Galois Theory and the Artin-Schreier Theorem

Ebba Mellquist

Examensarbete i matematik, 15 hp  
Handledare: Martin Herschend  
Examinator: Veronica Crispin Quinonez  
Juni 2020
Galois Theory and the Artin-Schreier Theorem

Ebba Mellquist

Contents

1 Introduction ........................................... 2

2 Groups .................................................. 3
   2.1 Groups ............................................. 3
   2.2 Subgroups ......................................... 6

3 Rings and fields ...................................... 7
   3.1 Rings ............................................... 7
   3.2 Subrings and ideals ................................ 8
   3.3 Ring morphisms .................................... 9
   3.4 Domains and fields ................................ 12
   3.5 Polynomials ........................................ 15
   3.6 Principal ideal domains ............................ 18
   3.7 Fields .............................................. 21

4 Field extensions ...................................... 24
   4.1 Extensions ......................................... 24
   4.2 Algebraic Extensions ............................... 27
   4.3 Algebraic closure .................................. 28
   4.4 Separable extensions ............................... 29

5 Galois theory ......................................... 32
   5.1 Splitting fields .................................... 32
   5.2 Normal extensions ................................ 33
   5.3 Galois Extensions ................................ 34

6 Real closed fields .................................. 37

7 The Artin-Schreier Theorem ......................... 38
1 Introduction

In this paper we will use the theory of groups, rings and fields and then field extensions to develop Galois theory and prove the Artin-Schreier theorem.

The Artin-Schreier theorem is a generalization of the fact that every field is one of three distinct types: algebraically closed, real closed or the field has irreducible polynomials of arbitrarily large degree. For example, \( \mathbb{C} \) is an algebraically closed field, \( \mathbb{R} \) is real closed and \( \mathbb{Q} \) has irreducible polynomials of arbitrarily large degree.

The Artin-Schreier theorem does not explicitly state a dependence on the characteristic of the field, however the proof of the theorem differs by a lot depending on if the characteristic is zero or positive. All three examples of \( \mathbb{C} \), \( \mathbb{R} \) and \( \mathbb{Q} \) are fields of characteristic 0. The proof of the Artin-Schreier theorem is straightforward when dealing with fields with characteristic 0. However, the Artin-Schreier theorem holds for fields with nonzero prime characteristic \( p \) as well. The proof becomes increasingly more complicated when dealing with fields of characteristic \( p \).

This thesis will start with a brief exploration of group theory. We will then move on to ring theory where we will go through subrings, ring morphisms, polynomials and principal ideal domains. After that we define what fields are as an extension of rings. Then we define field extensions, which follow naturally from the definition fields and subfields in the previous section and from the notion of vector spaces. The different types of field extensions like algebraic, separable and normal extension will then provide the needed theory to define Galois extensions in that section. We will also define what the algebraic closure of a field is. In the Galois theory section we will go through the Fundamental Theorem of Galois Theory. After that will will proceed to the notion of ordered fields, formally real fields and what it entails when a field is real closed. Then we have defined and proved everything necessary to state and prove the Artin-Schreier theorem which is the goal of this thesis.

As it is the aim for this thesis to be able to state and prove the Artin-Schreier theorem, the theory regarding all the topics have been chosen so that it is the most relevant for this objective. There are some topics which are only brought up to better the understanding for the reader and create context, but the majority is related to the Artin-Schreier theorem and necessary for that reason. The reader is assumed to be familiar with basic algebra and linear algebra.
2 Groups

We will begin by defining the most simple algebraic structure which is the group. After that we will define subgroups and their properties. Groups are needed to start developing Galois theory and will help us when we define rings and fields later on. This will provide the first tools we are going to use when we prove Artin-Schreier’s theorem later. In this section, we have used Chapter 1 in [1].

2.1 Groups

This first section is based of Section 2 in Chapter 2 of [1] and deals with the definitions of groups and the most basic properties of them.

Definition 2.1. A group is a set \( G \) together with a binary operation \( \cdot : G \times G \rightarrow G \), \((x, y) \mapsto x \cdot y = xy\) such that the following properties are satisfied:

(i) the operation is associative, i.e. \((xy)z = x(yz)\) for all \(x, y, z \in G\);

(ii) there exists an identity element, i.e. there exists an element \(e \in G\) such that \(ex = x = xe\) for all \(x \in G\);

(iii) every element in the group has an inverse, i.e. for every \(x \in G\), there exists \(y \in G\) such that \(xy = e = yx\).

We denote the group with just the name of the underlying set of the group. As well as satisfying these conditions, a group must also be closed under the operation, meaning for all \(x, y \in G\), then \(xy \in G\) as well. The operation in the group is most often either multiplication or addition, in this thesis we define it multiplicatively, but the additive notation is analogous. Moreover, a group is called abelian if its operation is also commutative, that is for all \(x, y \in G\) we have \(xy = yx\).

Definition 2.2. The order of a group \( G \) is the number of elements of \( G \). We denote it by \(|G|\).

To be able to use groups as needed we first need to prove some properties of groups.

Proposition 2.3. Let \( G \) be a group. Then

(i) the identity element is unique;

(ii) the inverse of an element \(x \in G\) is unique.

Proof. (i) Let \(e, e' \in G\) be two identity elements of \(G\). Then we have

\[ e = ee' = e', \]

by the second condition of the group definition, which shows that the identity element is unique.
(ii) Let \( x \in G \) and \( y, z \in G \) be two inverses of \( x \), i.e. \( xy = e = yx \) and \( xz = e = zx \). Then
\[
y = ey = (zx)y = z(xy) = ze = z,
\]
which shows that the inverse of \( x \) is unique.

For an additive group we denote the identity element by 0 and the inverse by \(-x\) for an element \( x \in G \). For a multiplicative group we can denote the identity element by 1 and the inverse element by \( x^{-1} \), for \( x \in G \).

**Proposition 2.4.** For a group \( G \), the cancellation laws hold:
\[
ca = cb \Rightarrow a = b,
\]
\[
ac = bc \Rightarrow a = b.
\]
Furthermore, the equations \( ax = b, ya = b \) have unique solutions \( x = a^{-1}b \) and \( y = ba^{-1} \).

**Proof.** Assume \( ca = cb \). Then
\[
a = 1a = (c^{-1}c)a = c^{-1}(ca) = c^{-1}(cb) = (c^{-1}c)b = 1b = b,
\]
as required. In the same way \( ac = ab \) implies \( a = b \) as well. Next, assume \( ax = b \). Then we can write \( x = a^{-1}ax = a^{-1}b \). On the other hand, assume \( x = a^{-1}b \). Then \( b = aa^{-1}b = ax \). Similarly \( ya = b \) if and only if \( y = a^{-1}b \). □

**Proposition 2.5.** In a group, we have
\[
(i) \ (x^{-1})^{-1} = x, \text{ for all } x \in G;
\]
\[
(ii) \ (x_1 x_2 \cdots x_m)^{-1} = x_m^{-1} \cdots x_2^{-1} x_1^{-1}, \text{ for all } x_1, x_2, \ldots, x_m \in G.
\]

**Proof.** (i) By Proposition 2.4 we have that \( x^{-1}x = 1 \) and so \( x = (x^{-1})^{-1} = (x^{-1})^{-1} \).

(ii) We can write
\[
(x_m^{-1} \cdots x_2^{-1} x_1^{-1})(x_1 x_2 \cdots x_m) = (x_m^{-1} \cdots x_2^{-1})(x_1^{-1} x_1)(x_2 \cdots x_m)
\]
\[
= (x_m^{-1} \cdots x_2^{-1})1(x_2 \cdots x_m)
\]
\[
= x_m^{-1} x_m
\]
\[
= 1.
\]
Then by part (i) we have \( (x_m^{-1} \cdots x_2^{-1} x_1^{-1}) = (x_1 \cdots x_m)^{-1} \). □
We want to define $x^n$ for all integers. First we set $x^n := x \cdots x$ and $x^0 := 1$. Using the latest proposition we can define negative powers. When $n$ is a positive integer we define $x^{-n} = (x^n)^{-1} = (x^{-1})^n$. For a group we have now defined $x^n$ for every $n \in \mathbb{Z}$. This allows us to prove further properties of powers in groups.

**Proposition 2.6.** Let $G$ be a group, $x, y \in G$ and $m, n \in \mathbb{Z}$. Then the following properties hold true:

(i) $x^m x^n = x^{m+n}$;

(ii) $(x^m)^n = x^{mn}$;

(iii) If $G$ is an abelian group, i.e. if $xy = yx$, then $(xy)^m = x^m y^m$.

**Proof.** (i) By our definition of $x^n$ we have

$$
    x^m x^n = \underbrace{x \cdots x}_{m \text{ factors}} \underbrace{x \cdots x}_{n \text{ factors}} = \underbrace{x \cdots x}_{m+n \text{ factors}} = x^{m+n}.
$$

(ii) We can use (i) and our definition of $x^n$ and write

$$
    (x^m)^n = \underbrace{x^m \cdots x^m}_{n \text{ factors}} = \underbrace{x^{m+m} \cdots x^{m}}_{n-1 \text{ factors}} = \cdots = \underbrace{x^{m+m+\cdots+m}}_{n \text{ terms}} = x^{mn}.
$$

(iii) We have that if $xy = yx$ then

$$
    (xy)^m = \underbrace{(xy)(xy) \cdots (xy)}_{m \text{ factors}} = \underbrace{xy \cdots xy}_{m \text{ factors}} = x^m y^m.
$$

**Definition 2.7.** Let $G$ be a group, and $a \in G$. Then the *order* of $a$, denoted $o(a)$, is defined as the smallest positive integer $l > 0$ such that $a^l = 1$. If $a^l \neq 1$ for all $l \in \mathbb{Z}_{>0}$ then we say that $a$ has infinite order.

**Example 2.8.** Some examples of groups include:

(i) The *trivial* group which consists of just the identity element $e$, $\{e\}$. We have $|\{e\}| = 1$.

(ii) $\mathbb{Z}$, the set of all integers, is a group together with addition. Moreover this is an abelian group and $|\mathbb{Z}| = \infty$.

(iii) $\mathbb{Z}_n$, the set of all integers modulo $n$, $n > 0$, is also an abelian, infinite group under addition.
2.2 Subgroups

Now we move on to subgroups of groups and their properties. Here the material is taken from Section 3 in Chapter 2 of [1].

Definition 2.9. Let $G$ be a group and $H \subseteq G$ be a subset of $G$. Then $H$ is called a subgroup of $G$ if the following properties hold true:

(i) $1_G \in H$;

(ii) $H$ is closed under multiplication, i.e. $x, y \in H$ implies $xy \in H$;

(iii) $H$ is closed under inverses, i.e. $x \in H$ implies $x^{-1} \in H$.

If $H$ is a subgroup of $G$, we write $H \leq G$.

Every group $G$ has at least two subgroups, the group $G$ itself and the trivial subgroup which consists of only the identity element $\{e\}$. We call a subgroup $H \neq \{e\}$ nontrivial and if a subgroup is not equal to the whole group $G$ we call it proper.

Proposition 2.10. Let $G$ be a group and $H \subseteq G$. The subset $H$ is a subgroup of $G$ if and only if $H \neq \emptyset$ and we have $xy^{-1} \in H$ for all $x, y \in H$.

Proof. For ($\Rightarrow$). Assume that $H \subseteq G$ is a subgroup. Then we know that $1_G \in H$ which implies that $H \neq \emptyset$. By the definition of subgroups we know that if $x, y \in H$ then $y^{-1} \in H$ too and since subgroups are closed under multiplication, we have $xy^{-1} \in H$ as required.

For ($\Leftarrow$). Assume that $H \neq \emptyset$ and that $x, y \in H$ implies $xy^{-1} \in H$. We know that there exists some element $x \in H$ since $H \neq \emptyset$ and thus $xx^{-1} \in H$ by assumption. But $xx^{-1} = 1$ so $1 \in H$. Then since we have $1, x \in H$ this implies that $1x^{-1} = x^{-1} \in H$ and so $H$ is closed under inverses. Lastly, let $x, y \in H$, and since $H$ is closed under inverses we have $x, y^{-1} \in H$. Then our assumption gives us $x(y^{-1})^{-1} = xy \in H$ and so $H$ is closed under multiplication as well. \square

Example 2.11. The set of all powers of an element $a$ in a group $G$ is a subgroup of $G$. We call this the cyclic subgroup of $G$ generated by $a$. We denote this by $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$. We call a group $G$ cyclic when it is generated by a single element, meaning $G = \langle a \rangle$ for some $a \in G$.

A group morphism is a mapping which preserves the group operation.

Definition 2.12. A group morphism of a group $G$ to a group $H$ is a mapping $\varphi : G \to H$ such that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$.

If this mapping is bijective then we call it an isomorphism of groups. An isomorphism from a group $G$ onto itself is called an automorphism. The automorphisms of a group $G$ form a group, with the operation being composition, and is denoted $\text{Aut}(G)$.
3 Rings and fields

The notion of a ring is the next algebraic structure we will discuss. It is an extension of the notion of an abelian group and provides a natural way to define fields which we will use in the next section. We start this section by defining rings and then we go through subrings and ideals. After that we move on to ring morphisms and then we define special types of rings, namely domains and fields which allows us to define principal ideal domains in the last section, just after redefining how polynomials work in rings. In this section we use Chapter 3 from [1].

3.1 Rings

We start this section by defining rings and showing some properties of rings. The material in the section is taken from Section 1 of Chapter 3 in [1].

Definition 3.1. A ring is a set $R$ together with two binary operations, addition $+: R \times R \to R$, $(x, y) \mapsto x + y$ and multiplication $\cdot: R \times R \to R$, $(x, y) \mapsto x \cdot y = xy$, such that the following axioms hold:

(i) $R$ together with addition is an abelian group;

(ii) multiplication is associative, i.e. for all $x, y, z \in R$, $x(yz) = (xy)z$;

(iii) multiplication is distributive, i.e. for all $x, y, z \in R$, $(x + y)z = xz + yz$ and $z(x + y) = zx + zy$;

(iv) there exists an identity element for the multiplication, i.e. there exists $1 \in R$ such that for all $x \in R$, $1x = x = x1$.

In particular (i) states that $R$ together with addition is a group called the additive group of $R$. This means that $(R, +)$ satisfies the three group axioms as well as being commutative; meaning for all $x, y, z \in R$ we know that

$$(x + y) + z = x + (y + z),$$

$$x + 0 = x = 0 + x,$$

$$x + (-x) = 0 = (-x) + x,$$

$$x + y = y + x.$$

We also note that (ii) and (iv) makes it clear that $R$ together with multiplication is a monoid, which is defined as a group without inverses. If the multiplication in a ring is also commutative, then we can say that the ring is commutative. This implies that if $xy = yx$ then $(xy)^n = x^n y^n$ for $n \geq 0$.

We can call the identity element for multiplication a unity and denote it by 1. Similarly, the identity element for the additive group, 0, can be called the zero element.

