Groups, Rings and Fields

Karl-Heinz Fieseler

Uppsala 2010

Preface

These notes give an introduction to the basic notions of abstract algebra, groups, rings (so far as they are necessary for the construction of field extensions) and Galois theory. Each section is followed by a series of problems, partly to check understanding (marked with the letter "R": *R*ecommended problem), partly to present further examples or to extend theory.

For useful hints and remarks I am indebted to my colleague Ernst Dieterich.

Uppsala, September 2010 Karl-Heinz Fieseler

Contents

1 Introduction 4

2 Groups 12
- 2.1 Definitions and Examples . . . 12
- 2.2 Homomorphisms . . . 17
- 2.3 Subgroups . . . 24
  - 2.3.1 Digression: Quaternions . . . 32
- 2.4 Order and Cyclic Groups . . . 37
- 2.5 Factor Groups . . . 39
  - 2.5.1 Digression: Free Groups . . . 44
- 2.6 Simple Groups and Composition Series . . . 52
- 2.7 Abelian Groups . . . 56
  - 2.7.1 Digression: Free Abelian Groups . . . 62
- 2.8 Sylow Subgroups . . . 63

3 Rings 70
- 3.1 Definitions and Examples . . . 70
- 3.2 Homomorphisms . . . 79
- 3.3 Ideals and Factor Rings . . . 82
  - 3.3.1 Digression: p-adic number fields . . . 90
- 3.4 Irreducibility Criteria . . . 95

4 Field Extensions and Galois Theory 100
- 4.1 Basic Definitions . . . 100
- 4.2 Automorphism Groups . . . 106
- 4.3 Formal Derivatives and Multiplicities . . . 112
- 4.4 Splitting Fields . . . 116
- 4.5 Finite Fields . . . 124
  - 4.5.1 Digression 1: Quadratic reciprocity . . . 126
  - 4.5.2 Digression 2: Further Simple Groups . . . 130
- 4.6 Galois Theory . . . 136
- 4.7 The Fundamental Theorem of Algebra . . . 142
- 4.8 Cyclotomic Extensions . . . 143
- 4.9 Solvability by Radicals . . . 147

5 Annex: Zorns Lemma 150

1 Introduction

Assume we want to solve an equation

$$0 = f(x) := x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0,$$

where the coefficients $a_{n-1}, ..., a_1, a_0 \in \mathbb{Q}$ of the polynomial $f(x)$ are rational numbers. The fundamental theorem of algebra[1] tells us that for any $n > 0$ and arbitrary complex coefficients $a_{n-1}, ..., a_0 \in \mathbb{C}$ there is a complex solution $x = \lambda \in \mathbb{C}$, and an iterated application of that fact then leads to a factorization

$$f(x) = (x - \lambda_1) \cdot ... \cdot (x - \lambda_n)$$

of the polynomial $f(x)$ with (not necessarily pairwise different) complex numbers $\lambda_1, ..., \lambda_n \in \mathbb{C}$. In particular $f(x) = 0$ if and only if $x = \lambda_j$ for some $j \in \{1, ..., n\}$.

But is it possible to describe these solutions explicitly? For $n = 2$ we have the solutions $x = \lambda_{1,2} \in \mathbb{C}$ given by the well known formula

$$\lambda_{1,2} = -\frac{a_1}{2} \pm \sqrt{\frac{a_1^2}{4} - a_0}\ ,$$

and for $n = 3, 4$ there are similar, but more complicated formulae due to Gerolamo Cardano (1501-1576) involving the four arithmetic operations $+, -, \cdot, :$ as well as taking square and cubic roots.

On the other hand for $n \geq 5$ there was no further progress during the next 300 years.. So one started to suspect:

Theorem 1.1. *For $n \geq 5$ there is no formula giving the solutions $\lambda_1, ..., \lambda_n \in \mathbb{C}$ of the equation*

$$0 = f(x) := x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0,$$

as a function of the coefficients $a_{n-1}, ..., a_0$ using only the four arithmetic operations $+, -, \cdot, :$ as well as taking r-th roots $z \mapsto \sqrt[r]{z}$ (with arbitrary $r \in \mathbb{N}$).

[1] There are several proofs of that result, all of them use completeness arguments. We shall present in section 4.7 an algebraic version, where the only result from analysis needed is the fact that a real polynomial of odd degree has a real zero.

Having thus no hope anymore in the general case we are led to the following

Question: Which polynomial equations $f(x) = 0$ are *solvable by radicals*, i.e. when can we obtain the solutions $\lambda_1, ..., \lambda_n \in \mathbb{C}$ of the equation

$$f(x) = 0$$

starting with rational numbers and using only the four arithmetic operations $+, -, \cdot, :$ as well as taking r-th roots $z \mapsto \sqrt[r]{z}$ (with arbitrary $r \in \mathbb{N}$)?

So here we do not require that we take the coefficients $a_0, ..., a_{n-1} \in \mathbb{Q}$ as starting point and perform the operations independently from the polynomial $f(x)$.

Example 1.2. For the polynomial $f(x) = x^n + a_0$ it is obviously possible: The numbers

$$\sqrt[n]{-a_0}$$

are the solutions of the equation $f(x) = 0$. On the other hand the solutions of the equation

$$x^5 - 4x + 2 = 0$$

do not admit such a representation as we shall see later on.

Strategy: First of all it can happen that some solutions λ_i can be obtained from rational numbers using only the four arithmetic operations $+, -, \cdot, :$ as well as taking roots and others can not, e.g. if

$$f(x) = (x^n + a_0)(x^5 - 4x + 2).$$

So we can expect a reasonable answer depending only on $f(x)$ only if we assume the polynomial $f(x)$ to be irreducible, i.e. there should be no factorization

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

of $f(x)$ as a product of nonconstant polynomials $g(x)$ and $h(x)$ with rational coefficients.

Example 1.3. The polynomial

$$f(x) = x^2 - 1 = (x-1)(x+1)$$

is not irreducible (or rather reducible), while

$$f(x) = x^2 + 1$$

is: Otherwise it would be the product of two linear polynomials each of which would give rise to a rational zero of $f(x)$.

The zeros $\lambda_1, ..., \lambda_n \in \mathbb{C}$ of an irreducible polynomial are pairwise different, and so the set

$$N(f) := \{x \in \mathbb{C}; f(x) = 0\} = \{\lambda_1, ..., \lambda_n\}$$

of all complex zeros of our polynomial $f(x)$ satisfies

$$|N(f)| = n.$$

Denote

$$\mathbb{S}(N(f)) := \{\pi : N(f) \longrightarrow N(f) \text{ bijective}\}.$$

the set of its permutations.

The **Galois group of the polynomial** $f(x)$ is a subset

$$\mathrm{Gal}(f) \subset \mathbb{S}(N(f))$$

closed with respect to the composition and inversion of maps, hence it forms a group in the sense of Def.2.1. And from the properties of $\mathrm{Gal}(f)$ as a group we can read off whether the equation $f(x) = 0$ is solvable by radicals or not.

In order to describe which permutations of $N(f)$ belong to the Galois group $\mathrm{Gal}(f)$ we first determine the **splitting field**

$$E = E(f) \subset \mathbb{C}$$

of the polynomial $f(x)$, a subset of the complex plane containing $N(f)$. This splitting field $E \subset \mathbb{C}$ admits natural symmetries, i.e. distinguished permutations

$$\sigma : E \longrightarrow E$$

called **automorphisms**. Each automorphism preserves $N(f) \subset E$, so we obtain a diagram

$$\begin{array}{ccccc} \sigma & : & E & \longrightarrow & E \\ & & \cup & & \cup \\ \sigma|_{N(f)} & : & N(f) & \longrightarrow & N(f) \end{array},$$

and an automorphism is uniquely determined by its restriction $\sigma|_{N(f)}$. The elements of the Galois group then are the restrictions of such automorphisms. Thus, if we denote

$$\mathrm{Aut}(E) \subset \mathbb{S}(E)$$

the set of all automorphisms we can simply write

$$\mathrm{Gal}(f) = \mathrm{Aut}(E)|_{N(f)}$$

using the suggestive notation

$$\mathrm{Aut}(E)|_{N(f)} := \{\sigma|_{N(f)}, \sigma \in \mathrm{Aut}(E)\}.$$

So finally what is a splitting field? And an automorphism?

First of all we give a restricted definition of a field, indeed an embedded version of the abstract notion of a field:

Definition 1.4. A field (kropp) is any subset $E \subset \mathbb{C}$ of the set of complex numbers containing the numbers $0, 1$ and being closed with respect to the four arithmetic operations.

Remark 1.5.

1. A subset $E \subset \mathbb{C}$ is a field iff $0, \pm 1 \in E$ and E is closed with respect to addition, multiplication and inversion of nonzero numbers.
2. Any field $E \subset \mathbb{C}$ contains $\mathbb{Q}$.
3. An arbitrary intersection of fields is again a field.

Example 1.6.

1. The subsets $E = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.
2. The subset
$$E = \mathbb{Q} + \mathbb{Q}i := \{a + bi; a, b \in \mathbb{Q}\}$$
is a field.

3. The subset
$$E = \mathbb{Q} + \mathbb{Q}\sqrt{d} := \{a + b\sqrt{d}; a, b \in \mathbb{Q}\}$$
is a field, where $d \in \mathbb{Q}_{>0}$ is not a square..

Definition 1.7. The splitting field $E = E(f) \subset \mathbb{C}$ of the polynomial
$$f(x) = (x - \lambda_1) \cdot ... \cdot (x - \lambda_n)$$
is defined as the intersection
$$E := \bigcap_{N(f) \subset F \text{ field}} F$$
of all fields $F \supset N(f)$. With other words $E = E(f)$ is the smallest field containing $N(f)$.

Remark 1.8. Here is an explicit description of the splitting field of $f(x) = (x - \lambda_1) \cdot ... \cdot (x - \lambda_n)$, namely
$$E = \left\{ \sum_{\nu_1,...,\nu_n \in \mathbb{N}} q_{\nu_1,...,\nu_n} \lambda_1^{\nu_1} \cdot ... \cdot \lambda_n^{\nu_n}; \forall \nu_1, ..., \nu_n \in \mathbb{N} : q_{\nu_1,...,\nu_n} \in \mathbb{Q} \right\}.$$
Obviously the right hand side contains $0, \pm 1$ and is closed with respect to addition and multiplication. Only the fact that with a nonzero element its reciprocal is again a sum of the given type is nontrivial: This follows from the fact that each λ_i is an "algebraic number", i.e. a zero of some polynomial $g_i(x)$ with rational coefficients (namely $g_i(x) = f(x)$).

Example 1.9. 1. The splitting field of $f(x) = x^2 + 1$ is $E = \mathbb{Q} + \mathbb{Q}i$.

2. The splitting field of $f(x) = x^2 - d$ is $E = \mathbb{Q} + \mathbb{Q}\sqrt{d}$.

The symmetries of the splitting field E are called automorphisms:

Definition 1.10. An automorphism of the field $E \subset \mathbb{C}$ is a bijective map
$$\sigma : E \longrightarrow E$$
compatible with the four arithmetic operations, i.e.
$$\sigma(x \pm y) = \sigma(x) \pm \sigma(y),\ \sigma(xy) = \sigma(x)\sigma(y),\ \sigma\left(\frac{x}{y}\right) = \frac{\sigma(x)}{\sigma(y)}.$$

We denote

$$\mathrm{Aut}(E) := \{\sigma : E \longrightarrow E \text{ automorphism } \}$$

the set of all automorphisms of the field E.

Remark 1.11. For an automorphism $\sigma \in \mathrm{Aut}(E)$ we have $\sigma(0) = 0$ and $\sigma(1) = 1$, since for example $\sigma(a) = \sigma(a+0) = \sigma(a)+\sigma(0)$. As a consequence $\sigma(n) = n$ for $n \in \mathbb{N}$ and finally

$$\sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}.$$

In particular

$$\sigma(f(\lambda)) = f(\sigma(\lambda))$$

for any polynomial $f(x)$ with rational coefficients and $\lambda \in E$.

Example 1.12. 1. For $E = \mathbb{Q} + \mathbb{Q}i$ we have

$$\mathrm{Aut}(E) = \{\mathrm{id}_E, \tau\},$$

where $\tau(z) = \overline{z}$ is complex conjugation. Indeed, if $\sigma \in \mathrm{Aut}(E)$, we have

$$\sigma(a + bi) = \sigma(a) + \sigma(b)\sigma(i) = a + b\sigma(i),$$

while $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$ implies $\sigma(i) = \pm i$. Hence $\sigma = \mathrm{id}_E$ or $\sigma = \tau$.

2. For $E = E(f)$ the equality $\sigma(f(\lambda)) = f(\sigma(\lambda))$ together with $\sigma(0) = 0$ implies that $\sigma(N(f)) = N(f)$, and the explicit description of the splitting field $E(f)$ in Rem.1.8 gives that σ can be reconstructed from its restriction $\sigma|_{N(f)}$. From the point of view of abstract group theory we need thus not distinguish between the Galois group

$$\mathrm{Gal}(f) = \mathrm{Aut}(E)|_{N(f)} \subset \mathbb{S}(N(f))$$

of the polynomial $f(x)$ and the automorphism group

$$\mathrm{Aut}(E) \subset \mathbb{S}(E)$$

of its splitting field $E = E(f)$.

In the general approach one considers not only polynomials $f(x)$ with rational coefficients. Instead they are taken from a fixed base field K, where now in contrast to the restricted definition Def.1.4 we mean an abstract, not an embedded field, i.e. a set K with two distinguished elements $0, 1$ and four arithmetic operations satisfying the "usual rules". Then given a polynomial one has first to construct the splitting field $E = E(f) \supset K$, since in general there is a priori no field at hand taking the rôle of the complex numbers in the case $K = \mathbb{Q}$. For that construction one has to study the basics of commutative ring theory. Finally the automorphism group $\mathrm{Aut}(E)$ is replaced with

$$\mathrm{Aut}_K(E) := \{\sigma : E \longrightarrow E \text{ automorphism}, \sigma|_K = \mathrm{id}_K\}\,.$$

Here is a short survey of the material presented in these notes:

1. **Chapter I: Groups**. Here we discuss the basic notions of group theory: Groups play an important rôle nearly in every part of mathematics and can be used to study the symmetries of a mathematical object.

2. **Chapter II: Rings**. Commutative rings R are sets with three arithmetic operations: Addition, subtraction and multiplication $\pm, \cdot$ as for example the set $\mathbb{Z}$ of all integers, while division in general is not always possible. We need rings, that are not fields, mainly in order to construct extensions of a given field K, but they play also an important rôle in algebraic number theory (Number theory deals with the ring $\mathbb{Z} \subset \mathbb{Q}$ of integers, but for a deeper understanding of $\mathbb{Z}$ one has to extend the notion of an integer and to study rings of algebraic integers $R \subset E$, where $E \subset \mathbb{C}$ is the splitting field of some polynomial with rational coefficients) and in algebraic geometry, where one investigates the set of solutions of polynomial equations in several variables.

3. **Chapter III: Field Extensions and Galois Theory**. The main result relates subgroups of $\mathrm{Aut}_K(E)$ for the splitting field $E \supset K$ of some polynomial with coefficients in K to intermediate fields of the extension $E \supset K$. As an easy application we prove the fundamental theorem of algebra and discuss cyclotomic fields, i.e. the splitting fields over $\mathbb{Q}$ of the polynomials $f(x) = x^n - 1$, before we eventually attack our

original problem, whether the zeros of an irreducible equation $f(x) = 0$ can be obtained from elements in the base field K with our five operations.

4. **Appendix**: **Zorns lemma**. Here we prove Zorns lemma. That lemma is usually needed if one wants to show the existence of certain objects in case one deals with infinite sets, e.g. the existence of bases of infinite dimensional vector spaces. An other example is this: There are no explicit automorphisms $\sigma \in \mathrm{Aut}(\mathbb{C})$ except the identity and complex conjugation, but with Zorns lemma we see that any automorphism of a splitting field $E \subset \mathbb{C}$ of a polynomial $f(x)$ with rational coefficients can be extended to an automorphism of $\mathbb{C}$.

2 Groups

2.1 Definitions and Examples

Definition 2.1. *A group is a pair (G, μ) with a non-empty set G and a "binary operation", i.e., a map*

$$\mu : G \times G \longrightarrow G, (a, b) \mapsto ab := \mu(a, b),$$

called the "group multiplication" or "group law", satisfying the following conditions

G_1: *Group multiplication is "associative", i.e. for all $a, b, c \in G$ we have*

$$(ab)c = a(bc) \quad .$$

G_2: *Existence of a "neutral element": There is an element $e \in G$ such that*

$$ea = a = ae$$

for all elements $a \in G$.

G_3: *Existence of "inverse elements": For all $a \in G$ there is an element $a^{-1} \in G$, such that*

$$aa^{-1} = e = a^{-1}a \quad .$$

Notation: Often one writes G instead of (G, μ). And the number $|G|$ is called the **order** of the group G. Here we denote $|M| \in \mathbb{N} \cup \{\infty\}$ the number of elements in the set M. We define powers a^n for $a \in G$ and $n \in \mathbb{N}$ inductively by

$$a^0 := e, a^{n+1} := a^n a,$$

and the associative law yields

$$a^{n+m} = a^n a^m \ .$$

Remark 2.2. 1. There is only one neutral element in a group G: If $\tilde{e} \in G$ is a further neutral element, we obtain $\tilde{e} = \tilde{e}e = e$.

2. There is only one inverse element a^{-1} for a given element $a \in G$: If $\tilde{a}$ is a further inverse element, we have

$$\tilde{a} = \tilde{a}e = \tilde{a}(aa^{-1}) = (\tilde{a}a)a^{-1} = ea^{-1} = a^{-1} \quad .$$

In particular we can also define negative powers

$$a^{-n} := (a^{-1})^n \ .$$

3. In many books for a group only the existence of a left neutral element e, i.e. such that $ea = a$ holds for all $a \in G$, and left inverse elements a^{-1} (with $e = a^{-1}a$) is required. So the group axioms are a priori weaker, but it turns out that they are equivalent to ours, though group multiplication need not be "commutative":

Definition 2.3. *A group is called* **commutative** *or* **abelian** (Niels Henrik Abel, 1802-1829) *iff* $ab = ba$ *holds for all* $a, b \in G$.

Notation: If a group G is commutative, one often writes the group law in additive notation:

$$a + b := \mu(a, b) \ ,$$

the symbol 0 denotes the neutral element, and $-a$ the inverse element of $a \in G$, while for $n \geq 0$ powers look as follows

$$na := \underbrace{a + ... + a}_{n \text{ times}}, \ (-n)a := n(-a) = \underbrace{(-a) + ... + (-a)}_{n \text{ times}} \ .$$

In that case we say that G is an "**additively written**" group.

Example 2.4. 1. A set $G := \{e\}$ with only one element e and the obvious group multiplication constitutes a group, the **trivial group**.

2. With the ordinary addition of numbers as group law the set $\mathbb{Z}$ of all integers forms a (commutative) group, and so do the rational, real and complex numbers:

   $\mathbb{Q} :=$ { all rational numbers} , $\mathbb{R} :=$ { all real numbers} and

   $\mathbb{C} :=$ { all complex numbers}.

3. A real or complex vector space V endowed with the addition of vectors is a (commutative) group.

4. Let $K = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. With the ordinary multiplication of numbers the set $K^* := K \setminus \{0\}$ becomes a (commutative) group. (We have to exclude 0, since it does not have an inverse element.)

5. For $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ we denote $K^{n,n}$ the set of all square matrices of size n with entries in K. Then the set

$$GL_n(K) := \{A \in K^{n,n}, \det A \neq 0\}$$

of all invertible matrices in $K^{n,n}$ with matrix multiplication as group law is a group, which for $n \geq 2$ is not commutative. It is called the (n-dimensional) **general linear group** over K.

6. For a set M let

$$\mathbb{S}(M) := \{f : M \longrightarrow M \text{ bijective map}\}$$

be the set of all bijective maps from M to itself ("**permutations**" of M). It constitutes a group together with the composition of maps as group law μ, i.e., $fg = \mu(f, g) := f \circ g$. (The neutral element is the identity id_M.)

7. Let V be a finite dimensional vector space over K with $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Then we define the **general linear group** $GL(V)$ of V as

$$GL(V) := \{f \in \mathbb{S}(V); f \ K\text{-linear}\},$$

endowed with the group multiplication induced by $\mathbb{S}(V)$.

8. For $M_n := \{1, ..., n\}$, the group

$$\mathbb{S}_n := \mathbb{S}(M_n)$$

is called the **symmetric group on n letters**. For $m \geq n$ we can understand $\mathbb{S}_n$ as subset of $\mathbb{S}_m$ by extending $f \in \mathbb{S}_n$ to $\hat{f} \in \mathbb{S}_m$ with $\hat{f}(k) = k$ for $k > n$.

There are two different ways to denote a permutation $f \in \mathbb{S}_n$, either as a $2 \times n$-matrix:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$$

or as product of "cycles": A permutation $f \in \mathbb{S}_n$ is called a **cycle** of length $r \geq 2$, if there are pairwise distinct numbers $a_1, \ldots, a_r \in M_n$, such that

$$f(k) = \begin{cases} a_{i+1} & , \text{ if } k = a_i, i < r \\ a_1 & , \text{ if } k = a_r \\ k & , \text{ otherwise} \end{cases} .$$

In that case we write also $f = (a_1, \ldots, a_r)$. Obviously $(a_1, ..., a_r) = (b_1, ..., b_s)$, iff $s = r$ and there is a number $\ell \in \mathbb{N}, 0 \leq \ell < r$, with

$$b_j = \begin{cases} a_{j+\ell}, & , \text{ if } j + \ell \leq r \\ a_{j+\ell-r}, & , \text{ if } j + \ell > r \end{cases} .$$

Two cycles $f = (a_1, ..., a_r), g = (b_1, ..., b_s)$ are called disjoint iff $a_i \neq b_j$ for all indices $i = 1, ..., r, j = 1, ..., s$. In that case the cycles commute: $fg = gf$, but otherwise, that need not be true, e.g.:

$$(1, 2, 3)(1, 2) = (1, 3) \neq (2, 3) = (1, 2)(1, 2, 3) .$$

An arbitrary permutation can be factorized as product of pairwise disjoint cycles, the factors being unique up to reordering (the identity "permutation" being the empty product: In a group a "product without factors" (a contradictio in se?) is defined to be the neutral element.) For example the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 7 & 5 & 4 & 6 & 3 & 8 & 1 \end{pmatrix}$$

becomes $(1, 2, 7, 8)(3, 5, 6)$, while $(1, 2, 3, 7)(4, 8)$ has the matrix

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 7 & 8 & 5 & 6 & 1 & 4 \end{pmatrix} .$$

We remark that $\mathbb{S}_n$ is abelian iff $n \leq 2$, cf. the above counterexample for $n \geq 3$.

9. If $G_1, ..., G_r$ are groups, then their cartesian product $G_1 \times ... \times G_r$ endowed with the componentwise multiplication

$$(g_1, ..., g_r)(h_1, ..., h_r) := (g_1 h_1, ..., g_r h_r)$$

is again a group, the **direct product** of the groups $G_1, ..., G_r$. The group $\mathbb{S}_2 \times \mathbb{S}_2$ is also called "**four-group**" or "**Klein's four-group**" (Felix Klein, 1849-1925).

Remark 2.5. If the group $G = \{e, a, b, c, ...\}$ is finite, the group multiplication can be given in a multiplication table

	e	a	b	c	...
e	e	a	b	c	...
a	a	a^2	ab	ac	...
b	b	ba	b^2	bc	...
c	c	ca	cb	c^2	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

,

where an element in G occurs in every row and column exactly once, since the equation

$$ax = b \text{ resp. } xa = b$$

has in G a unique solution, namely $x = a^{-1}b$ resp. $x = ba^{-1}$.
Two such tables are equivalent from the point of view of algebra, if one of them is obtained from the other by exchange of letters. The corresponding groups then are called isomorphic, cf. Def. 2.7.

Problems 2.6.

1. R: For a set M denote $\mathcal{P}(M)$ its power set. Consider the following binary operations $\mathcal{P}(M) \times \mathcal{P}(M) \longrightarrow \mathcal{P}(M)$ on it:

$$(A, B) \mapsto A \cup B,\ A \cap B,\ A \triangle B := (A \setminus B) \cup (B \setminus A)\ .$$

   Which one does provide on $\mathcal{P}(M)$ a group law?

2. Which of the following subsets of $\mathbb{R}^{n,n}$ endowed with either matrix addition or matrix multiplication becomes a group?

   (a) R: The diagonal matrices.

   (b) R: The diagonal matrices, where all entries in the diagonal are non-zero.

   (c) R: The symmetric matrices.

   (d) R: The invertible symmetric matrices.

   (e) The diagonalizable matrices.

   (f) The invertible diagonalizable matrices.

3. R: For $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ we denote $\mathrm{Aff}_n(K) \subset \mathbb{S}(K^n)$ the subset of all **affine linear transformations**:

$$\mathrm{Aff}_n(K) := \{f \in S(K^n); \exists\ A \in GL_n(K),\ b \in K^n :\ f(x) = Ax + b, \forall\ x \in K^n\}\ .$$

   Show: $\mathrm{Aff}_n(K)$ is a group together with the composition of maps as group multiplication. Is $\mathrm{Aff}(K) := \mathrm{Aff}_1(K)$ commutative?

4. R: Let $G := \{e, a, b, c\}$ be a set with four elements. Show that there are exactly two different multiplication tables for a group law on G (up to exchange of letters).

5. R: Let $f := (1, 2, 3),\ g := (1, 2) \in \mathbb{S}_3$. Show: $\mathbb{S}_3 = \{\mathrm{id}, f, f^2, g, gf, gf^2\}$. Using that notation write a multiplication table for $\mathbb{S}_3$!

6. R: Show: $|\mathbb{S}_n| = n!$.

7. R: A cycle $(i, j) \in \mathbb{S}_n$ of length 2 is called a **transposition**. Show: Every permutation $f \in \mathbb{S}_n$ can be written as a product of transpositions. Hint: Induction on n.

8. R: Show: A group, where $a^2 = e$ for all $a \in G$, is abelian.

9. A group is called **finitely generated** iff there are elements $a_1, ..., a_r \in G$ such that every $g \in G$ can be written $g = a_{i_1}^{k_1} \cdot ... \cdot a_{i_s}^{k_s}$ with integers $k_1, ..., k_s, 1 \leq i_1, .., i_s \leq r$. In that case the elements $a_1, ..., a_r$ are said to **genererate** the group G, or to be **generators** of G (but as such they are of course not uniquely determined - there are many different systems of generators!) If G is abelian, the defining condition for generators $a_1, ..., a_r$ can be simplified: It is enough to require that every $g \in G$ can be written $g = a_1^{k_1} \cdot ... \cdot a_r^{k_r}$ resp., with additive notation, $g = k_1 a_1 + ... + k_r a_r$ with integers $k_1, ..., k_r \in \mathbb{Z}$. Show: The group $\mathbb{Z}$ is generated by the element 1 as well as by $2, 3$. The group $(\mathbb{Q}, +)$ is not finitely generated!

10. Show: The symmetric group $\mathbb{S}_n$ is generated by the transpositions $(1, 2), ..., (1, n)$ resp. by $(1, 2), (2, 3), ..., (n - 1, n)$ resp. by $(1, 2), (1, 2, 3, ..., n)$.

2.2 Homomorphisms

Definition 2.7. *A map*

$$\varphi : G \longrightarrow H$$

between two groups G and H is called a **(group) homomorphism**, *iff*

$$\varphi(ab) = \varphi(a)\varphi(b) \quad \forall\ a, b \in G.$$

A bijective homomorphism is called a **(group) isomorphism**, *and an isomorphism $\varphi : G \longrightarrow G$ is called a* **(group) automorphism**.
Two groups G, H are called **isomorphic**, *iff there is a (group) isomorphism $\varphi : G \longrightarrow H$. In that case one writes $G \cong H$.*

Remark 2.8. For a group homomorphism we have always

$$\varphi(e_G) = e_H,\ \varphi(a^n) = \varphi(a)^n$$

with the neutral elements e_G and e_H of G resp. H, and arbitrary elements $a \in G, n \in \mathbb{Z}$.

