y)$.

Definition 4.24. A set of characters of $G$ in $E \{\sigma_1, \sigma_2, ..., \sigma_n\}$ of characters is said to be independent if there are no $a_i \in E$, not all zero, such that $a_1\sigma(x) + a_2\sigma(x) + ... + a_n\sigma(x) = 0$ for all $x \in G$.

Theorem 4.25. Dedekind’s lemma: Every set of distinct characters $\{\sigma_1, ..., \sigma_n\}$ of a group $G$ in a field $E$ are independent.

Proof. The proof is done by induction on the number of characters. $a\sigma(x) = 0$ for all $x \in G \Rightarrow a = 0$. Assume by induction that the result holds for less than $n$ characters and suppose

$$a_1\sigma_1(x) + ... + a_n\sigma_n(x) = 0.$$

For all $x \in G$. It may be assumed all $a_i$ are non-zero since otherwise, the result follows from the induction hypothesis. Multiplying by $a_n^{-1}$ one may assume $a_n = 1$. Now since $\sigma_1 \neq \sigma_n$ there is some $y \in G$ so that $\sigma_1(y) \neq \sigma_n(y)$, replacing $x$ by $xy$ one gets

$$a_1\sigma_1(x)\sigma_1(y) + ... + \sigma_n(x)\sigma_n(y) = 0.$$

This yields

$$a_1\sigma_n(y)^{-1}\sigma_1(y)\sigma_1(x) + ... + \sigma_n(x) = 0.$$

Subtracting from the original equation one gets

$$a_1[1 - \sigma_n(y)^{-1}\sigma_1(y)]\sigma_1(x) + ... + a_{n-1}[1 - \sigma_n^{-1}(y)\sigma_{n-1}(y)]\sigma_{n-1}(x) = 0.$$

By induction all the coefficients are 0, and hence $\sigma_n(y) = \sigma_1(y)$, a contradiction.

Since field automorphisms are characters, the following definition makes sense:

Definition 4.26. Let $G \subseteq \text{Aut}(E)$ be a set of automorphisms of $E$, then $E^G = \{x \in E : \sigma(x) = x, \forall x \in G\}$ is called the fixed field of $G$.

It is easy to see that $E^G$ is a subfield of $E$ (hence the name).

Theorem 4.27. Let $G = \{\sigma_1, ..., \sigma_n\}$ be a set of automorphisms of $E$, then $m = [E : E^G] \geq |G|$

Proof. Suppose to the contrary that $m < n$ and let $e_1, ..., e_m$ be the basis of $E/E^G$. Consider the following system of equations

$$a_1\sigma_1(e_1) + ... + a_n\sigma_n(e_1) = 0.$$

$$...$$

$$a_1\sigma_1(e_m) + ... + a_n\sigma_n(e_m) = 0.$$

By assumption there are more unknowns than variables, meaning that there is a non-zero solution $(a_1, ..., a_n) \in E^n$ of the system above. Since $e_1, ..., e_m$ forms a basis of $E/E^G$, $x \in E$ can be written as

$$x_1e_1 + ... + x_me_m.$$

For $x_i \in E^G$. Multiplying row $i$ by $x_i$ and summing up all the rows one gets:

$$a_1\sigma_1(x) + ... + a_n\sigma_n(x) = 0$$

For all $x \in E$, this contradicts the independence of characters, and hence the assumption that $n > m$ is false.
If G is also a group, there is an equality of \([E : E^G]\) and \(|G|\).

**Theorem 4.28.** Let \(G = \{\sigma_1, ..., \sigma_n\}\) be a group of automorphisms of the field \(E\). Then \([E : E^G] = |G|\).

**Proof.** By Theorem 4.25 only \([E : E^G] \leq n\) needs to be shown. Suppose to the contrary that \(n < m\) and suppose that \(\alpha_1, ..., \alpha_n, \alpha_{n+1}\) are linearly independent vectors in \(E/E^G\). The system of equations

\[
x_1\sigma_1(\alpha_1) + ... + x_{n+1}\sigma_1(\alpha_{n+1}) = 0.
\]

\[...
\]

\[
x_1\sigma_n(\alpha_1) + ... + x_{n+1}\sigma_n(\alpha_{n+1}) = 0.
\]

Since there are more unknowns than there are equations, there is some non-zero \((a_1, ..., a_{n+1})\) that solves the system. One may choose a solution with as few 0-components as possible, and by re-indexing one can let the first \(r\) components be non-zero and the rest 0, \(r \neq 1\) since then \(a_1\sigma_1(\alpha_1) = 0 \Rightarrow a_1 = 0\). Now one can normalize and pick a solution such that \(a_r = 1\). If all \(a_i \in E^G\) then the row corresponding to the identity automorphism would violate the linear independence of the \(\alpha_i\), by re-indexing one may assume \(a_1\) does not lie in \(E^G\). There is hence some \(\sigma_k\) such that \(\sigma_k(\alpha_1) \neq \alpha_1\), now applying \(\sigma_k\) to equation \(i\) one gets:

\[
\sigma_k\sigma_i(\alpha_1) + ... + \sigma_k\sigma_i(\alpha_r) = 0.
\]