Example 3.2. Under addition and multiplication we have that $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$(integers modulo $n$) are all rings.
Definition 3.3. In a ring $R$, we can define an *invertible element* or *unit* to be an element $u \in R$ that satisfies $uv = 1 = vu$. Then $v$ is the *inverse* of $u$, denoted $u^{-1}$, and it is moreover unique. Under multiplication, the units of $R$ form a group, this is denoted $R^*$ and we call it the *groups of units* of $R$.

3.2 Subrings and ideals

As in Section 2.2 when we defined subgroups from subset of groups, we now want to define what it means to be a subring of a ring. The material is based of the information in Section 2 in Chapter 3 of [1].

Definition 3.4. Let $R$ be a ring and $S$ be a subset of $R$ such that the following properties hold:

(i) $1_R \in S$;
(ii) $S$ is a subgroup of $R$ under addition;
(iii) $S$ is closed under multiplication, i.e. $x, y \in S$ implies $xy \in S$.

Then $S$ is called a *subring* of $R$.

Example 3.5. Every ring is a subring of itself, but the trivial subgroup $\{0\}$ is not a subring of $R$ unless $R$ is the zero ring.

Now we have defined enough to be able to define what an ideal is. This we will allow us to further develop the theory of rings.

Definition 3.6. A subgroup $I$ of a ring $R$ is called an *ideal* if $x \in I$ implies $xy \in I$ and $yx \in I$ for all $y \in R$. Furthermore, an ideal is called *proper* if it also is not the whole ring $R$.

From this definition we can see that an ideal is just an additive subgroup of a ring which is also closed under multiplication by elements in $R$, from both sides. If we intersect ideals of a ring $R$, then the intersection is also an ideal of $R$. This allows us to make a further definition.

Definition 3.7. We call the smallest ideal of a ring $R$ which contains the subset $S$, the ideal generated by $S$ and denote it $(S)$. If an ideal is generated by a single element $a$ we call it a *principal* ideal.

Proposition 3.8. The ideal $(S)$ in ring $R$, i.e. the ideal generated by a subset $S$, is the set of all finite sums with terms $x sy$ with $s \in S$ and $x, y \in R$. Moreover, if $R$ is commutative, then $(S)$ is the set of all finite linear combinations of elements of $S$ with coefficients in $R$.

Proof. Since the ideal $(S)$ contains $S$, then for $s \in S, x \in R$ we have that $xs \in (S)$ and then also $xsy \in (S), y \in R$. So $(S)$ contains all elements of the form $x sy$ with $s \in S$ and $x, y \in R$ and all finite sums of such elements. We shall now show that the set $I$ of all such sums is an ideal of $R$, i.e. $I = (S)$. First,
0 ∈ I, the empty sum, and by the definition of I it is closed under addition and furthermore -(x sy) = (-x) sy so I is closed under inverses too. Hence I is a subgroup of R under addition. We also have (xsy)r = xs(yr) for all r ∈ R, hence for all i ∈ I we have ir ∈ I. Likewise, i ∈ I implies ri ∈ I for all r ∈ R. Thus we have proved that I is an ideal of R under addition. We also have (x sy)r = x(yr) for all r ∈ R, hence for all i ∈ I we have ir ∈ I. Likewise, i ∈ I implies ri ∈ I for all r ∈ R. Thus we have proved that I is an ideal of R under addition.

Next assume that R is a commutative ring, then x sy = (xy)s, so (S) is the set of all finite sums, \(x_1 s_1 + \cdots + x_n s_n\) where \(n \geq 0\), \(x_1, \ldots, x_n \in R\) and \(s_1, \ldots, s_n \in S\).

**Proposition 3.9.** Let R be a commutative ring. Then the principal ideal generated by a ∈ R is the set of all multiples of a, denoted \((a) = Ra\).

**Proof.** This is a consequence of Proposition 3.8. A linear combination \(x_1 a + \cdots + x_n a\) is by distributivity a multiple of a, i.e. \((x_1 + \cdots + x_n)a\).

**Example 3.10.** Every ideal of \(\mathbb{Z}\) is generated by a unique non-negative integer and therefore every ideal is principal.

**Definition 3.11.** A maximal ideal is an ideal M of a ring R, such that M ≠ R and there does not exist an ideal I of R with M ⊊ I ⊊ R.

Moreover, all proper ideals in a ring R are contained in maximal ideal.

### 3.3 Ring morphisms

Ring morphisms are mappings between rings with certain properties, which we see in this section, where the material is taken from Section 1 and Section 3 of Chapter 3 in [1].

**Definition 3.12.** We can define a ring morphism from a ring R into a ring S as a mapping \(\varphi : R \to S\) which keeps the respective operations, and preserves the identity element:

\[
\varphi(x + y) = \varphi(x) + \varphi(y),
\]

\[
\varphi(xy) = \varphi(x)\varphi(y),
\]

\[
\varphi(1_R) = 1_S.
\]

Moreover, ring morphisms preserves the zero element of the ring, integer multiples and powers. That is, for a ring morphism \(\varphi\) we have

\[
\varphi(0) = 0,
\]

\[
\varphi(nx) = n\varphi(x),
\]

\[
\varphi(x^n) = \varphi(x)^n.
\]

We can define an isomorphism of rings as a bijective ring morphism, and say that if \(\varphi\) is a bijective ring morphism then the inverse \(\varphi^{-1}\) is also a ring morphism. We say that two rings are isomorphic when there exists an isomorphism between them and this allows us to think of these two rings as essentially the same ring, but in an abstract sense. If two rings R and S are isomorphic, we denote this by \(R \cong S\).
**Definition 3.13.** Let \( \varphi : R \to S \) be a ring morphism. We define the *image* of \( \varphi \) to be

\[
\text{Im } \varphi = \{ \varphi(x) : x \in R \},
\]
and the *kernel* of \( \varphi \) to be

\[
\text{Ker } \varphi = \{ x \in R : \varphi(x) = 0 \}.
\]

The image of a ring morphism \( \varphi : R \to S \) is a subring of \( S \) and the kernel of \( \varphi \) is an ideal of \( R \).

**Example 3.14.** Let \( S \) be a subring of \( R \). Then \( f : S \to R, \ f(s) = s \) is a ring morphism, more specifically the *inclusion morphism* of \( S \) into \( R \).

**Definition 3.15.** Let \( I \) be an ideal of \( R \).

(i) The *coset* of \( x \in R \) with respect to \( I \) is the set \( x + I = \{ x + i : i \in I \} \).

(ii) The *quotient* \( R/I \) is the set of cosets \( R/I = \{ x + I : x \in R \} \). Moreover, it is a ring with operations:

\[
(x + I) + (y + I) = x + y + I,
\]

\[
(x + I)(y + I) = xy + I,
\]

for any \( x + I, y + I \in R/I \).

**Lemma 3.16.** Let \( I \) be an ideal of a ring \( R \). The quotient ring \( R/I \) is well-defined.

*Proof.* We want to show that the quotient ring \( R/I \) satisfies the ring axioms. We shall show that \( R/I \) is an abelian group, multiplication is associative and distributive and that there exists an identity element for multiplication.

(i) First we show that addition in \( R/I \) is commutative. Let \( a, b \in R \) and note the fact that addition in \( R \) is commutative. Then

\[
(a + I) + (b + I) = (a + b) + I = (b + a) + I = (b + I) + (a + I).
\]

Addition in \( R \) is associative, thus addition in \( R/I \) is associative. The zero element is the element \( 0 + I \) which is just the coset \( I \) since for any \( a \in R \)

\[
(a + I) + (0 + I) = a + I.
\]

The inverse of an element \( a + I \in R/I \) is \( -a + I \) since

\[
a + I + (-a) + I = 0 + I.
\]

Thus \( R/I \) is an abelian group.
(ii) Multiplication is associative in $R/I$. This follows from the fact that multiplication is associative in $R$. Let $a, b, c \in R$ and $a + I, b + I, c + I \in R/I$. Then
\[
(a + I)((b + I)(c + I)) = (a + I)(bc + I) \\
= a(bc) + I \\
= (ab)c + I \\
= (ab + I)(c + I) \\
= ((a + I)(b + I))(c + I).
\]

(iii) Multiplication is distributive in $R/I$. This follows from the distributive property of multiplication in $R$. We only give the proof of left distributive property, the right is similar. Let $a, b, c \in R$ and $a + I, b + I, c + I \in R/I$. Then
\[
(a + I)((b + I) + (c + I)) = (a + I)(b + c + I) \\
= a(b + c) + I \\
= ab + ac + I \\
= (ab + I) + (ac + I) \\
= (a + I)(b + I) + (a + I)(c + I).
\]

(iv) There exist an identity element for the ring $R/I$. It is $1 + I$ since
\[
(a + I)(1 + I) = a + I = (1 + I)(a + I),
\]
for all $a \in R$, $a + I \in R/I$.

Moreover for $a, b \in R$ and $a + I \in R/I$ and $b + I \in R/I$ we have that the product $(a + I)(b + I)$ is contained in the coset $ab + I$ since for all $i, j \in I$ we can write $(a + i)(b + j) = ab + aj + bi + ij \in ab + I$. Hence multiplication is well-defined and thus $R/I$ is a well-defined ring.  

Definition 3.17. Let $I$ be an ideal of a ring $R$. The morphism $x \mapsto x + I$ is the canonical projection of $R$ onto $R/I$.

Example 3.18. We know that every ring is an ideal of itself so we have $R/R \cong \{0\}$. It is known that $\{0\}$ is also an ideal of $R$ which implies $R/\{0\} \cong R$. Another example is when you quotient $\mathbb{Z}$ with any of its ideals, all of which are principal. So for $n > 0$ we have $\mathbb{Z}/(n)$ which is the ring of integers modulo $n$, denoted $\mathbb{Z}_n$.

Theorem 3.19. If $\varphi : R \to S$ is a ring homomorphism, then there is a ring isomorphism $\theta : R/\ker \varphi \to \operatorname{Im} \varphi$ given by $\theta(x + \ker \varphi) = \varphi(x)$. 

11
Proof. See [1, Chapter 3, Theorem 3.6].

This is called the Isomorphism theorem for rings and can be stated with the following diagram.

$$R / \ker \varphi \cong \image \varphi$$

Proposition 3.20. Let $R$ be a ring. There exists a unique ring morphism of $\mathbb{Z}$ into $R$ where its image consists of all integer multiples of the identity element of $R$. The image is the smallest subring of $R$ and it is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$ for some unique $n > 0$.

Proof. Let $\varphi : \mathbb{Z} \to R$ be a ring morphism. Then by the definition of ring morphisms we have $\varphi(1) = 1$ and $\varphi(n) = \varphi(n1) = n\varphi(1) = n1 \in R$ for all $n \in \mathbb{Z}$. This implies that $\varphi$ is unique. We already know that $\varphi : n \mapsto n1$ is a ring morphism of $\mathbb{Z}$ into $R$. A subring of $R$ must contain the identity element and all its integer multiples by the definition of subrings. Since $\image \varphi$ is the set of all integer multiples of the identity element of $R$ and since it is a subring, then it is the smallest subring of that type.

To show which ring this image is isomorphic to we use Theorem 3.19. Then we have $\image \varphi \cong \mathbb{Z}/I$, where $I = \ker \varphi$ is an ideal of $\mathbb{Z}$. From Example 3.10 we know that all ideals of $\mathbb{Z}$ are principal so $I$ is principal, i.e. $I = (n)$ for some $n \geq 0$. In the first case, if $n = 0$ then we have $\image \varphi \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}$. Otherwise, if $n > 0$, then $\image \varphi \cong \mathbb{Z}/(n) = \mathbb{Z}_n$ and $n$ is unique with this property since all rings $\mathbb{Z}_n$ have different cardinality.

Definition 3.21. The characteristic of a ring $R$, denoted by $\text{char}(R)$, is the smallest positive integer $n$ such that $n1 = 0$. If there does not exist such an integer, we say that the characteristic is 0.

We can define the characteristic in another way, in relation to Proposition 3.20 and the isomorphism theorem. Let $\varphi : \mathbb{Z} \rightarrow R$ be a ring morphism. The characteristic is the number $n \in \mathbb{N}$ such that the ideal $(n)$ is the kernel of this morphism. The characteristic is also the number $n \in \mathbb{N}$ such that the image of $\varphi$ is the ring $\mathbb{Z}/(n)$ and it is isomorphic to a subring of $R$.

Example 3.22. Since $\mathbb{Z}/(n)$ is by definition the ring of integers modulo $n$, it is easy to see that $\mathbb{Z}_n$ has characteristic $n$.

3.4 Domains and fields

Now we move on to the types of rings more known as domains and fields, where the latter will play an important part in the next section. The material is taken from Section 4 of Chapter 3 in [1].

Definition 3.23. A domain is a commutative ring, not the zero ring, which does not contain any zero divisors, that is if $xy = 0$ then $x = 0$ or $y = 0$.

Example 3.24. Each of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are domains.
Now if we require each of the elements to also be invertible then we have the definition of a field.

**Definition 3.25.** A commutative ring $R$ is a field if it is not the zero ring and all elements of $R\setminus\{0\}$ are invertible.

**Proposition 3.26.** If $n > 0$, then the ring $\mathbb{Z}_n$ is a domain if and only if $n$ is prime and then moreover $\mathbb{Z}_n$ is a field.

**Proof.** Assume that $n > 0$ is not prime. Then either we have $n = 1$ or we have $n = xy$ for some $1 < x < n$ and $1 < y < n$. If $n = 1$ then this implies $\mathbb{Z}_n = 0$, the zero ring. If $n = xy$ then this implies $\bar{x}\bar{y} = \bar{n} = \bar{0}$ in $\mathbb{Z}_n$. Hence $\mathbb{Z}_n$ has a zero divisor. In both cases we have that $\mathbb{Z}_n$ is not a domain.

Next let $n$ be prime. If $1 \leq x < n$, then $ux + vn = 1$ for some $u,v \in \mathbb{Z}_n$, since $x$ and $n$ are relatively prime. Hence in $\mathbb{Z}_n$ we have $\bar{x}u = \bar{1}$ so $\bar{x}$ is a unit. Hence we have proved that $\mathbb{Z}_n$ is a field. $\square$

In domains, the cancellations holds as usual.

**Proposition 3.27.** If $xy = xz$ in a domain, then $y = z$, if $x \neq 0$.

**Proof.** If $xy = xz$ and $x \neq 0$ then $x(y - z) = 0$ which implies that $y - z = 0$, i.e. $y = z$, or else $x$ would be a zero divisor which is impossible in a domain. $\square$

Now we want to explore what characteristics a domain has. We have the following proposition.

**Proposition 3.28.** The characteristic of a domain is either 0 or prime.

**Proof.** The characteristic is the number $n$ such that image of the morphism $\varphi : \mathbb{Z} \to R$ is the ring $\mathbb{Z}/(n)$. As stated by Proposition 3.20 this is the smallest subring of $R$ and is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$ for some $n > 0$. Since any subring of a domain is a domain, and by Proposition 3.26 we have that this is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_p$ for some prime $p$. $\square$

The domains of nonzero characteristic, i.e. of prime characteristic, have the following property.