Example 2.9.

1. For all groups G, H the constant map $\varphi : G \longrightarrow H$ with $\varphi(a) = e := e_H, \forall a \in G$, is a homomorphism.

2. For every group the identity map $\varphi := \mathrm{id}_G : G \longrightarrow G$ is an automorphism.

3. Let G be a group and $a \in G$. Then the "exponential map" $\varphi_a : \mathbb{Z} \longrightarrow G, n \mapsto a^n$, is a homomorphism, since $\varphi_a(n+m) = a^{n+m} = a^n a^m = \varphi_a(n)\varphi_a(m)$.

4. Let G be a group and $n \in \mathbb{Z}$. We regard the n-th power map $p_n : G \longrightarrow G, a \mapsto a^n$, and find: p_0 and p_1 are always homomorphisms, cf. the previous points, while p_{-1} is a so called "anti-homomorphism", i.e., we have
$$(ab)^{-1} = b^{-1}a^{-1} \quad .$$
Only if G is abelian, all the power maps $p_n, n \in \mathbb{Z}$, are homomorphisms.

5. The complex exponential map $\varphi : \mathbb{C} \longrightarrow \mathbb{C}^*, z \mapsto e^{2\pi i z}$, is a group homomorphism from an additively written group into a multiplicatively written one, since $\varphi(z+w) = \varphi(z)\varphi(w)$.

6. Let $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ and V be a K-vector space, $\dim V = n < \infty$. If we choose a basis $e_1, ..., e_n$ of V, then
$$GL(V) \xrightarrow{\cong} GL_n(K), f \mapsto A_f,$$
where $A_f = (\alpha_{ij}) \in K^{n,n}$ denotes the matrix of f with respect to the basis $e_1, ..., e_n$, i.e. $f(e_j) = \sum_{i=1}^n \alpha_{ij} e_i$, is a group isomorphism.

7. The determinant $\det : GL_n(K) \longrightarrow K^*, A \mapsto \det(A)$, is a group homomorphism. ($K = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$).

8. The map $\text{sign} : \mathbb{S}_n \longrightarrow \mathbb{Q}^*$, where

$$\text{sign}(f) := \prod_{1 \leq i < j \leq n} \frac{f(i) - f(j)}{i - j} \quad ,$$

is a group homomorphism, and $\text{sign}(f) = \pm 1$ for all permutations $f \in \mathbb{S}_n$. The latter follows immediately from the fact that any factor $i - j$ equals a factor $f(\ell) - f(k)$ up to sign. In order to see that sign indeed is a group homomorphism, we consider for any set

$$A = \{i, j\} \subset M_n$$

consisting of of two different natural numbers i, j between 1 and n the rational number

$$\sigma_A(f) := \frac{f(i) - f(j)}{i - j}.$$

It is well defined, since the RHS remains unchanged after exchange of i and j. Denote $\mathcal{P}_2(n)$ the set of all subsets $A \subset M_n$ of order $|A| = 2$. Since

$$\sigma_A(g \circ f) = \sigma_{f(A)}(g) \cdot \sigma_A(f),$$

we obtain

$$\text{sign}(g \circ f) = \prod_{A \in \mathcal{P}_2(n)} \sigma_A(g \circ f) = \prod_{A \in \mathcal{P}_2(n)} \sigma_{f(A)}(g) \prod_{A \in \mathcal{P}_2(n)} \sigma_A(f)$$

$$\left(\prod_{A \in \mathcal{P}_2(n)} \sigma_A(g) \right) \cdot \text{sign}(f) = \text{sign}(g) \cdot \text{sign}(f).$$

9. For each element $g \in G$ in a group G the conjugation with g, i.e., the map

$$\kappa_g : G \longrightarrow G, a \mapsto gag^{-1} \ ,$$

is a group homomorphism. We remark, that κ_g even is an automorphism of the group G with inverse $\kappa_{g^{-1}}$. Such an automorphism is also called an "**inner automorphism**", since it can be described using the group multiplication of the group G. Indeed any automorphism is the restriction to G of an inner automorphism of a suitable bigger group $\tilde{G} \supset G$. Note that $\kappa_g = \text{id}_G$ for all $g \in G$ iff G is abelian.

10. The map $\kappa : G \longrightarrow \mathbb{S}(G), g \mapsto \kappa_g$, associating to $g \in G$ the conjugation with g, is a group homomorphism for every group G. Remember that $\mathbb{S}(G)$ is the group of all permutations of G; so we have to show that $\kappa_g \circ \kappa_h = \kappa_{gh}$ for all $g, h \in G$. Do that!

The homomorphisms $\varphi : G \longrightarrow \mathbb{S}(M)$ from a group G to the permutation group $\mathbb{S}(M)$ of a set M correspond to "G-actions on M":

Definition 2.10. *Let G be a group and M a set. A G-**action** on M is a map*

$$G \times M \longrightarrow M, (g, x) \mapsto gx \quad ,$$

satisfying the following conditions:

1. $ex = x, \ \forall x \in M$,
2. $g(hx) = (gh)x, \ \forall \ g, h \in G, \ \forall \ x \in M$.

A group action is called effective if $gx = x$ for all $x \in M$ implies $g = e$.

Remark 2.11. The G-actions on a set M correspond bijectively to group homomorphisms $\varphi : G \longrightarrow \mathbb{S}(M)$. Namely:

1. Given a G-action on M and an element $g \in G$, the map

   $$\varphi_g : M \longrightarrow M, x \mapsto gx,$$

   is bijective with inverse $\varphi_{g^{-1}}$. Hence we obtain a homomorphism

   $$\varphi : G \longrightarrow \mathbb{S}(M), g \mapsto \varphi_g.$$

2. On the other hand to a homomorphism $\varphi : G \longrightarrow \mathbb{S}(M), g \mapsto \varphi_g$, we associate the G-action $(g, x) \mapsto gx := \varphi_g(x)$.

In particular a group action is effective iff the homomorphism $\varphi : G \longrightarrow \mathbb{S}(M)$ is injective.

Example 2.12. 1. The symmetric group $\mathbb{S}_n$ acts naturally on $M_n := \{1, ..., n\}$ by $(f, k) \mapsto f(k)$.

2. The general linear group $GL_n(K)$ acts on K^n by $(A, x) \mapsto Ax$, where Ax denotes the product of the matrix A with the column vector $x \in K^n$.

3. The general linear group $GL_n(K)$ acts on $K^{n,n}$ by $(A, X) \mapsto AXA^{-1}$.

4. The general linear group $GL_n(K)$ acts on the subspace $Sym_n(K) \subset K^{n,n}$ of all symmetric matrices by $(A, X) \mapsto AXA^T$, where A^T denotes the transposed matrix.

5. For $M = G$ there are three different natural actions of G on itself (The products in the below formulae denote the group multiplication in G!):

   (a) Left translation: $G \times G \ni (g, x) \mapsto gx \in G$.

   (b) Right translation with the inverse element: $G \times G \ni (g, x) \mapsto xg^{-1} \in G$.

   (c) Conjugation, i.e., the first two (commuting!) actions simultaneously: $G \times G \ni (g, x) \mapsto \kappa_g(x) = gxg^{-1} \in G$.

Definition 2.13. *Let the group G act on the set M. The* **orbit** $Gx \subset M$ *of an element $x \in M$ is defined as*

$$Gx := \{gx; g \in G\}.$$

Example 2.14. With respect to the natural action of $GL_n(K)$ on K^n there are exactly two different orbits in K^n, namely $GL_n(K)0 = \{0\}$ and $GL_n(K)x = K^n \setminus \{0\}$, where $x \in K^n$ is an arbitrary vector $\neq 0$.

In general we have

Proposition 2.15. *Two orbits in a set M with G-action are either equal or disjoint. In particular M is the disjoint union of all orbits.*

Proof. If $y \in Gx$, we have $Gy = Gx$: Let $y = hx, h \in G$. $Gy \subset Gx$ follows from $gy = g(hx) = (gh)x$. But on the other hand also $x = h^{-1}y \in Gy$, so $Gx \subset Gy$ resp. $Gx = Gy$.
Assume now that $Gx \cap Gy \neq \emptyset$, say $z \in Gx \cap Gy$: According to what we already know, that implies $Gx = Gz = Gy$. □

Remark 2.16. If there is only one orbit (which then coincides with M), one says that G acts **transitively** on M. For example, that is the case, if G acts on itself by left translation or by right translation with the inverse element. But for conjugation the situation is different: The orbits

$$\kappa_G(x) = \{gxg^{-1}; g \in G\} \subset G$$

then are called **conjugacy classes** and two elements in the same orbit are called **conjugate**. Since $\kappa_G(e) = \{e\}$, the action of G on itself by conjugation is never transitive for a nontrivial group G. Note that a cunjugacy class $\kappa_G(x)$ is trivial, i.e. $\kappa_G(x) = \{x\}$, iff x commutes with all elements $g \in G$.

Definition 2.17. *Let G be a group. The* **center** $Z(G) \subset G$ *is the subset*

$$Z(G) := \{x \in G; \kappa_G(x) = \{x\}\} \ .$$

consisting of the elements $x \in G$ with trivial conjugacy class. Equivalently

$$Z(G) = \{x \in G; xg = gx \ \forall g \in G\} \ .$$

In particular, a group G is abelian iff $Z(G) = G$.

Problems 2.18.

1. R: Determine all automorphisms of Klein's four group $\mathbb{S}_2 \times \mathbb{S}_2$! What about the other group (cf. Problem 2.6.4) of order 4?
2. R: Compute sign(f) for a cycle $f \in \mathbb{S}_n$ of given length! Hint: Induction on the length starting with 2-cycles (transpositions) resp. $\tau = (1, 2)$.
3. R: Assume that $f \in \mathbb{S}_n$ admits two different factorizations as product of transpositions (2-cycles). Show that the numbers of factors have the same parity!
4. R: Show: Two permutations $f, g \in \mathbb{S}_n$ are conjugate iff in their respective factorization as product of disjoint cycles, for any given length $r \geq 2$, there are as many cycles of length r in the factorization of g as in the factorization of f. How many conjugacy classes are there in $\mathbb{S}_5$?

5. Show: An automorphism $\varphi : \mathbb{S}_n \longrightarrow \mathbb{S}_n$ mapping transpositions to transpositions is an inner automorphism, i.e. has the form κ_h with some $h \in \mathbb{S}_n$. Hint: Consider the transpositions $\tau_i := (i, i+1)$ for $i < n$.

6. Show: An automorphism $\varphi : \mathbb{S}_n \longrightarrow \mathbb{S}_n$ maps transpositions to permutations which are the product of mutually disjoint 2-cycles.

7. Show that for $n \neq 6$ every automorphism of $\mathbb{S}_n$ is an inner automorphism. Hint: Compute the number $|\kappa_{\mathbb{S}_n}(f)|$ of elements in the conjugacy class of a permutation $f \in \mathbb{S}_n$, which is the product of mutually disjoint 2-cycles.

8. R: Let $\mathbb{R}^*$ act on the plane $\mathbb{R}^2$ by $t \cdot (x, y) := (t^a x, t^b y)$ with integers $a, b \in \mathbb{Z}$. Sketch the orbits!

9. Classify the orbits of the $GL_2(\mathbb{C})$-action of Example 2.12.3.

10. Classify the orbits of the $GL_2(\mathbb{R})$-action of Example 2.12.4.

11. R: Show $Z(\mathbb{S}_n) = \{\mathrm{id}_{M_n}\}$ for $n \geq 3$.

12. R: Show $Z(GL_n(K)) = K^* E$ with the unit matrix E of size n.

13. The group $GL_{n+1}(K)$ acts in a natural way on the set

$$\mathbb{P}_n(K) := \{L \subset K^{n+1} \text{ a one dimensional subspace }\}$$

of all lines in K^{n+1} through the origin via:

$$GL_{n+1}(K) \times \mathbb{P}_n(K) \longrightarrow \mathbb{P}_n(K), (A, L) \mapsto A(L).$$

The set $\mathbb{P}_n(K)$ is also called the n-dimensional projective space over K. Determine the kernel of the corresponding group homomorphism $\varphi : GL_{n+1}(K) \longrightarrow \mathbb{S}(\mathbb{P}_n(K))$!

14. A continuation of the previous problem: Using the bijection

$$\widehat{K} := K \cup \{\infty\} \longrightarrow \mathbb{P}_1(K), x \mapsto K(x, 1), \infty \mapsto K(1, 0)$$

and writing $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ compute the corresponding action

$$GL_2(K) \times \widehat{K} \longrightarrow \widehat{K}, (A, x) \mapsto Ax = ? \ .$$

Show that given two triples (L_1, L_2, L_3) and $(\tilde{L}_1, \tilde{L}_2, \tilde{L}_3)$ of pairwise different lines there is a matrix $A \in GL_2(K)$, unique up to a nonzero scalar factor, satisfying $\tilde{L}_i = A(L_i)$ for $i = 1, 2, 3$.

For $K = \mathbb{C}$ the set $\widehat{\mathbb{C}}$ is nothing but the "Riemann sphere" from complex analysis, and the transformations $z \mapsto Az$ are called **Möbius transformations** (August Ferdinand Möbius, 1790-1868).

2.3 Subgroups

Definition 2.19. *Let G be a group. A non-empty subset $H \subset G$ is called a* **subgroup** *iff H is closed with respect to both, group multiplication and "inversion"*

$$a, b \in H \Longrightarrow ab \in H \ , \ a \in H \Longrightarrow a^{-1} \in H \ .$$

In order to emphasize that a subset $H \subset G$ actually is a subgroup, we also write

$$H \leq G.$$

Remark 2.20.

1. Let $H \leq G$ be a subgroup, $a \in H$. Since $a^{-1} \in H$, we get $e = aa^{-1} \in H$. In particular a subgroup is itself a group when endowed with the restriction of the group multiplication of G.

2. The intersection $H_1 \cap H_2$ of two subgroups $H_1, H_2 \leq G$ is again a subgroup: $H_1 \cap H_2 \leq G$. But the union $H_1 \cup H_2$ in general is not.

Example 2.21.

1. For any group G the subsets $H = \{e\} \subset G$ as well as $H = G$ provide subgroups.

2. Let $\varphi : G \longrightarrow F$ be a group homomorphism between the groups G and F. If $G_0 \leq G, F_0 \leq F$ are subgroups, the image $\varphi(G_0) \subset F$ of G_0 as well as the inverse image $\varphi^{-1}(F_0) \subset G$ of F_0 are subgroups of F resp. of G. If $G_0 = G$, we obtain the image

$$\varphi(G) = \{\varphi(g); g \in G\} \leq F$$

of φ, and if $F_0 = \{e\}$ the corresponding subgroup is called the kernel of the homomorphism φ:

Definition 2.22. *Let $\varphi : G \longrightarrow F$ be a group homomorphism between groups G and F. Its* **kernel** *is the subgroup*

$$\ker(\varphi) := \{g \in G; \varphi(g) = e\} \leq G \ ,$$

where $e := e_F$ denotes the neutral element in the group F.

Proposition 2.23. *A group homomorphism $\varphi : G \longrightarrow F$ is injective iff* $\ker(\varphi) = \{e\}$.

Proof. In any case we have $e \in \ker(\varphi)$; so if φ is injective, necessarily $\ker(\varphi) = \{e\}$. Assume now $\ker(\varphi) = \{e\}$ and $\varphi(a) = \varphi(b)$. Then we have $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e \in F$, i.e., $ab^{-1} \in \ker(\varphi) = \{e\}$ resp. $ab^{-1} = e$ resp. $a = b$. □

Example 2.24.

1. The center $Z(G) \leq G$ of a group G, cf. Def. 2.17, satisfies
$$Z(G) = \ker(\kappa : G \longrightarrow \mathbb{S}(G))$$
with the homomorphism $\kappa : G \longrightarrow \mathbb{S}(G), g \mapsto \kappa_g$, in particular it is a subgroup of G.

2. The unit circle
$$\mathbf{S}^1 := \{z \in \mathbb{C}; |z| = 1\}$$
is a subgroup of the multiplicative group $\mathbb{C}^*$ of nonzero complex numbers, in fact the kernel of the homomorphism $\mathbb{C}^* \longrightarrow \mathbb{R}^*, z \mapsto |z|$.

3. The kernel of the determinant homomorphism $\det : GL_n(K) \longrightarrow K^*$, the (sub)group $SL_n(K) := \ker(\det) \subset GL_n(K)$ is called the **special linear group**. Remember that the neutral element of K^* is $1 \in K^* = K \setminus \{0\}$; so
$$SL_n(K) = \{A \in GL_n(K); \det(A) = 1\} = \{A \in K^{n,n}; \det(A) = 1\}.$$

4. Let $\sigma : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$ be the the standard inner product, i.e., $\sigma(x, y) := x^T y$. Then
$$O(n) := \{A \in GL_n(\mathbb{R}); \sigma(Ax, Ay) = \sigma(x, y) \ \forall \ x, y \in \mathbb{R}^n\}$$
$$= \{A \in GL_n(\mathbb{R}); A^T A = E\}$$
($E \in \mathbb{R}^{n,n}$ denotes the unit matrix) is a subgroup of $GL_n(\mathbb{R})$, the **orthogonal group**.

5. The intersection $SO(n) := SL_n(\mathbb{R}) \cap O(n)$ is also a subgroup, the **special orthogonal group**. For $n = 2, 3$ the matrices $A \in SO(n)$ correspond to rotations around the origin resp. some axis through

the origin. In particular, if we identify $\mathbb{R}^2$ with the complex plane $\mathbb{C}$ and denote R_ϑ the counterclockwise rotation with angle $\vartheta \in \mathbb{R}$, i.e. $R_\vartheta(z) := e^{i\vartheta}z$, we obtain

$$SO(2) = \{R_\vartheta; \vartheta \in \mathbb{R}\} \cong \mathbf{S}^1.$$

The orthogonal group $O(2)$ itself is the union

$$O(2) = SO(2) \cup SO(2) \cdot S,$$

of its subgroup $SO(2) \subset O(2)$ and the set

$$SO(2) \cdot S = \{R_\vartheta S; \vartheta \in \mathbb{R}\}$$

of all reflections. Here S denotes the reflection at the real axis, i.e. complex conjugation $S(z) := \overline{z}$.

With $\mathbb{C}$ instead of $\mathbb{R}$ there is an analogous construction:

6. Let $\sigma : \mathbb{C}^n \times \mathbb{C}^n \longrightarrow \mathbb{C}$ be the standard inner product, i.e. $\sigma(x, y) := x^T\overline{y}$. Then

$$U(n) := \{A \in GL_n(\mathbb{C}); \sigma(Ax, Ay) = \sigma(x, y) \ \forall \ x, y \in \mathbb{C}^n\}$$

$$= \{A \in GL_n(\mathbb{C}); A^T\overline{A} = E\}$$

is a subgroup of $GL_n(\mathbb{C})$, the **unitary group**. And

$$SU(n) := SL_n(\mathbb{C}) \cap U(n)$$

is called the **special unitary group**. We remark that

$$SU(2) = \{A \in \mathbb{C}^{2,2}; A = \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}; z, w \in \mathbb{C}, z\overline{z} + w\overline{w} = 1\};$$

so as a topological space, it is nothing but the three dimensional unit sphere $\mathbf{S}^3 \subset \mathbb{C}^4 \cong \mathbb{C}^{2,2}$.

7. $\mathbb{A}_n := \ker(\text{sign}) \subset \mathbb{S}_n$ is called the **alternating group** on n letters. The permutations in $\mathbb{A}_n$ are called **even**, the other ones **odd**. As a consequence of problems 2.6.7 and 2.18.3 we see that if an even resp. odd permutation is a product of transpositions, then the number of factors is even resp. odd; this explains the etymology.

8. For $n \geq 1$ we consider the power map $p_n : \mathbb{C}^* \longrightarrow \mathbb{C}^*, z \mapsto z^n$. Its kernel $C_n := \ker(p_n)$ is called the **group of all n-th roots of unity**, i.e.

$$C_n = \{z \in \mathbb{C}; z^n = 1\} = \{1, \eta, ..., \eta^{n-1}\}$$

with $\eta := e^{\frac{2\pi i}{n}}$.

9. Given a subset $P \subset K^n$ with $K = \mathbb{R}$ or $K = \mathbb{C}$ we define the **symmetry group** of P as the subgroup $Sym(P) \subset GL_n(K)$ of the general linear group $GL_n(K)$ consisting of all matrices transforming P into itself:

$$Sym(P) := \{A \in GL_n(K); A(P) = P\} \leq GL_n(K).$$

10. The **dihedral group** $D_n, n \geq 3$: In the complex plane $\mathbb{C}$ we consider the regular n-gon P_n with the n-th roots of unity $1, \eta, ..., \eta^{n-1}$ as vertices (where $\eta := e^{\frac{2\pi i}{n}}$). We identify $\mathbb{C}$ with $\mathbb{R}^2$ as usual and define the dihedral group D_n as the (real) symmetry group of P_n, i.e.

$$D_n := Sym(P_n) \subset GL_n(\mathbb{R}).$$

Then, with the rotation $R := R_{2\pi/n}$ and the reflection S on the x-axis, we have

$$D_n = \{E, R, ..., R^{n-1}, S, RS, ..., R^{n-1}S\}, \tag{1}$$

where E denotes the identity map (or the unit matrix). We note the relations

$$R^n = E = S^2, \ SRS^{-1} = R^{-1}.$$

Of course $SRS^{-1} = SRS$ because of $S^2 = E$, but for systematic reasons we prefer the expression SRS^{-1}, since in order to classify groups up to isomorphy, it is important to understand how elements in the group act on others by conjugation.

Proof of Equality 1. Obviously the given $2n$ linear maps transform P_n into itself, and we have to show the opposite inclusion. A linear map $A \in D_n$ maps the vertices of P_n onto themselves, i.e. $A(C_n) = C_n$. In particular $A(1) = \eta^\nu$ for some $\nu, 0 \leq \nu \leq n-1$. Then $B := R^{-\nu}A \in D_n$ satisfies $B(1) = 1$; and since edges are mapped to edges we obtain

$B(\eta) = \eta$ or $B(\eta) = \eta^{n-1} = \overline{\eta}$. But $1, \eta$ is a basis of the real vector space $\mathbb{C}$, and thus $B = E$ or $B = S$. For the matrix A that means $A = R^\nu$ or $A = R^\nu S$. □

11. Let $I := [-1, 1] \subset \mathbb{R}$. The complex symmetry group of the 4-cube $I^4 \subset \mathbb{R}^4 \cong \mathbb{C}^2$ is the group

$$Sym_{\mathbb{C}}(I^4) := \{A \in GL_2(\mathbb{C}); A(I^4) = I^4\}$$

$$= \left\{ A \in GL_2(\mathbb{C}); A = \begin{pmatrix} \eta & 0 \\ 0 & \zeta \end{pmatrix} \text{ or } A = \begin{pmatrix} 0 & \eta \\ \zeta & 0 \end{pmatrix} \text{ with } \eta, \zeta \in C_4 \right\} .$$

In particular $|Sym_{\mathbb{C}}(I^4)| = 32$. As motivation we can say that a matrix $A \in Sym_{\mathbb{C}}(I^4)$ maps midpoints of the facets of the cube again to such midpoints (they are the arithmetic means of the vertices). But these are the points $(\alpha, 0)$ or $(0, \alpha)$ with $\alpha \in C_4$.

12. The intersection

$$Q := Sym_{\mathbb{C}}(I^4) \cap SL_2(\mathbb{C})$$

of the complex symmetry group $Sym_{\mathbb{C}}(I^4)$ of the 4-cube with $SL_2(\mathbb{C})$ is called the **quaternion group**, it has 8 elements:

$$Q = \{\pm E, \pm I, \pm J, \pm K\}$$

with the unit matrix E and

$$I := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} , J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} , K := IJ = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} .$$

We note that $-E$ commutes with all elements in Q and the relations $IJ = K = -JI, JK = I = -KJ, KI = J = -IK$.

13. For each group G the set

$$\mathrm{Aut}(G) := \{\varphi \in \mathbb{S}(G); \varphi \text{ group automorphism } \}$$

is a subgroup of the group $\mathbb{S}(G)$ of all permutations of the set G, it is called the **automorphism group** of G.

The subgroups of the additive group $\mathbb{Z}$ of all integers are determined in the next proposition:

Proposition 2.25. *The subgroups $H \subset \mathbb{Z}$ are the sets $\mathbb{Z}n := \{kn; k \in \mathbb{Z}\}$, where $n \in \mathbb{N}$.*

Proof. The subsets $H := \mathbb{Z}n \subset \mathbb{Z}$ obviously are subgroups. Consider now an arbitrary subgroup $H \leq \mathbb{Z}$. For $H = \{0\}$ we have $H = \mathbb{Z}0$, and for non-trivial H there is a least positive integer $n := \min(H \cap \mathbb{N}_{\geq 1})$ in H, the subset H being symmetric with respect to the origin: $a \in H \Longrightarrow -a \in H$. Let us show $H = \mathbb{Z}n$: On the one hand $n \in H \Longrightarrow \mathbb{Z}n \subset H$, since H is a subgroup. Now take any $a \in H$ and divide a by n with remainder: $a = qn + r$ with $q, r \in \mathbb{Z}, 0 \leq r < n$. But $r = a - qn \in H$, such that because of the choice of $n \in H$ only $r = 0$ is possible. Hence $a = qn \in \mathbb{Z}n$. □

Let $H \leq G$ be a subgroup of the group G. We restrict the left translation resp. right translation with the inverse to the subgroup $H \subset G$ and obtain H-actions

$$H \times G \longrightarrow G.$$

These actions are not any longer transitive; their orbits

$$aH := \{ah; h \in H\} = \{ah^{-1}; h \in H\} \qquad \text{resp. } Ha := \{ha; h \in H\} \ ,$$

are called left resp. right cosets:

Definition 2.26. *Let $H \leq G$ be a subgroup of the group G. A* **left coset** *resp.* **right coset** *or* **residue class** *mod(ulo) H is a set $aH \subset G$ resp. $Ha \subset G$, where $a \in G$. A* **representantive** *of the coset aH resp. Ha is any element $b \in aH$ resp. $b \in Ha$, i.e. any element $b = ah$ with some $h \in H$ resp. $b = ha$ with an $h \in H$. Then $aH = bH$ resp. $Ha = Hb$.*
If G is abelian, the left and right coset given by a representative $a \in G$ agree, and in additive notation it is written $a + H$ or $H + a$.
The set of all left resp. right cosets is denoted G/H resp. $H\backslash G$, i.e.

$$G/H := \{aH; a \in G\} \quad (\text{ resp. } H\backslash G := \{Ha; a \in G\}) \ .$$

Example 2.27. 1. Let $G := \mathbb{S}_n$ and $H := \{f \in \mathbb{S}_n; f(n) = n\} \cong \mathbb{S}_{n-1}$. Then there are n left resp. right cosets mod H, namely

$$(i, n)H = \{f \in \mathbb{S}_n; f(n) = i\}$$

resp.

$$H(i,n) = \{f \in \mathbb{S}_n; f(i) = n\},$$

where $1 \leq i \leq n$.

2. If $G = \mathbb{Z}$ and $H = \mathbb{Z}n, n \geq 1$, there are again n cosets, namely the sets

$$r + \mathbb{Z}n, 0 \leq r < n.$$

So a coset consists of all integers which give after division with n the same remainder $r, 0 \leq r < n$.

3. A geometric interpretation: Let $G = \mathbb{R}^2$ and $H \leq \mathbb{R}^2$ a line through the origin. The cosets mod H are then nothing but the lines parallel to H.