Since \(G\) is a group, \(\sigma_k\sigma_j = \sigma_i\) for some \(j\), and hence one can write \(\sigma_i(\alpha_1)\sigma_k(a_1) + ... + \sigma_i(\alpha_r)\), subtracting from the original equation one obtains

\[
(a_1 - \sigma_k(a_1))\sigma_i(\alpha_1) + ... + (a_{r-1} - \sigma_k(a_{r-1}))\sigma_i(\alpha_{r-1}) = 0.
\]

Since \(\sigma_k(a_1) \neq a_1\), this is a new solution to the original system with fewer than \(r\) non-zero terms, which is a contradiction, and hence \([E : E^G] \leq n\). \(\square\)

**Corollary 4.28.1.** Let \(E\) be a field and \(H\) and \(G\) be two finite subgroups of \(\text{Aut}(E)\), then \(E^G = E^H \Rightarrow G = H\).

**Proof.** If \(\sigma \in G = \{\sigma_1, ..., \sigma_n\}\) then \(\sigma\) clearly fixes \(E^G\) point-wise. Suppose conversely that \(\sigma\) fixes \(E^G\) point-wise. Then \(E^G\) is fixed by \(n + 1\) elements, \(G \cup \{\sigma\}\) and \(n = [E : E^G] \geq |G \cup \{\sigma\}| = n + 1\) which is a contradiction, hence \(G(E/E^G) = G\).

As such, \(\sigma \in G\) fixes \(E^G = E^H\), and hence \(\sigma \in H\), since \(|G| = |H|\) it follows that \(G = H\). \(\square\)
Chapter 5

Galois extensions

In this chapter Galois extensions will be discussed. First, three equivalent definitions of a Galois extension are given. Then intermediate field extensions are studied, and various conditions for an intermediate extension to be Galois are given. Finally, the fundamental theorem of Galois theory is stated and proved. Although the result will not find much usage in the rest of the text, it ought to be mentioned for completeness.

5.1 Galois extensions

Theorem 5.1. For a finite field extension, \( E/F \), the following are equivalent:

1) \( F = E^G \) where \( G = G(E/F) \).

2) Every irreducible \( p(x) \in F[x] \) with a root in \( E \) is separable and has all roots in \( E \).

3) \( E \) is the splitting field of some separable \( f(x) \in F \).

Proof.

1) \( \Rightarrow \) 2)

Let \( p(x) \in F[x] \) be irreducible with one root \( \alpha \in E \) and consider the polynomial

\[
g(x) = (x - \alpha)(x - \beta)...(x - \gamma).
\]

Where \( \alpha, \beta, ... \gamma \) are all the conjugates of \( \alpha \) by elements in \( G \) taken only once. Since \( F = E^G \), and \( g(x) \) is invariant under applying any element in \( G \), it follows that \( g(x) \in F[x] \). Since \( F[x] \) is a PID and \( p(x) \) is irreducible with \( \alpha \) as root, it follows that \( g(x) \) is a multiple of \( p(x) \), and hence \( p(x) \) is separable with all roots in \( E \).

2) \( \Rightarrow \) 3)

\( E/F \) is finite so \( E = F(\alpha_1, \alpha_2, ..., \alpha_n) \) where all the \( \alpha_i \) are algebraic over \( F \). Now let \( p_1(x) \) be the minimal polynomial of \( \alpha_1 \), by assumption \( p_1(x) \) is separable and splits in \( E \). Hence, the splitting field of \( p_1(x) \), \( B \), is a subfield of \( E \). If all the \( \alpha_i \) are in \( B \) then the result is immediate, if not pick the minimal polynomial of \( \alpha_2 \) and take the splitting field of \( p_1(x)p_2(x) \), etc. Since \( E/F \) is finite this process eventually stops, and the result follows.

3) \( \Rightarrow \) 1)

By Theorem 4.23 \( |G| = [E : F] \) and Theorem 4.26 gives \( |G| = [E : E^G] \) meaning \( [E : F] = [E : E^G] \), and since \( F \subseteq E^G \), it follows that \( F = E^G \).
If $F$ is a field and if $E/F$ is a splitting field of some $f(x) \in F[x]$, then the extension $E/F$ is finite since by assumption $F$ is generated by a finite number of algebraic elements.

**Definition 5.2.** A field extension $E/F$ that satisfies any of the above criteria is said to be a Galois extension.

**Definition 5.3.** Let $F \subseteq B \subseteq E$ be field extensions, then $B$ is said to be an intermediate field of $E$ and $F$.

**Theorem 5.4.** Let $E/F$ be a Galois extension and $B$ an intermediate field, then $E/B$ is a Galois extension.

**Proof.** Let $p(x) \in B[x]$ be an irreducible polynomial with a root $\alpha \in E$. Take all the conjugates of $\alpha$ under $G = G(E/F)$ and consider the polynomial

$$g(x) = (x - \alpha)(x - \beta) \cdots (x - \gamma).$$

So that $\alpha, \beta, \ldots, \gamma$ are the conjugates of $\alpha$ under $G$. Now $E/F$ is Galois, meaning $F = E^G$ and so $g(x) \in F[x]$, hence $g(x) \in B[x]$. Since $B[x]$ is a PID, this means that $p(x)$ is a factor of $g(x)$. It follows that $p(x)$ is separable and splits in $E$, i.e. $E/B$ is Galois.