**Proposition 3.29.** In a commutative ring $R$ of prime characteristic $p$, we have for all $x, y \in R$

$$
(x + y)^p = x^p + y^p,
$$
$$
(x - y)^p = x^p - y^p.
$$

**Proof.** We can use the binomial theorem and write $(x+y)^p = \sum_{0 \leq i \leq p} \binom{p}{i} x^i y^{p-i}$, where $\binom{p}{i} = \frac{p!}{i!(p-i)!}$. Now, if $0 < i < p$, then $p$ divides $i!$, but does not divide $i!$ or $(p-i)!$. Thus $p$ divides $\binom{p}{i}$ and so $\binom{p}{i}r = 0$ for all $r \in R$. Then

$$
(x+y)^p = \sum_{0 \leq i \leq p} \binom{p}{i} x^i y^{p-i} = \binom{p}{0} x^0 y^p + \sum_{0 < i < p} \binom{p}{i} x^i y^{p-i} + \binom{p}{p} x^p y^0 = x^p + y^p.
$$
Using this, we see that \((x - y)^p = x^p + (-1)^p y^p\). Thus if \(p\) is odd, we have \(x^p + (-1)^p y^p = x^p - y^p\). If \(p = 2\), then \(x^p + (-1)^p y^p = x^p + y^p = x^p - y^p\), since \(1 = -1\) in \(R\) if the characteristic is 2. □

This proposition proves that the morphism \(\varphi(x) = x^p\) is a ring morphism because
\[
\varphi(1) = 1^p = 1,
\]
\[
\varphi(xy) = (xy)^p = x^py^p = \varphi(x)\varphi(y),
\]
\[
\varphi(x + y) = (x + y)^p = x^p + y^p = \varphi(x) + \varphi(y).
\]

There exists some special ideals which provides a way to construct domains and fields using quotient rings.

**Definition 3.30.** A prime ideal of a commutative ring \(R\) is an ideal \(p \neq R\) such that \(xy \in p\) implies \(x \in p\) or \(y \in p\).

**Proposition 3.31.** If \(a\) is an ideal of a commutative ring then \(R/a\) is a domain if and only if \(a\) is a prime ideal.

*Proof.* Assume that \(a\) be a prime ideal. We want to show that \(R/a\) is a domain, where \(R\) is a commutative ring. Let \(x + a, y + a \in R/a\). Then we need to show that if \((x + a)(y + a) = 0\) then \(x + a = 0\) or \(y + a = 0\), where 0 is the zero element of the quotient ring \(R/a\). But the zero element of the ring \(R/a\) is the ideal \(a\). Therefore \((x + a)(y + a) = xy + a = 0\) implies \(xy \in a\). By the assumption that \(a\) is a prime ideal, it now follows that \(x \in a\) or \(y \in a\). Let’s assume \(x \in a\). Then \(x + a = a = 0\), hence \(R/a\) is a domain.

Conversely, assume that \(R/a\) is a domain. Let \(x, y \in R\) be such that \(xy \in a\). Then we can write \(0 = a = xy + a = (x + a)(y + a)\). By the assumption it follows that \(x + a = 0\) or \(y + a = 0\). But if \(x + a = 0\) then \(x \in a\) and if \(y + a = 0\) then \(y \in a\). Hence either \(x \in a\) or \(y \in a\) and so \(a\) is a prime ideal. □

**Proposition 3.32.** If \(a\) is an ideal of a commutative ring \(R\), then \(R/a\) is a field if and only if \(a\) is a maximal ideal.

*Proof.* First let us prove that a field \(F\) does not have any nonzero proper ideals. Let \(c \neq 0\) be an ideal of \(F\). If \(x \in c\) and \(x \neq 0\), then since we know that \(x\) is a unit we can take \(x^{-1} \in F\) and then \(xx^{-1} = 1 \in c\). Then every element in \(F\) can be multiplied with 1 and so \(c = F\). Next, we show that a commutative ring \(R\) with no proper ideal \(c \neq 0\) is a field. Let \(x \in R\) and \(x \neq 0\). Then 1 \(\in Rx = R\) and this holds for every \(x\), hence every element except 0 is invertible in \(R\). Hence \(R\) is a field.

Assume \(a\) is an ideal of a commutative ring \(R\). Then \(R/a\) is a field if and only if \(R/a \neq 0\) and \(R/a\) has no nonzero proper ideal, i.e. there does not exist an ideal \(\mathfrak{c}\) such that \(0 \subsetneq \mathfrak{c} \subsetneq R/a\). Every ideal of \(R/a\) is a quotient \(b/a\) of a unique ideal \(b\) of \(R\) that contains \(a\). Thus the desired statement holds if and only if \(a \neq R\) and \(R\) has no ideal such that \(a \subsetneq b \subsetneq R\). □

Two corollaries follows as consequences to this proposition.
Corollary 3.33. In a commutative ring, every maximal ideal is prime.

Corollary 3.34. An ideal \((n)\) of \(\mathbb{Z}\) is prime if and only if \(n\) is prime and then \((n)\) is maximal.

It is worth to note however, that \((0)\) is a prime ideal of \(\mathbb{Z}\) but \(0\) is not prime and \((0)\) is not a maximal ideal. Thus this statement holds for all ideals except the zero ideal.

3.5 Polynomials

Our usual definition of polynomials needs to be restated in terms of rings and their properties for us to use them as we want. We want to be able to add, multiply and evaluate polynomials as usual. The material in this section is taken from Section 5 in Chapter 3 of [1] and moreover this section will show us how to do that. In this section and hereafter, all rings are assumed to be commutative unless otherwise stated.

Definition 3.35. The set of all polynomials in \(X\) over \(R\) is denoted by \(R[X]\) and is the polynomial ring in one indeterminate \(X\) over \(R\).

\[ R[X] = \{a_0 + a_1X + \cdots + a_nX^n : a_i \in R\}. \]

Polynomials are added together pointwise,

\[ \sum_{i=0}^{n} a_iX^i + \sum_{j=0}^{m} b_jX^j = \sum_{k=0}^{\max(n,m)} (a_k + b_k)X^k, \]

and multiplied the standard way:

\[ \left( \sum_{i=0}^{n} a_iX^i \right) \left( \sum_{j=0}^{m} b_jX^j \right) = \sum_{k=0}^{m+n} c_kX^k, \]

with

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

With these operations, it is easy to see that \(R[X]\) is a ring and we can use the usual operations on every polynomial. An element \(r \in R\) can be seen as a constant polynomial with the coefficient \(a_0 = r\) and \(a_n = 0\) for all \(n > 0\).

Not surprisingly, the degree of a polynomial is the largest possible integer \(n\) such that the coefficient \(a_n \neq 0\). The degree of a constant polynomial is 0. The zero polynomial’s degree is controversial and can be defined by both \(-1\) or \(-\infty\), or could be left undefined. The most important part is that \(\deg 0 < \deg A\) for all nonzero polynomials \(A\). We can state the following properties for degrees of polynomials.
Proposition 3.36. For all nonzero polynomials $A, B$ in $R[X]$ the following properties are true:

(i) $\deg(A + B) \leq \max(\deg A, \deg B)$;

(ii) if $\deg A \neq \deg B$, then $\deg(A + B) = \max(\deg A, \deg B)$;

(iii) $\deg(AB) \leq \deg A + \deg B$;

(iv) if $R$ has no zero divisors, then $\deg(AB) = \deg A + \deg B$.

For example $\deg(A + B) < (\deg A, \deg B)$ happens when $B = -A$. If $uv = 0$ in $R$ then $(uX^m)(vX^n) = 0$ in $R[X]$. Thus if $R$ has zero divisors, then $\deg(AB) < \deg (A) + \deg (B)$ also occurs. Hence if $R$ is a domain then $R[X]$ is a domain too. In particular, if $R$ is a domain, then the units of $R[X]$ are the units of $R$. This is better stated with the next corollary.

Corollary 3.37. If $R$ has no zero divisors, then $A(X)$ is a unit of $R[X]$ if and only if $A$ is constant and $A(0) = a_0 = A$ is a unit of $R$.

Next we need to have knowledge about how to divide polynomials. We say that a polynomial is monic if its leading coefficient is 1.

Proposition 3.38. Let $B \in R[X]$ be a nonzero polynomial with its leading coefficient being a unit of $R$. For every polynomial $A \in R[X]$ there exist polynomials $Q, S \in R[X]$ such that $A = BQ + S$ and $S = 0$ or $\deg S < \deg B$.

Proof. Assume that $B$ is monic. We prove the proposition by using induction on the degree of $A$. Let $\deg B = n$. If $\deg A < n$, then $Q = 0$ and $S = A$ fit the part and we are done.

Next let $\deg A = m \geq n$. Then the polynomial $a_mX^{m-n}B$ has degree $m$ with leading coefficient $a_m$. Hence $A - a_mX^{m-n}B$ has degree less than $m$. Assume that this proposition holds for all polynomials of degree less than $\deg A = m$. Using this induction hypothesis we have $A - a_mX^{m-n}B = BQ_1 + S$ for some $Q_1, S \in R[X]$, with $\deg S < \deg B$. Consequently, by factorizing, we get $A = B(a_mX^{m-n} + Q_1) + S$ and so $A = BQ + S$ if $Q = a_mX^{m-n} + Q_1$.

If $B$ is not monic, then its leading coefficient $b_n$ is still a unit of $R$. Thus $b_n^{-1}B$ is monic and we have $A = Bb_n^{-1}Q + S$ with $\deg S < \deg B$, for some $Q$ and $S$.

The next step in the properties of polynomials of $R[X]$ is knowing how they are evaluated at elements of $R$.

Definition 3.39. If $A = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ and $r \in R$, then $A(r) = a_0 + a_1r + \cdots + a_nr^n \in R$. This is known as evaluation at $r \in R$ of the polynomial $A \in R[X]$.

Proposition 3.40. Let $R$ be a ring. Evaluation at $r \in R$ is a homomorphism $\epsilon_r : R[X] \to R$, $\epsilon_r(A) = A(r)$.
Proof. Let \( r \in R \) and \( A, B \) be polynomials in \( R[X] \). First, we have \( \epsilon_r(1) = 1(r) = 1 \). Moreover, for all \( A, B \in R[X] \) we have \( \epsilon_r(A + B) = (A + B)(r) = A(r) + B(r) = \epsilon_r(A) + \epsilon_r(B) \). Furthermore we have

\[
\epsilon_r(A)\epsilon_r(B) = A(r)B(r) = \left( \sum_i a_i r^i \right) \left( \sum_j b_j r^j \right) = \sum_{i,j} (a_i b_j r^{i+j}) = \sum_k \left( \sum_{i+j=k} a_i b_j \right) r^k = (AB)(r) = \epsilon_r(AB).
\]

\[
\square
\]

**Proposition 3.41.** If \( S \) is a subring of \( R \), then \( S[X] \) is a subring of \( R[X] \).

*Proof.* This is immediate from the definition. \( \square \)

**Definition 3.42.** A root of a polynomial \( A \) in \( R[X] \), where \( R \) is a ring, is an element \( r \) such that \( A(r) = 0 \).

Equivalently, \( r \) is a root of a polynomial \( A \) if \( \epsilon_r(A) = 0 \), where \( \epsilon \) is the evaluation morphism.

**Proposition 3.43.** Let \( r \in R \) and \( A \in R[X] \). Then \( A \) is a multiple of \( X - r \) if and only if \( A(r) = 0 \).

*Proof.* Assume \( A \) is a multiple of \( (X - r) \). Then we can write \( A = (X - r)Q \) for some \( Q \in R[X] \). Evaluating at \( r \) yields \( A(r) = 0 \), so the statement holds. Now assume that \( A(r) = 0 \). By polynomial division we get \( A = (X - r)Q + S \) with \( S = 0 \) or \( \deg S < \deg X - r = 1 \). Thus \( S \) is a constant. But then by the assumption we have \( A(r) = 0 = S \) so \( S = 0 \), hence \( A = (X - r)Q \) and so \( A \) is a multiple of \( (X - r) \). \( \square \)

**Definition 3.44.** Let \( r \in R \) be a root of \( A \in R[X] \). The multiplicity of \( r \) is the largest integer \( m > 0 \) such that \( (X - r)^m \) divides \( A \). If the multiplicity of \( r \) is 1, then \( r \) is a simple root, if not \( r \) is a multiple root.

To discover if there are multiple roots in polynomials we can use the derivative. To do that, we first need to know how the derivative is defined in a ring.

**Definition 3.45.** The formal derivative of \( A(X) = \sum_{n \geq 0} a_n X^n \in K[X] \) is \( A'(X) = \sum_{n \geq 1} n a_n X^{n-1} \in K[X] \).

The following can be stated about the properties of derivatives.
Proposition 3.46. For all polynomials $A, B \in K[X]$ where $n > 0$, $(A + B)' = A' + B'$. $(AB)' = A'B + AB'$ and $(A^n)' = nA^{n-1}A'$.

To find multiple roots using derivative we can use the following proposition. This will be helpful when we go through separable extensions later on.

Proposition 3.47. Let $R$ be a ring. Then a root $r \in R$ of a polynomial $A$ in $R[X]$ is simple if and only if $A'(r) \neq 0$.

Proof. Assume that $r$ has multiplicity $m$. By Proposition 3.43 we know that $A = (X - r)^mB$, where $B(r) \neq 0$. Otherwise $(X - r)^{m+1}$ divides $A$, since the multiplicity is the largest integer $m > 0$ such that $(X - r)^m$ divides $A$. If $r$ is simple then $m = 1$, and $A = (X - r)B$. By using Proposition 3.46 and the definition for the formal derivative we have $A' = B + (X - r)B'$. This implies $A'(r) = B(r) \neq 0$. Now, if $r$ is a multiple root then $m > 1$ and then using the same logic as before we have $A' = m(X - r)^{m-1}B + (X - \alpha)^mB'$. Then evaluating the derivative at $r$ yields $A'(r) = 0$ as required. \qed

3.6 Principal ideal domains

Some domains have special properties. In this section we explore what it means for a domain to be a principal ideal domain. Section 5 and Section 8 in Chapter 3 of [1] is the basis of this section.

Before stating the definition of a principal ideal domain, we need to go through some more properties about the ring $K[X]$ when $K$ is a field.

Proposition 3.48. Let $K$ be a field. Then $K[X]$ is a domain, every ideal of $K[X]$ is principal and more specifically, every nonzero ideal of $K[X]$ is generated by a unique monic polynomial.

Proof. The zero polynomial $0$ generates the trivial ideal $0 = \{0\}$. Let $\mathfrak{A} \neq 0$ be a nonzero ideal of $K[X]$. Then there exists a monic, nonzero polynomial $B \in \mathfrak{A}$ such that the degree of $B$ is the smallest possible to ensure that this is the generator of the ideal. We can assume that $B$ is monic, since it does not affect the degree to divide $B$ by its leading coefficient. Then we have $(B) \subseteq \mathfrak{A}$. To show the other inclusion, assume we have a polynomial $A \in \mathfrak{A}$. Then by polynomial division we can write $A$ as $A = BQ + R$, for some $Q, R \in K[X]$ with deg $R <$ deg $B$. As we have $A, B \in \mathfrak{A}$, we can write $R = A - BQ$ and so $R \in \mathfrak{A}$. But our assumption was that the degree of $B$ was the smallest possible for a polynomial and since deg $R <$ deg $B$, it follows that $R = 0$. Hence $A = BQ \in (B)$ and so $\mathfrak{A} = (B)$.