4. The cosets of $\mathbf{S}^1 \leq \mathbb{C}^*$ are the circles centered at the origin.

Proposition 2.28. *Let $H \leq G$ be a subgroup of the group G.*

1. *Two left (resp. right) cosets mod H are disjoint or coincide; we have $aH = bH$ (resp. $Ha = Hb$), iff $a^{-1}b \in H$ (resp. $ab^{-1} \in H$).*

2. *If H is finite, a coset mod H contains as many elements as H.*

3. *Let G be finite. Then*

$$|G| = |G/H| \cdot |H| = |H\backslash G| \cdot |H|;$$

in particular the order $|H|$ of the subgroup H divides the order $|G|$ of the group G.

4. *If G/H is finite, so is $H\backslash G$, more precisely $|G/H| = |H\backslash G|$.*

Definition 2.29. *Let $H \leq G$ be a subgroup of the group G. If G/H is finite, the number*

$$(G : H) := |G/H| = |H\backslash G|$$

is called the **index** *of the subgroup H in G.*

Proof. i) The first part is a consequence of Prop. 2.15, the second is left to the reader as an exercise.
ii) The left translation $\lambda_a : G \longrightarrow G, x \mapsto ax$, is bijective, and $\lambda_a(H) = aH$, whence $|aH| = |H|$ for all $a \in G$. (An analogous argument works for right cosets).
iii) follows immediately from i) and ii).
iv) The "inversion" $p_{-1} : G \longrightarrow G, a \mapsto a^{-1}$ is bijective and satisfies $p_{-1}(aH) = Ha^{-1}$, hence induces a bijection $G/H \longrightarrow H\backslash G$. □

Given an action of a group G on a set M we associate to each element $x \in M$ a subgroup $G_x \subset G$ as follows:

Definition 2.30. *Let G be a group acting on the set M. For an element $x \in M$ we define its* **isotropy group** *or* **stabilizer** *G_x by*

$$G_x := \{g \in G; gx = x\} \quad .$$

The left coset space G/G_x can be identified with the orbit $Gx \subset M$:

Proposition 2.31 (Class formula)**.** *Assume the group G acts on the set M. Then:*

1. *For any $x \in M$ the map $G/G_x \longrightarrow Gx, gG_x \mapsto gx$, is bijective; in particular we have $|Gx| = (G : G_x)$.*
2. *If M is finite and $Gx_1, .., Gx_r$ are the (pairwise different) G-orbits, the "class formula" says*

$$|M| = (G : G_{x_1}) + ... + (G : G_{x_r}) \quad .$$

Proof. The given map is obviously well defined and surjective, and it is injective as well, since $gx = hx$ implies $g^{-1}h \in G_x$ and thus $hG_x = g(g^{-1}h)G_x = gG_x$. (Its inverse is given by $y \mapsto \psi^{-1}(y)$ with the orbit map $\psi : G \longrightarrow Gx, g \mapsto gx$.) Finally M is the disjoint union of the orbits $Gx_1, ..., Gx_r$. □

If G acts on itself by conjugation, then the center $Z(G) \subset G$ consists exactly of the elements with one point conjugacy class. In that case the class formula reads as follows:

Corollary 2.32. *Let G be a finite group group and $x_1, ..., x_r \in G$ a system of representatives for the non-trivial conjugacy classes in G, i.e. every conjugacy class with more than one element is of the form $\kappa_G(x_i)$ and the $\kappa_G(x_i)$ are pairwise distinct. Then we have*

$$|G| = |Z(G)| + (G : G_{x_1}) + ... + (G : G_{x_r})$$

with the proper subgroups $G_{x_i} = \{a \in G; ax_ia^{-1} = x_i\} \subset G$. In particular if $|G| = p^r > 1$ with a prime number p, its center is nontrivial: $Z(G) \neq \{e\}$.

Proof. The order $|G|$ and the indices $(G : G_{x_i})$, $i = 1, ..., r$, are divisible with p, hence so is the order $|Z(G)|$ of the center, in particular $|Z(G)| > 1$. □

2.3.1 Digression: Quaternions

Motivated by the quaternion group, cf. Example 2.24.12, we conclude this section with a digression about quaternions in general:

The elements in the four-dimensional real vector space

$$\mathbb{H} := \left\{ \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}; z, w \in \mathbb{C} \right\} = \mathbb{R}_{\geq 0} \cdot SU(2) \subset \mathbb{C}^{2,2}$$

are called quaternions; they have been found by William Rowan Hamilton (1805-1865) - of course not in this form, but instead using a basis like E, I, J, K below. For the second equality we refer to Example 2.24.6; as a consequence we see that $\mathbb{H}$ is even closed with respect to matrix multiplication and that all non-zero quaternions $A \in \mathbb{H}$ are invertible, but note that $\mathbb{H} \subset \mathbb{C}^{2,2}$ is not a complex vector subspace! In fact

$$\mathbb{H} = \mathbb{R} \cdot E + \mathbb{R} \cdot I + \mathbb{R} \cdot J + \mathbb{R} \cdot K \cong \mathbb{R}^4$$

with the unit matrix $E \in \mathbb{C}^{2,2}$ and the matrices I, J, K of Example 2.24.12. There is more structure on the vector space $\mathbb{H}$: We have a conjugation:

$$\mathbb{H} \longrightarrow \mathbb{H}, A \mapsto A^* := \overline{A}^T$$

satisfying

$$(A + B)^* = A^* + B^*, \ (AB)^* = B^*A^*, \ (A^*)^* = A$$

and the inner product

$$\sigma : \mathbb{H} \times \mathbb{H} \longrightarrow \mathbb{R}, (A, B) \mapsto \sigma(A, B) := \frac{1}{2}\text{trace}(AB^*).$$

It satisfies

$$\sigma(AB, C) = \sigma(A, CB^*),$$

and the corresponding norm

$$|A| = \sqrt{\sigma(A, A)} = \sqrt{\det(A)}$$

is multiplicative, i.e.

$$|AB| = |A| \cdot |B| \text{ as well as } |A^*| = |A|$$

and has unit sphere

$$\mathbf{S}^3 = \{A \in \mathbb{H}; |A| = 1\} = SU(2).$$

We can write $\mathbb{H}$ as an orthogonal sum

$$\mathbb{H} = \text{Re}(\mathbb{H}) \oplus \text{Im}(\mathbb{H})$$

with the "real" subspace

$$\text{Re}(\mathbb{H}) := \{A \in \mathbb{H}; A^* = A\} = \mathbb{R} \cdot E$$

and the "imaginary" subspace

$$\text{Im}(\mathbb{H}) := \{A \in \mathbb{H}; A^* = -A\} = \mathbb{R} \cdot I + \mathbb{R} \cdot J + \mathbb{R} \cdot K \cong \mathbb{R}^3.$$

Note that $AA^* = |A|^2 \cdot E$, whence

$$A^2 = -|A|^2 \cdot E, \ \forall \ A \in \text{Im}(\mathbb{H}),$$

this motivates the name "imaginary subspace".

Realizations of the quaternion group: Let us now show that, given two orthogonal purely imaginary unit quaternions $A, B \in \text{Im}(\mathbb{H})$, we obtain an ON-basis

$$A, B, AB = -BA$$

of $\mathrm{Im}(\mathbb{H})$. From that and $A^2 = -E = B^2$ we easily derive that $\{\pm E, \pm A, \pm B, \pm C\}$ with $C := AB$ is a group isomorphic to the quaternion group Q.

First of all $AB, BA \in \mathrm{Im}(\mathbb{H}) = E^\perp$, since for example $\sigma(AB, E) = \sigma(A, B^*) = -\sigma(A, B) = 0$. Hence

$$AB = -(AB)^* = -B^*A^* = -(-B)(-A) = -BA.$$

Furthermore, AB is orthogonal to both A and B:

$$\sigma(AB, B) = \sigma(A, BB^*) = \sigma(A, E) = 0,$$

while

$$\sigma(AB, A) = \sigma(A, AB^*) = \sigma(AB^*, A) = \sigma(-AB, A) = -\sigma(AB, A),$$

whence $\sigma(AB, A) = 0$ as well. As a consequence of this discussion we see that the product of quaternions is closely related to vector geometry in three space: The map

$$\mathrm{Im}(\mathbb{H}) \times \mathrm{Im}(\mathbb{H}) \longrightarrow \mathrm{Im}(\mathbb{H}), (A, B) \longrightarrow \mathrm{Im}(AB) = \frac{1}{2}(AB - BA)$$

is nothing but the vector product of the "vectors" $A, B \in \mathrm{Im}(\mathbb{H}) \cong \mathbb{R}^3$: It is bilinear, alternating and associates to two orthogonal unit vectors a unit vector orthogonal to both factors.

Orthogonal and unitary groups: Finally let us use quaternions in order to find an interesting relationship between the special unitary group

$$SU(2) = \mathbf{S}^3 = \{A \in \mathbb{H}; |A| = 1\}$$

and the special orthogonal groups $SO(3)$ and $SO(4)$.

We have an action by conjugation

$$SU(2) \times \mathbb{H} \longrightarrow \mathbb{H}, (A, X) \mapsto AXA^* = AXA^{-1}.$$

Since $|AXA^*| = |X|$, that action is isometric. Furthermore since $\mathrm{Im}(\mathbb{H}) = E^\perp$ and $AEA^* = E$, the imaginary subspace $\mathrm{Im}(\mathbb{H}) \cong \mathbb{R}^3$ is invariant under that action; hence we obtain a group homomorphism

$$SU(2) \longrightarrow SO(3).$$

In fact, it is onto and has the kernel $\{\pm E\}$: Write $A = \cos(\vartheta)E + \sin(\vartheta)B$ with a matrix $B \in \mathrm{Im}(\mathbb{H})$ and $0 \leq \vartheta \leq \pi$. Take $C \in \mathrm{Im}(\mathbb{H})$ orthogonal to B and $D := BC$. Then E, B, C, D is an ON-basis for $\mathbb{H}$ and $\{\pm E, \pm B, \pm C, \pm D\} \subset \mathbf{S}^3$ is isomorphic to the quaternion group Q. An explicit calculation now shows that

$$ACA^* = \cos(2\vartheta)C + \sin(2\vartheta)D, ADA^* = -\sin(2\vartheta)C + \cos(2\vartheta)D$$

while $AAA^* = A$ implies $ABA^* = B$. With other words $X \mapsto AXA^*$ is a rotation around the axis $\mathbb{R} \cdot B \subset \mathrm{Im}(\mathbb{H})$. From this it follows immediately that any transformation in $SO(3)$ can be written in the above form and that $X \mapsto AXA^*$ is the identity iff $\vartheta = 0, \pi$ resp. $A = \pm E$.

There is also a similar description for $SO(4)$: We consider the action

$$SU(2)^2 \times \mathbb{H} \longrightarrow \mathbb{H}, ((A, B), X) \mapsto AXB^*.$$

It induces a surjective homomorphism

$$SU(2)^2 \longrightarrow SO(4)$$

with kernel $\{\pm(E, E)\}$, namely: If $F : \mathbb{H} \longrightarrow \mathbb{H}$ is an isometry, consider $G : \mathbb{H} \longrightarrow \mathbb{H}$ with $G(X) := F(E)^{-1} \cdot F(X)$. Then $G(E) = E$ implies $G(\mathrm{Im}(\mathbb{H})) = \mathrm{Im}(\mathbb{H})$, and we find as above a matrix $B \in SU(2)$ with $G(X) = BXB^*$. Finally take $A := F(E)B \in \mathbf{S}^3 = SU(2)$. On the other hand if $AXB^* = X$ for all X, then $X = E$ gives us $AB^* = E$ resp. $B = A$ and we may proceed as above.

Problems 2.33.

1. R: Show: If $a, b \in \mathbb{Z}$ are integers and $\gcd(a, b) = 1$, one has $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}$, in particular 1 can be written in the form $1 = ra + sb$ with integers $r, s \in \mathbb{Z}$.
2. R: Determine all subgroups of $\mathbb{S}_3, Q, C_2 \times C_2, D_4$!
3. R: Show that the subgroups of C_n are the groups C_m with $m|n$. Hint: Consider the homomorphism $\varphi_a : \mathbb{Z} \longrightarrow C_n, n \mapsto a^n$ with $a := e^{\frac{2\pi i}{n}}$.
4. R: Let G be a group and $a \in G$, $\eta := e^{\frac{2\pi i}{n}}$. Show: There is a homomorphism $\varphi : C_n \longrightarrow G$ with $\varphi(\eta) = a$, iff $a^n = 1$.
5. R: Show: $\mathrm{Aut}(C_2 \times C_2) \cong \mathbb{S}_3$.
6. Compute $\mathrm{Aut}(Q)$!

7. Show that the "Möbius-action"

$$GL_2(\mathbb{C}) \times \widehat{\mathbb{C}} \longrightarrow \widehat{\mathbb{C}},$$

see Problem 2.18.12, restricts to an action

$$SL_2(\mathbb{R}) \times \mathbf{H} \longrightarrow \mathbf{H}$$

on the upper half plane $\mathbf{H} := \{z = x + iy \in \mathbb{C}; y > 0\}$.

8. Show that for the Möbius action on triplets

$$GL_2(K) \times \mathbb{P}_1(K)^3 \longrightarrow \mathbb{P}_1(K)^3$$

the stabilizer of any triplet $(L_1, L_2, L_3) \in \mathbb{P}_1(K)^3$ with pairwise different lines $L_i \subset K^2$ is $K^* \cdot E \leq GL_2(K)$, see also Problem 2.18.11.

9. Show that $SL_2(\mathbb{Z}) := SL_2(\mathbb{Q}) \cap \mathbb{Z}^{2,2}$ is a subgroup of $SL_2(\mathbb{Q})$.

10. Show that $O(n) = Sym(B_n)$, i.e. $O(n)$ is the symmetry group of the closed unit ball $B_n := \{x \in \mathbb{R}^n; ||x|| \leq 1\}$.

11. R: Show: Every group is isomorphic to a subgroup of a permutation group $\mathbb{S}(M)$ with a suitable set M.

12. R: Let G be a group. Show that a non-empty set $H \subset G$ is a subgroup iff $ab^{-1} \in H$ for all $a, b \in H$.

13. R: Let $H_1, H_2 \subset G$ be subgroups of the group G. Show: The union $H_1 \cup H_2 \subset G$ is again a subgroup iff $H_1 \subset H_2$ or $H_2 \subset H_1$.

14. Show: A finitely generated subgroup H of $\mathbb{Q}$ can be generated by one element only, i.e. $H = \mathbb{Z}a$ with some $a \in \mathbb{Q}$.

15. Show that the following statements for a group G are equivalent:

    (a) Every subgroup $H \subset G$ is finitely generated.

    (b) Each increasing sequence $H_1 \subset H_2 \subset ...$ of subgroups $H_n \subset G$ becomes constant, i.e. there is $n_0 \in \mathbb{N}$ with $H_n = H_{n_0}$ for $n \geq n_0$.

    (c) Every set A, whose elements are (certain) subgroups of G, has (at least) one maximal element $H_0 \in A$, i.e. $A \ni H \supset H_0 \Longrightarrow H = H_0$.

16. Let $P \subset \mathbb{R}^3$ be a regular tetrahedron or a cube with the origin as barycenter. Is $Sym(P)$ isomorphic to one of the groups you have encountered up to now?

2.4 Order and Cyclic Groups

In this section we study the most basic nontrivial groups:

Definition 2.34. *For an element $a \in G$ of a group G the subgroup*

$$a^{\mathbb{Z}} := \{a^n;\ n \in \mathbb{Z}\} \leq G$$

is called the **cyclic (sub)group generated by** *$a \in G$. The group G is called* **cyclic** *iff*

$$G = a^{\mathbb{Z}}$$

for some $a \in G$.

In order to understand cyclic groups we need the notion of the order of an element $a \in G$:

Definition 2.35. *Let G be a group. The* **order** $\mathrm{ord}(a) \in \mathbb{N} \cup \{\infty\}$ *of the element $a \in G$ is defined as*

$$\mathrm{ord}(a) := \min\{n \in \mathbb{N}_{\geq 1}; a^n = e\} \quad ,$$

where we use the convention $\min \emptyset := \infty$.

Example 2.36.

1. In the multiplicative group $\mathbb{C}^*$ we have: $\mathrm{ord}(z) < \infty$ iff $z = \exp(2\pi i \frac{p}{q})$ with a rational number $\frac{p}{q} \in \mathbb{Q}$; in that case $\mathrm{ord}(\exp(2\pi i \frac{p}{q})) = q$, if $p, q \in \mathbb{Z}$ are relatively prime and $q > 0$.

2. For the elements R, S in the dihedral group D_n we have $\mathrm{ord}(R) = n$ and $\mathrm{ord}(S) = 2$.

Proposition 2.37. *Let G be a group, $a \in G$ and $\varphi_a : \mathbb{Z} \longrightarrow G$ the homomorphism $n \mapsto a^n$.*

1. *If* $\mathrm{ord}(a) = \infty$, *the homomorphism φ_a is injective, hence induces an isomorphism $\mathbb{Z} \cong a^{\mathbb{Z}}$.*

2. *If* $\mathrm{ord}(a) = d < \infty$, *then* $\ker(\varphi_a) = \mathbb{Z}d$, *and* $\exp(2\pi i \frac{k}{d}) \mapsto a^k$ *defines an isomorphism $C_d \cong a^{\mathbb{Z}}$. In particular the elements $e, a, .., a^{d-1} \in G$ are pairwise different and constitute $a^{\mathbb{Z}}$, i.e., $a^{\mathbb{Z}} = \{e, a, ..., a^{d-1}\}$, and $a^k = e$ iff $d|k$.*

3. $\mathrm{ord}(a) = |\ a^{\mathbb{Z}}|$.

Proof. 1. According to 2.23 it suffices to show $\ker(\varphi_a) = \{0\}$. Therefore let $n \in \ker(\varphi_a)$, i.e. $a^n = e$. Since $a^n = e \Leftrightarrow a^{-n} = e$, we may assume $n \geq 0$. But if $\mathrm{ord}(a) = \infty$ this is possible only with $n = 0$.
2. If $\mathrm{ord}(a) = d < \infty$, we even have $\ker(\varphi_a) = \mathbb{Z}d$: The inclusion $\supset$ is obvious; if on the other hand $a^n = e$, write $n = qd + r, 0 \leq r < d$, whence $e = a^n = (a^d)^q a^r = a^r$. But by the choice of d that implies $r = 0$ resp. $n \in \mathbb{Z}d$. Since $\exp(2\pi i\frac{k}{d}) = \exp(2\pi i\frac{\ell}{d})$ iff $d|(\ell - k)$ iff $\ell - k \in \ker(\varphi_a)$ iff $a^k = a^\ell$, the map $\exp(2\pi i\frac{k}{d}) \mapsto a^k$ is both well defined and injective, while the surjectivity is immediate.
3. follows immediately from *1.* and *2.* □

Corollary 2.38. Theorem of Lagrange (Joseph Louis Lagrange, 1736 - 1813) *Let G be a finite group. Then the order* $\mathrm{ord}(a)$ *of any element $a \in G$ divides the group order $|G|$, or with other words*

$$a^{|G|} = e$$

holds for all $a \in G$.

Proof. Since G is finite, every element $a \in G$ has finite order:
$\mathrm{ord}(a) = |a^{\mathbb{Z}}| = d < \infty$. On the other hand according to 2.28.*3.* the order of the subgroup $a^{\mathbb{Z}} \leq G$ divides $|G|$. □

Problems 2.39.

1. R: Let G be a group and $a, b \in G$ elements of order $m, n \in \mathbb{N}$ respectively. Show that $\mathrm{ord}(a^k) = m/\gcd(k, m)$ and $\mathrm{ord}(ab) = mn$, if $ab = ba$ and the numbers m, n are relatively prime.
2. R: Let $f \in \mathbb{S}_n$ be a permutation. Given a factorization of f as product of pairwise disjoint cycles determine the order of f!
3. Let $G := \bigcup_{n=1}^{\infty} C_{2^n}$. Show: The group G is not finitely generated, cf. Problem 2.6.9, but every proper subgroup is cyclic (and thus finitely generated), namely coincides with some C_{2^n}.
4. R: Show: The direct product $G \times H$ of two nontrivial cyclic groups is again cyclic, iff both G and H are finite and their orders are relatively prime.
5. Let p be a prime number. Show that $\mathbb{S}_p$ is generated by an arbitrary p-cycle and any transposition. Hint: Use problem 2.6.10.
6. R: Show: Every automorphism $C_n \longrightarrow C_n$ is of the form $p_k(a) = a^k$ with some $k \in \mathbb{Z}, \gcd(k, n) = 1$. When does $p_k = p_\ell$ hold? Hint: 2.39.1.
7. R: Let p be a prime number. Show that a group of order p^2 is isomorphic either to C_{p^2} or to $C_p \times C_p$! Hint: Corollary 2.32.

2.5 Factor Groups

Having discussed cyclic groups as the most basic non-trivial groups one can attack the problem of classification of (finite) groups by trying to decompose a given group into smaller pieces. If for example $H \subset G$ is a subgroup of the group G, one could look at H and the set G/H of all left cosets mod H. But is G/H again a group? If so, one would expect the quotient map $\varrho : G \longrightarrow G/H, a \mapsto aH$, to be a group homomorphism. That means nothing but:

$$aH \cdot bH = abH,$$

and it looks like we have succeeded in making G/H a group, taking the RHS as a definition of the LHS. But unfortunately, there is the following problem: The elements a and b are by no means distinguished representatives of the cosets aH and bH, and we have to show that the right hand side depends only on aH and bH as sets (and not on the way to write them), i.e. does not change if we replace a and b with other representatives $\tilde{a} = ah_1$ and $\tilde{b} = bh_2$, where $h_1, h_2 \in H$.

On the other hand if in some given situation the above definition works, then the subgroup $H \subset G$ is the kernel of the group homomorphism $\varrho : G \longrightarrow G/H$, and subgroups realized as the kernel of a suitable group homomorphism turn out to be "normal":

Definition 2.40. *A subgroup H of a group G is called* **normal** *if it is invariant under conjugation, i.e. if for all $a \in G$ we have*

$$\kappa_a(H) = aHa^{-1} = \{aha^{-1}; h \in H\} \subset H \ .$$

In that case we also write

$$H \trianglelefteq G.$$

Remark 2.41.

1. For a normal subgroup $H \trianglelefteq G$, the above condition is satisfied for all $a \in G$, in particular also for a^{-1}, i.e.

   $$a^{-1}H(a^{-1})^{-1} = a^{-1}Ha \subset H \Longleftrightarrow H \subset aHa^{-1}.$$

   Hence we could also have required $aHa^{-1} = H$ for all $a \in G$, but the given condition is a priori easier to check.

2. Since $aHa^{-1} = H$ is equivalent to $aH = Ha$, for a normal subgroup left and right cosets coincide. In particular $G/H = H\backslash G$ for a normal subgroup $H \subset G$.

3. Let us emphasize that for normality we do not require $aha^{-1} = h, \forall h \in H, \forall a \in G$. If H satisfies that condition, it is of course normal, but not vice versa.

Example 2.42. 1. Let $h := (1,2,3), g := (1,2) \in \mathbb{S}_3$. Then $h^{\mathbb{Z}} \trianglelefteq \mathbb{S}_3$ is normal, but $g^{\mathbb{Z}} \leq \mathbb{S}_3$ is not.

2. In an abelian group every subgroup is normal.

3. The center $Z(G) \leq G$ of a group G is a normal subgroup.

4. A subgroup $H \leq G$ of index $(G : H) = 2$ is normal, since for $a \in G \setminus H$ we have $aH = G \setminus eH = G \setminus He = Ha$.

5. The kernel $\ker(\varphi)$ of a group homomorphism $\varphi : G \longrightarrow F$ is a normal subgroup, since $h \in \ker(\varphi) \Longrightarrow \varphi(aha^{-1}) = \varphi(a)\varphi(h)\varphi(a^{-1}) = \varphi(a)e\varphi(a)^{-1} = e$, i.e. $aha^{-1} \in \ker(\varphi)$.

6. Note that $F \trianglelefteq H \trianglelefteq G$ does not imply $F \trianglelefteq G$. For example consider $G = D_4$. We have $H := \{E, R^2 = -E, S, SR^2 = -S\} \trianglelefteq G$, but $F = S^{\mathbb{Z}} = \{E, S\} \trianglelefteq H$ is not a normal subgroup of D_4, since $RSR^{-1} = R^2S = -S$.

Hence H has to be a normal subgroup, in order to have on G/H a natural group structure. Luckily that is the only condition needed:

Proposition 2.43. *If H is a normal subgroup of the group G, then*

$$aH \cdot bH := abH$$

defines a group multiplication on G/H, and the coset map $\varrho : G \longrightarrow G/H, a \mapsto aH$ becomes a group homomorphism.

Proof. It is sufficient to show that the group multiplication is well defined, i.e. does not depend on choices of representatives. So let $\tilde{a} := ah_1, \tilde{b} := bh_2$ with elements $h_i \in H$. Then we have

$$\tilde{a}\tilde{b} = ah_1bh_2 = ab(b^{-1}h_1b)h_2 = abh$$

with $h = (b^{-1}h_1b)h_2 \in H$, since H is normal. With other words $\tilde{a}\tilde{b}H = abH$. □

Definition 2.44. *If H is a normal subgroup of the group G, then the (left) coset space G/H with the multiplication*

$$aH \cdot bH := abH$$

is called the factor group of G with respect to (or mod(ulo)) H.

Proposition 2.45. *Let $\varphi : G \longrightarrow F$ be a group homomorphism and $H \leq \ker(\varphi)$ a normal subgroup of G. Then there is a unique homomorphism $\overline{\varphi} : G/H \longrightarrow F$ with $\varphi = \overline{\varphi} \circ \varrho$, where $\varrho : G \longrightarrow G/H$ is the coset map.*
We have $\ker(\overline{\varphi}) = \ker(\varphi)/H$. In particular, if $\varphi : G \longrightarrow F$ is surjective, $\overline{\varphi} : G/\ker(\varphi) \longrightarrow F$ is a group isomorphism: $G/\ker(\varphi) \cong F$.

We leave the proof as an exercise to the reader.

Notation: If it is clear from the context which groups G and H are involved, we usually write $\overline{a}$ instead of aH.

Example 2.46. 1. For $G := \mathbb{Z}$ and $H := \mathbb{Z}n$ we write

$$\mathbb{Z}_n := \mathbb{Z}/\mathbb{Z}n$$

additively, i.e.

$$\mathbb{Z}_n = \left\{\overline{0} = \mathbb{Z}n = 0 + \mathbb{Z}n, \overline{1} = 1 + \mathbb{Z}n, .., \overline{n-1} = (n-1) + \mathbb{Z}n\right\} .$$

2. Let G be a group, $a \in G$ an element of order $\mathrm{ord}(a) = d < \infty$. Then the homomorphism $\varphi_a : \mathbb{Z} \longrightarrow G, n \mapsto a^n$, has the kernel $\ker(\varphi_a) = \mathbb{Z}d$ and we obtain an isomorphy $\mathbb{Z}_d \cong a^{\mathbb{Z}}$ with the isomorphism $\mathbb{Z}_d \ni \overline{k} \mapsto a^k$.
   In particular with $G = C_d, a = \exp(\frac{2\pi i}{d})$ we find $\mathbb{Z}_d \cong C_d$.

3. The homomorphism $\exp : \mathbb{R} \longrightarrow \mathbf{S}^1, \vartheta \mapsto e^{2\pi i\vartheta}$, induces an isomorphism $\mathbb{R}/\mathbb{Z} \cong \mathbf{S}^1$.

4. The homomorphism $\mathrm{sign} : \mathbb{S}_n \longrightarrow \mathbb{Q}^*$ induces an isomorphism $\mathbb{S}_n/\mathbb{A}_n \cong \mathrm{sign}(\mathbb{S}_n) = C_2 \cong \mathbb{Z}_2$.