**Definition 5.5.** Let $E/F$ be a Galois extension with $B$ and $C$ intermediate fields, then $B$ and $C$ are said to be conjugates if there is an isomorphism $\tau : B \rightarrow C$ fixing $F$.

**Theorem 5.6.** Let $E/F$ be a Galois extension and $B$ an intermediate field. The following statements are equivalent:

1) $B$ has no other conjugates than itself.

2) If $\sigma \in G(E/F)$ then $\sigma|_B \in G(B/F)$.

3) $B/F$ is a Galois extension.

**Proof.** The Theorem will be proven in the order 1) $\Rightarrow$ 2) $\Rightarrow$ 3) $\Rightarrow$ 1)

1) $\Rightarrow$ 2) is evident

2) $\Rightarrow$ 3)

Let $p(x)$ be an irreducible polynomial in $F[x]$ with $\alpha \in B$ as a root. By assumption $p(x)$ splits in $E$ and is separable since $E/F$ is Galois. If $\beta \in E$ is another root of $p(x)$ in $E$, then there is an isomorphism $\tau : F(\alpha) \rightarrow F(\beta)$ fixing $F$, and since $E/F$ is the splitting field of some polynomial over $F(\alpha)$ and $F(\beta)$ this extends to a $\sigma \in G(E/F)$. Now $\sigma|_B \in G(B/F)$, meaning that $\sigma(\alpha) = \beta$ is in $B$, and hence $p(x)$ splits over $B$, and $B/F$ is Galois.

3) $\Rightarrow$ 1)

B is the splitting field of some separable $p(x) \in F[x]$, meaning that $B = F(\alpha_1, \ldots, \alpha_n)$ where $\alpha_i$ are the roots of $p(x)$. Any isomorphism $\phi : B \rightarrow C$ where $C \subseteq E$ fixing $F$ extends to an automorphism in $G(E/F)$, and since $B/F$ is a splitting field, it permutes the roots $\alpha_i$, and hence maps $B$ to itself, so 1) follows. 

50
§5.2. The fundamental theorem

Theorem 5.7. Let $E/F$ be a Galois extension with $G = G(E/F)$ as its Galois group.

- The map $\gamma : \text{Sub}(G) \rightarrow \text{Lat}(E/F)$ defined by $\gamma(H) = E^H$ is an order reversing lattice isomorphism with inverse $\delta : \text{Lat}(E/F) \rightarrow \text{sub}(G)$ given by $\delta(B) = G(E/B)$.

- $[B : F] = \frac{|G|}{|G(E/B)|}$.

- $B/F$ is Galois if and only if $G(E/B) \triangleleft G$.

Proof. The map can easily be seen to be order reversing by $K \leq H \Rightarrow E^H \subseteq E^K$, it is injective since $\gamma(K) = \gamma(H)$ means $E^K = E^H$, and by Corollary 4.26.1 $H = K$.

Surjectivity can be seen by the fact that $\gamma(\delta(B)) = E^{G(E/B)}$, which is $B$ by Theorem 5.4. Note that

$$[B : F] = \frac{[E : F]}{[E : B]} = \frac{|G|}{|G(E/B)|}.$$  

From which the equality follows. If $B/F$ is Galois where $B$ is an intermediate field then by Theorem 4.19 $G(E/B) \triangleleft G$. Conversely suppose that $H \triangleleft G$, and consider the field $E^H$. This is a Galois extension by Theorem 5.6 since for any $\sigma \in G$ and $\tau \in H$, there is $\tau' \in H$ such that $\sigma \tau = \tau \sigma$, meaning if $\alpha \in E^H$ then $\tau \sigma(\alpha) = \sigma \tau'(\alpha) = \sigma(\alpha)$, i.e $\sigma(\alpha)$ is fixed by $H$, and as such $\sigma(E^H) \subseteq E^H$. Since $\sigma$ is an isomorphism, the dimension of $\sigma(E^H)$ over $F$ is the same as that of $E^H$, and hence $\sigma(E^H) = E^H$. The result follows from the fact that $G(E/E^H) = H$. $\square$
Chapter 6

The Abel Ruffini Theorem

In this chapter, the Abel Ruffini theorem is stated and proved i.e. that not every 5th degree polynomial over the rationals is solvable by radicals. It turns out that this is related to the solvability of the Galois group the polynomial, and as such results from Chapter 1 will be used.

6.1 Solvable extensions

Example 6.1. consider the polynomial

\[ p(x) = x^4 - 2 \in \mathbb{Q}[x]. \]

One can obtain a splitting field of \( p(x) \) via a step-by-step process as follows: First, embed \( \mathbb{Q} \) in \( \mathbb{C} \) and add the real fourth root of \( 2 \) to obtain the extension \( \mathbb{Q}(\sqrt[4]{2}). \) This is a simple extension \( F(\alpha) \) with a special property, namely that that the added element, \( \sqrt[4]{2} \) can be raised to some power \( r \) (in this case 4) such that \( \alpha^r \in F. \) The splitting field also needs to contain the element \( i, \) so one gets \( \mathbb{Q}(\sqrt[4]{2}, i). \) One has the following tower of fields: \( \mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, i). \)

Definition 6.2. A field extension \( F \subseteq E \) is called a pure extension if \( E = F(\alpha) \) where \( \alpha^m \in F \) for some integer \( m. \) A tower of fields

\[ F \subseteq F_1 \subseteq ... \subseteq F_n. \]

Is a radical tower if \( F_{i+1}/F_i \) is a pure extension and \( F_n/F \) is called a radical extension.