To show that this generator is unique, we assume $\mathfrak{A} = (B) = (C) \neq 0$. Then we can write $C = BQ_1$ and $B = CQ_2$ for some $Q_1, Q_2 \in K[X]$. Therefore deg $B = $deg $C$ and so $Q_1$ and $Q_2$ must be constants. Assuming $C$ is monic like $B$, the leading coefficients show that $Q_1 = Q_2 = 1$, hence $C = B$. \qed

Now we can define a principal ideal domain.
Definition 3.49. A principal ideal domain, or PID, is a domain where every ideal is principal.

Example 3.50. Some examples of PID’s include $\mathbb{Z}$ and $K[X]$ where $K$ is a field as proved in Proposition 3.48.

Proposition 3.51. Let $R$ be a domain. The ideal generated by an element of $R$ is unique up to multiplication by a unit, i.e. $(a) = (b)$ for some $a, b \in R$ if and only if $a = ub$ where $u \in R^\times$.

Proof. The ideal generated by $a$, $(a)$, is the set of all multiples of $a$ in a ring $R$, i.e. $(a) = Ra$, and similarly, $(b) = Rb$. If $u$ is a unit and $a = ub$, then we can write $Ru = R$ which implies $Rb = Rub = Ra$, i.e $(a) = (b)$. For the opposite implication, assume $Ra = Rb$. Then $a = ub$, $b = va$ for some $u, v \in R$. Now if $a = 0$, then $b = 0$ and $a = 1b$. If $a \neq 0$, then then $a = ub = uva$, i.e. $a = uva$, and by the cancellation laws for domains, this implies $uv = 1$, hence $u$ is a unit. \qed

If $(a) = (b)$ holds for some $a, b$ then we call them associates and write $a \sim b$. We can now define some properties for special elements in domains and particularly in principal ideal domains.

Definition 3.52. In a domain $R$, an element $p \in R$ is called prime if

(i) $p \neq 0$;
(ii) $p \notin R^\times$;
(iii) $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Definition 3.53. In a domain $R$, an element $q \in R$ is called irreducible if

(i) $q \neq 0$;
(ii) $q \notin R^\times$;
(iii) $q = ab$ implies $a \in R^\times$ or $b \in R^\times$.

In a PID, the property of an element being prime and being irreducible are interchangeable and the associated ideal with this element have special properties.

Proposition 3.54. Let $R$ be a principal ideal domain and $p \in R$. The following are equivalent:

(i) $p$ is irreducible;
(ii) $p$ is prime;
(iii) $Rp$ is a nonzero prime ideal;
(iv) $Rp$ is a nonzero maximal ideal.
Proof. By Corollary 3.33, (iv) implies (iii). Moreover, (iii) implies (ii) trivially. To show that (ii) implies (i), we let \( p \) be prime and write \( p = ab \). By definition \( p \) divides \( a \) or \( b \). Assume \( p \) divides \( a \). Since \( p = ab \), \( a \) already divides \( p \) so by Proposition 3.51, \( b \) must be a unit.

Finally, we show that (i) implies (iv). Assume that \( Rp \) is not a maximal ideal, meaning it can be contained in another ideal \( a = Ra \) of \( R \). Then we can write \( p = ab \) for some \( b \in R \). But \( p \) is irreducible by (i), and so either \( a \in R^\times \) which implies \( a = R \) or \( b \in R^\times \) which implies \( a = Rp \). Either way, we can draw the conclusion that \( Rp \) is a nonzero maximal ideal. \( \square \)

**Theorem 3.55.** Let \( R \) be a principal ideal domain. Then every nonzero element which is not a unit is a product of irreducible elements. If we have \( p_1p_2\cdots p_m = q_1q_2\cdots q_n \) where all \( p_i \)'s and \( q_j \)'s are irreducible, then \( m = n \) and we can rearrange the terms so that \( p_i \sim q_i \).

**Proof.** See [1, Chapter 3, Theorem 8.4]. \( \square \)

**Corollary 3.56.** In \( K[X] \), where \( K \) is a field, every nonzero polynomial is a product of a constant and positive powers of distinct monic irreducible polynomials, unique up to order.

**Proposition 3.57.** Let \( K \) be a field. Then the following are true in \( K[X] \):

(i) every polynomial of degree 1 is irreducible;

(ii) irreducible polynomials of degree 2 or more has no root in \( K \);

(iii) a polynomial of degree 2 or 3 with no root in \( K \) is irreducible.

This proposition can lead to some confusion, for example, \((X^2 + 1)^2 \in \mathbb{R}[X]\) is not irreducible but does not have a root in \( \mathbb{R} \), meaning we can not add polynomials of degree 4 to statement (iii). Furthermore, we need to further explain what happens when \( K = \mathbb{C} \) and \( K = \mathbb{R} \).

**Proposition 3.58.** A polynomial over \( \mathbb{C} \) is irreducible if and only if it has degree 1.

**Proof.** See [1, Chapter 3, Proposition 8.10]. \( \square \)

**Proposition 3.59.** A polynomial over \( \mathbb{R} \) is irreducible if and only if it has either degree 1, or degree 2 and no root in \( \mathbb{R} \).

**Proof.** By Proposition 3.57 we know that if a polynomial has these properties then it is irreducible. For the other implication, let \( f(X) \in \mathbb{R} \) and \( f \neq 0 \). Viewing \( f \) as a polynomial over \( \mathbb{C} \), then by Corollary 3.56 it is a product of a constant and monic irreducible polynomials. Since irreducible polynomials in \( \mathbb{C} \) have degree 1, as stated in Proposition 3.58 we can write \( f \) as:

\[
f(X) = a_n(X - r_1)(X - r_2)\cdots(X - r_n).
\]

20
The degree of $f$ is $n$, the leading coefficient is $a_n$ and $r_1, \ldots, r_n$ are the roots of $f$ in $\mathbb{C}$, which are not necessarily distinct. If we take the complex conjugate of $f(X)$ and note that $f$ has real coefficients, then we have

$$f(X) = \overline{f(X)} = a_n(X - \overline{r_1})(X - \overline{r_2}) \cdots (X - \overline{r_n}).$$

We can then draw the conclusion that the roots of $f$ are $\{r_1, \ldots, r_n\} = \{\overline{r_1}, \ldots, \overline{r_n}\}$, because $f$ can only be factorized one such way. Hence the roots of $f$ are either real or pairs of nonreal complex conjugate roots. Thus $f$ is a product of the leading coefficient $a_n$, the polynomials $X - r \in \mathbb{R}[X]$ where $r \in \mathbb{R}$ and the polynomials

$$(X - z)(X - \overline{z}) = X^2 - (z + \overline{z})X + z\overline{z} \in \mathbb{R}[X], \ z \in \mathbb{C} \setminus \mathbb{R}$$

which has no root in $\mathbb{R}$. Thus if $f$ is irreducible in $\mathbb{R}[X]$, then $f$ has either degree 1, or it has degree 2 and no root in $\mathbb{R}$.

3.7 Fields

We already defined what a field is in Section 3.4; it is a domain where all elements except zero are invertible under multiplication. Now we continue to develop the theory of fields. This section’s information is taken from Section 4 and 5 of Chapter 3 and Section 1 of Chapter 4, both in [1].

Definition 3.60. A subset $K$ of a field $F$ is a subfield of $F$ if the following hold true:

(i) $0, 1 \in K$;

(ii) for all $x, y \in K$ we have that $x - y \in K$;

(iii) for all $x, y \in K$ such that $y \neq 0$ we have that $xy^{-1} \in K$.

In particular this states that $K$ is a subgroup under addition of $F$ and $K \setminus \{0\}$ is a multiplicative subgroup of $F \setminus \{0\}$.

Example 3.61. Some known subfields are $\mathbb{Q}$ of $\mathbb{R}$ and $\mathbb{R}$ of $\mathbb{C}$. As a counterexample, $\mathbb{Z}$ is not a subfield of $\mathbb{Q}$.

The definition of a field morphism is the same as for a ring morphisms. Just like for rings, a field isomorphism is a bijective field morphism. Moreover, a field automorphism is a field isomorphism of a field $K$ onto $K$. Furthermore we have a property that can be stated as:

Proposition 3.62. Every field morphism is injective.

Proof. Let $\varphi : K \to F$ be a field morphism. We know that $\text{Ker} \varphi$ is a ideal in $K$. Moreover $\varphi(1) = 1 \neq 0$ so $\text{Ker} \varphi$ is a proper ideal and from the proof of Proposition 3.32 we know that fields does not have any nonzero proper ideals, this implies that $\text{Ker} \varphi = 0$ and this in turn implies that $\varphi$ is injective. \qed
This proposition means that we can restate Theorem 3.19 but for fields this time.

**Proposition 3.63.** If \( \varphi : K \to L \) is a field morphism, then \( \text{Im } \varphi \) is a subfield of \( L \) and \( K \cong \text{Im } \varphi \).

Field morphisms can induce ring morphisms.

**Proposition 3.64.** Every field morphism \( \varphi : K \to L \) induces a ring morphism \( K[\![X]\!] \to L[\![X]\!] \), \( f \mapsto \varphi f \). If \( f(X) = a_0 + a_1X + \cdots + a_nX^n \), then \( \varphi f(X) = \varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n \).

This notion is revisited later in Galois theory. We can restate Proposition 3.28 with regard to fields and the result follows immediately.

**Proposition 3.65.** The characteristic of a field is either 0 or a prime number.

**Proposition 3.66.** Every field \( K \) has a smallest subfield, which is either isomorphic to \( \mathbb{Q} \) if \( K \) has characteristic 0 or to \( \mathbb{Z}_p \) if \( K \) has characteristic \( p \neq 0 \).

**Proof.** It follows immediately from Proposition 3.65 that if \( K \) has characteristic \( p \neq 0 \) then \( p \) is prime. Then the smallest subring of \( K \) is a field and thus it is the smallest subfield of \( K \). By Proposition 3.26 we have that this subfield is isomorphic to \( \mathbb{Z}_p \).

If \( K \) has characteristic 0, then we have that the injection \( m \mapsto m1 \) of \( \mathbb{Z} \) into \( K \) extends to a morphism \( \varphi \) from \( \mathbb{Q} \) into \( K \), i.e. \( \varphi(m/n) = m1(n1)^{-1} \). Then by Proposition 3.63 \( \text{Im } \varphi \cong \mathbb{Q} \) is a subfield of \( K \). Every subfield must contain the identity, 1, and every element \( m1(n1)^{-1} \) of \( \text{Im } \varphi \), hence this subfield is the smallest subfield of \( \mathbb{Q} \).

There exist some special elements in a field which we call roots of unity. We are going to need to use them in a later section, therefore it is good to introduce them here.

**Definition 3.67.** Let \( K \) be a field. An element \( r \in K \) is an \( n \)-th root of unity when \( r^n = 1 \).

**Example 3.68.** The \( n \)-th roots of unity in \( \mathbb{C} \) are \( e^{2ik\pi/n} \), with \( k = 0, 1, \ldots, n - 1 \). These form a cyclic group under multiplication with generator \( e^{2\pi i/n} \).

In general, roots of unity form a group under multiplication. Let \( K \) be a field. For a root of unity \( r \in K \) we have \( r^n = 1 \). The associativity is immediate. Certainly \( r^n1^n = r^n = 1^n r^n \) so the identity element is 1. Since \( K \) is a field all nonzero elements are units, meaning there exists an element \( r^{-1} \). This element is also a root of unity since \( (r^{-1})^n = (r^n)^{-1} = 1^n = 1 \) and so the set is closed under inverses. Thus the roots of unity satisfies all group axioms. Moreover if \( r^n = 1 \) and \( s^n = 1 \) for \( r, s \in R \) then \( (rs)^n = r^n s^n = 1 \) so this group is closed under multiplication.

Moreover we can say the following general property about fields.
Proposition 3.69. Every finite multiplicative subgroup of a field is cyclic.

Proof. See [1, Chapter 4, Proposition 1.6].

These subgroups consists of roots of unity, since all its elements have finite order. We also want to state how subfields can be constructed.

Proposition 3.70. Every intersection of subfields of a field \( F \) is a subfield of \( F \).

Generally, the union of subfields is not a subfield. However, by Proposition 3.70 we know that for every subset \( S \) of a field \( F \) there exists a smallest subfield of \( F \) that contains \( S \). This is the subfield of \( F \) that is generated by \( S \). Now assume that \( K \) is the smallest subfield of \( F \). Then the union of \( K \) and the subset \( S \) yields the subfield generated by just \( S \).

Definition 3.71. Let \( K \) be a subfield of a field \( F \) and let \( S \) be a subset of \( F \).

(i) The subring \( K[S] \) of \( F \) is the smallest subring of \( F \) containing both \( K \) and \( S \).

(ii) The subfield \( K(S) \) of \( F \) is the smallest subfield of \( F \) containing both \( K \) and \( S \).

Proposition 3.72. Let \( K \) be a subfield of a field \( F \) and let \( S \) be a subset of \( F \).

(i) The subring \( K[S] \) generated by \( K \cup S \) is the set of all finite linear combinations with coefficients in \( K \) of finite products of powers of elements of \( S \).

(ii) The subfield \( K(S) \) of \( F \) generated by \( K \cup S \) is the set of all \( ab^{-1} \in F \) with \( a, b \in K[S], \ b \neq 0 \) and it is isomorphic to the field of fractions of \( K[S] \).

Proof. The proof is similar to the proof how ideals are constructed by subsets of a ring. For details see [1, Chapter 4, Proposition 1.9].

It is worth to note that although its elements look like polynomials, \( K[S] \) is not a polynomial ring. Likewise, even though the elements of \( K(S) \) look like rational fractions, it is not a field of rational fractions. Another note is that \( K[S] \) and \( K(S) \) not only depends on \( K \) and \( S \) but also on \( F \). If \( S \) is a finite set, \( S = \{s_1, \ldots, s_n\} \), then \( K[S] \) and \( K(S) \) can be written as \( K[s_1, \ldots, s_n] \) and \( K(s_1, \ldots, s_n) \). This yields the properties in the following corollary.

Corollary 3.73. Let \( F \) be a field, \( K \) a subfield of \( F \), \( S \) a subset of \( F \) and let \( x, \alpha_1, \ldots, \alpha_n \in F \).

(i) \( x \in K[\alpha_1, \ldots, \alpha_n] \) if and only if \( x = f(\alpha_1, \ldots, \alpha_n) \) for some polynomial \( f \in K[X_1, \ldots, X_n] \).

(ii) \( x \in K(\alpha_1, \ldots, \alpha_n) \) if and only if \( x = r(\alpha_1, \ldots, \alpha_n) \) for some rational fraction \( r \in K(X_1, \ldots, X_n) \).

(iii) \( x \in K[S] \) if and only if \( x \in K[\alpha_1, \ldots, \alpha_n] \) for some \( \alpha_1, \ldots, \alpha_n \in S \).

(iv) \( x \in K(S) \) if and only if \( x \in K(\alpha_1, \ldots, \alpha_n) \) for some \( \alpha_1, \ldots, \alpha_n \in S \).
4 Field extensions

The material in this section is taken from Chapter 4 of [1].