Corollary 2.47. *Let G be a group and $E, H \trianglelefteq G$ normal subgroups of G and $E \subset H$. Then H/E is a normal subgroup of G/E, and there is a natural isomorphism*

$$\frac{G/E}{H/E} \xrightarrow{\cong} G/H,\ aE(H/E) \mapsto aH.$$

Proof. The kernel of the coset map $G \longrightarrow G/H$ contains $E \subset G$, hence, according to 2.45, factors through a unique surjective group homomorphism $G/E \longrightarrow G/H$, the kernel of which is $H/E \subset G/E$. Now apply once again 2.45. □

Returning to our motivation in the beginning of this section we ask whether a group G can be reconstructed from a normal subgroup $H \trianglelefteq G$ and the factor group G/H. Unfortunately the answer is no: For $H = C_2 \trianglelefteq G = C_4$ and $\tilde{H} = C_2 \times \{1\} \trianglelefteq \tilde{G} = C_2 \times C_2$ we have $\tilde{H} \cong H$ and $\tilde{G}/\tilde{H} \cong G/H$, but $\tilde{G} \ncong G$. In order to avoid such counterexamples let us assume that $H \trianglelefteq G$ admits a complementary subgroup $F \leq G$, i.e. such that the composition

$$F \hookrightarrow G \longrightarrow G/H$$

of the inclusion $F \hookrightarrow G$ and the coset map $G \longrightarrow G/H$ is an isomorphism. Then the map

$$H \times F \longrightarrow G, (h, f) \mapsto hf$$

is bijective, but unfortunately only a group homomorphism if $fh = hf$ holds for all $f \in F, h \in H$.

For example take $G := \mathbb{S}_3$ and $H := h^{\mathbb{Z}} \cong \mathbb{Z}_3, F := g^{\mathbb{Z}} \cong \mathbb{Z}_2$ with the 3-cycle $h := (1, 2, 3)$ and the transposition $g := (1, 2)$. Then $G \ncong H \times F$, since $H \times F \cong C_3 \times C_2 \cong C_6$ is abelian. In fact, the information lost when passing from G to $H, G/H$ is the way how the complementary subgroup $F \subset G$ acts on the normal subgroup H by conjugation, i.e. the homomorphism

$$\sigma : F \longrightarrow \mathrm{Aut}(H), f \mapsto \kappa_f|_H \quad .$$

If $\sigma \equiv \mathrm{id}_H$, then $G \cong H \times F$. Otherwise we can reconstruct G from H, F and σ as follows:

Definition 2.48. *Let F, H be groups and $\sigma : F \longrightarrow \mathrm{Aut}(H), f \mapsto \sigma_f := \sigma(f)$ a group homomorphism. Then the group*

$$H \times_\sigma F := (H \times F, \mu := \mu_\sigma), \text{ where } \mu_\sigma((h, f), (h', f')) := (h\sigma_f(h'), ff')$$

is called the **semidirect product** *of H and F with respect to the homomorphism σ.*

So the underlying set of a semidirect product is in any case the cartesian product, but the group multiplication is the componentwise multiplication only if $\sigma : F \longrightarrow \mathrm{Aut}(H)$ is the trivial homomorphism: $\sigma_f = \mathrm{id}_H$ for all $f \in F$.

The proof that μ really is a group multiplication is left to the reader.

Remark 2.49. 1. The sets $H \times \{e\}$ and $\{e\} \times F$ are subgroups of $H \times_\sigma F$ isomorphic to H resp. F, and $H \times \{e\}$ is normal; furthermore

$$F \cong \{e\} \times F \hookrightarrow H \times_\sigma F \longrightarrow (H \times_\sigma F)/(H \times \{e\})$$

is an isomorphism.

2. Let G be a group and $F, H \subset G$ subgroups, H normal. If the restriction $\varrho|_F : F \longrightarrow G/H$ of the coset map $\varrho : G \longrightarrow G/H$ is an isomorphism and we take $\sigma : F \longrightarrow \mathrm{Aut}(H)$ with $\sigma_f := \kappa_f|_H : H \longrightarrow H, h \mapsto fhf^{-1}$, then

$$H \times_\sigma F \xrightarrow{\cong} G,\ (h, f) \mapsto hf$$

is a group isomorphism.

3. Let us now consider the case that G/H is cyclic: $G/H = \overline{a}^{\mathbb{Z}}$. Take $F := a^{\mathbb{Z}} \cong \mathbb{Z}_n$, i.e. $n = 0$, if $\mathrm{ord}(a) = \infty$ and $n = \mathrm{ord}(a)$ otherwise (where $\mathbb{Z}_0 \cong \mathbb{Z}$). Define $d \in \mathbb{N}$ by $H \cap F = (a^d)^{\mathbb{Z}}$, where we may assume that $d|n$. The homomorphism $\sigma : F \longrightarrow \mathrm{Aut}(H)$ is defined by $\sigma_{a^\ell} := (\kappa_a|_H)^\ell$ with the restriction $\kappa_a|_H : H \longrightarrow H$ of the conjugation. We remark that $\kappa_a^n = \kappa_{a^n} = \mathrm{id}_H$ as well as $\kappa_a(a^d) = a^d$. Finally we obtain an isomorphism

$$(H \times_\sigma F)/(a^{-d}, a^d)^{\mathbb{Z}} \xrightarrow{\cong} G,\ \overline{(h, a^\ell)} \mapsto ha^\ell.$$

The corresponding abstract construction starts with a group H, natural numbers $d, n \in \mathbb{N}$ with $d|n$ and a group isomorphism $\psi : H \longrightarrow H$ (playing the rôle of $\kappa_a|_H$), such that $\psi^n = \mathrm{id}_H$, furthermore an element $h_0 \in H$ (corresponding to $a^d \in H$) with $\psi(h_0) = h_0$. The rôle of F is played by the (additive) group $\mathbb{Z}_n$. Let now $\sigma : \mathbb{Z}_n \longrightarrow \mathrm{Aut}(H)$ be the homomorphism with $\sigma_{\overline{k}} = \psi^k$. The cyclic subgroup $(h_0^{-1}, \overline{d})^{\mathbb{Z}} \leq (H \times_\sigma \mathbb{Z}_n)$ is normal, and the group we associate to these data is

$$(H \times_\sigma \mathbb{Z}_n)/(h_0^{-1}, \overline{d})^{\mathbb{Z}}\ .$$

Example 2.50. 1. Let $H := C_3$ and $F := \mathbb{Z}_2$. The automorphism group $\mathrm{Aut}(C_3)$ consists of two maps, the power maps $p_1 = \mathrm{id}_{C_3}$ and p_{-1} (remember that $p_n(a) := a^n$), hence there are two possibilities for $\sigma : \mathbb{Z}_2 \longrightarrow \mathrm{Aut}(C_3)$: Either $\sigma_{\overline{1}} = \mathrm{id}_{C_3} = p_1$ or $\sigma_{\overline{1}} = p_{-1} : C_3 \longrightarrow C_3$. In the first case we obtain the direct product $C_3 \times \mathbb{Z}_2 \cong C_3 \times C_2 \cong C_6$, while in the second case we get $C_3 \times_\sigma \mathbb{Z}_2 \cong \mathbb{S}_3$.

2. We consider the quaternion group Q, with $H := I^{\mathbb{Z}} \cong C_4, F := J^{\mathbb{Z}} \cong C_4 \cong \mathbb{Z}_4$. We find $F \cap H = (-E)^{\mathbb{Z}} = (J^2)^{\mathbb{Z}}$ and thus $n = 4, d = 2$ with $\psi = p_{-1}$ and $a = J,\ h_0 = a^2 = -E$. So the abstract construction is

$$Q \cong (C_4 \times_\sigma \mathbb{Z}_4)/(-1, \overline{2})^{\mathbb{Z}} \ ,$$

where $\sigma : \mathbb{Z}_4 \longrightarrow \mathrm{Aut}(C_4)$ is determined by $\sigma_{\overline{1}} = \psi = p_{-1}$ and $h_0 = -1 \in C_4$.

2.5.1 Digression: Free Groups

In this section we present a method how to describe infinite groups in a concise way. Indeed, it is even useful for finite groups, since in general it is not very economic to write down a complete multiplication table. First of all we need the notion of a set ("system") of generators of a group G:

Definition 2.51. Let G be a group, $M \subset G$ a subset. Then the intersection of all subgroups $H \leq G$ containing M, i.e.

$$\langle M \rangle := \bigcap_{M \subset H \leq G} H,$$

is called the subgroup of G generated by the subset M. If $G = \langle M \rangle$, the set $M \subset G$ is also called a system of generators for the group G.

Remark 2.52. The subgroup $\langle M \rangle \leq G$ generated by a subset $M \subset G$ admits also an explicit description:

$$\langle M \rangle = \{a_1^{n_1} \cdot \ldots \cdot a_r^{n_r}; a_1, \ldots, a_r \in M, r \in \mathbb{N}_{>0}, n_1, \ldots, n_r \in \mathbb{Z}\},$$

the right hand side being a subgroup contained in any subgroup $H \leq G$ containing M.

Notation: If $M = \{c_1, ..., c_s\}$ we often simply write

$$\langle c_1, ..., c_s \rangle := \langle \{c_1, ..., c_s\} \rangle.$$

Example 2.53. 1. A group admits a generator system with only one element iff it is cyclic.

2. $\mathbb{Z} = \langle 1 \rangle = \langle 2, 3 \rangle$, so distinct minimal generator systems (a generator system which can not be shrinked) may have different cardinalities!

3. The cyclic group C_n of all n-th roots of unity is generated by $e^{2\pi i/n}$, i.e.

$$C_n = \langle e^{2\pi i/n} \rangle.$$

4. The dihedral group D_n satisfies

$$D_n = \langle R, S \rangle$$

with the counterclockwise rotation $R(z) = e^{2\pi i/n} z$ and the reflection $S(z) = \overline{z}$ at the real axis.

5. The quaternion group Q satisfies

$$Q = \langle I, J \rangle.$$

6. The symmetric group $\mathbb{S}_n$ satisfies

$$\mathbb{S}_n = \langle T \rangle,$$

where $T := \{(i, j); 1 \leq i < j \leq n\}$ is the set of all transpositions.

7. Commutator subgroup $C(G) \leq G$: If G is any group and

$$M := \{aba^{-1}b^{-1}; a, b \in G\},$$

the subgroup $C(G) := \langle M \rangle$ is called the commutator subgroup. It is a "characteristic subgroup" of G, i.e. invariant under every automorphism $\sigma : G \longrightarrow G$: $\sigma(C(G)) = C(G)$. So in particular it is a normal subgroup: $C(G) \trianglelefteq G$.

In order to describe a group G one often finds the following: A system $M \subset G$ of generators is specified together with a set of relations, i.e. a number of equalities

$$L_i = R_i, i = 1, ..., s,$$

where both L_i and R_i are products of elements and inverses of elements of the system M of generators.

Example 2.54. 1. A finite group $G = \langle a, b\rangle$ with $\langle a\rangle \trianglelefteq G$ can be characterized by the relations

$$a^n = e,$$

where n denotes the order of $a \in G$,

$$b^m = a^r,$$

where m is the order of $\overline{b} \in G/\langle a\rangle$, and the conjugation relation

$$bab^{-1} = a^s.$$

In particular:

2. For the dihedral group $D_n = \langle R, S\rangle$ we have the relations

$$R^n = E,\ S^2 = E,\ SRS^{-1} = R^{-1}.$$

3. For the quaternion group $Q = \langle I, J\rangle$ a possible set of relations is

$$I^4 = E,\ J^2 = I^2,\ JIJ^{-1} = I^3.$$

We want to explain what people mean with such a description: First we should understand the case, where there are no relations at all: Such a system of generators is called free:

Definition 2.55. *A system of generators $M \subset F$ of a group F is called free, if the pair (F, M) satisfies the following "universal mapping property": Given any map $\varphi : M \longrightarrow G$ into a group G, there is a unique group homomorphism $\hat{\varphi} : F \longrightarrow G$ extending φ, i.e. $\hat{\varphi}|_M = \varphi$. A group F is called free if it admits a free system of generators.*

Example 2.56. 1. The trivial group $F = \{e\}$ is free: Take $M = \emptyset$.

2. The additive group $\mathbb{Z}$ of integers is free: Take $M = \{1\}$.

3. A free generator system M of a commutative group F is either empty or contains one element: If $M = \{a, b, ...\}$ is a free generator system of an abelian group F with $a \neq b$ and $g, h \in G$ arbitrary elements in some group G, there is a group homomorphism $\hat{\varphi} : F \longrightarrow G$ with $\hat{\varphi}(a) = g, \hat{\varphi}(b) = h$. But then $ab = ba$ implies $gh = hg$, so we could conclude that any group is abelian!

4. The elements of a free system of generators M have infinite order (hence the trivial group is the only free finite group!). If $a \in M$, there is a group homomorphism $\hat{\varphi} : F \longrightarrow \mathbb{R}^*$ with $\hat{\varphi}(a) = 2$. Since $2 \in \mathbb{R}^*$ has infinite order, the element $a \in F$ has as well.

Hence given a set M with more than one element, it is not at all clear whether there is a group $F \supset M$ freely generated by M, but if it exists, it is unique up to isomorphy:

Remark 2.57. Let $F_i \supset M$ be groups freely generated by M for $i = 1, 2$ and $\varphi_i : M \hookrightarrow F_i$ the inclusion. Then $\hat{\varphi}_2 : F_1 \longrightarrow F_2$ is an isomorphism. In order to see that we apply the universal mapping property for (F_2, M) to the inclusion $\varphi_1 : M \hookrightarrow F_1$ and obtain the extension $\hat{\varphi}_1 : F_2 \longrightarrow F_1$. Since both $\hat{\varphi}_1 \circ \hat{\varphi}_2$ and id_{F_1} extend the identity id_M, we get $\hat{\varphi}_1 \circ \hat{\varphi}_2 = \mathrm{id}_{F_1}$, and in the same way, $\hat{\varphi}_2 \circ \hat{\varphi}_1 = \mathrm{id}_{F_2}$.

Fortunately we have:

Proposition 2.58. *For every set M there is a group $F(M) \supset M$ freely generated by M. Indeed any element $g \in F \setminus \{e\}$ has a unique representation*

$$g = a_1^{n_1} \cdot ... \cdot a_r^{n_r},$$

where $r \in \mathbb{N}_{>0}, a_1, ..., a_r \in M$, the exponents are nonzero: $n_1, ..., n_r \in \mathbb{Z} \setminus \{0\}$ and immediate neighbours are different: $a_{i+1} \neq a_i$ for $1 \leq i < r$.

Before we prove the proposition we come back to our original problem. Consider any group G with a system of generators $M \subset G$. Denote $\iota : M \longrightarrow G$ the inclusion. Then the group homomorphism

$$\widehat{\iota} \colon F(M) \longrightarrow G$$

is onto, hence $G \cong F(M)/H$ with the normal subgroup $H := \ker(\widehat{\iota})$. Thus in order to describe G up to isomorphy it suffices to determine a system of generators for the subgroup H. But since $H \trianglelefteq G$ is a normal subgroup it is enough to give a system of generators of H as a normal subgroup: Given a subset $\mathfrak{R} \subset F(M)$ we denote $N(\mathfrak{R}) \trianglelefteq F(M)$ the smallest normal subgroup of $F(M)$ containing $\mathfrak{R}$; in fact

$$N(\mathfrak{R}) = \bigcap_{\mathfrak{R} \subset N \trianglelefteq F(M)} N \ .$$

Or equivalently, $N(\mathfrak{R})$ is the subgroup generated by

$$\kappa_{F(M)}(\mathfrak{R}) := \bigcup_{g \in F(M)} \kappa_g(\mathfrak{R}),$$

where $\kappa_g : F(M) \longrightarrow F(M), x \mapsto gxg^{-1}$, denotes the conjugation with g.

Hence in order to describe a group G completely one gives a set $M \subset G$ of generators and a set $\mathfrak{R} \subset F(M)$, such that $H = N(\mathfrak{R})$ respectively

$$G \cong F(M)/N(\mathfrak{R}) \ .$$

The elements in $\mathfrak{R}$ then correspond to relations $L_i = R_i$ with the right hand side $R_i = e$.

On the other hand, if it is said that a group G is generated by M with relations $L_i = R_i, i = 1, ..., s$, one means that the natural map $F(M) \longrightarrow G$ has kernel $N(\mathfrak{R})$ with

$$\mathfrak{R} = \{L_i R_i^{-1}, i = 1, ..., s\},$$

where L_i, R_i are understood as elements in $F(M)$. Of course $\mathfrak{R} = \{R_i^{-1} L_i, i = 1, ..., s\}$ or $\mathfrak{R} = \{L_i^{-1} R_i, i = 1, ..., s\}$ etc. are possible choices as well.

Example 2.59. 1. For the generator system $M = \{R, S\}$ of the dihedral group D_n we may take

$$\mathfrak{R} := \{R^n, S^2, SRSR\} \subset F(M).$$

In order to see that, we consider the surjective group homomorphism $F(M) \longrightarrow D_n$; it factors through $F(M)/N(\mathfrak{R})$. Hence it is sufficient to show that $F(M)/N(\mathfrak{R})$ has at most order $2n = |D_n|$; and this we leave as an exercise for the reader.

2. For the generator system $M = \{I, J\}$ of the quaternion group Q we may take
$$\mathfrak{R} = \{I^4, I^2J^2, JIJ^{-1}I\} \subset F(M).$$

Proof of Proposition 2.58. We take a second (with M disjoint) copy M^{-1} of the set M, the elements being denoted $b^{-1}, b \in M$ (this is nothing but a notation). Thus there is a bijection
$$M \longrightarrow M^{-1}, b \mapsto b^{-1}$$
with the inverse
$$M^{-1} \longrightarrow M, c = b^{-1} \mapsto c^{-1} := b.$$
Hence, if $A := M \cup M^{-1}$, then $A \longrightarrow A, a \mapsto a^{-1}$ is a permutation of A interchanging M and M^{-1}. Set
$$W(A) := \{e, (a_1, ..., a_r); a_1, ..., a_r \in A, r \in \mathbb{N}_{>0}\},$$
so the elements in $W(A)$ are finite sequences, whose elements belong to A (they are also called "words" in the "alphabet" A), and e denotes the empty sequence (word). Words can be composed by concatenation and be simplified: A simplification step looks as follows
$$\mathbf{u} = (a_1, ..., a_{i-1}, a, a^{-1}, a_{i+2}, ..., a_r) \longrightarrow \mathbf{u}' = (a_1, ..., a_{i-1}, a_{i+2}, ..., a_r)$$
with $\mathbf{u}' = e$ for $\mathbf{u} = (a, a^{-1})$. Call a word $\mathbf{u} = (a_1, ..., a_r)$ reduced if it can not be simplified to a shorter word, i.e. if $a_{i+1} \neq a_i^{-1}$ for $i = 1, ..., r-1$. Denote $RW(A) \subset W(A)$ the subset of all reduced words.

It is clear that any word $\mathbf{u} \in W(A)$ can be transformed into a reduced word $\mathbf{u}_0 \in RW(A)$ by a finite number of simplifications. Indeed, the resulting reduced word depends only on $\mathbf{u}$ and not on the simplification steps applied:

Lemma 2.60. *Let $\mathbf{u} \in W(A)$ be a word. Then there is a unique reduced word $\mathbf{u}_0 \in RW(A)$, such that $\mathbf{u}_0$ is the outcome of any iterated simplification procedure leading from $\mathbf{u}$ to a reduced word.*

Let us now derive our claim from Lemma 2.60. Set $F(M) := RW(A)$ with the group law:
$$F(M) \times F(M) \longrightarrow F(M), (\mathbf{u}, \mathbf{v}) \mapsto (\mathbf{uv})_0,$$

where $\mathbf{uv}$ denotes the concatenation of the words $\mathbf{u}, \mathbf{v}$. The neutral element is the empty word e, the element $\mathbf{u} = (a_1, ..., a_r)$ has the inverse $(a_r^{-1}, ..., a_1^{-1})$. Finally associativity is obtained as follows:

$$((\mathbf{uv})_0\mathbf{w})_0 = (\mathbf{uvw})_0 = (\mathbf{u}(\mathbf{vw})_0)_0.$$

Namely: The left hand side is obtained from $\mathbf{uvw}$ by simplifying first to $(\mathbf{uv})_0\mathbf{w}$ and then to the reduced word $((\mathbf{wv})_0\mathbf{u})_0$. Now Lemma 2.60 gives the first equality; the second one follows with an analogous argument.

Identify $A = M \cup M^{-1}$ with the one letter words in $F(M) = RW(A)$. Now given a map $\varphi : M \longrightarrow G$ extend it first to $\psi : A \longrightarrow G$ by setting $\psi(a^{-1}) := \varphi(a)^{-1}$ and then to $\hat{\psi} : W(A) \longrightarrow G$ with

$$\hat{\psi}((a_1, ..., a_r)) := \psi(a_1) \cdot ... \cdot \psi(a_r), \psi(e) = e_G$$

where $(a_1, ..., a_r)$ is any word. Obviously $\hat{\psi}(\mathbf{uv}) = \hat{\psi}(\mathbf{u})\hat{\psi}(\mathbf{v})$ and $\hat{\psi}(\mathbf{w}_0) = \hat{\psi}(\mathbf{w})$. It follows immediately that $\hat{\varphi} := \hat{\psi}|_{RW(A)} : F(M) = RW(A) \longrightarrow G$ is a group homomorphism. □

Proof of Lemma 2.60. We do induction on the length of the word $\mathbf{u}$. Assume the word $\mathbf{u}$ may be reduced to the reduced words $\mathbf{u}_1$ and $\mathbf{u}_2$. If $\mathbf{u}$ itself is reduced, we obviously have $\mathbf{u}_1 = \mathbf{u} = \mathbf{u}_2$. Otherwise denote $\mathbf{v}_i$ the result of the first simplification on the way from $\mathbf{u}$ to $\mathbf{u}_i$. If $\mathbf{v}_1 = \mathbf{v}_2 =: \mathbf{v}$, we may apply the induction hypothesis to $\mathbf{v}$ and obtain $\mathbf{u}_1 = \mathbf{u}_2$. Otherwise $\mathbf{u} = (a_1, ..., a_r)$ and $\mathbf{v}_1 = (a_1, ..., a_{i-1}, a_{i+2}, ..., a_r), \mathbf{v}_2 = (a_1, ..., a_{j-1}, a_{j+2}, ..., a_r)$, where we may assume $i \leq j$. Since $j = i, i+1$ gives $\mathbf{v}_1 = \mathbf{v}_2$, we have $i + 2 \leq j$, and then $\mathbf{v} := (a_1, ..., a_{i-1}, a_{i+2}, ..., a_{j-1}, a_{j+2}, ..., a_r)$ for $j > i + 2$ resp. $\mathbf{v} := (a_1, ..., a_{i-1}, a_{j+2}, ..., a_r)$ for $j = i + 2$ is both a simplification of $\mathbf{v}_1$ and $\mathbf{v}_2$.

But $\mathbf{v}_i$ being shorter than $\mathbf{u}$ has according to the induction hypothesis $\mathbf{u}_i$ as its unique reduction. Since we can obtain it via an iterated simplification procedure through $\mathbf{v}$, we have $\mathbf{u}_1 = \mathbf{u}_2$.

Remark 2.61. It is not difficult to see that $F(M) \cong F(N)$ implies $|M| = |N|$. A more surprising fact is, that any subgroup $H \leq F(M)$ of a free group again is free, i.e. $H \cong F(N)$ with some set N, but that not necessarily $|N| \leq |M|$, if $|M| \geq 2$.

□

Problems 2.62. 1. R: Show: $\mathbb{C}/\mathbb{Z} \cong \mathbb{C}^* \ncong \mathbb{C}$.

2. R: Determine all groups of order 6.

3. R: Determine all non-commutative groups of order 8.

4. R: Let $H \subset \mathbb{S}_4$ be the subgroup consisting of the identity and the products of two disjoint 2-cycles. Show: $H \subset \mathbb{S}_4$ is a normal subgroup and $\mathbb{S}_4/H \cong \mathbb{S}_3$. Hint: $\mathbb{S}_3 \cap H = \{\mathrm{id}\}$.

5. Let $\mathrm{Aff}_n(\mathbb{R}) := \{f \in \mathbb{S}(\mathbb{R}^n); f(x) = Ax + b \text{ with } A \in GL_n(\mathbb{R}), b \in \mathbb{R}^n\}$ be the affine linear group, cf. problem 2.6.3. Show: The subgroup $T := \{\tau_b; b \in \mathbb{R}^n\}$ (where $\tau_b(x) = x + b$ is the translation with the vector $b \in \mathbb{R}^n$) is normal. Determine a homomorphism $\sigma : GL_n(\mathbb{R}) \longrightarrow \mathrm{Aut}(\mathbb{R}^n)$, such that $\mathrm{Aff}_n(\mathbb{R}) \cong \mathbb{R}^n \times_\sigma GL_n(\mathbb{R})$! Is $GL_n(\mathbb{R}) \leq \mathrm{Aff}_n(\mathbb{R})$ a normal subgroup?

6. R: We define on $\mathbb{Z}_n^* := \{\overline{a} \in \mathbb{Z}_n; \gcd(a, n) = 1\ \}$ a group structure: $\overline{a} \cdot \overline{b} := \overline{ab}$. Show that this defines a group multiplication, and that $\mathbb{Z}_n^* \longrightarrow \mathrm{Aut}(C_n), \overline{k} \mapsto p_k : C_n \longrightarrow C_n$ with $p_k(\eta) = \eta^k$ is a group isomorphism. Hint: Problem 2.39.6. If we replace C_n with the isomorphic group $\mathbb{Z}_n$, what does the corresponding automorphism look like?

7. Let p be a prime number. Give an example of a non-abelian group of order p^3. Hint: Consider semidirect products $\mathbb{Z}_{p^2} \times_\sigma \mathbb{Z}_p$ and use the previous problem.

8. Let p be a prime, $n \in \mathbb{N}_{>0}$. Show that

$$U(p^n) := \{\overline{1 + kp} \in \mathbb{Z}_{p^n}^*;\ k \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Z}_{p^n}^*$ of order p^{n-1}, and that $U(p^n)$ is cyclic for $p > 2$, more precisely $U(p^n) = \overline{1 + rp}^{\mathbb{Z}}$ for any $r \notin \mathbb{Z}p$.

9. Show: The permutations $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ of the form $f(\overline{x}) = k\overline{x} + \overline{b}$, where $k \in \mathbb{Z}$ and $\gcd(k, n) = 1$ as well as $\overline{b} \in \mathbb{Z}_n$ constitute a subgroup of $\mathbb{S}(\mathbb{Z}_n)$. Show that it is a semidirect product $\mathbb{Z}_n \times_\sigma \mathbb{Z}_n^*$! Cf. with problem 2.62.6 and the group $\mathrm{Aff}_1(\mathbb{R})$ in problem 2.62.5.

10. Let $\sigma, \tilde{\sigma} : F \longrightarrow \mathrm{Aut}(H)$ be group homomorphisms. Assume there are automorphisms $\psi : F \longrightarrow F$ and $\varphi : H \longrightarrow H$, such that $\tilde{\sigma}_f = \varphi\sigma_{\psi(f)}\varphi^{-1}$ for all $f \in F$. Show: $H \times_{\tilde{\sigma}} F \cong H \times_\sigma F$.

11. Assume $G = \langle a \rangle$ with the relations $a^n = e, a^m = e$, where $n, m \in \mathbb{N}_{>0}$. Compute $|G|$!

12. Let $n, m, r \in \mathbb{N}_{>0}$ and $G = \langle a, b \rangle$ be the group generated by the two elements a, b with the relations $a^n = e = b^m, ba = a^r b$, where $n, m, r \in \mathbb{N}_{>0}$. Show $|G| \leq nm$ with equality iff $r^m \equiv 1 \mod (n)$. Compute the order of a and b as well as $|G|$ in the general case!

    Hint: $\langle a \rangle \trianglelefteq G$ and $\langle b \rangle \longrightarrow \mathrm{Aut}(\langle a \rangle), g \mapsto \kappa_g$ is a group homomorphism.

13. Write $C_{2^\infty} := \bigcup_{n=1}^{\infty} C_{2^n}$ as a factor group $F(M)/N(\mathfrak{R})$!

14. Let M be a finite set, say $|M| = n$. Show $F(M)/C(F(M)) \cong \mathbb{Z}^n$. Use that in order to conclude: $F(M) \cong F(N) \Longrightarrow |M| = |N|$, where M, N denote finite sets.