The idea is that to have a field with a solution of a polynomial in terms of radicals, one builds the field up by adding one n’th root of some element in the previous field at a time.

Definition 6.3. A polynomial \( p(x) \in F[x] \) is said to be solvable by radicals if there is a radical extension of \( F \) that contains a splitting field of \( p(x) \) over \( F. \) In general, a field extension \( L/F \) is said to be solvable if \( L \) is contained in a radical extension of \( F \)

The key result of this section will be that if \( F \) is a field of characteristic 0, then \( f(x) \in F[x] \) is solvable by radicals if and only if the Galois group of \( f(x) \) over \( F \) is solvable. To give a proof, there first needs to be a discussion about roots of unity in a field.
6.2 Roots of unity

Let $F$ be a field and consider the equation $x^n - 1$ where 1 is the multiplicative identity of $F$. One can see for any field extension $E/F$ the elements that solve this equation form a subgroup of $E^*$ since $1^n = 1$, $(ab)^n = a^n b^n$ and $a a^{n-1} = 1$.

**Theorem 6.4.** Let $E$ be a field and $G \leq E^*$ be a finite subgroup with $|G| = n$, then $G$ is cyclic.

**Proof.** Let $d|n$ be any divisor, the goal of this proof is to show there is at most one cyclic subgroup of order $d$ in $G$. Suppose that $x \in G$ has order $d$, then $x^d = 1$, but since there are at most $d$ such elements (i.e. the powers of $x$) it follows that there is at most one such group, and hence $G$ is cyclic by Theorem 2.17.

In particular, this means that the group consisting of elements that solve the equation $x^n = 1$ is cyclic, and as such the splitting field of such a polynomial is a simple extension. A generator of the $n$’th roots of 1 is called a primitive root of unity.

**Theorem 6.5.** Let $F$ be a field and $\omega$ be a primitive $n$’th root of unity, if $E = F(\omega)$ then the Galois group $G(E/F)$ is abelian.

**Proof.** Any $\sigma \in G(E/F)$ is determined by the image of $\alpha$, which is also a root of $x^n = 1$, so $\sigma(\omega) = \omega^i$ for some $i$. Now let $\sigma, \tau \in G(E/F)$. One has

$$\sigma(\tau(\omega)) = \sigma(\omega^i) = \omega^{ij} = \omega^i \tau(\omega^j) = \tau(\sigma(\omega)).$$

Meaning that $G(E/F)$ is abelian. □

Now, returning to the topic at hand.

**Theorem 6.6.** Let $L$ be a splitting field of the polynomial $g(x) = x^n - a$ over the field $F$, then $G(L/K)$ is solvable.

**Proof.** The field $L$ can be written $L = F(\alpha, \omega)$ where $\omega$ is a primitive $n$’th root of unity and $\alpha$ is any element such that $\alpha^n = a$. Consider now the tower of groups

$$\{e\} \triangleleft G(L/F(\omega)) \leq G(L/F).$$

First of all one can note that $G(L/F(\omega))$ is cyclic since any automorphism is determined by the image of $\alpha$, which is also a root of $x^n = 1$. This means that $\sigma(\alpha) = \alpha \omega^i$, and hence that

$$\tau \sigma(\alpha) = \tau(\alpha \omega^i) = \tau(\alpha) \tau(\omega^i) = \alpha \omega^j \omega^i = \alpha \omega^{i+j}.$$  

From this one can determine that it is cyclic. Finally, by Theorem 4.19 one has $G(L/F(\omega)) \triangleleft G(L/F)$ and

$$G(L/F)/G(L/F(\omega)) \cong G(F(\omega)/F).$$

$G(F(\omega)/F)$ is abelian, and hence $G(L/F)$ is solvable. □

**Theorem 6.7.** Let $K \subseteq L$ and $L \subseteq L'$ be two field extensions:
CHAPTER 6. THE ABEL RUFFINI THEOREM 6.2. ROOTS OF UNITY

- If $\sigma : L \to L'$ is an isomorphism fixing $K$ and $K \subseteq L$ is a radical extension then so is $K \subseteq L'$.

- If $L$ is a radical $m$-extension of $K$ and $L'$ is a radical extension of $K'$ where $K \subseteq K' \subseteq L$ with $L$ and $L'$ contained in a field $M$, then $L \lor L'$ is a radical extension of $K$.

Proof. Consider the radical tower

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L.$$  

Where $L = K(\alpha_1, \ldots, \alpha_b)$, then $L' = \sigma(L) = K(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$ with

$$K = K_0 \subseteq K(\sigma(\alpha_1)) \subseteq \ldots \subseteq K(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)).$$

a radical tower since $\sigma(\alpha_i)^m = \sigma(\alpha_i^m)$ which lies in $\sigma(K_{i-1})$, thus, the first result is proved.