4.1 Extensions

In this section we will state and prove some basic properties of field extensions. The material in this section is taken from Section 2 of Chapter 4 in [1].

Definition 4.1. A field extension of a field \( K \) is a field \( E \) of which \( K \) is a subfield.

If it is understood that \( K \) and \( E \) are fields then we denote this as \( K \subseteq E \).

In field extensions we can define \( K \)-homomorphisms as a way for different field extensions to relate to each other.

Definition 4.2. Let \( K \subseteq E \) and \( K \subseteq F \) be field extensions of \( K \). A \( K \)-homomorphism of \( E \) into \( F \) is a field morphism \( \varphi : E \to F \) that acts as the identity on \( K \), i.e. \( \varphi(x) = x \) for all \( x \in K \).

Moreover, a \( K \)-isomorphism is a bijective \( K \)-morphism and a \( K \)-automorphism of a field extension \( K \subseteq E \) is a \( K \)-isomorphism of \( E \) onto \( E \).

An important fact about field extensions is that if \( K \) is a subfield of a field \( E \), then \( E \) is a vector space over \( K \) equipped with addition \( E \times E \to E \) and scalar multiplication \( K \times E \to E \). Since we can view \( E \) as a vector space over \( K \), then we can also discuss what dimension this vector space has.

Definition 4.3. The degree of a field extension \( K \subseteq E \), denoted \( [E : K] \), is the dimension of \( E \) as a vector space over \( K \).

Moreover a field extension \( K \subseteq E \) is finite when it is of finite degree and otherwise it is infinite.

Example 4.4. (i) \( \mathbb{C} \) is a finite extension of \( \mathbb{R} \) with \( [\mathbb{C} : \mathbb{R}] = 2 \).

(ii) \( \mathbb{R} \) is an infinite extension of \( \mathbb{Q} \), i.e. \( [\mathbb{R} : \mathbb{Q}] = \infty \).

Observe that a finite field extension does not imply that the cardinality of the fields are finite, it only admits information about the dimension of the extension.

Proposition 4.5. If \( K \subseteq E \subseteq F \), then \( [F : K] = [F : E][E : K] \).

Proof. First, let \( (\alpha_i)_{i \in I} \) be a basis of \( E \) over \( K \). Next let \( (\beta_j)_{j \in J} \) be a basis of \( F \) over \( E \) and so every element of \( F \) is a linear combination of \( \beta_j \)'s with coefficients in \( E \). Those coefficients are themselves linear combinations of \( \alpha_i \)'s with coefficients in \( K \), since \( (\alpha_i)_{i \in I} \) is a basis. In conclusion, every element of \( F \) is a linear combination of \( \alpha_i \beta_j \)'s with coefficients in \( K \).

Viewing \( F \) as a vector space over \( K \) we show that \( (\alpha_i \beta_j)_{(i,j) \in I \times J} \) is a linearly independent family. Suppose \( \sum_{(i,j) \in I \times J} x_{i,j} \alpha_i \beta_j = 0 \), with \( x_{i,j} = 0 \) for almost
exists an evaluation morphism \( f \). We know that each \( \sum_{i,j} x_{i,j} \alpha_i \) is an element of \( E \) so \( \sum_{i,j} x_{i,j} \alpha_i = 0 \) for all \( j \) since \( (\beta_j)_{j\in J} \) is linearly independent over \( E \). Moreover this implies \( x_{i,j} = 0 \) for all \( i,j \) since \( (\alpha_i)_{i\in I} \) is linearly independent over \( K \). Therefore \( (\alpha_i \beta_j)_{(i,j)\in I\times J} \) is a basis of \( F \) over \( K \) and moreover \( |F : K| = |I\times J| = |I||J| = |F : E||E : K| \).

**Definition 4.6.** A field extension \( K \subseteq E \) is finitely generated when \( E = K(\alpha_1, \ldots, \alpha_n) \) for some \( \alpha_1, \ldots, \alpha_n \in E \). A field extension \( K \subseteq E \) is simple when \( E = K(\alpha) \) for some \( \alpha \in E \), and then \( \alpha \) is a primitive element of \( E \).

For a field extension \( K \subseteq E, \alpha \in E \), we have by Proposition 3.40 that there exists an evaluation morphism \( f \rightarrow f(\alpha) \) of \( K[X] \) into \( E \). The kernel of this morphism is an ideal of \( K[X] \) and is either 0 or generated by a unique monic polynomial. We have the following proposition which states this.

**Proposition 4.7.** Let \( K \subseteq E \) be a field extension and let \( \alpha \in E \). Moreover let \( \psi : K[X] \rightarrow E \), \( f(X) \rightarrow f(\alpha) \) be the evaluation morphism. Then either

(i) \( f(\alpha) \neq 0 \) for every nonzero polynomial \( f(X) \in K[X] \). Then there exists an isomorphism \( K(\alpha) \cong K(X) \);

(ii) \( f(\alpha) = 0 \) for some nonzero polynomial \( f(X) \in K[X] \). Then there is a unique monic irreducible polynomial \( q \) such that \( q(\alpha) = 0 \). Then \( f(\alpha) = 0 \) if and only if \( q \) divides \( f \) and we have that \( K[\alpha] = K(\alpha) \cong K[X]/(q) \). Moreover \( [K(\alpha) : K] = \deg q \) and \( 1, \alpha, \ldots, \alpha^{n-1} \) is a basis of \( K(\alpha) \) over \( K \) where \( \deg q = n \).

**Proof.** As in the proposition, we divide the proof into two parts. Note that since \( \psi \) is the evaluation morphism, by Corollary 3.73 part (i) it is clear that \( \text{Im } \psi = K[\alpha] \subseteq E \).

(i) If \( f(\alpha) \neq 0 \), for every nonzero polynomial \( f(X) \in K[X] \) then \( \ker \psi = 0 \) and then \( K[\alpha] \cong K[X] \). Let \( \varphi : K(X) \rightarrow E \) be a field morphism with \( \varphi(\frac{f}{g}) = \frac{f(\alpha)}{g(\alpha)} \). Then \( \text{Im } \varphi = K(\alpha) \) and since \( \varphi \) is a field isomorphism, it is injective and hence \( K(X) \) is isomorphic to \( \text{Im } \varphi \). Hence \( K(\alpha) \cong K(X) \).

(ii) The other case is if \( \ker \psi \) is not 0. Since the kernel is always an ideal, we know by Proposition 3.48 that \( \ker \psi \) is generated by a unique monic polynomial \( q \). Since \( q \) generates the kernel, the evaluation morphism \( f(\alpha) = 0 \) if and only if \( q \) divides \( f \). Moreover by the isomorphism theorem applied to \( \psi \) we have \( K[\alpha] \cong K[X]/\ker \psi = K[X]/(q) \). Since \( K[\alpha] \) is a subring of a domain, it is a domain. Thus \( K[X]/(q) \) is also a domain since it is isomorphic to \( K[\alpha] \). By Proposition 3.31 \( (q) \) is a prime ideal. Then by Proposition 3.54 \( (q) \) is a maximal ideal and \( q \) is irreducible. Hence \( K[\alpha] \cong K[X]/(q) \) is a field by Proposition 3.32. Therefore \( K(\alpha) = K[\alpha] \). Now if \( p \in K[X] \) is a monic and irreducible polynomial with \( p(\alpha) = 0 \), since \( q \) is the generator of \( \ker \psi \), \( q \) divides \( p \), but \( p \) was said to be irreducible thus \( q = p \). Hence \( q \) is unique.
Now let \( n = \text{deg}(q) > 0 \). We have \( f = qg + r \) for every \( f \in K[X] \) where \( \text{deg}(r) < n \). Since \( q(\alpha) = 0 \), \( f(\alpha) = r(\alpha) \) and so every element \( f(\alpha) \) of \( K[\alpha] \) is a linear combination of \( 1, \alpha, \ldots, \alpha^{n-1} \) and has coefficients in \( K \). Furthermore \( 1, \alpha, \ldots, \alpha^{n-1} \) are linearly independent over \( K \).

To show that they are linearly independent, let’s assume that they are not. Then \( r(\alpha) = 0 \), with \( r \in K[X] \) and \( \text{deg}(r) < n \), and then \( q \) divides \( r \). If \( q \) divides \( r \) then \( \text{deg} r \geq \text{deg} q \) which is a contradiction, hence \( r = 0 \). Hence \( 1, \alpha, \ldots, \alpha^{n-1} \) are linearly independent over \( K \). In conclusion, if we view \( K[\alpha] \) as a vector space then \( 1, \alpha, \ldots, \alpha^{n-1} \) is a basis of \( K[\alpha] \) over \( K \).

\[ \square \]

Now we are ready to define some special elements in field extensions. These are called algebraic and transcendental elements.

**Definition 4.8.** Let \( K \subseteq E \) be a field extension. If \( f(\alpha) = 0 \), for an element \( \alpha \in E \) and some nonzero polynomial \( f(X) \in K[X] \), then \( \alpha \) is algebraic over \( K \). Otherwise \( \alpha \) is transcendental over \( K \).

This definition of algebraic elements is equivalent to the next proposition.

**Proposition 4.9.** Let \( K \subseteq E \) be fields and let \( \alpha \in E \). Then \( \alpha \) is algebraic over \( K \) if and only if \( [K(\alpha) : K] \) is finite.

**Proof.** This follows because of Proposition 4.7. Let \( \alpha \) be algebraic over \( K \), then \( f(\alpha) = 0 \) for some \( f \in K[X] \). Then by part (ii) of the proposition there exists a monic irreducible polynomial \( q \) such that \( q \) divides \( f \) and \( [K(\alpha) : K] = \text{deg} q \). Hence \( [K(\alpha) : K] \) is finite. Conversely, assume that \( [K(\alpha) : K] \) is finite. Let \( n = [K(\alpha) : K] \). Then there exists a set of \( n+1 \) elements \( \{1, \ldots, \alpha^n\} \) which must be linearly dependent over \( K \). Hence there exists coefficients \( a_0, \ldots, a_n \in K \) such that \( a_0 + a_1 \alpha + \cdots + a_n \alpha^n = 0 \) which implies that \( \alpha \) is algebraic over \( K \).

\[ \square \]

**Example 4.10.** Every complex number is algebraic over \( \mathbb{R} \).

**Definition 4.11.** Let \( \alpha \) be algebraic over a field \( K \). The unique monic irreducible polynomial \( q(X) = \text{irrpol}_K(\alpha) \in K[X] \) such that \( q(\alpha) = 0 \) is the irreducible polynomial of \( \alpha \) over \( K \). The degree of \( \alpha \) over \( K \) is the degree of \( \text{irrpol}_K(\alpha) \).

**Example 4.12.** We have that \( \text{irrpol}_\mathbb{R}(i) = X^2 + 1 \) and \( i \) has degree 2 over \( \mathbb{R} \).

Every irreducible polynomial \( q \in K[X] \) has a root in some extension of \( K \).

**Proposition 4.13.** Let \( K \) be a field and let \( q \in K[X] \) be irreducible. Up to isomorphism, \( E = K[X]/(q) \) is a simple field extension of \( K \), i.e. \( E = K(\alpha) \) where \( \alpha = X + (q) \). Furthermore, \( [E : K] = \text{deg} q \) and \( q = \text{irrpol}_K(\alpha) \).

**Proof.** Since \( q \) is irreducible, the ideal \((q)\) is maximal in \( K[X] \), by Proposition 3.54. Thus by Proposition 3.32 \( E = K[X]/(q) \) is a field. Then \( x \mapsto x + (q) \) is...
a field morphism of $K$ into $E$. We can say $x \in K$ and $x + (q) \in E$ and then $E$ is an extension of $K$.

Let $\alpha = X + (q) \in E$. The evaluation morphism $f(X) \mapsto f(\alpha)$ and the canonical projection $K[X] \twoheadrightarrow E$ coincide and $f(X) + (q) = f(\alpha)$ for all $f \in K[X]$. Therefore $E = K[\alpha]$, by Corollary 3.73. Since $E$ is a field, $K[\alpha]$ is field and so $E = K(\alpha)$. Moreover, for $q \in K[X]$, we have $q(X) + (q) = q(\alpha)$. But $q(X) + (q) = 0$ in $E = K[X]/(q)$, hence $q(\alpha) = 0$. This implies that $\alpha$ is algebraic over $K$ and so $\text{irrpol}_{K}(\alpha) = q$. By Definition 4.11 it follows that $[E : K] = \deg q$.

**Example 4.14.** For instance, $\mathbb{R}[X]/(X^2 + 1)$ is a simple extension $\mathbb{R}(\alpha)$ of $\mathbb{R}$. Its basis is $1, \alpha$ by Proposition 4.7 and also $\alpha^2 + 1 = 0$. Thus $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$.

### 4.2 Algebraic Extensions

This section is about algebraic extensions and their properties. The information is taken from Chapter 4, Section 3 in [1].

**Definition 4.15.** Let $K \subseteq E$ be a field extension. We say that this extension is **algebraic** and that $E$ is **algebraic over $K$** when every element of $E$ is algebraic over $K$.

**Example 4.16.** For example, $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$.

**Proposition 4.17.** Every finite field extension is algebraic.

**Proposition 4.18.** If $E = K(\alpha_1, \ldots, \alpha_n)$ and every $\alpha_i$ is algebraic over $K$, then $E$ is finite over $K$, hence also algebraic over $K$.

**Proof.** Let $E = K(\alpha_1, \ldots, \alpha_n)$, where every $\alpha_i$ are algebraic over $K$. We shall show that $E$ is finite over $K$ by using induction on $n$. If $n = 0$, then $E = K$ and this is certainly finite over $K$. Assume that the proposition holds for $n > 0$ upto $n - 1$ i.e. $F = K(\alpha_1, \ldots, \alpha_{n-1})$ is finite over $K$. This is our induction hypothesis. But $\alpha_n$ is algebraic over $K$, i.e. there exists some nonzero $f \in K[X]$ such that $f(\alpha_n) = 0$. Since $K[X] \subseteq F[X]$ we have $E = F(\alpha_n)$ is finite over $E$ by part (ii) of Proposition 4.7. Then by the law for the degrees of extensions, Proposition 4.5, $E$ is finite over $K$. \qed

Some further properties of algebraic extensions follows.

**Proposition 4.19.** If every $\alpha \in S$ is algebraic over $K$, then $K(S)$ is algebraic over $K$.

**Proposition 4.20.** Let $K \subseteq E \subseteq F$ be fields. If $F$ is algebraic over $K$, then $E$ is algebraic over $K$ and $F$ is algebraic over $E$.

**Proposition 4.21.** Let $K \subseteq E \subseteq F$ be fields. If $E$ is algebraic over $K$ and $F$ is algebraic over $E$ then $F$ is algebraic over $E$.

This is called the Tower property.
4.3 Algebraic closure

This section deals with the algebraic closure of a field, which is the greatest algebraic extension of that field, up to isomorphism. We have based this section of Section 4 of Chapter 4 in [1].