15. Let $M := \{a, b\}$ be a set with two elements. Set

$$M_0 := \{b^k a b^{-k}; k \in \mathbb{N}\}.$$

For the subgroup $\langle M_0 \rangle \leq F(M)$ show $\langle M_0 \rangle \cong F(M_0)$.

2.6 Simple Groups and Composition Series

We motivated factor groups with the idea to break down a given group into smaller pieces. The final idea behind is that a group should somehow be composed of smallest pieces, "atomic groups":

Definition 2.63. *A group G is called* **simple** *if there are no normal subgroups of G except the trivial subgroup $\{e\}$ and the entire group G itself.*

Example 2.64. A non-trivial abelian group is simple iff it is cyclic of prime order, i.e. isomorphic to C_p (or $\mathbb{Z}_p$) for some prime number p.

Here is a series of non-commutative simple groups:

Proposition 2.65. *The alternating groups $\mathbb{A}_n$ with $n \geq 5$ are simple.*

Proof. The proof is divided into three steps:
1.) The conjugacy class $\kappa_{\mathbb{A}_n}((1,2,3))$ consists of all 3-cycles: Let (i,j,k) be any three cycle. For the permutation $g \in \mathbb{S}_n$ with $g(1) = i, g(2) = j, g(3) = k$ and $g(\ell) = \ell$ for $\ell > 3$ we have $(i,j,k) = \kappa_g((1,2,3))$. If g has sign 1 and thus $g \in \mathbb{A}_n$, we are done, otherwise replace g with $\tilde{g} := \tau \circ g \in \mathbb{A}_n$, where $\tau = (r,s)$ with two different numbers $\neq i, j, k$.
2.) The group $\mathbb{A}_n$ is generated by 3-cycles: According to Problem 2.6.7 any $f \in \mathbb{S}_n$ is a product of transpositions; if even $f \in \mathbb{A}_n$, there is an even number of such factors (transpositions having sign -1); so it will be sufficient to represent any product $\neq$ id of two transpositions as a product of 3-cycles. Consider first $f = (i,j)(k,\ell)$ with four pairwise different numbers i, j, k, ℓ. Then $f = (i,j)(j,k)(j,k)(k,\ell) = (i,j,k)(j,k,\ell)$. The second non-trivial case is $f = (i,j)(j,k)$ with three pairwise different numbers i, j, k. Then $f = (i,j,k)$ is itself a 3-cycle!
3.) Finally we show that a non-trivial normal subgroup $N \subset \mathbb{A}_n$ contains a 3-cycle. We take any $f \in N \setminus \{\mathrm{id}\}$. If it already is a 3-cycle, we are done. Otherwise we consider the elements $h := f\kappa_g(f^{-1}) \in N$ for $g \in \mathbb{A}_n$. We rewrite $f\kappa_g(f^{-1}) = \kappa_f(g)g^{-1}$ and choose g as a 3-cycle $g = (a,b,c)$, such that $\kappa_f(g) = (f(a), f(b), f(c))$. We distinguish three cases:

a) If f contains a cycle $(i,j,k,\ell,...)...(...)$ of length at least 4, we take $g=(i,j,k)$ and obtain $\kappa_f(g)=(j,k,\ell), g^{-1}=(k,j,i)$ and $h=(i,\ell,j)$.

b) If $f=(i,j,k)(\ell,m,...)...(...)$ contains a 3-cycle, we take $g=(i,j,\ell)$ and obtain $\kappa_f(g)=(j,k,m), g^{-1}=(\ell,j,i)$ and $h=(i,\ell,k,m,j)$, hence can apply the case a) with h instead of f.

c) If $f=(i,j)(k,\ell)...(...)$ contains two 2-cycles, we choose m different from i,j,k,ℓ and take $g=(i,k,m)$ and obtain $\kappa_f(g)=(j,\ell,f(m)), g^{-1}=(m,k,i)$ and then have the following possibilities for h: If $f(m)=m$, then $h=(i,j,\ell,m,k)$, so we may apply the case a) with h instead of f. Otherwise $h=(j,\ell,f(m))(m,k,i)$ and we may again apply the case b) with h instead of f. □

Remark 2.66. The classification of all finite simple groups was a great challenge; in fact, it has been completed only so late as in the early 1980-ies: There are 17 series of finite simple groups, the first one consisting of the alternating groups $\mathbb{A}_n, n\geq 5$. The remaining 16 series contain the simple groups of "Lie type": Given a finite field $\mathbb{F}$ (cf. section 4.5), their construction is analogous to that of simple real or complex Lie groups (Marius Sophus Lie, 1842 - 1899) with $\mathbb{F}$ replacing $\mathbb{R}$ resp. $\mathbb{C}$: They are realized as factor groups of subgroups of the general linear group $GL_n(\mathbb{F})$ over the finite field $\mathbb{F}$. The first of these 16 series is discussed in Theorem 4.57. Eventually, there are 26 "sporadic" simple groups, which do not fit in one of the above 17 series. For more detailed information see [3].

Now let us consider an arbitrary finite group G and study, how we can find the simple groups it is "composed" of. That is done using the notion of a "composition series":

Definition 2.67. *Let G be a group. A* **normal series** *is a finite increasing sequence of subgroups*

$$G_0=\{e\}\trianglelefteq G_1\trianglelefteq ...\trianglelefteq G_r=G \quad ,$$

i.e. G_i is a normal subgroup of G_{i+1} for $i<r$. The successive factor groups G_{i+1}/G_i for $i=0,..,r-1$ are called the **factors** *of the normal series. A* **composition series** *is a strictly increasing normal series with simple factors.*

Every finite group G admits a composition series, as one proves by induction on the group order: Choose a maximal proper normal subgroup H. Then H has by induction hypothesis such a composition series and we can extend it with G, since G/H is simple.

In fact the multiplicity of a simple group as a factor of a composition series of a given group G depends only on G itself, i.e. is independent of the actual composition series:

Proposition 2.68. Theorem of Jordan-Hölder (Camille Jordan, 1838-1922, and Otto Hölder, 1859-1937) *Let G be a finite group and $\{e\} = G_0 \subset G_1 \subset ... \subset G_r = G$ as well as $\{e\} = H_0 \subset H_1 \subset ... \subset H_s = G$ composition series. Then $s = r$ and there is a permutation $f \in \mathbb{S}_r$, such that for $j = f(i)$ we have*

$$G_i/G_{i-1} \cong H_j/H_{j-1} \ .$$

Proof. We forget about the condition that a composition series be strictly increasing and prove the statement for normal series with simple factors, but of given length - we may extend the shorter series by adding terms $\{e\}$ or G. This gives our theorem, since the trivial group then has the same multiplicity in both sequences.

Assume first $r = s = 2$. Then our composition series are of the form $\{e\} \subset E \subset G$ and $\{e\} \subset F \subset G$ with simple normal subgroups $E, F \subset G$ and simple $G/E, G/F$. If G itself is simple or $F = E$, nothing remains to be shown. Otherwise we have w.l.o.g. $E \cap F \subsetneq F$. But then, F being simple, the proper normal subgroup $E \cap F$ is trivial. Now consider the injective homomorphism $E \hookrightarrow G \longrightarrow G/F$: Its image is a normal non-trivial subgroup of G/F, since $E \subset G$ is normal, hence the entire group, i.e. $E \cong G/F$. By symmetry we have $F \cong G/E$ as well.

In the general case we consider the groups

$$G_{ij} := G_i \cap H_j \subset G$$

and composition series of length $r + s$ starting with G_{00} and ending with G_{rs} and inclusion steps

$$G_{ij} \subset G_{i+1,j} \text{ or } G_{ij} \subset G_{i,j+1}.$$

Then the composition series

$$G_{00} \subset G_{10} \subset ... \subset G_{r0} \subset G_{r1} \subset .... \subset G_{rs}$$

resp.

$$G_{00} \subset G_{01} \subset ... \subset G_{0s} \subset G_{1s} \subset .... \subset G_{rs}$$

has the same non-trivial(!) factors as $H_0 \subset H_1 \subset ... \subset H_s$ resp. $G_0 \subset G_1 \subset ... \subset G_r$, and the first one can be connected to the second one by a chain of composition series of length $r + s$, such that two successive series differ only in two successive inclusions:

$$G_{ij} \subset G_{i+1,j} \subset G_{i+1,j+1}$$

is replaced with

$$G_{ij} \subset G_{i,j+1} \subset G_{i+1,j+1}.$$

But then it is clear from our initial argument that the two successive composition series have the same simple factors taken with multiplicities. □

If all the simple factors of a finite group are cyclic, it can successively be obtained from cyclic groups using the extension procedure described in 2.49.3. Such groups are called "solvable":

Definition 2.69. *A group G is called solvable if it has a normal series with abelian factors.*

In fact we have:

Lemma 2.70. *A finite group G is solvable if and only if all its simple factors are cyclic of prime order.*

Proof. The non-trivial implication is as follows: Take a normal series with abelian factors $G_{i+1}/G_i, i = 1, ..., r-1$. For each factor of that normal series take a series with simple factors

$$\{eG_i\} = H_0^{i+1} \subset ... \subset H_{s_{i+1}}^{i+1} = G_{i+1}/G_i$$

and then refine the original normal series by inserting the subgroups $\varrho_{i+1}^{-1}(H_j^{i+1}), j = 0, ..., s_{i+1}$ for $i = 1, ..., r-1$. Here $\varrho_{i+1} : G_{i+1} \longrightarrow G_{i+1}/G_i$ denotes the coset map. As a consequence of 2.47 the simple factors of G are, counted with multiplicities, exactly the simple factors of the $G_{i+1}/G_i, i = 1, ..., r-1$. □

Remark 2.71. 1. Abelian groups are solvable.

2. A subgroup $H \subset G$ of a solvable group is solvable: A normal series $G_0 \subset ... \subset G_r$ with abelian factors for G induces a normal series $H_i := G_i \cap H \subset H$ for H with factors $H_{i+1}/H_i \hookrightarrow G_{i+1}/G_i$, i.e. the restricted sequence has abelian factors as well.

3. If H is a normal subgroup of a group G, we have: G is solvable if both, H and G/H are. That follows immediately from the fact that the simple factors of G are obtained as the union of the simple factors of H and those of G/H.

4. A group G of order $|G| < 60$ is solvable. This can be seen using the results of the next section.

We shall prove here that p-groups are solvable:

Definition 2.72. *Let p be a prime number. A group G is called a* **p-group** *if $|G| = p^r$ is a power of p.*

Proposition 2.73. *A p-group is solvable*

Proof. We use induction on $|G|$. The center $Z(G) \subset G$ is, according to Corollary 2.32 and Example 2.42.3 a non-trivial normal subgroup. Hence we may apply the induction hypothesis to $G/Z(G)$ and conclude that with $G/Z(G)$ and $Z(G)$ (the latter being abelian) also G is solvable. □

In fact, all finite groups of odd order are solvable, as conjectured 1902 by Burnside (William Burnside, 1852-1927) and proved 1963 by Feit and Thompson (Walter Feit, 1930- , John Griggs Thompson, 1932-).

Problems 2.74.
1. R: For $G = C_{pq}$ with different primes p, q determine all composition series!

2.7 Abelian Groups

In this section we present a complete classification of finite (or more generally: finitely generated) abelian groups: They are all direct products of cyclic groups. In order to have a systematic notation we shall write all groups additively, such that for example ab, a^n, e, aH is replaced with $a + b, na, 0$ and $a + H$.

An abelian group contains as a characteristic subgroup, i.e. a subgroup invariant under all automorphisms, its *torsion subgroup*:

Definition 2.75. *Let G be a group. We denote $T(G) \subset G$ the subset*

$$T(G) := \{a \in G; \mathrm{ord}(a) < \infty\}$$

consisting of all torsion elements, i.e. elements of finite order. For an abelian group $T(G) \leq G$ is a subgroup, invariant under all automorphisms. We call G torsion free if $T(G) = \{0\}$.

We remark that for nonabelian groups $T(G) \subset G$ need not be a subgroup. As one easily sees the factor group $G/T(G)$ is torsion free. So one could start the classification of abelian groups by looking for a complementary subgroup $F \leq G$, i.e. such that $F \hookrightarrow G \longrightarrow G/T(G)$ is an isomorphism, and hence, G being abelian, even $G \cong T(G) \times F$. Such a "complementary subgroup" F exists always for a *finitely generated group* (though not in a "natural way"):

Definition 2.76. *An abelian group G is called* **finitely generated**, *if there is a surjective homomorphism $\mathbb{Z}^n \longrightarrow G$ for some natural number $n \in \mathbb{N}$, i.e. if there are elements $a_1, ..., a_n \in G$, such that*

$$G = \mathbb{Z}a_1 + ... + \mathbb{Z}a_n := \{k_1a_1 + ... + k_na_n; k_1, ..., k_n \in \mathbb{Z}\} \ .$$

A finitely generated abelian group G is called **free**, *if $G \cong \mathbb{Z}^n$ for some $n \in \mathbb{N}$.*

Here we have to insert a warning about the use of the word "free": A finitely generated free abelian group is not a group which is free (cf. 2.55), finitely generated and abelian! In fact, a free group $F(M)$ is abelian if and only if $|M| \leq 1$ (then $F(M)$ is trivial or isomorphic to $\mathbb{Z}$); and vice versa, the finitely generated free abelian group $\mathbb{Z}^n$ is a free group only for $n = 1$.

For such a group G, the number n, such that $G \cong \mathbb{Z}^n$, is called the **rank** of G. It is well defined because of

Lemma 2.77. *If $\mathbb{Z}^r \cong \mathbb{Z}^s$, then $r = s$.*

Proof. If $\mathbb{Z}^r \cong \mathbb{Z}^s$, then also

$$(\mathbb{Z}_2)^r \cong \mathbb{Z}^r/2\mathbb{Z}^r \cong \mathbb{Z}^s/2\mathbb{Z}^s \cong (\mathbb{Z}_2)^s,$$

whence $2^r = |\mathbb{Z}_2^r| = |\mathbb{Z}_2^s| = 2^s$ resp. $r = s$. □

Example 2.78. 1. A finite (abelian) group is finitely generated.

2. The additive group $\mathbb{Q}$ is not finitely generated: If $\mathbb{Q} = \mathbb{Z}a_1 + ... + \mathbb{Z}a_n$ with $a_i = \frac{p_i}{q_i}, p_i \in \mathbb{Z}, q_i \in \mathbb{Z} \setminus \{0\}$, we would have $\mathbb{Q} \subset q^{-1}\mathbb{Z}$ with $q := q_1 \cdot ... \cdot q_n$. Contradiction!

Eventually we shall not go on with a direct proof of the existence of a subgroup complementary to the torsion subgroup; instead it will be a byproduct of a more general theorem.

First note that an abelian group G is finitely generated iff it is isomorphic to a factor group F/H with a subgroup $H \leq F$ of a finitely generated free abelian group $F \cong \mathbb{Z}^n$. The next proposition is a generalization of Proposition 2.25: It describes the possible subgroups $H \leq F$ up to an automorphism of F (Note that $F = \mathbb{Z}$ admits only the automorphisms $\mathbb{Z} \longrightarrow \mathbb{Z}, x \mapsto \pm x$):

Theorem 2.79. *Let $H \subset F$ be a subgroup of the finitely generated free abelian group $F \cong \mathbb{Z}^n$. Then there are natural numbers $q_1, ..., q_n \in \mathbb{N}$ with $q_i | q_{i+1}$ and an isomorphism*

$$\varphi : F \xrightarrow{\cong} \mathbb{Z}^n, \text{ such that } \varphi(H) = q_1\mathbb{Z} \times ... \times q_n\mathbb{Z} \subset \mathbb{Z}^n \ .$$

We remark that the numbers $q_1, ..., q_n$ are uniquely determined by $H \leq F$ as a consequence of Th. 2.84. – The proof of the above theorem is divided into several steps, formulated as lemmata. Let us first show that H itself is again a finitely generated free abelian group:

Lemma 2.80. *Every subgroup $H \subset \mathbb{Z}^n$ is isomorphic to a group $\mathbb{Z}^r, r \leq n$.*

Proof. We prove the lemma by induction on n. The case $n = 1$ is nothing but Prop. 2.25. For $n > 1$ take $H_0 := H \cap (\mathbb{Z}^{n-1} \times \{0\})$. According to the induction hypothesis there is an isomorphism $\varphi : \mathbb{Z}^s \longrightarrow H_0, s \leq n-1$. Let now $\pi := \pi_n : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ be the projection onto the last component. Its image $\pi(H) \subset \mathbb{Z}$ is a subgroup and has therefore, again because of Prop. 2.25, the form $\pi(H) = \mathbb{Z}q$ with some $q \in \mathbb{N}$. If $q = 0$, we have $H = H_0$ and we are done. Otherwise choose $v \in H$ with $\pi(v) = q$. Then $\mathbb{Z}^s \times \mathbb{Z} \longrightarrow H, (u, k) \mapsto \varphi(u) + kv$ is an isomorphism. □

Furthermore we need the following easy, but useful fact:

Lemma 2.81. *Let F be a finitely generated free abelian group and $e \in F$ a primitive element (or "vector"), i.e.*

$$e = \lambda w,\ \lambda \in \mathbb{Z},\ w \in F \Longrightarrow \lambda = \pm 1.$$

Then there is a group homomorphism $\pi : F \longrightarrow \mathbb{Z}$ with $\pi(e) = 1$.

Proof. We may assume $F = \mathbb{Z}^n$ and $e = (k_1, ..., k_n)$ with $\gcd(k_1, ..., k_n) = 1$. But then there are integers $r_1, ..., r_n \in \mathbb{Z}$ with $r_1k_1 + ... + r_nk_n = 1$ and we define $\pi : F \longrightarrow \mathbb{Z}$ by $\pi(x_1, ..., x_n) = r_1x_1 + ... + r_nx_n$. □

Remark 2.82. As we see from the proof of Lemma 2.80, a nonzero element $e \in F$ is primitive, iff the subgroup $\mathbb{Z}e \leq F$ admits a complementary subgroup $F_0 \leq F$, i.e. such that the inclusions $\mathbb{Z}e, F_0 \hookrightarrow F$ induce an isomorphism $F_0 \times \mathbb{Z}e \cong F$. Equivalently, an element $e \in F$ is primitive, iff it can serve as the first element of a basis of F, i.e. iff there are elements $e_2, ..., e_n \in F$, such that $e_1 := e, e_2, ..., e_n$ is a "basis" of F, i.e. such that $\mathbb{Z}^n \longrightarrow F, (k_1, ..., k_n) \mapsto k_1e_1 + ... + k_ne_n$, is a group isomorphism.

The essential argument in the proof of Th. 2.79 is the following:

Lemma 2.83. *Let $H \leq F$ be a subgroup of the finitely generated free abelian group F. If H is not contained in kF for any $k > 1$, then H contains a primitive vector.*

Proof. We consider the set $\mathrm{Pr}(F)$ of all projections, i.e. surjective group homomorphisms $\pi : F \longrightarrow \mathbb{Z}$. Choose some $\pi \in \mathrm{Pr}(F)$ with maximal $\pi(H) \leq \mathbb{Z}$. Writing $\pi(H) = \mathbb{Z}q,\ q \geq 0$, we are done if we succeed in showing $q = 1$, since an element $v \in F$ with $\pi(v) = 1$ is primitive. Assume the contrary: $q > 1$. Take now $v \in H$ with $\pi(v) = q$. Write $v = \lambda e$ with $\lambda \geq 1$ and a primitive vector $e \in F$. Obviously $q = \lambda\pi(e)$. We show $\lambda = q$ and thus $\pi(e) = 1$. By Lemma 2.81 there is $\tilde{\pi} \in \mathrm{Pr}(F)$ with $\tilde{\pi}(e) = 1$ resp. $\tilde{\pi}(v) = \lambda$. Thus $\tilde{\pi}(H) \supset \mathbb{Z}\lambda \supset \mathbb{Z}q = \pi(H)$ resp. $\tilde{\pi}(H) = \pi(H)$ because of the maximality of $\pi(H)$. With other words $q = \lambda$ and $\pi(e) = 1$. Let $F_0 := \ker(\pi), H_0 := H \cap F_0$. Then the map

$$F_0 \times \mathbb{Z} \longrightarrow F, (u, k) \mapsto u + ke$$

is an isomorphism restricting to an isomorphism

$$H_0 \times \mathbb{Z}q \longrightarrow H.$$

Since $H \not\subset qF$, there is a vector $v_0 = \mu e_0 \in H_0$ with $\mu \notin \mathbb{Z}q$ and primitive $e_0 \in F_0$. Now apply Lemma 2.80 once again and obtain a projection $\pi_0 : F_0 \longrightarrow \mathbb{Z}$ with $\pi_0(e_0) = 1$. Then $\tilde{\pi} := \pi_0 + \mathrm{id}_{\mathbb{Z}} : F_0 \times \mathbb{Z} \longrightarrow \mathbb{Z}$ is a projection with $\mu, q \in \tilde{\pi}(H)$, in particular $\pi(H) = \mathbb{Z}q \subsetneqq \tilde{\pi}(H)$, a contradiction. □

Proof of 2.79. We use induction on n. Take $q \geq 1$ maximal with $H \leq qF$. We apply Lemma 2.83 to $H \leq qF$ and find a primitive vector $e \in F$ with $qe \in H$ (the primitive vectors in qF are of the form qe with primitive $e \in F$). Choose a projection $\pi : F \longrightarrow \mathbb{Z}$ with $\pi(e) = 1$ and define $F_0 \geq H_0$ as in the proof of 2.83. By the induction hypothesis $H_0 \leq F_0$ satisfies 2.79, so we find numbers $q_2, ..., q_n$ with the given properties. Set $q_1 := q$ and note that $q|q_2$ because of $H_0 \leq qF_0$. □

As a corollary we obtain the classification of all finitely generated abelian groups:

Theorem 2.84. Fundamental Theorem on finitely generated abelian groups: *A finitely generated abelian group G is isomorphic to a finite direct product of cyclic groups:*

$$G \cong \mathbb{Z}_{q_1} \times ... \times \mathbb{Z}_{q_n} \ ,$$

where $\mathbb{Z}_0 := \mathbb{Z}$ and the natural numbers $q_1, ..., q_n \in \mathbb{N} \setminus \{1\}$ satisfy one of the following two conditions:

1. *The number q_i divides q_{i+1} for $i = 1, ..., n-1$.*
2. *All $q_i > 0$ are prime powers.*

The numbers $q_1, ..., q_n$ are unique in case 1) and unique up to order in case 2). (PS: The number n need not be the same in both cases!).

If we apply the above theorem to $G := F/H$ in Th. 2.79, we see that the numbers $q_1, ..., q_n$ there are uniquely determined by $H \leq F$.

Proof. Existence: *1.)* Let us start with the first case: We have $G \cong \mathbb{Z}^n/H$ with a subgroup $H \subset \mathbb{Z}^n$ as in Th.2.79; hence

$$G \cong \frac{\mathbb{Z} \times ... \times \mathbb{Z}}{q_1\mathbb{Z} \times ... \times q_n\mathbb{Z}} \cong \mathbb{Z}_{q_1} \times ... \times \mathbb{Z}_{q_n},$$

where we of course may assume $q_i \neq 1$ for $i = 1, ..., n$.

2.) We use the first part and apply the below Chinese remainder theorem to all $q = q_i > 1$.

Proposition 2.85 (Chinese Remainder Theorem)**.** *Let $q = p_1^{k_1} \cdot ... \cdot p_r^{k_r}$ be the prime factorization of $q \in \mathbb{Z}$ ($p_1, .., p_r$ pairwise distinct). Then*

$$\mathbb{Z}_q \longrightarrow \mathbb{Z}_{p_1^{k_1}} \times ... \times \mathbb{Z}_{p_r^{k_r}}, \overline{\ell} = \ell + \mathbb{Z}q \mapsto (\ell + \mathbb{Z}p_1^{k_1}, ..., \ell + \mathbb{Z}p_r^{k_r})$$

defines an isomorphism of groups.

Proof. If $\ell + \mathbb{Z}p_i^{k_i} = \overline{0}$ for all $i = 1, ..., r$, then all $p_i^{k_i}$ divide the number ℓ, hence $q|\ell$ resp. $\ell + \mathbb{Z}q = \overline{0}$. So our group homomorphism is injective, but then also surjective since the start and the target group have the same order. □

Uniqueness: The number $r \geq 0$ of zeroes in $q_1, ..., q_n$ is nothing but the rank of the free abelian group $G/T(G)$. The numbers $q_i > 0$ can be read off from $T(G) \leq G$ as follows:

2.) For $m \in \mathbb{N}_{>0}$ the m-torsion subgroup

$$T_m(G) := \{a \in G; ma = 0\}$$

behaves as follows:

Remark 2.86.

1. $T_m(G \times H) = T_m(G) \times T_m(H)$.
2. $T_m(\mathbb{Z}) = \{0\}$.
3. For $\gcd(m, n) = 1$ we have

   $$T_m(\mathbb{Z}_n) = \{0\},$$

   since with $r, s \in \mathbb{Z}, rm + sn = 1$, and $a \in T_m(\mathbb{Z}_n)$ we have

   $$a = (rm + sn)a = r(ma) + s(na) = r \cdot 0 + s \cdot 0 = 0.$$

4. Let $p \in \mathbb{N}_{>1}$ be a prime number. Then

   $$T_{p^\ell}(\mathbb{Z}_{p^k}) = \begin{cases} p^{k-\ell}\mathbb{Z}_{p^k} & , \text{ if } \ell \leq k \\ \mathbb{Z}_{p^k} & , \text{ if } \ell \geq k \end{cases}.$$

   Hence

   $$\frac{T_{p^{\ell+1}}(\mathbb{Z}_{p^k})}{T_{p^\ell}(\mathbb{Z}_{p^k})} \cong \begin{cases} \mathbb{Z}_p & , \text{ if } \ell < k \\ \{0\} & , \text{ if } \ell \geq k \end{cases}.$$

As a consequence we obtain

$$|T_{p^{\ell+1}}(G)/T_{p^\ell}(G)| = p^s,$$

where $s = s(p,\ell)$ is the number of the $q_i = p^k$ with $k > \ell$. Obviously the numbers $s(p,\ell)$ determine the prime powers $q_i > 0$

1.) Given the numbers q_i in a decomposition of type *1.)* and a prime number p, denote $\mu(p,i) \geq 0$ the multiplicity of p as divisor of q_i. Now a decomposition of type *2.)* is determined by the group G itself and provides for every prime number p the supply of possible $\mu(p,i)$. Since on the other hand $\mu(p,i) \leq \mu(p,i+1)$, we can reconstruct the numbers q_i. □

2.7.1 Digression: Free Abelian Groups

In many applications one even needs not necessarily finitely generated free abelian groups. We give here a short comment only: Let M be a set. We consider the group

$$\mathbb{Z}^M := \{f : M \longrightarrow \mathbb{Z}\}$$

of all maps from M to $\mathbb{Z}$ with the argument-wise addition $(f+g)(x) = f(x) + g(x)$. Its subgroup

$$\mathbb{Z}[M] := \{f \in \mathbb{Z}^M, |f^{-1}(\mathbb{Z} \setminus \{0\})| < \infty\}$$

containing the maps $f : M \longrightarrow \mathbb{Z}$, which are non-zero only on a finite subset of M is called **the free abelian group generated by** M. If for $a \in M$, we denote χ_a the map $\chi_a(x) = \delta_{ax}$, any $f \in \mathbb{Z}[M]$ can uniquely be written

$$f = \sum_{a \in M} n_a \chi_a$$

with $n_a := f(a)$. Formally, the above sum is infinite, and as such not well defined in the framework of algebra, but since $n_a = 0$ for only finitely many $a \in M$, one can define

$$\sum_{a \in M} n_a \chi_a := \sum_{a, n_a \neq 0} n_a \chi_a.$$

Furthermore one usually writes simply a instead of χ_a and thinks of the elements in $\mathbb{Z}[M]$ as finite "formal sums"

$$\sum_{a \in M} n_a \cdot a$$

with integral coefficients in the elements of M. Now a free abelian group is defined to be a group isomorphic to a group $\mathbb{Z}[M]$; so an abelian group is free iff there is a subset M (a "basis"), such that any element has a unique representation as a finite linear combination $\sum_{a\in M} n_a a$. Finally note that the abelian group $\mathbb{Z}[M]$ satisfies a similar universal property as $F(M)$: Any map $\varphi : M \longrightarrow G$ to an abelian group G has a unique extension to a group homomorphism $\hat{\varphi} : \mathbb{Z}[M] \longrightarrow G$, or, more down to earth, the values of a group homomorphism can be arbitrarily prescribed on the elements of M, and these values determine the entire homomorphism. We leave it to the reader to check that

$$\mathbb{Z}[M] \cong F(M)/N(\mathfrak{K})$$

with the set

$$\mathfrak{K} := \{aba^{-1}b^{-1}; a, b \in M\}$$

of all "commutators" of elements $a, b \in M$. Note that $N(\mathfrak{K}) \subset F(M)$ is the subgroup generated (in the ordinary sense) by all commutators $aba^{-1}b^{-1}$ with $a, b \in F(M)$, the conjugate of a commutator being again a commutator.