Now consider the radical tower

$$K \subseteq K(\alpha_1) \subseteq \ldots \subseteq K(\alpha_1, \ldots, \alpha_n) = L \subseteq K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) = L \lor L'.$$

The $\beta_i$ are the elements adjoined to $K'$ to obtain $L'$, that is $L' = K'(\beta_1, \ldots, \beta_m)$. The tower obtained is radical since $\alpha_i^{m+1}$ is in $K_i$ for each $i$ and $\beta_j^{m+1}$ is in $K_j'$, which is in the previous field as $K'$ is contained in $L$.

**Theorem 6.8.** Let $L$ be a radical extension of a field $K$, then there is a splitting field containing $L$, say $E$, which is also a radical extension.

Proof. Let $L = K(\alpha_1, \ldots, \alpha_n)$ where

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L.$$  

With $K_{i+1} = K_i(\alpha_{i+1})$ and $\alpha_i^{m+1} \in K_i$. Pick the minimal polynomial of each $\alpha_i$ over $K_i$, $f_i$. Now consider the splitting field $N$ of

$$f = f_1 f_2 \ldots f_n.$$  

If $\beta_i$ is any root of $f_i$ there is an isomorphism $\tau : K(\alpha_i) \to K(\beta_i)$ fixing $K$ and mapping $\alpha_i$ to $\beta_i$. This extends to an isomorphism $\sigma : N \to N$. This maps $L$ to $\sigma(L)$, which is also a radical extension by the first part of Theorem 6.4. $N$ is then the composite of all such fields, i.e. $\sigma_1(L) \lor \ldots \lor \sigma_k(L)$, and by the second part of Theorem 6.7 this is a radical extension.

**Theorem 6.9.** Let $L$ be a radical Galois extension of $K$. Then $G(L/K)$ is a solvable group.

Proof. Consider $L = K(\alpha_1, \ldots, \alpha_n)$ and the following radical tower:

$$K \subseteq K(\alpha_1) \subseteq \ldots \subseteq K(\alpha_1, \ldots, \alpha_n).$$

The claim is proved by induction on the number of radical extensions. Consider a radical extension $K \subseteq K(\alpha)$, since $\alpha^n = a \in K$ for some $n$, pick the smallest such $n$. Let $N$ be the splitting field of the polynomial $x^n = a$ over $K$, then $N = K(\alpha, \omega)$.
for some primitive nth root of unity $\omega$. By Theorem 6.6 $G(N/K)$ is solvable, now $K(\alpha)/K$ is Galois so

$$G(K(\alpha)/K) \cong G(N/K)/G(N/K(\alpha)).$$

Meaning $G(K(\alpha)/K)$ is also solvable by Corollary 2.27.1.

Now assume the claim is true when for towers with $n$ or fewer fields and consider the following towers

$$K = K_0 \subseteq K_1 \subseteq ... \subseteq K_n = L.$$

$$K = K_0 \subseteq K_1 \subseteq K_1(\omega) \subseteq ... \subseteq K_n(\omega) = L(\omega).$$

Where $\omega$ is a primitive root of unity. Then the number of fields in the tower from $K_1(\omega)$ to $L(\omega)$ is $n$, hence the group $G(L(\omega)/K_1(\omega))$ is solvable by induction. Now according to Theorem 6.6 $G(K_1(\omega)/K)$ is solvable and

$$G(K_1(\omega)/K) \cong G(L(\omega)/K)/G(L(\omega)/K_1(\omega)).$$

It follows from Theorem 2.25 that $G(L(\omega)/K)$ is solvable, and from Corollary 2.27.1 that

$$G(L/K) \cong G(L(\omega)/K)/G(L(\omega)/L).$$

Is solvable.

**Theorem 6.10.** Let $F$ be a field of characteristic 0, then $f(x) \in F[x]$ is solvable by radicals only if the Galois group of $f(x)$ is solvable as a group.

**Proof.** If $f(x)$ is solvable by radicals then there is a splitting field $E$ of $f(x)$ over $F[x]$ that is contained within some radical extension $L$, by Theorem 6.8 $L$ may be taken to be a splitting field of some polynomial over $F$, and since $\text{char}(K) = 0$ $L/F$ is a Galois extension. As such $G(L/K)$ is solvable, and by Theorem, so is

$$G(E/K) \cong G(L/K)/G(L/E).$$

Which finishes the proof.

This means that all that has to be shown to prove that not all 5th-degree polynomials are solvable by radicals is to find one whose Galois group is not solvable.

### 6.3 $S_n$ and $A_n$

Before moving on it will be necessary to find examples of groups that are not solvable, the most basic examples of such groups are $S_n$ and $A_n$ for $n \geq 5$. Let $n \geq 2$ and consider the symmetric polynomial of $n$ variables

$$\Delta_n = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Now let $\sigma \in S_n$ and observe the polynomial

$$\sigma(\Delta_n) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

56
Since \( \sigma \) is a bijection, the terms in the product will be the same, except with a potential minus sign resulting from the pair \((i, j), i < j\) having \( \sigma(j) < \sigma(i) \). From this, it follows that \( \sigma(\Delta_n) = (-1)^m \Delta_n \) where \( m \) is the number of swaps as described above.