**Proposition 4.22.** Let $K$ be a field. The following are equivalent:

1. the only algebraic extension of $K$ is $K$ itself;
2. in $K[X]$, every irreducible polynomial has degree 1;
3. every non constant polynomial in $K[X]$ has a root in $K$.

**Proof.** (1) implies (2). If $q \in K$ is irreducible, then by using Proposition 4.13 we know that $E = K[X]/(q)$ has degree $[E : K] = \deg q$. Since we assumed that the only algebraic extension of $K$ is itself, i.e $[E : K] = 1$, this implies that $\deg q = 1$.

(2) implies (3). Every non constant polynomial $f \in K[X]$ is a nonempty product of irreducible polynomials.

(3) implies (1). When an element $\alpha$ is algebraic over $K$, we know that $q = \text{irrpol}_K(\alpha)$ has a root $r$ in $K$ and the fact that $q(\alpha) = 0$ tells us that $\alpha = r \in K$.

**Definition 4.23.** If the conditions in Proposition 4.22 are satisfied by a field, we say that field is algebraically closed.

**Example 4.24.** For example, the field $\mathbb{C}$ is algebraically closed, while $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{Z}_p$ are not algebraically closed fields.

Homomorphisms behave in a certain way in algebraically closed fields.

**Theorem 4.25.** Every homomorphism of a field $K$ into an algebraically closed field can be extended to every algebraic extension of $K$.

**Proof.** See [1, Chapter 4, Theorem 4.2].

**Definition 4.26.** The algebraic closure of a field $K$ is an algebraic extension $\overline{K}$ of $K$ that is algebraically closed.

We call this the algebraic closure of $K$ because all algebraic closures of a field $K$ are $K$-isomorphic.

**Corollary 4.27.** For every algebraic extension $E \subseteq K$, $\overline{E}$ is an algebraic closure of $K$. Hence $E$ is $K$-isomorphic to an intermediate field $K \subseteq F \subseteq \overline{K}$ of any algebraic closure of $K$.

**Proposition 4.28.** Every $K$-endomorphism of $\overline{K}$ is a $K$-automorphism.

**Proof.** See [1, Chapter 4, Proposition 4.6].

**Proposition 4.29.** If $K \subseteq E \subseteq \overline{K}$ is an algebraic extension of $K$, then every $K$-homomorphism of $E$ into $\overline{K}$ extends to a $K$-automorphism of $\overline{K}$.
Proof. Every $K$-homomorphism of $E$ into $\overline{K}$ extends to a $K$-endomorphism of $\overline{K}$, this follows by Theorem 4.25. Since every $K$-endomorphism of $\overline{K}$ is a $K$-automorphism by Proposition 4.28, the result follows.

4.4 Separable extensions

When the irreducible polynomials of an algebraic extension have no multiple roots, i.e. its elements are separable, then we say that that extension is separable. This section deals with separability of extensions and is based on Section 5 of Chapter 4 in [1].

Before defining what a separable polynomial is, we shall go through the different components of a polynomial. Let $f \in K[X]$ be a non constant polynomial with coefficients in a field $K$. We can view $f$ as a polynomial with coefficients in any algebraic closure $\overline{K}$ of $K$. Then $f$ factors uniquely, up to order, into a product of positive powers of irreducible polynomials of degree 1. This can be written as:

$$f(X) = a(X - \alpha_1)^{m_1}(X - \alpha_2)^{m_2}\cdots(X - \alpha_r)^{m_r}.$$ 

Here $a \in K$ denotes the leading coefficient of $f$, $r > 0$, $m_1, \ldots, m_r > 0$ and $\alpha_1, \ldots, \alpha_r \in \overline{K}$ are the distinct roots of $f$ in $\overline{K}$, with $m_i$ the multiplicity of $\alpha_i$.

Definition 4.30. A separable polynomial $f \in K[X]$ is a polynomial which has no multiple roots in $\overline{K}$.

Remember that a root is a multiple root when the multiplicity is greater than 1.

Example 4.31. Let $f(X) = X^4 + 2X^2 + 1$ and $g(X) = X^2 + 1$ be two polynomials in $\mathbb{R}[X]$.

(i) We have that $f(X) = X^4 + 2X^2 + 1 \in \mathbb{R}[X]$ factors into $f(X) = (X^2 + 1)^2 = (X - i)^2(X + i)^2$ in $\mathbb{C}[X]$. Hence in the algebraic closure of $\mathbb{R}$, $\mathbb{R} = \mathbb{C}$, $f(X)$ has two multiple roots and is therefore not separable.

(ii) We have that $g(X) = X^2 + 1 \in \mathbb{R}[X]$ factors into $g(X) = (X - i)(X + i)$ in $\mathbb{C}[X]$. Hence $g(X)$ is separable since its roots are of multiplicity 1 in $\mathbb{R} = \mathbb{C}$.

Proposition 4.32. Let $q \in K[X]$ be irreducible.

(i) If $K$ has characteristic 0, then $q$ is separable.

(ii) If $K$ has characteristic $p \neq 0$, then all roots of $q$ in $\overline{K}$ have the same multiplicity. This multiplicity is a power of $p$, $p^m$, and there exists a separable irreducible polynomial $s \in K[X]$ such that $q(X) = s(X^{p^m})$.

Proof. (i) Assume that $q$ is monic. By Proposition 3.47, $\alpha \in \overline{K}$ is a multiple root of $q$ if $q(\alpha) = 0$ and $q'(\alpha) = 0$. Then since $q(\alpha) = 0$, $\alpha$ is algebraic over $K$. Since $q$ is irreducible $q = \text{irrpol}_K(\alpha)$. Thus $q$ divides $q'$, but then
\( q' = 0 \) since \( \deg q' < \deg q \) always. But \( q' \neq 0 \) if \( K \) has characteristic 0 because \( q \) is not constant. Thus the assumption that \( q \) has a multiple root is false and \( q \) is separable.

(ii) Let \( K \) have characteristic \( p \neq 0 \). We write \( q \) as \( q(X) = \sum_{n \geq 0} a_n X^n \) and note that if it has a multiple root, then as in part (i) the formal derivative must be 0, i.e. \( q'(X) = \sum_{n \geq 1} n a_n X^{n-1} = 0 \). For this to hold true, since \( K \) has characteristic \( p \), all coefficients \( a_n = 0 \), whenever \( n \) is not a multiple of \( p \). Thus \( q \) only contains powers of \( X^p \). This implies that we can write \( q \) as \( q(X) = r(X^p) \) for some \( r \in K[X] \), where \( r \) is a monic and irreducible polynomial in \( K[X] \). If \( r \) could be factorized then so could \( q \), which is not true, hence why \( r \) is irreducible. We also have \( \deg r < \deg q \).

Now if \( r \) is not separable, then we can use the same logic as before and write \( r(X) = t(X^p) \) and this implies and \( q(X) = t(X^p^2) \), where \( t \) is monic and irreducible in \( K[X] \) and \( \deg t < \deg r < \deg q \). We apply this logic again and again, until the process stops and then \( q(X) = s(X^{p^m}) \), where \( s \in K[X] \) is a monic, irreducible and separable polynomial.

Let \( \beta_1, \ldots, \beta_n \) be the distinct roots of \( s \) in \( \overline{K} \). Then \( s \) can be written as \( s(X) = (X - \beta_1)(X - \beta_2) \cdots (X - \beta_n) \). However since \( \overline{K} \) is algebraically closed, it is possible to write the roots as \( \beta_i = \alpha_i^{p^m} \) for some \( \alpha_i \in \overline{K} \). Moreover, \( \alpha_1, \ldots, \alpha_n \) are distinct. In \( K \) and \( \overline{K} \), \( (x - y)^p = x^p - y^p \) for all \( x, y \) by Proposition 3.29. Applying this to the polynomial \( s \) and its roots we have:

\[
q(X) = s(X^{p^m}) = \prod_i (X^{p^m} - \alpha_i^{p^m}) = \prod_i (X - \alpha_i)^{p^m}.
\]

Hence the roots of \( q \) in \( \overline{K} \) are \( \alpha_1, \ldots, \alpha_n \) and every one of them has multiplicity \( p^m \).

There is a way to relate the separability of a polynomial to the number of \( K \)-homomorphisms into \( \overline{K} \). This is called the separability degree and is defined as follows.

**Definition 4.33.** The *separability degree* of an algebraic extension \( K \subseteq E \) is the number of \( K \)-homomorphisms of \( E \) into an algebraic closure \( \overline{K} \) of \( K \). This is denoted by \([E : K]_S\).

Since the algebraic closure \( \overline{K} \) is unique up to \( K \)-isomorphism the number \([E : K]_S\) is independent of the choice of \( \overline{K} \). As for extensions, we have a tower law for separable extensions.

**Proposition 4.34.** If \( K \subseteq E \subseteq F \) are field extensions and \( F \) is algebraic over \( K \), then \([F : K]_S = [F : E]_S [E : K]_S\).

**Proof.** See [1] Chapter 4, Proposition 5.3].
Definition 4.35. An element $\alpha$ is \textit{separable} over $K$ when $\alpha$ is algebraic over $K$ and $\text{irrpol}_K(\alpha)$ is separable. An algebraic extension $E$ of $K$ is \textit{separable} when every element of $E$ is separable over $K$. We say that $E$ is \textit{separable} over $K$.

By Proposition 4.32 we can now state the following.

Proposition 4.36. If $K$ has characteristic 0, then every algebraic extension of $K$ is separable.

Proposition 4.37. For a finite extension $K \subseteq E$ the following conditions are equivalent:

(i) $E$ is separable over $K$;

(ii) $E$ is generated by finitely many separable elements;

(iii) $[E : K]_s = [E : K]$.

Proof. See \cite[Chapter 4, Proposition 5.6]{1}.

Separable extensions have some useful properties.

Proposition 4.38. If every $\alpha \in S$ is separable over $K$, then $K(S)$ is separable over $K$.

Proposition 4.39. Let $K \subseteq E \subseteq F$ be algebraic extensions. If $F$ is separable over $K$, then $E$ is separable over $K$ and $F$ is separable over $E$.

Proof. Assume that $F$ is separable over $K$. By the definition of separable extensions, all elements $\alpha \in F$ is separable over $K$. But since $E \subseteq F$ this holds for all $\alpha \in E$ as well, thus $E$ is separable over $K$. Now let $\alpha \in F$. We have that $\text{irrpol}_E(\alpha)$ divides $\text{irrpol}_K(\alpha)$. But $\text{irrpol}_K(\alpha)$ is separable since $F$ is separable over $K$ and hence $\alpha$ is separable over $E$ as well. Thus $E \subseteq F$ is separable.

The Tower property can be stated for separable extensions as well.

Proposition 4.40. Let $K \subseteq E \subseteq F$ be algebraic extensions. If $E$ is separable over $K$ and $F$ is separable over $E$, then $F$ is separable over $K$.

Proof. Assume that the extensions $K \subseteq E$ and $E \subseteq F$ are separable. We know from Proposition 4.37 that $[E : K] = [E : K]_s$ and $[F : E] = [F : E]_s$. Moreover by the tower law for extensions we have $[F : K] = [F : E][E : K]$ and also the tower law for separable extensions states that $[F : K]_s = [F : E]_s[E : K]_s$. It follows that $[F : K] = [F : K]_s$ and so $F$ is separable over $K$.

Proposition 4.41. Every finite separable extension is simple.

Proof. Let $E$ be a finite separable extension of a field $K$. We have two cases, either $K$ is finite or $K$ is infinite.

If $K$ is finite, then $E$ must also be finite. Then the multiplicative group of units $E \setminus \{0\}$ is a cyclic group by Proposition 3.69. Hence $E$, as an extension, is generated by a single element.
Now let $K$ be infinite. If we can show that every finite separable extension $E = K(\alpha, \beta)$ of $K$ that has two generators is simple, then it follows by induction on $k$ that every finite separable extension $K(\alpha_1, \ldots, \alpha_k)$ is simple too.

Since $K \subseteq E$ is separable, the separability degree is the same as the degree. Now let $n = [E : K] = [E : K]_S$ and $\varphi_1, \ldots, \varphi_n$ be distinct $K$-homomorphisms of $E$ into $\overline{K}$. Then let $f$ be a polynomial in $\overline{K}[X]$ written as

$$f(X) = \prod_{i<j} (\varphi_i \alpha + (\varphi_i \beta)X - \varphi_j \alpha - (\varphi_j \beta)X).$$

Since $\varphi_1, \ldots, \varphi_n$ are distinct, $f$ is not the zero polynomial, then since $K$ is assumed to be infinite, $f(t) = 0$ cannot happen for all $t \in K$. Hence we have $f(t) \neq 0$ for some $t \in K$. Then the elements $\varphi_1(\alpha + \beta t), \ldots, \varphi_n(\alpha + \beta t)$ are distinct. This implies that there exist at least $n$ $K$-homomorphisms of $K(\alpha + \beta t)$ into $\overline{K}$ and moreover $[K(\alpha + \beta t) : K] \geq n$. So $[K(\alpha + \beta t) : K] = [E : K]$ and therefore $E = K(\alpha + \beta t)$.

**Proposition 4.42.** If $E$ is separable over $K$ and \text{irrpol}_{K}(\alpha)$ has degree at most $n$ for every $\alpha \in E$, then $E$ is finite over $K$ and $[E : K] \leq n$.

**Proof.** Let $\alpha \in E$ be an element so that the degree $m$ of the irreducible polynomial of $\alpha$ over $K$ is maximal, $m = \deg \text{irrpol}_{K}(\alpha)$. Then we know that $[K(\alpha) : K] = m$. Every finite separable extension is simple by Proposition 4.41 so for every $\beta \in E$, we can write $K(\alpha, \beta) = K(\gamma)$ for some $\gamma \in E$. Thus $\deg \text{irrpol}_{K}(\gamma) \leq m$ and so $[K(\gamma) : K] \leq m$. However we know that $K(\gamma)$ contains $K(\alpha)$ and because $[K(\alpha) : K] = m$ it follows that $K(\gamma) = K(\alpha)$. But $K(\gamma) = K(\alpha, \beta)$ by definition, which implies that every $\beta \in E$ is contained in $K(\alpha)$ meaning $E = K(\alpha)$. Therefore $[E : K] = m \leq n$. \qed

## 5 Galois theory

The material in this section is taken from Chapter 5 of [1], mainly section 1, 2 and 3. We begin this section with splitting fields, after that we move on to normal extensions which is the last piece to be able define Galois extensions, which are dealt with in the third section.

### 5.1 Splitting fields

In this section we cover the definition of splitting fields and some basic properties of those fields. We say that a polynomial splits in a field extension when all of its roots are contained in that extension. Here the section is based of Section 1 of Chapter 5 in [1].

**Definition 5.1.** A polynomial $f \in K[X]$ splits in a field extension $E$ of $K$ when it has a factorization $f(X) = a(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$ in $E[X].$
As usual, in this definition \( a \in K \) is the leading coefficient of \( f \), \( n \) is the degree of \( f \), and \( \alpha_1, \ldots, \alpha_n \in E \) are the (not necessarily distinct) roots of \( f \) in \( E \). In particular, every polynomial \( f \in K[X] \) splits in the algebraic closure \( \overline{K} \) of \( K \).