Problems 2.87.

1. R: Give an example of a (non-commutative) group G, for which the elements of finite order do not constitute a subgroup!
2. R: Let $H \subset \mathbb{Z}^2$ be the subgroup generated by $(a, b), (c, d) \in \mathbb{Z}$. Write the factor group $\mathbb{Z}^2/H$ as in Th.2.84!
3. Show that $\mathrm{Aut}(\mathbb{Z}^n) \cong GL_n(\mathbb{Z}) := \{A \in \mathbb{Z}^{n,n}, \det(A) = \pm 1\}$. Furthermore for $A \in \mathbb{Z}^{n,n}, \det A \neq 0$, that the index of the subgroup $A(\mathbb{Z}^n) \subset \mathbb{Z}^n$ is $|\det A|$.
4. R: Write the groups $\mathbb{Z}_n^*$, cf. 2.62.6, for $n = 13, 16, 25, 72, 624$ as a direct product of cyclic groups as in Th.2.84! Hint: The "Chinese remainder isomorphism" 2.85 induces an isomorphism $\mathbb{Z}_q^* \longrightarrow \mathbb{Z}^*_{p_1^{k_1}} \times ... \times \mathbb{Z}^*_{p_r^{k_r}}$ for $q = p_1^{k_1} \cdot ... \cdot p_r^{k_r}$.
5. Show: $\mathbb{Z}_4^* \cong \mathbb{Z}_2$ and $\mathbb{Z}_{2^n}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$ for $n > 2$. More precisely $\mathbb{Z}_{2^n}^* \cong < -\overline{1} > \times < \overline{1+4r} >$ with any odd number $r \in \mathbb{Z}$.
6. Show that $T(G) \subset G$ in general does not have a complementary subgroup $F \subset G$, i.e. such that $F \longrightarrow G \longrightarrow G/T(G)$ is an isomorphism.

2.8 Sylow Subgroups

According to Proposition 2.73 a p-group is solvable, hence, at least theoretically, understandable. That explains, why one in the study of a general finite group G looks for subgroups which are p-groups.

Definition 2.88. *A subgroup $H \subset G$ of a finite group G is called a* **p-Sylow-subgroup** *(*Peter Ludvig Mejdell Sylow, 1832-1918*), if $|H|$ is the maximal p-power dividing $|G|$.*

First of all we are not talking about the empty set:

Theorem 2.89. *Let G be a finite group. For every prime p dividing the group order $|G|$, there is a p-Sylow-subgroup.*

Proof. We do induction on the group order $|G|$: Choose a system of representatives $x_1, ..., x_r \in G$ of the non-trivial conjugacy classes, i.e. $|\kappa_G(x_i)| > 1$. If an index $(G : G_{x_i})$ of an isotropy group is not divisible with p, then a p-Sylow subgroup of G_{x_i} is also a p-Sylow subgroup of G, and the induction hypothesis can be applied to the proper subgroup $G_{x_i} \subsetneq G$. Otherwise as a consequence of Proposition 2.32 also $|Z(G)|$ is divisible with p, and there is an element $a \in Z(G)$ of order p: This follows immediately from 2.84. But a commutes with all elements in G; so $< a > \subset G$ is a normal subgroup and we may apply the induction hypothesis to the factor group $G/ < a >$ and find a p-Sylow subgroup $H \subset G/ < a >$. Then the inverse image $\varrho^{-1}(H) \subset G$ with respect to the coset map $\varrho : G \longrightarrow G/ < a >$ is a p-Sylow subgroup of G. □

Theorem 2.90. *Let G be a finite group and p a prime number. Then*

1. *Any p-subgroup F of G (i.e., $F \subset G$ is a subgroup and $|F|$ is a p-power) is contained in a p-Sylow-subgroup.*

2. *Any two p-Sylow-subgroups are conjugate.*

3. *The number of p-Sylow-subgroups divides the group order $|G|$ and has the form $1 + kp$ with a natural number $k \in \mathbb{N}$.*

Proof. The first two parts are an immediate consequence of the following fact: Given a p-Sylow subgroup $H \subset G$ and a p-subgroup $F \subset G$, there is an $a \in G$ with $F \subset \kappa_a(H)$: Denote $\mathrm{Syl}_p(G)$ the set of all p-Sylow subgroups of G. The group G acts by conjugation on $\mathrm{Syl}_p(G)$:

$$G \times \mathrm{Syl}_p(G) \ni (g, H) \longmapsto \kappa_g(H) = gHg^{-1} \in \mathrm{Syl}_p(G) \ .$$

Choose some p-Sylow-subgroup $H \in \mathrm{Syl}_p(G)$. Its stabilizer $G_H := \{g \in G; \kappa_g(H) = H\}$ is usually called the **normalizer** of the subgroup H in G

and denoted $N_G(H)$. Obviously $N_G(H) = G_H$ contains H - indeed $N_G(H)$ is the largest subgroup of G containing H as normal subgroup - , hence its index $(G : G_H)$ is not divisible with p. We consider now the induced F-action $F \times \mathrm{Syl}_p(G) \longrightarrow \mathrm{Syl}_p(G)$ (i.e., obtained by restriction): The G-orbit $\kappa_G(H) \subset \mathrm{Syl}_p(G)$ of $H \in \mathrm{Syl}_p(G)$ then is a disjoint union of F-orbits $\kappa_F(H_i), i = 1, ..., r$ with $H_i = \kappa_{a_i}(H)$, and the number of elements in such an F-orbit is some p-power $= p^{r_i} = (F : F_{H_i})$. If $r_i > 0$ for all i, then $|\kappa_G(H)| = (G : G_H)$ is divisible with p. So there is an F-orbit consisting only of one element, say H_1. With other words, F normalizes H_1, and thus

$$FH_1 := \{fh_1; f \in F, h_1 \in H_1\} \subset G$$

is a subgroup satisfying

$$(FH_1)/H_1 \cong F/(F \cap H_1)$$

with an isomorphism induced by the homomorphism $F \hookrightarrow FH_1 \longrightarrow (FH_1)/H_1$, the composite of the inclusion and the factor map.

As a consequence it is as a factor group of the p-group F again a p-group, but on the other side also H_1 is p-group, and thus FH_1 as well because of $|FH_1| = |H_1| \cdot |(FH_1)/H_1| = |H_1| \cdot |F/(F \cap H_1)|$. Since $|H_1|$ is the maximal p-power dividing $|G|$, it follows that $H_1 = FH_1$ resp. $F \subset H_1$ with the p-Sylow-subgroup $H_1 = \kappa_{a_1}(H)$.
In particular G acts transitively on $\mathrm{Syl}_p(G)$ and therefore $|\mathrm{Syl}_p(G)| = (G : G_H)$ is a divisor of $|G|$, where $H \in \mathrm{Syl}_p(G)$ is arbitrary. But a p-Sylow-subgroup F instead of G acts no longer transitively because of $\kappa_F(F) = \{F\}$, while according to the above reasoning the remaining F-orbits contain more than one element: Since the number of elements in such an orbit is a p-power $p^r, r > 0$, we have shown 3). □

As an application we prove:

Theorem 2.91. *A non-abelian simple group G of order $|G| \leq 60$ is isomorphic to the alternating group on 5 letters: $G \cong \mathbb{A}_5$. In particular, a group G of order $|G| \leq 60$ is either solvable or isomorphic to $\mathbb{A}_5$.*

Proof. First, given a group G of non-prime order $|G| < 60$ we hunt for a non-trivial normal proper subgroup $H \subset G$, then consider the case $|G| = 60$:

If $|G| = p^r, r \geq 2$, we may choose $H := Z(G) \neq \{e\}$, cf. Corollary 2.32.

The next case is:

Proposition 2.92. *Let p, q be different prime numbers. Then any group of order pq or pq^2 has a normal Sylow subgroup.*

Proof. Let us first consider the case $p < q$. Then the number of q-Sylow subgroups is of the form $1 + nq$, and we want to show $n = 0$. Since on the other hand $1 + nq$ divides $|G| = pq^2$ or $= pq$, we obtain $(1 + nq)|p$, but that is obviously possible only for $n = 0$. Secondly, if $p > q$, we denote $1 + np$ the number of p-Sylow subgroups of G. Now we get $(1 + np)|q^2$, i.e., $1 + np = 1$, so $n = 0$, or $1 + np = q$ (but that is absurd!) or $1 + np = q^2$. Thus $p|(q^2 - 1) = (q + 1)(q - 1)$, whence $p|(q + 1)$ or rather $p = q + 1$, i.e., $q = 2, p = 3$, in particular $|G| = 12$. We now assume that a 2-Sylow subgroup $H \subset G$ is not normal and show that then there is exactly one (and hence normal) 3-Sylow subgroup: Take a conjugate H'. Since $|H \cap H'| \leq 2$, we have at least 5 elements of order 2 or 4 in G, hence at most 6 elements of order 3. As a consequence, there are not more than 3 different 3-Sylow subgroups. On the other hand, there are $1 + 3n$ such subgroups; so $n = 0$ is the only remaining possibility. □

Hence the cases still to be considered are $|G| = 24, 30, 36, 40, 42, 48, 54, 56$. We remark first, that if p, but not p^2, divides G, and $H \subset G$ is a non-normal p-Sylow subgroup, then G contains at least $(p + 1)(p - 1) = p^2 - 1$ elements of order p.

Proposition 2.93. *A group G of order 30 or 56 has a normal Sylow subgroup.*

Proof. Assume $|G| = 30 = 2 \cdot 3 \cdot 5$. If no Sylow subgroup is normal we get, counting the elements of order $1, 2, 3, 5$, following the above reasoning $30 \geq 1 + 3(2 - 1) + 4(3 - 1) + 6(5 - 1) = 36$, a contradiction. Now assume $|G| = 56 = 7 \cdot 8$. If there is no normal 7-Sylow subgroup, we obtain at least $48 = 8(7 - 1)$ elements of order 7, so there are at most 7 elements of even order. But that means, that there is only one 2-Sylow-subgroup. □

Proposition 2.94. *A group of order $40, 42$ or 54 admits a normal p-Sylow subgroup with p the biggest prime dividing the group order.*

Proof. If $1 + np$ divides $|G|$, then necessarily $n = 0$. □

When looking at the cases $|G| = 24, 36, 48, 60$ we shall encounter the following situation: Let $F \subset G$ be a subgroup. Denote

$$X := \kappa_G(F) = \{\kappa_g(F); g \in G\}$$

the set of all subgroups of G conjugate to F. It satisfies

$$m := |X| = [G : N_G(F)] \leq [G : F]$$

with the normalizer $N_G(F) \supset F$ of F in G. We consider the homomorphism

$$\pi : G \longrightarrow \mathbb{S}(X) \cong \mathbb{S}_m, g \mapsto \pi_g \tag{2}$$

with the permutation

$$\pi_g : X \longrightarrow X, H \mapsto \kappa_g(H).$$

Proposition 2.95. *Let G be a group of order $|G| = 2^r \cdot 3, r \geq 2$. Then G admits a non-trivial normal 2-subgroup (but not necessarily a normal 2-Sylow-subgroup!).*

Proof. We take as subgroup $F \subset G$ a 2-Sylow subgroup. If it is normal, choose $H := F$. Otherwise the set X of its conjugates contains $m = 3$ elements. The image $\pi(G)$ of the homomorphism $\pi : G \longrightarrow \mathbb{S}(X) \cong \mathbb{S}_3$ contains a 3-cycle, since it acts transitively on X, hence $H := \ker(\pi)$ is a nontrivial ($r \geq 2$) normal 2-subgroup of G. □

Finally:

Proposition 2.96. *A group G of order $|G| = 36$ admits a non-trivial normal 3-group H (but not necessarily a normal 3-Sylow-subgroup!).*

Proof. Take $F \subset G$ as a 3-Sylow subgroup. If it is normal, choose $H := F$. Otherwise we have $m = 4$. Since $|\mathbb{S}_4| = 24$, the kernel $K := \ker(\pi)$ contains a 3-group. It has index $[G : K] > 2$, since a group of order 2 can not act transitively on a set X with 4 elements. If $|K| = 9$, it is itself a 9-Sylow subgroup, hence, according to our assumption, not normal, a contradiction. If $|K| = 3$, we choose $H := K$, and if $|K| = 6$, we have $K \cong C_2 \times C_3$ or $K \cong \mathbb{S}_3$. In both cases the elements in K of order 3 constitute a 3-subgroup H of K, invariant with respect to every automorphism of K (why?), in particular normal in G. □

Eventually we come to the case $|G| = 60$:

Proposition 2.97. *A simple group G of order $|G| = 60$ is isomorphic to the alternating group on 5 letters: $G \cong \mathbb{A}_5$.*

Proof. We show that the index $[G : F]$ of any non-trivial proper subgroup $F \subset G$ of a non-abelian simple group G is at least 5, and that in our case $|G| = 60$ there really is a subgroup $F \subset G$ of index $[G : F] = 5$.

Since the kernel of any homomorphism is a normal subgroup, our homomorphism

$$\pi : G \longrightarrow \mathbb{S}(X) \cong \mathbb{S}_m$$

is injective (F being not normal and G being simple). Hence $G \cong \pi(G) \subset \mathbb{S}_m$ with $m = |X|$. But $\mathbb{S}_m$ being solvable for $m \leq 4$, we have $5 \leq m \leq [G : F]$.

Now let us look for a subgroup F of index $[G : F] = 5$: We consider a 2-Sylow subgroup $H \subset G$. Since it is not normal in G, there is a conjugate $H' = \kappa_g(H) \neq H$. Consider the subgroup $E \subset G$ generated by H and H'. It contains $H \cap H'$ as a normal subgroup (since either $H \cap H' = \{e\}$ or $H \cap H' \subset H, H'$ is normal as a subgroup of index 2) and has an index $[G : E] < [G : H] = 15$, so either $[G : E] = 5, 1$ - the possibility $[G : E] = 3$ having already being excluded by the above argument applied to $F = E$. If $[G : E] = 5$, we choose $F := E$. Otherwise we have $E = G$ and it follows that $H \cap H' = \{e\}$ as a proper normal subgroup of G. So we may assume that $H \cap H' = \{e\}$ for different 2-Sylow subgroups H, H'.

Now consider the normalizer $N_G(H) \supset H$. It has the possible indices 5 or 15, (3 being again impossible) and thus we are done, if we can see that 15 is not possible either: In that case there are 15 pairwise different 2-Sylow subgroups $H_1, ..., H_{15}$, with the $H_i^* = H_i \setminus \{e\}$ being pairwise disjoint. So there are 45 elements in G of order 2 or 4, on the other hand there are at least 24 elements of order 5 (Take a 5-Sylow subgroup $U \subset G$: Since it is not normal, it has at least 6 pairwise different conjugates which (pairwise) only have the neutral element in common), but $1 + 45 + 24 > 60$: Contradiction!

Finally, identifying G with its image $\pi(G) \subset \mathbb{S}_5$, we show $G = \mathbb{A}_5$: If not, $\mathbb{A}_5 \cap G \subset G$ is a proper normal subgroup of G, hence trivial: $G \cap \mathbb{A}_5 = \{\mathrm{id}\}$. But then G necessarily contains a 4-cycle f, implying $\mathrm{id} \neq f^2 \in G \cap \mathbb{A}_5$, a contradiction! So $\mathbb{A}_5 \subset G$ resp. $\mathbb{A}_5 = G$ because of $|G| = 60$.

□

This finishes the proof of Theorem 2.91. □

Problems 2.98. 1. R: Determine all Sylow-subgroups of $\mathbb{S}_3, D_n, \mathbb{S}_4, \mathbb{A}_4$!

2. R: Show: A group G of order $|G| = 15$ is cyclic.

3. Let G be a group of order $|G| = 12$. Show: There is a normal p-Sylow-subgroup in G ($p = 2$ or $p = 3$). Then G is isomorphic with a semidirect product. Classify now all groups of order 12.

4. R: Show: If all Sylow-subgroups of a finite group G are normal, then G is isomorphic with the direct product of its Sylow-subgroups. Hint: If $H, F \subset G$ are different Sylow-subgroups, we have $H \cap F = \{e\}$. Conclude $ab = ba$ for all $a \in H, b \in F$ because of $F \ni (aba^{-1})b^{-1} = a(ba^{-1}b^{-1}) \in H$.

3 Rings

3.1 Definitions and Examples

Definition 3.1. *A ring is a triple (R, α, μ), with a set R together with two maps,*

$$\alpha : R \times R \longrightarrow R, (a, b) \mapsto a + b := \alpha(a, b) \quad ,$$

the "addition", and

$$\mu : R \times R \longrightarrow R, (a, b) \mapsto ab := \mu(a, b) \quad ,$$

the "multiplication", such that

R_1 *: The pair (R, α) is an (additively written) abelian group.*

R_2 *: The multiplication μ is associative:*

$$(ab)c = a(bc), \quad \forall a, b, c \in R \ .$$

R_3 *: The multiplication is "distributive" over the addition:*

$$a(b + c) = ab + ac \ , \ (a + b)c = ac + bc \ , \quad \forall a, b, c \in R \ .$$

R_4 *: There is an element $1 \in R \setminus \{0\}$, such that*

$$1a = a = a1 \ , \quad \forall a \in R \ .$$

R_5 *: The multiplication is commutative*

$$ab = ba \ , \quad \forall a, b \in R \ .$$

Remark 3.2. 1. Usually only the conditions R_1 - R_3 are required for a ring in the literature; if even R_4, R_5 hold, it is called a "commutative ring with unity". Since we shall exclusively deal with commutative rings with unity, we have chosen to follow the convention, that the word "ring" should mean a commutative ring with unity.

2. The above axioms ensure that the arithmetic in a ring R is "more or less" the familiar one: To be on the safe side let us mention the following rules:

$$0 \cdot a = 0 = a \cdot 0$$

holds, since $a = 1 \cdot a = (1+0)a = a + 0 \cdot a$ and

$$(-1)a = a(-1) = -a$$

follows from $0 = (1+(-1))a = a + (-1)a$. But there is no cancellation rule for the multiplication, since there may be nontrivial "zero divisors", i.e. elements $a \in R \setminus \{0\}$, such that

$$ab = 0$$

for some $b \neq 0$, and it can happen that

$$1 + ... + 1 = 0 \ .$$

So we should actually derive all computation rules we use from the ring axioms!

Example 3.3. 1. The sets $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with the usual addition and multiplication of integers resp. rational, real or complex numbers are rings.

2. The factor groups $\mathbb{Z}_n$, cf. 2.26, constitute rings with their group law as addition $\overline{a} + \overline{b} = \overline{a+b}$ and the multiplication $\overline{a}\overline{b} := \overline{ab}$. We have to check that the multiplication is well defined, since then the axioms $R_1 - R_5$ carry over from $\mathbb{Z}$ to $\mathbb{Z}_n$. So let $\overline{a}_1 = \overline{a}, \overline{b}_1 = \overline{b}$, i.e. $a_1 = a + kn, b_1 = b + \ell n$ with integers $k, \ell \in \mathbb{Z}$. Then we obtain $a_1 b_1 = (a+kn)(b+\ell n) = ab + (a\ell + bk + k\ell n)n$ resp. $\overline{a_1 b_1} = \overline{ab}$.

3. If $R_1, ..., R_n$ are rings, their **direct product**

$$\prod_{i=1}^{n} R_i := R_1 \times ... \times R_n$$

is the cartesian product of the sets $R_1, ..., R_n$ with the componentwise ring operations. In particular for a ring R the n-fold cartesian product R^n is again a ring.

4. If M is any set and R a ring, so is the set

$$R^M := \{f : M \longrightarrow R\}$$

of all R-valued maps on M with the argumentwise addition and multiplication of functions:

$$(f+g)(x) := f(x) + g(x), (fg)(x) := f(x)g(x).$$

5. **Formal power series over a ring R :** For a ring R we define

$$R[[T]] := R^{\mathbb{N}} \text{ as additive group.}$$

Hence, the elements in $R[[T]]$ can be thought of as sequences $(a_\nu)_{\nu\in\mathbb{N}}$, where $a_\nu \in R, \forall \nu \in \mathbb{N}$, by identifying a function $f : \mathbb{N} \longrightarrow R$ with the sequence $(f(\nu))_{\nu\in\mathbb{N}}$, and the addition is componentwise. But we define a new multiplication, sometimes also called **Cauchy multiplication**, on $R[[T]]$:

$$(a_\nu) \cdot (b_\nu) := (c_\nu), \text{where } c_\nu := \sum_{k=0}^{\nu} a_k b_{\nu-k} = \sum_{k+\ell=\nu} a_k b_\ell \quad .$$

Unity then is the sequence $(1, 0, 0, ...)$, and, if we abbreviate $T := (0, 1, 0, 0, ...)$, we find

$$T^n = (\underbrace{0, ..., 0}_{n \text{ times}}, 1, 0, 0, ...) \ .$$

So, if we identify an element $a \in R$ with the sequence $(a, 0, 0, ...)$, we can write a sequence (a_ν), where almost all (i.e. with only finitely many exceptions) elements $a_\nu = 0$:

$$(a_0, a_1, ..., a_n, 0, 0, ...) = a_n T^n + a_{n-1} T^{n-1} + ... + a_1 T + a_0 = \sum_{\nu=0}^{n} a_\nu T^\nu \ .$$

The ring $R[[T]]$ is called the **power series ring in one variable over** R, and the elements are usually, in analogy to the above equality written as "formal series" $\sum_{\nu=0}^{\infty} a_\nu T^\nu$ corresponding to the sequences (a_ν). But since we do not have the notion of an infinite sum, this is a priori nothing but a notational convention, and only in the finite case it can be interpreted as a sum in a ring.

6. The **polynomial ring** $R[T]$ **in one variable over a ring** R is the subset:

$$R[T] := \left\{ \sum_{\nu=0}^{n} a_\nu T^\nu ; n \in \mathbb{N}, a_0, ..., a_n \in R \right\} \subset R[[T]] \ ,$$

which is obviously closed with respect to the ring operations of $R[[T]]$ and itself a ring. If one wants to avoid the above abstract definition, one can introduce polynomials over a ring R in a more naive way: We define them as "finite formal sums"

$$f = \sum_{\nu=0}^{n} a_\nu T^\nu ; n \in \mathbb{N}, a_0, ..., a_n \in R$$

meaning that $\sum_\nu a_\nu T^\nu = \sum_\nu b_\nu T^\nu$ if and only if $a_\nu = b_\nu$ for all $\nu \in \mathbb{N}$. The addition and multiplication are then as follows

$$\sum_\nu a_\nu T^\nu + \sum_\nu b_\nu T^\nu = \sum_\nu (a_\nu + b_\nu) T^\nu \quad ,$$

$$(\sum_\nu a_\nu T^\nu)(\sum_\nu b_\nu T^\nu) = \sum_\nu (\sum_{k=0}^{\nu} a_k b_{\nu-k}) T^\nu \quad .$$

A polynomial $f \in R[T]$ is called **monic** if it has the form $f = T^n + \sum_{\nu<n} a_\nu T^\nu$.

Definition 3.4. *Let R ba a ring. The degree function*

$$\deg : R[T] \longrightarrow \mathbb{N} \cup \{-\infty\}$$

is defined for $f \in R[T]$ by

$$\deg(f) := \begin{cases} n & , \text{ if } f = \sum_{\nu=0}^{n} a_\nu T^\nu, a_n \neq 0 \\ -\infty & , \text{ if } f = 0 \end{cases} \quad .$$

Remark 3.5. We have

$$\deg(f+g) \leq \max(\deg(f), \deg(g)) \ , \ \deg(fg) \leq \deg(f) + \deg(g)$$

and

$$\deg(fg) = \deg(f) + \deg(g)$$

if one of the polynomials f, g is monic.

The division algorithm for polynomials plays a central role in the arithmetics of a polynomial ring:

Theorem 3.6 (**Division algorithm for polynomials).** *Let $g \in R[T]$ be a monic polynomial. Then every polynomial $f \in R[T]$ can be written as*

$$f = qg + r$$

with uniquely determined polynomials $q, r \in R[T], \deg(r) < n = \deg(g)$.

Proof. Uniqueness: Let $f = qg + r = \tilde{q}g + \tilde{r}$. Then we have:

$$(q - \tilde{q})g = (\tilde{r} - r) \ .$$

Now the polynomial on the right hand side has a degree $< n$, while for $q - \tilde{q} \neq 0$ the left hand side has at least degree n (since g is monic). Hence $q = \tilde{q}$ and then of course also $r = \tilde{r}$.
Existence: We do induction on $\deg(f)$: For $\deg(f) < n$ we take $q = 0$ and $r = f$.
If $\deg(f) =: m \geq n$, say $f = b_m T^m + ... + b_0$, we consider the polynomial $\tilde{f} := f - b_m T^{m-n} g$. Being of a degree $< \deg(f)$, the induction hypothesis provides $\tilde{q}, \tilde{r}$ with

$$\tilde{f} = \tilde{q}g + \tilde{r}$$

and $\deg(\tilde{r}) < n$. Finally choose $q := \tilde{q} + b_m T^{m-n}, r := \tilde{r}$. □

Definition 3.7. *Let R be a ring.*

1. *An element $a \in R$ is called a* **nonzero divisor**, *iff $ab = 0 \Longrightarrow b = 0$. If all elements in $R \setminus \{0\}$ are nonzero divisors and $1 \neq 0$, the ring R is called an* **integral domain (integritetsområde)**.

2. *An element $a \in R \setminus \{0\}$ is called a* **unit** *iff there is an element $a^{-1} \in R$, such that $aa^{-1} = 1 (= a^{-1}a)$. We denote R^* the set of all units in R:*

$$R^* := \{a \in R; \exists \ a^{-1} \in R : aa^{-1} = 1\} \ \ ,$$

   and call R^* the **group of units** *of the ring R.*

3. *A ring R is called a* **field (kropp)** *iff $R^* = R \setminus \{0\}$.

Note that R^* is a (multiplicatively written) abelian group.

Example 3.8. 1. Units are are nonzero divisors, in particular fields are integral domains: If $a \in R^*$ and $ab = 0$, we find $0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$.

2. The rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are actually fields.

3. The ring $\mathbb{Z}$ of integers is an integral domain, but not a field: We have $\mathbb{Z}^* = C_2 = \{\pm 1\}$.

4. In a finite ring R nonzero divisors are even units: For a nonzero divisor $a \in R$ the multiplication with a, the map $\mu_a : R \longrightarrow R, x \mapsto ax$, is injective, hence also surjective, R being finite. Therefore there is an element $b \in R$ with $ab = 1$, i.e. $a \in R^*$.