Now note that \((\phi \circ \sigma)(\Delta_n) = \prod_{1 \leq i < j \leq n}(x_{(\phi \circ \sigma)(i)} - x_{(\phi \circ \sigma)(j)})\), but since applying \( \sigma \) only adds the term \((-1)^m\) it is then equal to \((-1)^m \prod_{1 \leq i < j \leq n}(x_{\phi(i)} - x_{\phi(j)}) = (-1)^m(-1)^k \Delta \). The map \( \epsilon: S_n \to \{+1, -1\} \cong \mathbb{Z}_2 \) defined by \( \epsilon(\sigma) = (-1)^m \) is hence a group homomorphism. It turns out that this map is also surjective. Consider the transposition \( \sigma = (12) \) switching 1 and 2. \( \sigma(\Delta_n) \) has most terms left unchanged, and since the pairs \((1, k)\) is swapped with \((2, k)\), the ordering is also preserved for terms when \( k \neq 2 \) as \( 2 < k \) means \( 1 < k \) and \( 1 < k \neq 2 \) means \( 2 < k \). The only pair that has its order swapped is \((1, 2)\), so exactly one minus sign is induced and hence \( \epsilon \) is surjective.

**Definition 6.11.** The kernel of the map \( \epsilon \) is known as the alternating group on \( n \) elements, \( A_n \). Permutations that are in \( A_n \) are said to be even, and the ones that are not are said to be odd.

**Remark:** In this section composition of cycles in cycle notation will be written from left to right instead of from the usual right to left. This is done to simplify the writing out of large expressions.

Using this terminology it is not too hard to see that all transpositions \((ij)\) are odd, since \((ij) = \alpha(12)\alpha\) where \( \alpha = (1i)(2j) \), and hence \( \epsilon((ij)) = \epsilon(\alpha(12)\alpha) = \epsilon(\alpha)^2\epsilon((12)) = \epsilon((12)) = -1 \).

**Theorem 6.12.** Let \( n \) be a natural number

1) Every permutation \( \sigma \in S_n \) can be written as a product of disjoint cycles.

2) Every cycle can be written as a product of transpositions.

**Proof.**

1) Consider \( \text{id} \neq \sigma \in S_n \) (the identity is trivially a 1-cycle) and let \( i \) be any element \( \sigma \) does not fix. Since there are only finitely many elements that \( S_n \) permutes

\[
\sigma^m(i) = \sigma^k(i).
\]

For some \( k < m \). Taking \( m \) to be the smallest integer where this happens, one can note that \( \sigma^{-k}(i) = i \), meaning the first time there is a repeat of elements, is when the element returns to itself. Now \( \sigma \) is a bijection, meaning any element not of the form \( \sigma^k(i) \) cannot possibly be mapped to any element in this cycle, by induction it follows that every permutation is a product of disjoint cycles.

2) It can easily be seen that \((i_1i_2...i_m) = (i_1i_m)(i_2i_m)...(i_{m-1}i_m). \)

From this it follows trivially that every permutation can be written as the product of a finite number of transpositions, and importantly:

**Corollary 6.12.1.** Even permutations can be written as an even number of transpositions but not an odd number, odd permutations can be written as an odd number of transpositions but not an even number.
Proof. By Theorem 6.8 it follows that every permutation can be written as a product of transpositions, so write

\[ \sigma = \tau_1 \tau_2 \ldots \tau_m. \]

Where \( \tau_j = (i_j i_{j+1}) \) is a transposition. Now

\[ \epsilon(\sigma) = \epsilon(\tau_1) \epsilon(\tau_2) \ldots \epsilon(\tau_m) = (-1)^m. \]

This means that one can not write a given permutation as both an even and odd number of permutations, moreover, if the permutation is odd/even then only an odd/even number of permutations works.

The next theorem characterizes the alternating groups in another way that will be important later on.

**Theorem 6.13.** \( A_n \) is generated by 3-cycles.

Proof. For \( n = 1, 2 \) the result is immediate since \( A_n \) is trivial, for \( n > 2 \) consider the identities:

\[ (ij)(ij) = \text{id}. \]
\[ (ij)(jk) = (ikj). \]
\[ (ij)(kr) = (ikj)(jrk). \]

Now Since every even permutation can be written as a product of an even number of transpositions, they can be paired up, and every pair can be written as a product of 3-cycles, the original permutation can be as well.

**Theorem 6.14.** Let \( n \geq 5 \), then \( A_n \) is the commutator group \( S'_n \) of \( S_n \), i.e. the smallest subgroup of \( S_n \) containing all commutators.

Proof. pick two 3-cycles \( a = (ijk) \) and \( b = (krs) \) with only one element in common. The commutator \( aba^{-1}b^{-1} \) then results in the mapping

\[
\begin{align*}
    i &\mapsto i \mapsto k \mapsto r \mapsto r. \\
    j &\mapsto j \mapsto i \mapsto i \mapsto j. \\
    k &\mapsto s \mapsto s \mapsto k \mapsto i. \\
    r &\mapsto k \mapsto j \mapsto j \mapsto k. \\
    s &\mapsto r \mapsto r \mapsto s \mapsto s.
\end{align*}
\]

So the resulting map is \( aba^{-1}b^{-1} = (irk) \), and since the letters are arbitrary, it follows that every 3-cycle can be written as a commutator of 3-cycles, meaning \( A_n \) is a subgroup of the commutator group of \( S_n \).