**Definition 5.2.** Let \( K \) be a field. A splitting field over \( K \) of a polynomial \( f \in K[X] \) is field extension \( E \) of \( K \) such that \( f \) splits in \( E \) and \( E \) is generated over \( K \) by the roots of \( f \). We can also define the splitting field over \( K \) of a set \( S \subseteq K[X] \) of polynomials is a field extension \( E \) of \( K \) such that every \( f \in S \) splits in \( E \) and \( E \) is generated over \( K \) by the roots of \( f \in S \).

It is known that all splitting fields of a set of polynomials are isomorphic to each other. We also know that all finite fields are extensions of \( \mathbb{Z}_p \) and have prime characteristic. Hence a finite field \( F \) has \( p^n \) elements for \( n = [F : \mathbb{Z}_p] \).

**Theorem 5.3.** For every prime \( p \) and every \( n > 0 \), there is, up to isomorphism, exactly one field \( F \) of order \( p^n \). Moreover \( F \) is a splitting field of \( X^{p^n} - X \) over \( \mathbb{Z}_p \) and all its elements are roots of \( X^{p^n} - X \).

**Proof.** Let \( F \) be a field with order \( p^n \). We know that the units of \( F \) form a group \( F^\times = F \setminus \{0\} \) under multiplication. By Proposition 3.69 this group is cyclic. Since \( |F| = p^n \) and \( F^\times \) does not contain 0, it follows that \( |F^\times| = p^n - 1 \). This implies that \( xp^{n-1} = 1 \) for all \( x \in F^\times \). Therefore \( xp^n = x \) for all \( x \in F \).

We draw the conclusion that all elements of \( F \) are roots of the polynomial \( f(X) = X^{p^n} - X \). Moreover this polynomial has at most \( p^n \) roots, and \( F \) has \( p^n \) elements, thus \( F \) consists of all the roots of \( F \). Hence \( F \) is a splitting field of the polynomials \( f(X) = X^{p^n} - X \) over \( \mathbb{Z}_p \) and this field is unique up to isomorphism.

Now for the other way, let \( F \) be a splitting field of \( f(X) = X^{p^n} - X \) over \( \mathbb{Z}_p \), so that the characteristic of \( F \) is \( p \).

We want to show that the roots of \( f \) generates a subfield of \( F \). We know that 0 and 1 are roots of \( f \). If \( \alpha \) and \( \beta \) are roots of \( f \) it can be shown that \( \alpha - \beta \) and \( \alpha \beta^{-1} \) are too. This is because \( (\alpha - \beta)p^n = \alpha p^n - \beta p^n = \alpha - \beta \) by Proposition 3.29 and \( (\alpha \beta^{-1})p^n = \alpha p^n \beta^{-p^n} = \alpha \beta^{-1} \). Since the roots are a subfield and \( F \) is generated by the roots of \( f \) it follows that \( F \) consists of the roots of \( f \). it is easy to see that \( f'(X) = -1 \) and so by Proposition 3.47 it follows that all roots of \( f \) are simple. Therefore \( F \) has \( p^n \) roots in \( F \), and \( F \) has \( p^n \) elements. \( \square \)

### 5.2 Normal extensions

This section contains basic properties of normal extensions, which are splitting fields of a set of polynomials and the last piece we need to be able to define Galois extensions. This section also mentions a special kind of normal extensions which are perfect fields. All information is taken from Section 2, Chapter 5 in [1].

**Proposition 5.4.** For every field extension \( K \subseteq E \), the following statements are equivalent.
(i) $E$ is a splitting field over $K$ of a set of polynomials.

(ii) $K \subseteq E$ is algebraic and $\text{irrpol}_K(\alpha)$ splits over $E$ for all $\alpha \in E$.

This proposition can be used to define normal extensions.

**Definition 5.5.** A normal extension of a field $K$ is an algebraic extension of $K$ that satisfies the equivalent conditions in Proposition 5.4.

We want to state some basic properties of normal extensions.

**Proposition 5.6.** If $F$ is normal over $K$ and $K \subseteq E \subseteq F$, then $F$ is normal over $E$.

**Proposition 5.7.** Every intersection of normal extensions $E \subseteq K$ of $K$ is a normal extension of $K$.

We can use our knowledge of normal extensions to define a new kind of field which is easy to work with.

**Definition 5.8.** If a field $K$ has characteristic 0 or if $K$ has characteristic $p \neq 0$ and also every element in $K$ has a $p$-th root in $K$, then we call $K$ perfect.

**Proposition 5.9.** Finite fields and algebraically closed fields are perfect.

*Proof.* It is immediate that algebraically closed fields are perfect and extremely so. Let $K$ be a finite field. Then $K$ has a nonzero prime characteristic $p \neq 0$. By Proposition 3.29 and our definition of the morphism $\pi : K \to K, x \mapsto x^p$, $\pi$ is injective. Since $K$ is finite it is moreover surjective and so $K$ is perfect.

**Proposition 5.10.** Every algebraic extension of a perfect field is separable.

*Proof.* See 1 Chapter 5, Proposition 2.13.

### 5.3 Galois Extensions

Galois extensions are the most important extensions in Galois theory, not surprisingly. Galois extensions are normal and separable extensions and have many useful properties. This section’s material is taken from mainly from Section 3 and some parts of Section 7 of Chapter 5 in 1.

**Definition 5.11.** A field extension $E$ of $K$ which is a normal and separable extension is a Galois extension of $K$. We say that $E$ is Galois over $K$.

For a field of characteristic 0, it is easy to see which extensions are Galois.

**Example 5.12.** Let $K$ be a field of characteristic 0. Then all extensions are separable and hence all normal extensions of $K$ are Galois extensions of $K$.

**Example 5.13.** A finite field of characteristic $p$ is a Galois extension of $\mathbb{Z}_p$. 

34
We have some basic properties of Galois extensions which can be stated in the following way. These follow from the properties of normal and separable extensions.

**Proposition 5.14.**

(i) If $F$ is Galois over $K$ and $K \subseteq E \subseteq F$, then $F$ is Galois over $E$.

(ii) If $F$ is Galois over $K$ and $E \subseteq F$ is normal over $K$, then $E$ is Galois over $K$.

There are two constructions which are important when dealing with Galois theory. These are called the Galois group and the fixed field.

**Definition 5.15.** The **Galois group** of a Galois extension $K \subseteq E$ is the group of all $K$-automorphisms of $E$. We say that it is the Galois group of $E$ over $K$ and denote it

$$\text{Gal}(E/K) := \{ \sigma \in \text{Aut}(E) : \sigma(x) = x, \forall x \in K \} \leq \text{Aut}(E).$$

**Example 5.16.** The Galois group of the Galois extension $\mathbb{R} \subseteq \mathbb{C} = \mathbb{C}$ has two elements, the identity morphism on $\mathbb{C}$ and complex conjugation.

**Proposition 5.17.** If $E$ is Galois over $K$, then $|\text{Gal}(E/K)| = [E : K]$.

**Proof.** Since $K \subseteq E$ is a Galois extension, then it is normal. This is equivalent to saying that $E \subseteq \overline{K}$ is normal over $K$. Since it is normal every $K$-homomorphism of $E$ into $\overline{K}$, sends $E$ onto $E$. These $K$-homomorphisms are then clearly $K$-automorphisms of $E$ (as a set of ordered pairs). The number of $K$-automorphisms is equal to the separability degree, hence $|\text{Gal}(E/K)| = [E : K]_S$. But $E$ is separable over $K$, since it is Galois over $K$ and so $|\text{Gal}(E/K)| = [E : K] = [E : K]_S = \leq |E : K|$.

**Definition 5.18.** Let $E$ be a field and let $G$ be a group of automorphisms of $E$, $G \subseteq \text{Aut}(E)$. The **fixed field** of $G$ is the subfield formed by all elements of $E$ which are fixed under every $\sigma \in G$. We denote

$$\text{Fix}_E(G) = \{ \alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in G \}.$$

**Example 5.19.** Let $G = \text{Gal}(\mathbb{C}/\mathbb{R})$. Then $\text{Fix}_E(G) = \mathbb{R}$.

**Proposition 5.20.** Let $G$ be a finite group of automorphisms of a field $E$, then $E$ is a finite Galois extension of $F = \text{Fix}_E(G)$ and $\text{Gal}(E/F) = G$.

**Proof.** Let $\alpha \in E$. As given, $G$ is finite, thus $G \alpha$ is a finite set. This implies we can write $G \alpha$ as $G \alpha = \{ \alpha_1, \ldots, \alpha_n \}$, with $n \leq |G|$, and $\alpha_1, \ldots, \alpha_n \in E$ are distinct and we set $\alpha_1 = \alpha$ without loss of generality.

Next, let $f_\alpha \in E[X]$ be the polynomial $f_\alpha(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$. It follows that $f_\alpha(\alpha) = 0$ and also that $f_\alpha$ is separable. Furthermore, every $\sigma \in G$ permutes the roots $\alpha_1, \ldots, \alpha_n$ so $^\sigma f_\alpha = f_\alpha$. Therefore $f_\alpha \in F[X]$. Since $f_\alpha(\alpha) = 0$, $\alpha$ is algebraic over $F$. Moreover $\text{irrpol}_F(\alpha)$ divides $f_\alpha$ and $\alpha$ is separable over $F$. Thus $E$ is algebraic and separable over $F$, and moreover
$E$ is finite over $F$, because $[E : F] \leq |G|$. This follows from Proposition 4.42 because $\deg \text{irrpol}_F(\alpha) \leq \deg f_\alpha \leq |G|$ for every $\alpha \in E$. Now it is clear that $E$ is a splitting field of the polynomials $f_\alpha \in F[X]$, therefore $E$ is normal over $F$. So $E$ is both normal and separable over $F$ and so it is Galois.

Then by Proposition 5.17 $|\text{Gal}(E/K)| = [E : K] \leq |G|$. However every $\sigma \in G$ is an $F$-automorphism of $E$, hence $G \subseteq \text{Gal}(E/F)$. In conclusion, $\text{Gal}(E/F) = G$. 

**Proposition 5.21.** If $E$ is a Galois extension of $K$, then the fixed field of $\text{Gal}(E/K)$ is $K$.

**Proof.** Let $G = \text{Gal}(E/K)$. Then $K \subseteq \text{Fix}_E(G)$.

To show the other inclusion, let $\alpha \in \text{Fix}_E(G)$. Then there exists an algebraic closure $\overline{K} \supseteq E$ by Corollary 4.27. Furthermore Proposition 4.29 tells us that every $K$-homomorphism $\varphi$ of $K(\alpha)$ into $\overline{K}$ extends to a $K$-automorphism of $E$. As $E$ is Galois over $K$, $E$ is normal over $K$ and so $\psi$ has a restriction $\tau$ to $E$. Moreover $\tau$ is a $K$-automorphism of $E$. Hence $\varphi(\alpha) = \tau(\alpha) = \alpha$ and $\varphi$ is the inclusion morphism of $K(\alpha)$ into $\overline{K}$. Since the separability degree is the number of $K$-homomorphism of $E$ into $\overline{K}$, it follows that $[K(\alpha) : K]_s = 1$. Then since $K(\alpha) \subseteq E$ is separable over $K$, $[E : K]_s = [E : K]$ which implies that $K(\alpha) = K$. 

These two propositions are the foundation to one of the most important theorems in Galois Theory.

**Theorem 5.22** (Fundamental Theorem of Galois Theory). Let $E$ be a finite Galois extension of a field $K$.

(i) If $F$ is a subfield of $E$ that contains $K$, then $E$ is a finite Galois extension of $F$ and $F$ is the fixed field of $\text{Gal}(E/F)$.

(ii) If $H$ is a subgroup of $\text{Gal}(E/K)$, then $F = \text{Fix}_E(H)$ is a subfield of $E$ that contains $K$, and $\text{Gal}(E/K)$.

This defines a one-to-one correspondence between intermediate fields $K \subseteq F \subseteq E$ and subgroups of $\text{Gal}(E/K)$.

To simplify this theorem we have the following diagram:

$$K \subseteq F \subseteq E \iff \text{Gal}(E/F) \subseteq \text{Gal}(E/K)$$

$$K \subseteq \text{Fix}_E(H) \subseteq E \iff H \subseteq \text{Aut}(E/K)$$

We need to define some special Galois extensions, called cyclic extensions, because we need their special properties when proving other propositions later on.

**Definition 5.23.** A cyclic extension is a finite Galois extension whose Galois group is cyclic.
Proposition 5.24. Let $n > 0$ and let $K$ be a field whose characteristic is either 0 or not a divisor of $n$, and that contains a primitive $n$-th root of unity. If $E$ is a cyclic extension of $K$ of degree $n$, then $E = K(\alpha)$, where $\alpha^n \in K$. If $E = K(\alpha)$, where $\alpha^n \in K$, then $E$ is a cyclic extension of $K$. Moreover $m = [E : K]$ divides $n$ and $\alpha^m \in K$.

Proof. See [1, Chapter 5, Proposition 7.8].

Proposition 5.25. Let $K$ be a field with characteristic $p \neq 0$. If $E$ is a cyclic extension of $K$ of degree $p$, then $E = K(\alpha)$, where $\alpha^p - \alpha \in K$. If $E = K(\alpha)$, where $\alpha^p - \alpha \in K$, $\alpha \notin K$. Then $E$ is a cyclic extension of $K$ of degree $p$.

Proof. See [1, Chapter 5, Proposition 7.10].

6 Real closed fields

The last section before we prove Artin-Schreier’s theorem is about real closed fields. This section’s material is taken from Section 1 and 2 of Chapter 6 in [1].

First we need to know what an ordered field is, then we define what a formally real field is and last we define real closed fields.

Definition 6.1. An ordered field is a field $F$ together with a total order relation $\leq$ on $F$ such that for all $x, y, z \in F$

(i) $x \leq y$ implies $x + z \leq y + z$;

(ii) if $z \geq 0$ then $x \leq y$ implies $xz \leq yz$.

As expected $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields and all usual properties from $\mathbb{Q}$ and $\mathbb{R}$ hold for all ordered fields as well. The question remains about which fields are not ordered. If in an ordered field we have $-1 \geq 0$, then multiplying with $-1$ gives us $1 \geq 0$, by part (ii). We then add $-1$ to both sides as in part (i) and we get $0 \leq -1$, which is a contradiction. It follows that $1 > 0$ and then $1 + 1 > 1 > 0$ and so on. Hence an ordered field has characteristic 0.

Moreover in an ordered field we have $x^2 \geq 0$. This follows from the fact that $x \geq 0$ or $-x \geq 0$. Then multiplying by $x$ on both sides yields $x^2 \geq 0$ or $x^2 \geq 0$. From this we see that $\mathbb{C}$ is not ordered because $-1 = i^2 \geq 0$ which cannot happen in an ordered field.

Proposition 6.2. A field $F$ can be ordered if and only if $-1$ is not a sum of squares of elements of $F$.

Proof. See [1, Chapter 6, Proposition 1.1].

Definition 6.3. Let $F$ be a field. If there exists a total order relation on $F$ which makes $F$ an ordered field, then $F$ is called formally real.