5. A residue class $\bar{a} \in \mathbb{Z}_n$ is a nonzero divisor iff $\gcd(a, n) = 1$. Hence according to the previous point, we obtain the equality[2]:

$$\mathbb{Z}_n^* = \{\bar{a} \in \mathbb{Z}_n; \gcd(a, n) = 1\} \ .$$

The function $\varphi : \mathbb{N}_{>0} \longrightarrow \mathbb{N}$ defined as

$$\varphi(n) := \begin{cases} 1 & , \quad \text{if } n = 1 \\ |\mathbb{Z}_n^*| & , \quad \text{if } n \geq 2 \end{cases}$$

is called **Eulers φ-function** (Leonhard Euler, 1707-1783). For a prime power $n = p^k$ we get: Zero divisors in $\mathbb{Z}_{p^k}$ are exactly the elements in $p\mathbb{Z}_{p^k}$, and thus $|\mathbb{Z}_{p^k}^*| = |\mathbb{Z}_{p^k}| - |p\mathbb{Z}_{p^k}| = p^k - p^{k-1} = p^{k-1}(p-1)$. Hence we have found

$$\varphi(p^k) = p^{k-1}(p-1) \ \text{ for } k \geq 1.$$

6. The residue class ring $\mathbb{Z}_n$ is a field iff it is an integral domain iff $n = p$ is prime.

7. Let R be an integral domain. Then also the polynomial ring $R[T]$ is an integral domain with the same group of units as the original ring R, i.e. $R[T]^* = R^*$, where we identify R with the "constant" polynomials, i.e. of degree ≤ 0.

[2]In Problem 2.62.6 we took its RHS as a definition for the LHS.

Proof. The ring R being an integral domain, we have

$$\deg(fg) = \deg(f) + \deg(g) \ .$$

Since only the zero polynomial has degree $-\infty$, this implies that $R[T]$ is an integral domain. The inclusion $R^* \subset R[T]^*$ is obvious. On the other hand the "constant" polynomial 1 has degree $= 0$, so the above degree equality gives, that units have degree 0 and thus are units in R, i.e. $R[T]^* \subset R^*$. □

8. In the same way as one obtains from $\mathbb{Z}$ the rationals one can associate to any integral domain R a field $Q(R)$ containing R: More generally, a subset $S \subset R \setminus \{0\}$ is called **multiplicative**, if $1 \in S$ and $s, t \in S \Longrightarrow st \in S$. On the cartesian product $R \times S$ we define an equivalence relation $\sim$ as follows

$$(a, s) \sim (b, t) :\Longleftrightarrow at = bs \ .$$

The set $S^{-1}R := (R \times S)/\sim$ of its equivalence classes can be made a ring: Denote $\frac{a}{s}$ the equivalence class of the pair (a, s). Then the addition and multiplication

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st} \ , \ \frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}$$

provide well defined (check that!) ring operations; the resulting ring $S^{-1}R$ is called the **localization of R with respect to the multiplicative subset** S. If $S = R \setminus \{0\}$, the localization $S^{-1}R$ is actually a field, called the **field of fractions**

$$Q(R) := (R \setminus \{0\})^{-1}R$$

of the integral domain R. The most important examples of this construction are the rationals $\mathbb{Q} := Q(\mathbb{Z})$ and, with a field K, the field of fractions

$$K(T) := Q(K[T])$$

of the polynomial ring $K[T]$, also called the **field of rational functions in one variable over K**.

9. If R is an integral domain, so is the formal power series ring $R[[T]]$ over R, but in contrast to the polynomial ring $R[T]$ the group of units is quite big:

$$R[[T]]^* = \{f = \sum_{\nu=0}^{\infty} a_\nu T^\nu ; a_0 \in R^*\} \ .$$

Proof. We replace the degree function with the order function $\omega : R[[T]] \longrightarrow \mathbb{N} \cup \{\infty\}$ defined as

$$\omega(f) := \begin{cases} n & , \text{ if } f = \sum_{\nu=n}^{\infty} a_\nu T^\nu, a_n \neq 0 \\ \infty & , \text{ if } f = 0 \end{cases} \ .$$

So $\omega(f)$ is the "order of f at 0". We have $\omega(fg) \geq \omega(f) + \omega(g)$, and even $\omega(fg) = \omega(f) + \omega(g)$, if R is an integral domain. So, since only $f = 0$ has order ∞, it follows, that there are no zero divisors in $R[[T]]$ if there are none in R.

In order to investigate the group of units $R[[T]]^*$, we have to define certain infinite sums of power series: Let $(f_k)_{k\in\mathbb{N}} \subset R[[T]]$ be a sequence of formal series, say $f_k = \sum_{\nu=0}^{\infty} a_\nu^k T^\nu$, such that $\lim_{k\to\infty} \omega(f_k) = \infty$. Then we can define

$$\sum_{k=0}^{\infty} f_k := \sum_{\nu=0}^{\infty} a_\nu T^\nu \ \text{ with } a_\nu = \sum_{k=0}^{\infty} a_\nu^k \ ,$$

where for each index ν only finitely many a_ν^k are $\neq 0$. So the sum defining the coefficient a_ν is in fact finite!

We show now that a series $f = \sum_{\nu=0}^{\infty} a_\nu T^\nu$ is a unit iff the coefficient a_0 is a unit in R. The condition is necessary, since $(a_0 + ...)(b_0 + ...) = (a_0 b_0 + ...) = 1$ implies $a_0 b_0 = 1$. On the other hand, if $a_0 \in R^*$ it of course suffices to consider the series $a_0^{-1} f$, i.e. we may assume $a_0 = 1$ and write then $f = 1 - g$, where the series g has order $\omega(g) \geq 1$. Then it follows $\omega(g^k) \geq k$, such that the geometric series $h := \sum_{k=0}^{\infty} g^k$ defines a formal series, satisfying $h(1 - g) = 1$. □

Problems 3.9. 1. R: An element $x \in R$ in a ring is called **nilpotent** if there is a natural number $n \in \mathbb{N}$ with $x^n = 0$. The set $\mathfrak{n} = \sqrt{\{0\}}$ of all nilpotent element is called the **nilradical** of R. Show: $1 + \mathfrak{n} \subset R^*$. Hint: Geometric series!

2. R: Let K be a field. Show: $R := K + T^2 K[T] := \{f = 1 + T^2 g \ ; g \in K[T]\}$ with the from $K[T]$ induced ring operations is an integral domain with $Q(R) = K(T)$.

3. R: For a subset $P_0 \subset P$ of the set $P \subset \mathbb{N}$ of all primes denote $S(P_0)$ the multiplicative subset consisting of 1 and all natural numbers, which are a product of primes in P_0. Show: All rings $R \subset \mathbb{Q}$ (endowed with the induced ring operations) have the form $R = S(P_0)^{-1}\mathbb{Z}$ with a suitable subset $P_0 \subset P$.

4. For a ring R we define its **affine linear group** $\mathrm{Aff}(R) \subset \mathbb{S}(R)$ by $\mathrm{Aff}(R) := \{f \in \mathbb{S}(R);\ \exists\, a \in R^*, b \in R : f(x) = ax + b\ \forall\, x \in R\}$. Show: $\mathrm{Aff}(R)$ is a semidirect product $\mathrm{Aff}(R) \cong R^+ \times_\sigma R^*$ with some homomorphism $\sigma : R^* \longrightarrow \mathrm{Aut}(R^+)$, where R^+ denotes the ring R considered as additive group.

5. Let $d \in \mathbb{N}$ be not a square. Show that $R := \mathbb{Z} + \mathbb{Z}\sqrt{d} \subset \mathbb{R}$ is a ring. Furthermore that the "norm" $N : R \longrightarrow \mathbb{Z}, x = a + b\sqrt{d} \mapsto N(x) := a^2 - b^2 d$ satisfies $N(xy) = N(x)N(y)$ and conclude $x \in R^* \Longleftrightarrow N(x) = \pm 1$. Assuming that there is $x \in R \setminus \mathbb{Z}$ with $N(x) = \pm 1$ (that is always true, but non-trivial!) show $R^* \cong \mathbb{Z} \times \mathbb{Z}_2$ as groups. Hint: The units $x > 1$ are of the form $x = a + b\sqrt{d}$ with $a, b > 0$. Conclude that there is a smallest unit $x \in R^*, x > 1$.

6. R: Let $R \subset \mathbb{C}$ be a ring with $z \in R \Longrightarrow |z|^2 \in \mathbb{N}$, invariant under complex conjugation, i.e. $z \in R \Longrightarrow \overline{z} \in R$. Determine R^*.

7. R: Let $\eta \in \mathbb{C} \setminus \mathbb{R}$ be a complex number with $\eta^2 \in \mathbb{Z} + \mathbb{Z}\eta := \{a + b\eta; a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Show, that $\mathbb{Z}+\mathbb{Z}\eta$ endowed with the addition and multiplication of complex numbers is a ring, satisfying the conditions of the ring $R \subset \mathbb{C}$ in the previous problem. (Hint: If $\eta^2 = a + b\eta$, then $(T - \eta)(T - \overline{\eta}) = T^2 - aT - b$.) Show that R^* is finite! For $\eta = i, \eta = \varepsilon := e^{\frac{2\pi i}{3}} = \frac{1}{2}(-1 + i\sqrt{3})$ determine the group of units explicitly! What does hold for the remaining rings $R = \mathbb{Z} + \mathbb{Z}\eta$?

8. Let K be a field. Interpret $K^{\mathbb{N}}$ as a subset of $K^{\mathbb{Z}}$ by extending a function $\mathbb{N} \longrightarrow K$, such that it assigns the value 0 to negative numbers in $\mathbb{Z} \supset \mathbb{N}$. The set $K((T))$ of all "**formal Laurent series with finite principal part**" consists of all functions $\in K^{\mathbb{Z}}$ which vanish for almost all $n < 0$. Show that the Cauchy multiplication for $K[[T]] = K^{\mathbb{N}}$ can be extended to $K((T)) \subset K^{\mathbb{Z}}$ and that $K((T))$ is a field, the field of fractions of $K[[T]]$. Indeed

$$K((T)) = Q(K[[T]]) = T^{-\mathbb{N}}K[[T]] = K[[T]] \oplus \bigoplus_{n=1}^{\infty} KT^{-n},$$

where $T^{-\mathbb{N}}K[[T]] := S^{-1}K[[T]]$ denotes the localization of $K[[T]]$ with respect to the multiplicative set $S = T^{\mathbb{N}}$ of all T-powers.

9. **Formal Laurent Series from a topological point of view:** Let K be a field. We extend the order function $\omega : K[[T]] \longrightarrow \mathbb{Z} \cup \{\infty\}$ to $K((T))$ by setting $\omega(T^n h) = \omega(h) - n$ for $g \in K[[T]]$ and define the absolute value $|f| \in \mathbb{R}_{\geq 0}$ of a series $f \in K((T))$ by $|f| := 2^{-\omega(f)}$ (with the convention $2^{-\infty} = 0$). Show: The absolute value satisfies

$$|f + g| \leq \max\{|f|, |g|\}\ ,\ |fg| = |f| \cdot |g|$$

for all $f, g \in K((T))$ (The first inequality is sometimes called the strong triangle inequality). Then $d(f, g) := |f - g|$ is a metric (distance function) on the set $K((T))$

and the resulting metric space is complete, i.e. every Cauchy sequence has a limit. Indeed $K[[T]] = \{f \in K((T)); |f| \leq 1\}$ then is nothing but the closed ball of radius 1 around 0, and any series $\sum_{\nu=-\ell}^{\infty} a_\nu T^\nu = \lim_{n\to\infty} \sum_{\nu=-\ell}^{n} a_\nu T^\nu$ is the limit of its partial sums - but note that this convergence is not a convergence of functions! In K there is no notion of convergence!

3.2 Homomorphisms

Definition 3.10. *Let R, S be rings. A map $\varphi : R \longrightarrow S$ is called a* **ring homomorphism** *iff*

$$\varphi(a+b) = \varphi(a) + \varphi(b) \ , \ \varphi(ab) = \varphi(a)\varphi(b) \ ,$$

for all $a, b \in R$ and

$$\varphi(1) = 1 \ ,$$

where 1 denotes the unity in the respective ring R or S. It is called a **ring isomorphism** *iff it is in addition bijective, and R is* **isomorphic** *to S, in symbols: $R \cong S$, iff there is a ring isomorphism $\varphi : R \longrightarrow S$.*

Remark 3.11. The condition $\varphi(1) = 1$ guarantees that $\varphi \equiv 0$ is not admitted as a ring homomorphism. As an other consequence, the map $R \longrightarrow R^2, a \mapsto (a, 0)$, is not a ring homomorphism either, though it is compatible with the ring operations.

Example 3.12. For every ring R there is exactly one ring homomorphism $\varphi : \mathbb{Z} \longrightarrow R$, mapping $0 \in \mathbb{Z}$ to $0 \in R$, $n \in \mathbb{Z}_{>0}$ to the n-fold sum $1 + ... + 1$ and $-n \in \mathbb{Z}_{<0}$ to $(-1) + ... + (-1)$ (n times). Indeed, this is nothing but the group homomorphism $\varphi_a : \mathbb{Z} \longrightarrow G$ of Example 2.9.3, with the additive group R instead of a multiplicatively written G, and $a = 1$. Often one writes simply n instead of $\varphi(n)$; but note that φ need not be injective: $n = 0$ can hold in R, though $n > 0$ i $\mathbb{Z}$. For example take $R = \mathbb{Z}_n$!

Definition 3.13. *Let R be a ring and $\varphi : \mathbb{Z} \longrightarrow R$ the natural ring homomorphism.*

1. *The* **characteristic** $\mathrm{char}(R)$ *of the ring R is defined as the natural number n such that*

$$\ker(\varphi) = \varphi^{-1}(\{0\}) = \mathbb{Z}n \ .$$

With other words: Either $\mathrm{char}(R) = 0$ *or*

$$\mathrm{char}(R) = \min\{k \in \mathbb{N}_{>0}; k = 0 \text{ in } R\} > 1.$$

2. *The* **prime field** $P(K) \subset K$ *of a field* K *is defined as*

$$P(K) := \varphi(\mathbb{Z}),$$

if $\mathrm{char}(K) > 0$ *and as*

$$P(K) := \hat{\varphi}(\mathbb{Q}),$$

if $\mathrm{char}(K) = 0$ *and* $\hat{\varphi} : \mathbb{Q} = Q(\mathbb{Z}) \longrightarrow K$ *is the unique extension of the natural ring homomorphism* $\varphi : \mathbb{Z} \longrightarrow K$.

Remark 3.14. 1. $\mathrm{char}(\mathbb{Z}_n) = n$.

2. For an integral domain R, its characteristic satisfies $\mathrm{char}(R) = 0$ or $\mathrm{char}(R) = p$ is a prime. This is a consequence of the fact, that $\mathbb{Z}_{\mathrm{char}(R)} \cong \varphi(\mathbb{Z}) \subset R$ is an integral domain as well.

3. For a field K of characteristic 0 we have $P(K) \cong \mathbb{Q}$, while for $\mathrm{char}(K) = p > 0$ we find $P(K) \cong \mathbb{Z}_p$.

4. Let $n = p_1^{k_1} \cdot ... \cdot p_r^{k_r}$ be the prime factorization of the natural number $n \in \mathbb{N}$. The Chinese remainder theorem 2.85 provides even a ring isomorphism

$$\mathbb{Z}_n \xrightarrow{\cong} \mathbb{Z}_{p_1^{k_1}} \times ... \times \mathbb{Z}_{p_r^{k_r}}, \overline{\ell} = \ell + \mathbb{Z}n \mapsto (\ell + \mathbb{Z}p_1^{k_1}, ..., \ell + \mathbb{Z}p_r^{k_r}) \quad ,$$

hence in particular a group isomorphism of the corresponding groups of units

$$\mathbb{Z}_n^* \xrightarrow{\cong} \mathbb{Z}_{p_1^{k_1}}^* \times ... \times \mathbb{Z}_{p_r^{k_r}}^* \ .$$

As a consequence, Eulers φ-function satisfies

$$\varphi(n) = \varphi(p_1^{k_1}) \cdot ... \cdot \varphi(p_r^{k_r}) \ .$$

The polynomial ring is, similarly as for example free groups, characterized by a "universal mapping property":

Proposition 3.15. *Let* $\psi : R \longrightarrow S$ *be a ring homomorphism and* $a \in S$. *Then there is a unique ring homomorphism* $\psi_a : R[T] \longrightarrow S$ *with* $\psi_a|_R = \psi$ *and* $\psi_a(T) = a$.

Proof. For $f = \sum a_\nu T^\nu$ set $\psi_a(f) = \sum \psi(a_\nu) a^\nu$. Since $f = 0$ iff all coefficients $a_\nu = 0$, the homomorphism ψ_a is well defined and obviously unique. □

Remark 3.16. If $R \subset S$ and $\psi : R \hookrightarrow S$ is the inclusion, we also write $f(a)$ instead of $\psi_a(f)$, i.e.

$$f(a) = \sum a_\nu a^\nu \in R \ \ , \text{ if } f = \sum a_\nu T^\nu,$$

and call the ring homomorphism $\psi_a : R[T] \longrightarrow R, f \mapsto f(a)$, the **evaluation (homomorphism)** at $a \in S$.
Thus a polynomial $f \in R[T]$ induces a function

$$\hat{f} : R \longrightarrow R \ , \ a \mapsto f(a) \ ,$$

and the map $R[T] \longrightarrow R^R, f \mapsto \hat{f}$ is a not necessarily injective ring homomorphism: For example consider $R = \mathbb{Z}_p$ and $f = T^p - T$: Obviously $f(0) = 0$, while all elements $a \in \mathbb{Z}_p^*$ have order $p-1$, whence $a^p = a$ resp. $f(a) = 0$. Indeed this can happen only for finite integral domains:

Calling an element $a \in R$ with $f(a) = 0$ a **zero** of f, we have:

Proposition 3.17. *A polynomial $f \in R[T] \setminus \{0\}$ over an integral domain R has at most $\deg(f)$ distinct zeros in R.*

Proof. We do induction on $\deg(f)$. We may assume that $\deg(f) > 0$. If $a \in R$ is a zero of f, the division algorithm 3.6 yields $f = q \cdot (T - a) + r$, where $\deg(r) < 1$, i.e. $r = b \in R$. Hence $0 = f(a) = q(a)(a - a) + b = b$ resp. $f = q \cdot (T - a)$. Since $\deg(q) < \deg(f)$, the induction hypothesis tells us, that q has at most $\deg(q)$ distinct zeros in R. But R being an integral domain, a zero of f is either a zero of q or of $T - a$, i.e. equals a. Hence we are done. □

Corollary 3.18. *For an infinite integral domain R the homomorphism $R[T] \longrightarrow R^R, f \mapsto \hat{f}$ is injective, i.e. for a polynomial $f \in R[T]$ we have*

$$f = 0 \Longleftrightarrow f(a) = 0 \ , \forall \ a \in R \ .$$

Problems 3.19. 1. R: An element $e \in R$ in a ring R is called **idempotent** iff $e^2 = e$. Show: If R is an integral domain, then $0, 1$ are the only idempotent elements. Furthermore: If $1 = e_1 + ... + e_s$ with elements $e_i \neq 0$ and $e_i e_j = 0$ for $i \neq j$, the elements e_i are idempotent and

$$R \cong \prod_{i=1}^{s} R_i$$

with the rings $R_i := Re_i$.

2. R: Show: There is a (unique) ring homomorphism $\mathbb{Z}_n \longrightarrow \mathbb{Z}_m$, iff $m|n$.
3. R: Show for $q := p^n$ with a prime number p that $\mathbb{Z}_q[T]^* = \mathbb{Z}_q^* + pT\mathbb{Z}_q[T]$.
4. R: A universal mapping property: Let R be an integral domain and $S \subset R \setminus \{0\}$ a multiplicative subset. Show: Every ring homomorphism $\psi : R \longrightarrow P$ to a ring P with $\psi(S) \subset P^*$ can uniquely be extended to a homomorphism $\hat{\psi} : S^{-1}R \longrightarrow P$.
5. R: Let $H \subset R^*$ be a finite subgroup of the group of units R^* of an integral domain R. Show: H is a cyclic group. Hint: Show first: If all elements $a \in H$ have an order $< |H|$, there is an exponent $q < |H|$ with $a^q = 1$ for all $a \in H$. Then consider the zeros of the polynomial $T^q - 1 \in R[T]$! Show as well $H = C_n(R) := \{a \in R; a^n = 1\}$ with $n := |H|$.
6. R: Every ring homomorphism $\psi : R[T] \longrightarrow R[T]$ with $\psi|_R = \mathrm{id}_R$ has the form $\psi = \psi_g$ with a polynomial $g \in R[T]$, i.e. it is a substitution homomorphism, where $\psi(f)$ is obtained by substituting T with g, i.e. $\psi_g(f) = f(g)$. Furthermore: If R is an integral domain: ψ_g is an isomorphism (or automorphism) iff $g = aT + b$ with $a \in R^*, b \in R$. Determine an isomorphism $\mathrm{Aff}(R) \xrightarrow{\cong} \mathrm{Aut}_R(R[T])$ between the affine linear group $\mathrm{Aff}(R)$, and the group $\mathrm{Aut}_R(R[T])$ of all automorphisms of $R[T]$ fixing the elements in the ring R.
7. A continuation of the previous problem: Show: Every ring homomorphism $\psi_g : R[T] \longrightarrow R[[T]]$ with a power series $g \in TR[[T]]$ extends uniquely to a ring homomorphism $\hat{\psi}_g : R[[T]] \longrightarrow R[[T]]$ (such that we may define substitutions even for formal power series: $f(g) := \hat{\psi}_g(f)$ in case $g \in TR[[T]]$). It is an isomorphism iff $g \in R^*T + R[[T]]T^2$. Hint: An equality in $R[[T]]$ holds iff it does in $R[[T]]/(T^n) \cong R[T]/(T^n)$ for all $n \in \mathbb{N}$.
8. R: Let K be a field, $a_1, ..., a_s, b_1, ..., b_s \in K$, with the elements $a_1, ..., a_s$ pairwise distinct. Show: There is a polynomial $f \in K[T]$ with $f(a_i) = b_i$ for $i = 1, ..., s$.
9. Let K be a field and $A \in K^{n,n}$. For $f = \sum_\nu a_\nu T^\nu \in K[T]$ let $f(A) := a_0 E + \sum_{\nu>0} a_\nu A^\nu \in K^{n,n}$. Show:

   $$K[A] := \{B \in K^{n,n}; B = f(A) \text{ for some } f \in K[T]\}$$

   is a ring, in particular commutative. Furthermore: If A is diagonalizable, then $K[A] \cong K^r$ with some $r \in \mathbb{N}$.

3.3 Ideals and Factor Rings

Let K be a field and $f \in K[T]$ a polynomial without zeros in K. In this section we explain how we can find a larger field $E \supset K$, where f has a zero.

To begin with, let us first assume that $E \supset K$ together with a zero $a \in E$ of f are already given. Then the evaluation homomorphism

$$\psi_a : K[T] \longrightarrow E, p \mapsto p(a),$$

induces an isomorphism

$$K[T]/\ker\psi_a \xrightarrow{\cong} K[a] := \{p(a) \in E; p \in K[T]\}$$

of abelian groups. Indeed it is an isomorphism of rings as well: First of all, given any ring homomorphism

$$\psi : R \longrightarrow S$$

its kernel $\ker\psi \subset R$ is

1. an additive subgroup
$$\ker\psi \leq R$$
and
2. satisfies
$$R \cdot \ker\psi \subset \ker\psi.$$

Thus we are led to the notion of an "ideal" of a ring R.

Definition 3.20. *Let R be a ring. An* **ideal** $\mathfrak{a} \subset R$ *is an additive subgroup satisfying*

$$a \in \mathfrak{a}, b \in R \Longrightarrow ab \in \mathfrak{a}.$$

An ideal $\mathfrak{a} \subset R$ is called a **proper ideal** *iff $\mathfrak{a} \neq R$ or equivalently, iff $1 \notin \mathfrak{a}$.*

Proposition 3.21. *Let $\mathfrak{a} \subset R$ be a proper ideal. Then the (additive) factor group $R/\mathfrak{a}$ endowed with the multiplication*

$$\overline{a} \cdot \overline{b} := \overline{ab}$$

is a ring.

Proof. We have to show that the multiplication is well defined. So let $\overline{a}_1 = \overline{a}, \overline{b}_1 = \overline{b}$, i.e. $a_1 = a + c, b_1 = b + d$ with elements $c, d \in \mathfrak{a}$. Then we have $a_1 b_1 = (a + c)(b + d) = ab + (ad + bc + cd)$, where the expression in the parenthesis belongs to $\mathfrak{a}$. Hence $\overline{a_1 b_1} = \overline{ab}$. □

Example 3.22. 1. The most basic ideals are the entire ring R itself, also called the **unit ideal**, and the **zero ideal** $\{0\}$.

2. Given an element $a \in R$ the set $(a) := Ra := \{ba, b \in R\}$ of all multiples of a is an ideal, the **principal ideal** generated by a.

3. A ring R is a field iff the unit and the zero ideal are the only ideals in R.

   Proof. "$\Longrightarrow$": If R is a field and $\mathfrak{a} \subset R$ a non-zero ideal, there is an element $a \in \mathfrak{a}, a \neq 0$. But then it follows $1 = a^{-1}a \in \mathfrak{a}$ and thus $\mathfrak{a} = R$.
   "$\Longleftarrow$": We have to show $R^* = R \setminus \{0\}$ or rather "$\supset$": Let $a \in R \setminus \{0\}$. Then $Ra \neq \{0\}$, hence $Ra = R$. So there is $b \in R$ with $1 = ba$, i.e. $a \in R^*$. □

4. In the ring $\mathbb{Z}$ additive subgroups and ideals coincide; indeed in 2.25 we have seen that they are all principal ideals $\mathfrak{a} = \mathbb{Z}n$ with a (unique) $n \in \mathbb{N}$.

5. Let $\mathfrak{a}, \mathfrak{b} \subset R$ be ideals. Then also their intersection $\mathfrak{a} \cap \mathfrak{b}$, their sum

   $$\mathfrak{a} + \mathfrak{b} := \{a + b; a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

   as well as their product

   $$\mathfrak{a} \cdot \mathfrak{b} := \{a_1 b_1 + ... + a_r b_r; r \in \mathbb{N}, a_i \in \mathfrak{a}, b_i \in \mathfrak{b},\ i = 1, ..., r\}$$

   are ideals. In fact

   $$\mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}, \mathfrak{b} \subset \mathfrak{a} + \mathfrak{b}.$$

6. The elements $a_1, ..., a_r \in R$ are said to generate the ideal $\mathfrak{a} \subset R$ iff

   $$\mathfrak{a} = Ra_1 + ... + Ra_r.$$

7. Let $\varphi : R \longrightarrow S$ be a ring homomorphism between the rings R and S, $\mathfrak{a} \subset R, \mathfrak{b} \subset S$ ideals. Then the inverse image $\varphi^{-1}(\mathfrak{b}) \subset R$ is an ideal in R, while the image $\varphi(\mathfrak{a}) \subset S$ is an ideal in the ring S, if φ is surjective. In particular its kernel

   $$\ker(\varphi) = \varphi^{-1}(\{0\})$$

   is an ideal in R.

8. A ring homomorphism $\varphi : K \longrightarrow S$ from a field to some ring $S \neq \{0\}$ is injective (since $1 \notin \ker(\varphi)$ we have $\ker(\varphi) = \{0\}$) and therefore often treated as an inclusion.