Since \( S_n/A_n \cong \mathbb{Z}_2 \) is abelian it follows from Theorem 2.21 that every commutator is in \( A_n \) and \( S'_n \subseteq A_n \). From the discussion above every 3-cycle is in \( S'_n \) and hence \( S'_n = A_n \).

**Theorem 6.15.** The symmetric group on \( n \) elements \( S_n \) is not solvable for \( n \geq 5 \)
CHAPTER 6. THE ABEL RUFFINI THEOREM 6.4. GALOIS GROUP $S_5$

Proof. If $S_n$ were solvable then, it would mean that there is a tower
$$\{e\} \triangleleft G_1 \triangleleft \ldots \triangleleft G_m \triangleleft S_n.$$ Where the quotients are abelian. By Theorem 2.21 this means that $G_m$ contains all commutators, and by Theorem 6.13 it follows that $A_n \subseteq G_m$. Since $A_n$ contains all 3-cycles in $S_n$, follows that all the groups in this tower contain all 3-cycles, a clear contradiction. This means that $S_n$ is not solvable. \hfill $\Box$

Theorem 6.16. Let $p$ be a prime number and $H \leq S_p$, suppose that $p$ divides the order of $H$ and that $H$ contains a transposition, then $H = S_p$.

Proof. By relabeling, the transposition can be written as $\tau = (12)$. Cauchy’s Theorem implies there is an element $\alpha \in H$ of order $p$, and by part 1 of Theorem 6.12, it follows that $\alpha$ is a $p$-cycle. By relabeling and raising to some power one gets the $p$-cycle $\sigma = (123\ldots p)$. By conjugating one gets
$$\sigma_1 = \tau \sigma \tau = (213\ldots p)$$
also in $H$, and then $\sigma_1^{-1} \tau \sigma_1 = (13)$. Continuing this process one can get all the transpositions $(12), (13), \ldots, (1p)$, and since $(1j)(1i)(1j) = (ij)$, it follows that every transposition is in $H$, and hence $H = S_p$. \hfill $\Box$

6.4 Galois group $S_5$

Now one only has to find a polynomial of degree 5 that has Galois group $S_5$. Irreducible polynomials over the rationals will be of interest, one can hence guess that Eisenstein’s criterion might come into play, and this is indeed the case:

Theorem 6.17. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree $p$. If $f(x)$ has exactly 2 non-real roots, then its Galois group is $S_p$.

Proof. Let $E$ be a splitting field of $f(x)$ over $\mathbb{Q}$ and $G = G(E/\mathbb{Q})$. Note that $G$ can be thought of as a subgroup of $S_p$ since every element permutes the roots and any automorphism fixing the roots fixed all of $E$. As $f(x)$ is irreducible
$$|G| = [E : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}][E : \mathbb{Q}(\alpha)] = p[E : \mathbb{Q}(\alpha)].$$ That is, $p$ divides $|G|$. There are two non-real roots, so complex conjugation $\tau$ is also an automorphism that fixes $\mathbb{Q}$. It follows from Theorem 6.16 that $H = S_p$. \hfill $\Box$

And finally, the pièce de résistance:

Theorem 6.18. The Abel-Ruffini theorem: The general degree 5 polynomial over the rational numbers is not solvable by radicals.

Proof. Consider the polynomial
$$p(x) = x^5 - 4x - 2 \in \mathbb{Q}[x].$$ By Eisenstein’s criterion $p(x)$ is irreducible and $p(x)$ has exactly 3 real roots, this can be seen as follows: The derivative of $p(x)$, $p'(x) = 5x^4 - 4$ only has 2 real roots and is
strictly positive outside the interval $[-\sqrt{\frac{2}{4\sqrt{5}}}, \sqrt{\frac{2}{4\sqrt{5}}}]$, since $p(-\sqrt{\frac{2}{4\sqrt{5}}}) > 0$ and $p(\sqrt{\frac{2}{4\sqrt{5}}}) < 0$

there are two roots outside of the interval by the intermediate value theorem from topology (see e.g Theorem 24.3 [9]) outside $[-\sqrt{\frac{2}{4\sqrt{5}}}, \sqrt{\frac{2}{4\sqrt{5}}}]$, namely one on the interval $(-\infty, -\sqrt{\frac{2}{4\sqrt{5}}})$ and the other on $(\sqrt{\frac{2}{4\sqrt{5}}}, \infty)$ (note that $p(x) \to ^{\pm \infty}$ as $x \to ^{\pm \infty}$). Inside the interval $p'(x) \leq 0$, and hence there is exactly one root there. This proves that $p(x)$ has exactly 3 real roots.

By the fundamental Theorem of algebra (e.g. Chapter 2, Corollary 4.6 [10]) this implies there are exactly 2 complex roots, and by Theorems 6.7, 6.11, and 6.13, $p(x)$ is not solvable by radicals. \qed
Chapter 7

Discussion and further topics

With the advent of Galois theory, it was clear that finding solutions for higher degree polynomials in terms of radicals is in general pointless. As was shown in Theorem 6.10 a polynomial over a field of characteristic 0 (in particular the rationals) is solvable by radicals only if its Galois group is solvable. It is, in fact, true that a polynomial over a field of characteristic 0 is solvable by radicals if and only if its Galois group is solvable, which gives an exact characterization of polynomials solvable by radicals (e.g Theorem 98 [7]). By the Abel-Ruffini theorem, this already becomes a problem for degree 5 polynomials, for those of higher degree this becomes even more unpractical. However, Theorem 6.10 only says that solutions in terms of radicals in general can not be found, not that there is no systematic way of solving such equations.