Since formally real fields are ordered field we see that by Proposition 6.2 a field is formally real if and only if it $-1$ is not a sum of squares in $F$. Moreover all subfields of formally real fields are formally real.
Proposition 6.4. If \( F \) is a formally real field and \( \alpha^2 \in F \) with \( \alpha^2 > 0 \), then \( F(\alpha) \) is formally real.

Proof. Assume \( \alpha \notin F \), otherwise we are already done. Then we can write every element of \( F(\alpha) \) as \( x + \alpha y \) for some unique \( x, y \in F \). Moreover if \( \alpha^2 > 0 \) in \( F \), then \( F(\alpha) \) is formally real. This follows from the fact that if we have:

\[
-1 = \sum (x_i + \alpha y_i)^2 = \sum (x_i^2 + \alpha^2 y_i^2) + \alpha \sum (2x_i y_i),
\]

for some \( x_i, y_i \in F \), this would imply that \( -1 = \sum (x_i^2 + \alpha^2 y_i^2) \geq 0 \), which is a contradiction.

Definition 6.5. A field \( R \) is real closed when it is formally real and there is no formally real algebraic extension \( E \supseteq R \).

Example 6.6. An example of a real closed field is \( \mathbb{R} \). The only algebraic extension \( E \supseteq \mathbb{R} \) of \( \mathbb{R} \) is \( \mathbb{C} \) and as stated before \( \mathbb{C} \) is not formally real.

Theorem 6.7. A formally real field \( R \) is real closed if and only if

(i) every positive element of \( R \) is a square in \( R \), and

(ii) every polynomial of odd degree in \( R[X] \) has a root in \( R \) and then \( \overline{R} = R(i) \), where \( i^2 = -1 \).

Proof. See [1, Chapter 6, Theorem 2.3].

Corollary 6.8. If \( R \) is real closed, then \( f \in R[X] \) is irreducible if and only if either \( f \) has degree 1, or \( f \) has degree 2 and no root in \( R \).

This Corollary is very similar to Proposition 3.59, in fact the proof for that proposition generalizes to this case.

7 The Artin-Schreier Theorem

In this section we will state and prove Artin-Schreier’s theorem. This theorem is a characterization of real closed fields. Here we are using theory from all the previous sections, especially Section 5 about Galois Theory. The theorem and its proof is taken from Theorem 2.8 in Section 2, Chapter 6 of [1].

Theorem 7.1 (Artin-Schreier’s Theorem). For a field \( K \neq \overline{K} \) the following properties are equivalent:

(1) \( K \) is real closed;

(2) \( [\overline{K} : K] < \infty \);

(3) There is an upper bound for the degrees of irreducible polynomials in \( K[X] \).

Proof. To be able to prove this theorem, we are going to need three lemmas.
**Lemma 7.2.** If the degrees of irreducible polynomials have an upper bound in $K[X]$, then $K$ is perfect.

**Proof.** Recall that a field $K$ is perfect if it either has characteristic $0$ or if it has characteristic $p 
eq 0$ and also there exists a $p$-th root for every element in $K$.

For the first case, if $\text{char}(K) = 0$, then by the definition of a perfect field, $K$ is perfect, so the lemma holds.

Now assume that $K$ has characteristic $p 
eq 0$ and that $a \in K$ is not a $p$-th power in $K$. We want to prove that $f(X) = X^p - a$, where $f(X) \in K[X]$, is irreducible for all $k > 0$. Since $f(X) \in K[X]$, $f$ is a product of monic irreducible polynomials $q_1q_2 \cdots q_r$, i.e. $f = q_1q_2 \cdots q_r$. Next, let $\alpha \in \overline{K}$ be a root of $f$, meaning $f(\alpha) = 0$. This implies that $\alpha^p = a$ and so we can write $f(X) = X^p - \alpha^p = (X - \alpha)^p$. The last equality follows from Proposition 3.29.

Thus each $q_i$ is a power of $X - \alpha$, i.e. $q_i(X) = (X - \alpha)^{t_i}$ for some $t_i > 0$. If $t = \min(t_1, \ldots, t_k)$, then $q = (X - \alpha)^t$ is irreducible and divides each of the polynomials $q_1, \ldots, q_r$. It follows that $q_1 = \cdots = q_r = q$ and we have $f = q^r$. Since $q = (X - \alpha)^t$, we see that $f = (X - \alpha)^p = (X - \alpha)^{rt}$ so $p^r = rt$ so $r$ is a power of $p$. Moreover, $f = X^p - a = X^{rt} - \alpha^{rt}$ which implies $\alpha^{rt} = a$. But since $\alpha^t \in K$ and $a = (\alpha^t)^r$ is not a $p$-th power in $K$, $r$ is not a multiple of $p$. Hence $r = 1$ and $f = q$ is irreducible. \hfill \Box

**Lemma 7.3.** Let $F$ be a field in which $-1$ is a square. Then $\overline{F}$ is not a Galois extension of $F$ of prime degree.

**Proof.** We want to show that a Galois extension $E \subseteq \overline{F}$ of $F$ of prime degree $p$ cannot be algebraically closed. By Proposition 3.17 $|\text{Gal}(E/F)| = [E : F]$ so $\text{Gal}(E/F)$ has order $p$, then it is cyclic. Since a cyclic extension is a finite Galois extension whose Galois group is cyclic, then certainly this extension is cyclic.

We treat the cases $\text{char}(F) = p$ and $\text{char}(F) \neq p$ separately, in each case showing that there is a polynomial in $E[X]$ without roots in $E$.

We know by Proposition 5.25 that if $F$ has characteristic $p$, then $E = F(\alpha)$, and $\alpha^p - \alpha \in F$. We set $c = \alpha^p - \alpha$ and then $\text{irrpol}_F(\alpha) = X^p - X - c$. Note the fact that $1, \alpha, \ldots, \alpha^{p-1}$ is a basis of $E$ over $F$.

Next, let $\beta = b_0 + b_1\alpha + \cdots + b_{p-1}\alpha^{p-1} \in E$, with coefficients $b_0, \ldots, b_{p-1} \in F$. Then

$$\beta^p = b_0^p + b_1^p\alpha^p + \cdots + b_{p-1}^p\alpha^{(p-1)p} = b_0^p + b_1^p(\alpha + c) + \cdots + b_{p-1}^p(\alpha + c)^{p-1},$$

since $\alpha^p = \alpha + c$ by the definition of $c$.

Now we can write

$$\beta^p - \beta = (b_0^p + b_1^p(\alpha + c) + \cdots + b_{p-1}^p(\alpha + c)^{p-1}) - (b_0 + b_1\alpha + \cdots + b_{p-1}\alpha^{p-1}).$$

39
We simplify this and get

$$\beta^p - \beta - c_\alpha^{p-1} = a_0 + a_1\alpha + \cdots + a_{p-1}\alpha^{p-1},$$

where $a_{p-1} = b_{p-1}^p - b_{p-1} - c$. If $\beta^p - \beta - c_\alpha^{p-1} = 0$, then $a_{p-1} = 0$ and then $X^p - X - c$ has a root $b_{p-1}$. But $X^p - X - c$ is irreducible in $F$, thus $\beta^p - \beta - c_\alpha^{p-1} \neq 0$. Since $\beta$ was arbitrary, $X^p - X - c_\alpha^{p-1}\in E[X]$ has no root in $E$. Therefore $F$ cannot have characteristic $p$.

Next, assume that $F$ does not have characteristic $p$. To be algebraically closed, $E$ has to contain a primitive $p$-th root of unity $\varepsilon$. Then $\varepsilon$ is a root of $(X^p - 1)/(X - 1) \in F[X]$ and $[F(\varepsilon) : F] < p$. Since $[F(\varepsilon) : F]$ divides $[F : E] = p$ we have $[F(\varepsilon) : F] = 1$ and so $F(\varepsilon) = F$ and therefore $\varepsilon \in E$. Since $E$ is a cyclic extension, it follows by Proposition 5.24 that $E = F(\alpha)$, with $\alpha^p \in F$ and $\alpha \notin F$.

Assume that $\alpha$ has a $p$-th root $\beta$ in $E$, $\beta^p = \alpha$. Then $\beta^p = \alpha^p$ but we already know that $\alpha^p \in F$. Thus $\beta^p \in F$. Moreover let $\sigma \in \text{Gal}(E/F)$. Then

$$\sigma(\beta^p) = \beta^p.$$

Let $\xi \in E$ be such that $\sigma(\beta) = \xi\beta$. Then

$$\beta^p = \sigma(\beta^p) = \sigma(\beta)^p = (\xi\beta)^p = \xi^p\beta^p.$$

Hence $\xi$ satisfies $\xi^p = 1$ and so $\xi^p$ is a $p$-th root of unity, hence $\xi^p \in F$. Since $\xi^p \in F$, then

$$\sigma(\xi^p) = \xi^p.$$

Now let $\eta \in E$ be such that $\sigma(\xi) = \eta\xi$. Then

$$\xi^p = \sigma(\xi^p) = \sigma(\xi)^p = (\eta\xi)^p = \eta^p\xi^p.$$

This satisfies $\eta^p = 1$ so $\eta$ is a $p$-th root of unity hence $\eta \in F$. By our definition of $\xi$ we have $\sigma(\beta) = \xi\beta$. Applying $\sigma$ again we get

$$\sigma^2(\beta) = \sigma(\xi)\sigma(\beta).$$

Again by definition of $\xi$ and also by definition of $\eta$ we can simplify this to

$$\sigma^2(\beta) = (\eta\xi)(\xi\beta) = \eta\xi^2\beta.$$

Applying $\sigma$ once again we arrive at

$$\sigma^3(\beta) = \sigma(\eta\xi^2\beta) = \sigma(\eta)\sigma(\xi^2)\sigma(\beta).$$

We have $\sigma(\xi^k) = \eta^k\xi^k$ and since $\eta \in F$, we have $\sigma(\eta) = \eta$. Thus

$$\sigma^3(\beta) = (\eta)(\eta^2\xi^2)(\xi\beta) = \eta^3\xi^3\beta.$$

Continuing,

$$\sigma^4(\beta) = \sigma(\eta^3\xi^3\beta) = \sigma(\eta^3)\sigma(\xi^3)\sigma(\beta) = (\eta^3)(\eta^5\xi^3)(\xi\beta) = \eta^6\xi^4\beta.$$
Then using induction we conclude that
\[ \sigma^k(\beta) = \eta^{k(k-1)/2} \xi^k \beta, \]
for all \( k \geq 0 \).

Since \( \sigma^p = 1 \), we can write \( \beta = \sigma^p(\beta) = \eta^{p(p-1)/2} \xi^p \beta \) and thus
\[ \eta^{p(p-1)/2} \xi^p = 1. \]

Now we have two cases, either \( p = 2 \) or \( p \) is odd. If \( p \) is odd, then it divides \( p(p-1)/2 \) and so \( \eta^{p(p-1)/2} = 1 \), since \( \eta^p = 1 \). Then \( \xi^p = 1 \).

If \( p = 2 \) then \( \xi^4 = 1 \) and \( \xi^2 = \pm 1 \). First case, if \( \xi^2 = 1 \), then \( \eta^{p(p-1)/2} = 1 \). If \( \xi^2 = -1 \) then \( \xi \in F \), since \( F \) contains a square root of \(-1\) and then since \( p(p-1)/2 = 1 \) when \( p = 2 \) we can write
\[ \eta^{p(p-1)/2} = \eta = (\sigma(\xi))/\xi = 1. \]

But this is a contradiction since we get \(-1 = 1\) but \( p = 2 \) is not the characteristic of \( F \). Hence this is an empty case and so it follows that \( \xi^p = 1 \). Now we can write
\[ \sigma(\alpha) = \sigma(\beta^p) = \sigma(\beta^p) = (\xi \beta)^p = \xi^p \beta^p = \beta^p = \alpha. \]

However \( E = F(\alpha) \), so \( \sigma(\alpha) \neq \alpha \) for some \( \sigma \in \text{Gal}(E/F) \). In conclusion, \( X^p - \alpha \in E[X] \) has no root in \( E \). \( \square \)

**Lemma 7.4.** If \([\overline{K} : K] = n \) is finite, then every irreducible polynomial in \( K[X] \) has degree at most \( n \), \( K \) is perfect and \( \overline{K} = K(i) \), where \( i^2 = -1 \).

**Proof.** By definition, every irreducible polynomial \( q \in K[X] \) has a root \( \alpha \in \overline{K} \). We set \( q = \text{irrpol}_K(\alpha) \) with degree \([K(\alpha) : K] \leq n \). Since we have an upper bound for the degree of irreducible polynomials, \( K \) is perfect by Lemma 7.2. The extension \( K \subset \overline{K} \) is finite, hence it is algebraic. Moreover it is normal since \( \overline{K} \) is the splitting field of all polynomials and since \( K \) is perfect and \( K \subset \overline{K} \) is algebraic it is separable by Proposition 5.10. Thus \( \overline{K} \) is Galois over \( K \).

Now let \( i \in \overline{K} \) be a root of the polynomial \( X^2 + 1 \in K[X] \). Assume \( K(i) \subset \overline{K} \). Since \( \overline{K} \) is Galois over \( K \) it follows by Proposition 5.14 that \( \overline{K} \) is Galois over \( K(i) \). Then \( \text{Gal}(\overline{K}/K(i)) \) has a subgroup \( H \) of prime order. Moreover, \( \overline{K} \) is Galois over the fixed field \( F \) of \( H \), which has prime degree \([\overline{K} : F] = |H| \). This is a contradiction to Lemma 7.3 hence \( K(i) = \overline{K} \). \( \square \)

Now we have proved the three lemmas and we are ready to prove Artin-Schreier’s theorem. By Theorem 6.7, it follows immediately that (1) implies (2) and by Lemma 7.4 it follows that (2) implies (3).

Using Lemma 7.2 it is easy to prove that (3) implies (2). Assume that there exists an upper bound for the degrees of the irreducible polynomials in \( K[X] \) i.e. every irreducible has degree at most \( n \), then by the lemma \( K \) is perfect. By Proposition 5.10 \( \overline{K} \) is separable over \( K \). Furthermore, every element of \( \overline{K} \) has degree at most \( n \) over \( K \). Hence \([\overline{K} : K] \leq n \), using Proposition 4.42.
Finally, we shall prove that (2) implies (1). Assume that \([K : K]\) is finite. Then \(K\) is perfect and \(\overline{K} = K(i)\), \(i^2 = -1\), by Lemma 7.4. But since \(K \neq \overline{K}\), we know that \(i \notin K\). An element in \(\overline{K}\) can be written \(z = x + iy \in \overline{K}\) and every element has two conjugates, \(z\) and \(\overline{z} = x - iy\). Moreover, \(z\overline{z} = x^2 + y^2 \in K\). For every \(x, y \in K\) we have \(x + iy = u^2\) for some \(u \in \overline{K}\). Thus \(x^2 + y^2 = u^2u^2 = (u\overline{u})^2\) is a square in \(K\). Hence every sum of squares is a square in \(K\), but \(-1\) is not a square in \(K\), since \(i \notin K\). Hence \(K\) is formally real and furthermore \(K\) is real closed since the only algebraic extension \(K \subseteq E = \overline{K}\) of \(K\) is not formally real. \(\square\)

References