In 1858 the French mathematician Charles Hermite managed to solve the degree 5 polynomial using the Tschirnhaus transform and elliptic functions [11]. Shortly afterward others, for example Kronecker [12], also found a general solution. But, the most important work on the topic was not published until 1884, by Felix Klein in his book Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade (Lectures on the Icosahedron; and the Solution of Equations of the Fifth Degree) [13]. As the title suggests there is a relationship between the group of symmetries of an icosahedron and the roots of a degree 5 polynomial. For those interested in his work, the English translation of Klein’s original work [14] is recommended, for a more modern approach see for example [15]. The reader might be familiar with a method of solving cubic equations using trigonometric functions, many methods used to solve degree 5 equations are similar but rather use elliptic functions, which will be defined shortly. While a full solution to the problem will not be given, some key concepts are introduced.

The general quintic equation turns out to be reducible in a way that greatly simplifies the problem.

**Theorem 7.1.** The general degree 5 polynomial over the complex numbers

\[ p(x) = x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0. \]

May be reduced to the form

\[ y^5 + \alpha y^2 + \beta y + \gamma. \]

Using a substitution \( y = x^2 + mx + n. \)
Proof. See e.g. Section 3 in [16].

**Definition 7.2.** The substitution given in Theorem 7.1 is called a Tschirnhaus transformation.

This means only polynomials of the form
\[ y^5 + \alpha y^2 + \beta y + \gamma. \]

Need be considered when trying to solve the general quintic.

Recall from complex analysis (see e.g [10]) that a meromorphic function is a function on the complex plane that is analytic everywhere except for a discrete set of singular points, all of which are poles (alternatively a holomorphic function from the complex plane to the Riemann sphere).

**Definition 7.3.** If a complex function \( f(z) \) satisfies \( f(z) = f(z + \omega_1) = f(z + \omega_2) \) for all \( z \in \mathbb{C} \) and \( \frac{\omega_1}{\omega_2} \) is not real, then \( f(z) \) is said to be doubly periodic. An elliptic function \( f(z) \) is a complex function that is doubly periodic and meromorphic.

The theory of elliptic functions is a rich topic in its own right, and the interested reader might consult Chapters 9 and 10 in [10] for a more detailed view.

The key class of functions in the theory of elliptic functions are the so-called Weierstrass \( \wp \)-functions, which are constructed as follows. Consider a lattice of evenly spaced points in \( \mathbb{C} \) given by the points
\[ \Lambda = \{n\omega_1 + m\omega_2 : n, m \in \mathbb{Z}\}. \]

Where \( \omega_1, \omega_2 \) satisfies that \( \frac{\omega_1}{\omega_2} \) is not real. The Weierstrass \( \wp \)-function for the lattice \( \Lambda \) is then defined as the series
\[ \wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda/\{0\}} \left( \frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right). \]

Which can be shown to converge absolutely and uniformly on compact sets excluding the poles (which are exactly the lattice points). As such it defines a meromorphic function that is doubly periodic with periods \( \omega_1 \) and \( \omega_2 \), meaning it is elliptic. It turns out that \( \wp(z) \) and \( \wp'(z) \) generate all elliptic functions with the given periods by considering rational functions in \( \wp \) and \( \wp' \).

An important class of functions that also appears when solving the quintic equation, is the class of theta functions.

**Definition 7.4.** The theta function is defined as
\[ \Theta(z; \tau) = \sum_{n=-\infty}^{\infty} exp(\pi in^2 \tau + 2\pi inz). \]

Where \( z \in \mathbb{C} \) and \( \text{im}(\tau) > 0 \).
Note that the theta function is a function of two complex variables. By modifying the inputs into the function and fixing either variable, one can obtain a larger class of functions, generally called the theta functions. While the theta functions are not themselves elliptic, they have a close connection to the theory of elliptic functions, and one can reconstruct the Weierstrass $\wp$-function from them. It was by using theta functions and their relation to the elliptic functions that Hermite managed to originally solve the problem. He used various known properties of the theta functions to construct an auxiliary function $\Phi(\tau)$ whose values at given values of $\tau$ satisfy a special quintic equation, which turned out to be sufficient for the general case.

Many other interesting ideas could be discussed, like the connection with the icosahedron or Kiepert’s algorithm, but this is only intended to be a brief outline, the reader interested in a more thorough treatment of the topic of solving higher-order equations may refer to [17].
I want to thank my supervisor Per Åhag for helping me during my time writing this thesis, for reading it, and for providing crucial feedback and encouragement. His help has been of utmost importance and has made writing this thesis much easier. I also want to thank my high school math teacher Birgit Gustafsson for helping me initiate my mathematics journey here at Umeå, as well as Catarina Rudälv, who has supported me during my studies. Finally, I want to thank my examiner Olow Sande for taking the time to read my paper.
Bibliography