Let us return to our starting point: The ring

$$K[a] \cong K[T]/\mathfrak{a}$$

with $\mathfrak{a} = \ker \psi_a$ is an integral domain. In general we define:

Definition 3.23. *A proper ideal $\mathfrak{a} \subset R$ of a ring R is called*

1. **prime** *or a* **prime ideal** *if the factor ring $R/\mathfrak{a}$ is an integral domain or equivalently if*
$$ab \in \mathfrak{a} \Longrightarrow a \in \mathfrak{a} \vee b \in \mathfrak{a} \quad .$$

2. **maximal** *iff there is no proper ideal $\mathfrak{b} \subset R$ in R containing $\mathfrak{a}$ but $\mathfrak{a}$ itself:*
$$\mathfrak{a} \subset \mathfrak{b} \Longrightarrow \mathfrak{b} = \mathfrak{a}.$$

3. *a* **principal ideal**, *if it has the form $\mathfrak{a} = Ra$ with some element $a \in R$, it is then called the principal ideal generated by a. A different notation is $(a) := Ra$.*

An integral domain R is called a **principal ideal domain**, *a* **PID** *for short, if every ideal in R is a principal ideal.*

Example 3.24. 1. Since the ideals in $\mathbb{Z}$ are nothing but the additive subgroups, Proposition 2.25 yields that $\mathbb{Z}$ is a principal ideal domain; the maximal ideals are the ideals $(p) = \mathbb{Z}p$ with a prime number $p \in \mathbb{N}$ and beside the maximal ideals there is only one prime ideal, the zero ideal $(0) = \mathbb{Z}0$.

2. If $\mathfrak{p} \subset R$ is a prime ideal in the integral domain R, its complement $S := R \setminus \mathfrak{p}$ is a multiplicative set. The ring $R_\mathfrak{p} := S^{-1}R$ is called the **localization** of R with respect to the prime ideal $\mathfrak{p}$.

Remark 3.25. One can show that every proper ideal $\mathfrak{a} \subset R$ is contained in a maximal ideal $\mathfrak{m} \subset R$, cf. 5.7.

As with prime ideals, maximal ideals can be defined in terms of the corresponding factor ring:

Proposition 3.26. *A proper ideal $\mathfrak{a} \subset R$ is a maximal ideal iff the factor ring $R/\mathfrak{a}$ is a field. In particular a maximal ideal is a prime ideal.*

Proof. Use Example 3.22.3 together with the fact that given an ideal $\mathfrak{a} \subset R$ in the ring R, there is a bijective correspondence between the set of all ideals in the factor ring $R/\mathfrak{a}$ and the set off all ideals in R, which contain $\mathfrak{a}$: To an ideal $\mathfrak{b} \supset \mathfrak{a}$ we associate the ideal $\varrho(\mathfrak{b}) \subset R/\mathfrak{a}$, where $\varrho : R \longrightarrow R/\mathfrak{a}$ denotes the quotient projection. On the other hand to $\mathfrak{c} \subset R/\mathfrak{a}$ corresponds the inverse image $\varrho^{-1}(\mathfrak{c}) \subset R$. □

Back to our original situation: Since $\psi_a(f) = f(a) = 0$, the prime ideal $\mathfrak{a} = \ker \psi_a \subset K[T]$ contains f. But, as we shall see later on, a nontrivial prime ideal of $K[T]$ is maximal. Consequently the minimal solutions of our problem are given by

$$E := K[T]/\mathfrak{m},\ a := \overline{T},$$

where $\mathfrak{m} \subset K[T]$ is a maximal ideal containing f (we remark that the composition $K \hookrightarrow K[T] \longrightarrow E$ is injective according to 3.22.8). By this we mean that an arbitrary solution contains one of the above type.

On the other hand as a consequence of the next result, nontrivial ideals in $K[T]$ are in one-to-one correspondence with monic polynomials:

Proposition 3.27. *The polynomial ring $K[T]$ over a field K is a principal ideal domain.*

Proof. Let $\mathfrak{a} \subset K[T]$ be an ideal. If $\mathfrak{a} \neq \{0\}$, we can choose a polynomial $f \in \mathfrak{a} \setminus \{0\}$ of minimal degree, and since K is a field, we may assume that f is monic. Then we have $\mathfrak{a} = (f)$. The inclusion "$\supset$" is obvious. "$\subset$": Consider a polynomial $h \in \mathfrak{a}$. We apply the division algorithm 3.6 and write $h = qf + r$, where $\deg(r) < \deg(f)$. But then, since even $r = h - qf \in \mathfrak{a}$, necessarily $r = 0$ by the choice of f. So $h = qf \in (f)$. □

Example 3.28. For the ring $K[[T]]$ of formal power series over a field K the situation is strikingly different from that one for the polynomial ring: There are only the following ideals: $(T^n), n \in \mathbb{N}$ and the zero ideal; (T) is the only maximal ideal, and beside the zero ideal the only prime ideal. In particular $K[[T]]$ is a principal ideal domain. The proof relies on the fact that its group of units $K[[T]]^*$ consists of all series with a nonzero constant term.

In particular we obtain that a maximal ideal $\mathfrak{m} \ni f$ is of the form

$$\mathfrak{m} = K[T]g$$

with an irreducible polynomial $g \in K[T]$ dividing f (a polynomial is irreducible if it does not admit a factorization as a product of polynomials of lower degree): For a reducible polynomial g the factor ring $K[T]/\mathfrak{m}$ would not be an integral domain.

We discuss the relevant notions in general for an arbitrary integral domain:

Definition 3.29. *Let R be an integral domain.*

1. *An element $u \in R \setminus (R^* \cup \{0\})$ is called* **irreducible**, *iff $u = ab \Longrightarrow a \in R^* \vee b \in R^*$, i.e. u can not be written as the product of two non-units.*

2. *Two elements $u, u' \in R \setminus \{0\}$ are called* **associated**, *iff $(u) = (u')$ iff $u' = eu$ with a unit $e \in R^*$.*

3. *An element $p \in R \setminus (R^* \cup \{0\})$ is called* **prime**, *iff $(p) = Rp$ is a prime ideal iff*
$$p|ab \Longrightarrow p|a \vee p|b \ .$$

Obviously, $(u) = (u')$ holds for associated elements $u, u' \in R$. If on the other hand $(u) = (u')$, we can write $u' = eu$ and $u = e'u'$ with elements $e, e' \in R$, whence $u = e'eu$ resp. $0 = (1 - e'e)u$. The ring R being an integral domain, we conclude $1 - e'e = 0$ resp. $e \in R^*$.

Remark 3.30.

1. A prime element $p \in R$ is irreducible. Show that!

2. Since $K[T]^* = K^*$, two polynomials $f, g \in K[T]$ are associated iff their differ by a nonzero constant: $g = \lambda f$ with some $\lambda \in K^*$.

3. A polynomial $f \in K[T]$ is irreducible, if it can not be written $f = gh$ with polynomials g, h of lower degree.

Proposition 3.31. *An irreducible element $u \in R$ in a principal ideal domain R is prime.*

Proof. We assume $u|ab$, and show that if u does not divide a, then it divides b. Consider the ideal $Ru + Ra := \{ru + sa; r, s \in R\}$, consisting of all linear combinations of u and a with coefficients in R. Since R is a principal ideal domain, there is an element $d \in R$ with $Ru + Ra = Rd$. In particular $d|u$, say $u = cd$. But u being irreducible either c or d is a unit. If $c \in R^*$, we obtain, since $d|a$, that also $u|a$, a contradiction to our assumption. So d is a unit, and therefore $1 \in Rd = Ru + Ra$: As a consequence we may write $1 = ru + sa$ with elements $r, s \in R$. Now we multiply with b and find that $b = rub + s(ab)$ is divisible by u. □

As an immediate consequence we obtain:

Corollary 3.32. *i) Let R be a principal ideal domain which is not a field. An ideal $(a) := Ra$ is*

- *prime, iff $a = 0$ or a is irreducible.*
- *maximal, iff a is irreducible.*

ii) Let K be a field and $f \in K[T]$ an irreducible polynomial. Then $K[T]/(f)$ is a field.

Proof. The zero ideal is prime, since R is an integral domain, but not maximal, $R \cong R/\{0\}$ being not a field. On the other hand, let $(a) \subset R$ be a prime ideal, $a \neq 0$. Then a is irreducible: Assume $a = bc$ with non-units b, c. So one of the factors, say b, is contained in (a), and thus $(b) \subset (a) \subset (b)$, i.e. b is associated to a respectively $c \in R^*$.
It remains to show, that (a) is maximal, if a is irreducible: Consider an ideal $\mathfrak{b}$ containing (a). Since R is a principal ideal domain, it is of the form $\mathfrak{b} = (b)$, hence $a \in (b)$ or $a = bc$ with some element $c \in R$. But a being irreducible, either b or c is a unit, with other words either $(b) = R$ or $(b) = (a)$.
The second part follows now from the fact that $K[T]$ is a principal ideal domain and the first part. □

Irreducible polynomials being prime, we obtain a factorization of a polynomial analogous to the prime factorization of a natural number:

Proposition 3.33. *Every monic polynomial $f \in K[T]$ can be written uniquely (up to order) as a product*

$$f = f_1^{k_1} \cdot ... \cdot f_r^{k_r}$$

with pairwise distinct irreducible monic polynomials $f_i \in K[T]$ and exponents $k_i \geq 1$.
In particular, for every polynomial $f \in K[T]$ there exists a field E containing K, such that f has a zero in E, namely $E := E_i := K[T]/(f_i)$ with some $i, 1 \leq i \leq r$.

Proof. The existence of such a factorization follows by induction on $\deg(f)$: If f is irreducible, nothing has to be shown; if not, we write $f = gh$ with polynomials of strictly lower degree, which according to the induction hypothesis are products of irreducible polynomials, hence f itself as well. The uniqueness follows from the fact that irreducible polynomials are prime: We use induction on the number $k := k_1 + ... + k_r$ of factors in such a representation. For $k = 1$ the statement is clear, since then $f = f_1$ is irreducible and does not admit a nontrivial factorization. Assume now there is an other factorization $f = g_1 \cdot ... \cdot g_\ell$ with irreducible monic polynomials $g_j \in K[T]$. Since f_1 is prime, we find that for some index j we have $f_1 | g_j$ or rather $f_1 = g_j$, the polynomial g_j being irreducible and both f_1, g_j monic. We may assume $j = 1$ and then obtain $f_1^{k_1 - 1} f_2^{k_2} \cdot .... \cdot f_r^{k_r} = g_2 \cdot ... \cdot g_\ell$ and can apply the induction hypothesis. □

Integral domains admitting unique prime factorization get a name:

Definition 3.34. An integral domain R is called **factorial** (or a **UFD**= **U**nique **F**actorization **D**omain), iff

1. every irreducible element $u \in R$ is prime,

2. every non-unit is a finite product of irreducible elements.

Example 3.35. The ring $\mathbb{Z}$ as well as the ring $K[T]$ are UFDs.

For a factorial ring an analogue of Prop. 3.33 holds: Every non-unit can be written as a product of irreducible elements, and the factors are unique up to order and multiplication with units.

Here are more factorial rings:

Proposition 3.36. *A PID is a UFD.*

Proof. Call a non-unit $u \in R \setminus \{0\}$ nonfactorizable, if it is not a product of (finitely many) irreducible elements. Because of Prop. 3.31 it suffices to show that there are no nonfactorizable elements in a PID. Otherwise we can construct a strictly increasing sequence of principal ideals $\mathfrak{a}_i = Ru_i$ generated by nonfactorizable elements $u_i \in R$, i.e. such that

$$\mathfrak{a}_0 \subsetneqq \mathfrak{a}_1 \subsetneqq \ldots\ldots \ .$$

Start with any nonfactorizable element $u_0 \in R$. The nonfactorizable element u_i being found, write it as a product of two non-units. At least one of the two factors is again nonfactorizable, choose it as the element u_{i+1}. Now

$$\mathfrak{a} := \bigcup_{i=0}^{\infty} \mathfrak{a}_i$$

is an ideal. But R is a PID; thus $\mathfrak{a} = Ru$. Then $u \in \mathfrak{a}_n$ for some $n \in \mathbb{N}$ and hence

$$\mathfrak{a}_i = \mathfrak{a} = \mathfrak{a}_n$$

holds for $i \geq n$, a contradiction. □

Remark 3.37.

1. An example of an integral domain with nonfactorizable elements is discussed in Problem 3.38.15.
2. The polynomial ring over a UFD is again a UFD, see Problem 3.46.8. On the other hand: The polynomial ring over a PID, which is not a field, is never a PID.

3.3.1 Digression: p-adic number fields

Let p be a prime number. The ring $\hat{\mathbb{Z}}_p$ of all p-**adic integers** is defined as a subring

$$\hat{\mathbb{Z}}_p \subset \prod_{n=1}^{\infty} \mathbb{Z}_{p^n}$$

of the direct product of the residue class rings $\mathbb{Z}_{p^n}, n \in \mathbb{N}_{>0}$, namely

$$\hat{\mathbb{Z}}_p := \left\{ (\xi_n)_{n\geq 1} \in \prod_{n=1}^{\infty} \mathbb{Z}_{p^n}; \forall\ n \geq 2\ : \pi_n(\xi_n) = \xi_{n-1} \right\} ,$$

where $\pi_n : \mathbb{Z}_{p^n} \longrightarrow \mathbb{Z}_{p^{n-1}}$ is the natural ring homomorphism. Since the sequence $(\xi_n := 1+(p^n))_{n\geq 1}$ has infinite order, it has characteristic $\mathrm{char}(\hat{\mathbb{Z}}_p) = 0$, in particular $\mathbb{Z} \subset \hat{\mathbb{Z}}_p$, and its group of units is

$$\hat{\mathbb{Z}}_p^* = \left\{ e = (\varepsilon_n) \in \hat{\mathbb{Z}}_p; \varepsilon_1 \neq 0 \right\}.$$

Indeed any $x = (\xi_n) \in \hat{\mathbb{Z}}_p \setminus \{0\}$ can uniquely be written as a product

$$x = p^r e,\ r \in \mathbb{N}_{\geq 0}, e \in \hat{\mathbb{Z}}_p^*.$$

This is seen as follows: If $\xi_n = 0$ for $n \leq r$ and $\xi_{r+1} \neq 0$, then, writing $\xi_n = a_n + (p^n)$, we have $a_n = p^r b_n$ for $n \geq r$, and may take $\varepsilon_n = b_{n+r} + (p^n)$. As a consequence $\hat{\mathbb{Z}}_p$ is a PID with the $(p^r), r \in \mathbb{N}$, as the nonzero ideals.

The ring $\hat{\mathbb{Z}}_p \supset \mathbb{Z}$ can be understood as a completion of $\mathbb{Z}$: For a p-adic integer $x \in \hat{\mathbb{Z}}_p$ its absolute value $|x| \in \mathbb{R}_{\geq 0}$ is defined as

$$|x| := \begin{cases} p^{-r} & , \text{ if } x \in p^r \cdot \hat{\mathbb{Z}}_p^* \\ 0 & , \text{ if } x = 0 \end{cases}.$$

The absolute value satisfies

$$|x+y| \leq \max\{|x|, |y|\}\ ,\ |xy| = |x| \cdot |y|\ ,\ |x| \leq 1$$

for all $x, y \in \hat{\mathbb{Z}}_p$ (The first inequality is sometimes called the strong triangle inequality). Then $d(x,y) := |x-y|$ is a metric (distance function) on the set $\hat{\mathbb{Z}}_p$ and the resulting metric space is complete, i.e. every Cauchy sequence has a limit, with $\mathbb{Z} \subset \hat{\mathbb{Z}}_p$ as dense subset: For $x = (\xi_n = a_n + (p^n))$, we have $x = \lim_{n\to\infty} a_n$. Assuming $0 \leq a_n < p^n$, the coefficients c_k of the finite p-adic expansions $a_n = \sum_{k<n} c_k p^k, 0 \leq c_k < p$, do not depend on n and provide an infinite unique p-adic expansion

$$x = \sum_{k=0}^{\infty} c_k p^k, 0 \leq c_k < p.$$

This suggests that there should be a relation between p-adic integers and formal power series with integer coefficients: Since $|p| < 1$ and $|c| \leq 1$ for all $c \in \hat{\mathbb{Z}}_p$, the series $\sum c_k p^k$ converges for any choice of the coefficients $c_k \in \mathbb{Z}$; in particular we may define an evaluation homomorphism

$$\mathbb{Z}[[T]] \longrightarrow \hat{\mathbb{Z}}_p, f = \sum_{k=0}^{\infty} c_k T^k \mapsto f(p) := \sum_{k=0}^{\infty} c_k p^k;$$

it is surjective and has kernel $(T-p) \subset \mathbb{Z}[[T]]$: If $f(p) = 0$, necessarily $c_0 = -pb_0$ with some $b_0 \in \mathbb{Z}$, since otherwise $|c_0| = 1$ and $|f(p)| = |c_0| = 1$ (using $|x+y| = \max\{|x|, |y|\}$ for $|x| \neq |y|$). Now replace $f_0 := f$ with $f_1 = T^{-1}(f - (T-p)b_0)$ and repeat the same argument to find b_1 etc.; the resulting series $g = \sum b_k T^k$ satisfies $f = (T-p)g$. Altogether we have found an alternative description of the ring of p-adic integers:

$$\hat{\mathbb{Z}}_p \cong \mathbb{Z}[[T]]/(T-p) \ .$$

The field of fractions $\mathbb{Q}_p := Q(\hat{\mathbb{Z}}_p)$ can be realized as

$$\mathbb{Q}_p = p^{-\mathbb{N}}\hat{\mathbb{Z}}_p$$

with the multiplicative subset $S = p^{\mathbb{N}}$ (writing $(p^{\mathbb{N}})^{-1} = p^{-\mathbb{N}}$), and the absolute value extends in an obvious way, indeed

$$\mathbb{Q}_p = \{0\} \cup \bigcup_{r=-\infty}^{\infty} p^r \hat{\mathbb{Z}}_p^* \ ,$$

where $p^r\hat{\mathbb{Z}}_p^*$ is the "sphere" of radius p^{-r} and center 0. Furthermore the equality

$$\hat{\mathbb{Z}}_p^* \cap \mathbb{Q} = \left\{ \frac{a}{b}; a, b \in \mathbb{Z}, \gcd(a,p) = 1 = \gcd(b,p) \right\}$$

explains how to compute $|x|$ for $x \in \mathbb{Q} \subset \mathbb{Q}_p$.

The elements in $\mathbb{Q}_p$ are called **p-adic numbers** and the field $\mathbb{Q}_p$ the **p-adic number field**, introduced by Kurt Hensel (1861-1941).

Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, the p-adic numbers can, as the reals, be thought of as a completion of the rationals, but note that $\mathbb{Z} \subset \mathbb{R}$ is discrete:

$$\mathbb{R} \supset \overline{\mathbb{Z}} = \mathbb{Z},$$

and unbounded, while $\mathbb{Z} \subset \mathbb{Q}_p$ is bounded, indeed its closure $\overline{\mathbb{Z}} \subset \mathbb{Q}_p$ is the closed unit ball:

$$\mathbb{Q}_p \supset \overline{\mathbb{Z}} = \{x \in \mathbb{Q}_p; |x| \leq 1\} = \hat{\mathbb{Z}}_p.$$

There are more strange features from the topological point of view: The strong triangle inequality implies, that the open balls

$$B_\varepsilon(0) := \{x \in \hat{\mathbb{Z}}_p; |x| < \varepsilon\}, \ \varepsilon \leq 1,$$

form ideals in $\hat{\mathbb{Z}}_p$; in particular two balls $B_\varepsilon(x) = x + B_\varepsilon(0)$ and $B_\varepsilon(y) = y + B_\varepsilon(0)$ being ideal residue classes either coincide or are disjoint. Hence a ball $B_\varepsilon(x)$ is both open and closed – its complement is the union of all $B_\varepsilon(y),\ y \notin B_\varepsilon(x)$. As a consequence the metric space $\hat{\mathbb{Z}}_p$ is totally disconnected, i.e. there are no non-empty connected open sets in $\hat{\mathbb{Z}}_p$. Furthermore the natural order relation on $\mathbb{Z}$ can not be extended continuously to the ring of p-adic integers: E.g. the negative number $1 - p$ is a unit with the multiplicative inverse

$$(1-p)^{-1} = \sum_{n=0}^{\infty} p^n \ ,$$

an infinite sum of positive numbers!

Problems 3.38.

1. R: Show that a ring R has exactly one maximal ideal iff the non-units in R, i.e. the set $R \setminus R^*$, provide an ideal. In that case R is called a **local ring**. Which local rings do you know?

2. R: The **nilradical** of a ring R is defined as

$$\mathfrak{n} := \sqrt{\{0\}} := \{x \in R;\ \exists\ n \in \mathbb{N} :\ x^n = 0\} \ .$$

   Show: The nilradical is an ideal and the factor ring $R/\mathfrak{n}$ is **reduced**, i.e., does not contain non-zero nilpotent elements, or equivalently, its nilradical is the zero ideal.

3. R: Let K be a field and $R := \{f \in K[T]; f = a_0 + T^2 g,\ g \in K[T]\}$, cf. Problem 3.9.2. Show: The elements T^2, T^3 are irreducible in R, but not prime.

4. R: A ring is called euclidean if it is an integral domain and there is a function $R \setminus \{0\} \longrightarrow \mathbb{N}, x \mapsto ||x||$ satisfying:

   (a) If $b|a$, then $||b|| \leq ||a||$

   (b) If $a, b \in R, b \neq 0$, we can write $a = qb + r$, where the "remainder" r satisfies either $r = 0$ or $||r|| < ||b||$.

   Show: A euclidean ring is a principal ideal domain.

   (In fact, the first condition is not needed in the proof, we have only added it following the tradition!)

5. R: Show that a subring $R \subset \mathbb{C}$ is euclidean if $z \in R \Longrightarrow |z|^2 \in \mathbb{N}$ and for every $w \in \mathbb{C}$ there is an element $z \in R$ with $|z - w| < 1$. Hint: In order to check the division algorithm for $a, b \in R$, regard $w := \frac{a}{b} \in \mathbb{C}$!

6. R: Show that the ring $\mathbb{Z}[i]$ is euclidean and hence a principal ideal domain! (Its elements are called gaussian integers.) Determine the units in $\mathbb{Z}[i]$! Is the number $5 \in \mathbb{Z}[i]$ irreducible? If not, factorize it!

7. R: Let $\varepsilon := e^{\frac{2\pi i}{3}}$. Regard the rings $\mathbb{Z}[\varepsilon] \supset \mathbb{Z}[i\sqrt{3}]$. Show: In the smaller ring the elements $2, 2\varepsilon, 2\varepsilon^2$ are non-associated irreducible elements and $2 \cdot 2 = 4 = 2\varepsilon \cdot 2\varepsilon^2$, while the bigger ring $\mathbb{Z}[\varepsilon]$ is even euclidean.

8. R: Let K be a field and $h_1, ..., h_r \in K[T]$ polynomials without a common divisor. Show: There are polynomials $g_1, ..., g_r \in K[T]$ with $g_1h_1 + ... + g_rh_r = 1$.

9. Some linear algebra: Let K be a field, $A \in K^{n,n}$ and $f \in K[T]$ the minimal polynomial of A. Let $f = f_1^{k_1} \cdot ... \cdot f_r^{k_r}$ be the factorization of f in irreducible monic polynomials $f_1, ..., f_r$. Set

$$h_i := f_1^{k_1} \cdot ... \cdot f_{i-1}^{k_{i-1}} f_{i+1}^{k_{i+1}} \cdot ... \cdot f_r^{k_r}$$

and choose $g_i \in K[T]$ as in the previous problem with $g_1h_1 + ... + g_rh_r = 1$. Show: The matrices $P_i := g_i(A)h_i(A)$ satisfy $E = P_1 + ... + P_r$ with the unit matrix $E \in K^{n,n}$ and $P_iP_j = \delta_{ij}P_i$, and

$$K[A] \cong \bigoplus_{i=1}^{r} K[A_i]$$

with $A_i := AP_i$. Furthermore that A_i has the minimal polynomial $f_i^{k_i}$. And that the vector space $V := K^n$ is the direct sum of the A-invariant subspaces $V_i := \mathrm{Im}(P_i)$ (Hint: $AP_i = P_iA$ and $\mathrm{Im}(P_i)$ is the eigenspace of P_i for the eigenvalue 1!). What does the polynomial f_i look like for $K = \mathbb{C}$? Show: $\mathbb{C}[A_i] \cong \mathbb{C}[T]/[T^{k_i}]$. Is there a relationship to the Jordan normal form? (Camille Jordan, 1838-1922)

10. If one replaces in the definition of the p-adic integers the rings $\mathbb{Z}_{p^n}$ with $R[T]/(T^n)$, where R is an arbitrary ring, what does one obtain?

11. Show that the following conditions for a ring R are equivalent:

    (a) Every ideal $\mathfrak{a} \subset R$ is finitely generated, i.e., there are elements $f_1, ..., f_r \in R$, such that
    $$\mathfrak{a} = Rf_1 + ... + Rf_r = \{\sum_{i=1}^{r} g_if_i; g_1, ..., g_r \in R\}$$

    (b) Every increasing sequence (chain) of ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset ...$ in the ring R becomes stationary, i.e. there is $n \in \mathbb{N}$ such that $\mathfrak{a}_m = \mathfrak{a}_n \ \forall\ m \geq n$.

    (c) Every subset $A \subset$ Ideal(R) of the set Ideal(R) of all ideals in R, has a maximal element $\mathfrak{b} \in A$, i.e. such that there is no ideal in A containing $\mathfrak{b}$ as a proper subset, i.e., $\forall\ \mathfrak{a} \in A : \mathfrak{b} \subset \mathfrak{a} \Longrightarrow \mathfrak{b} = \mathfrak{a}$.

    A ring R is called **noetherian** (Emmy Noether, 1882-1935) if one (and thus all) of the above conditions are satisfied.

12. Show "Hilberts Basissatz" (David Hilbert, 1862-1943): The polynomial ring $R[T]$ over a noetherian ring is again noetherian. Hint: For an ideal $\mathfrak{b} \subset R[T]$ regard the chain $\mathfrak{a}_n := \{a \in R; \exists f = aT^n + ... \in \mathfrak{b}\} \subset R$ of ideals in the ring R.

13. Show: In a noetherian integral domain every element can be written as a product of (finitely many) irreducible elements. Hint: Assuming the contrary construct with the previous problem a strictly increasing infinite chain of ideals.

14. Show: The ideal $\mathfrak{a} \subset \mathbb{C}^{\mathbb{N}}$ consisting of all sequences $(a_\nu)_{\nu\in\mathbb{N}}$ with only finitely many $a_\nu \neq 0$ is not finitely generated.

15. Let $\mathcal{O}(\mathbb{C})$ be the ring of all entire functions (i.e. holomorphic everywhere in the complex plane $\mathbb{C}$) and

$$\mathfrak{a} := \{f \in \mathcal{O}(\mathbb{C});\ \exists\ n(f) \in \mathbb{N} :\ \forall\ n \in \mathbb{N},\ n \geq n(f) : f(n) = 0\}.$$

    Show, that the ideal $\mathfrak{a}$ is not finitely generated. (Do you see a connection with the situation of the preceding theorem?) Show: An irreducible function is prime, but not all functions can be written as a product of "prime functions". (Instead there is an infinite factorization according to Weierstraß' theorem! (Karl Theodor Wilhelm Weierstraß, 1815-1897).

16. Let $C(\mathbb{R})$ be the ring of all continuous real valued functions on $\mathbb{R}$. Show: The ideal $\mathfrak{m}_0 := \{f \in C(\mathbb{R}); f(0) = 0\}$ is not finitely generated.

17. Let $C^\infty(\mathbb{R})$ be the ring of all infinitely often differentiable real valued functions on $\mathbb{R}$. Show: $\mathfrak{p} := \{f \in C^\infty(\mathbb{R}); f^{(n)}(0) = 0\ \forall\ n \in \mathbb{N}\}$ is a prime ideal. Here $f^{(n)}$ denotes the n-th derivative of the function f. (Indeed $C^\infty(\mathbb{R})/\mathfrak{p} \cong \mathbb{C}[[T]]$.)

3.4 Irreducibility Criteria

If a polynomial $f \in K[T]$ of degree $\deg(f) > 1$ is irreducible, it has no zero $a \in K$: Otherwise we could factorize $f = (T - a)g$ with some polynomial $g \in K[T] \setminus K$. On the other hand a polynomial $f \in K[T]$ of degree $\deg(f) \leq 3$ without a zero in K is also irreducible: If we can write $f = gh$ with polynomials g, h of lower degree, one factor is linear, and thus provides a zero of f.
But how to check whether f has zeros or not? If K is finite, then, at least theoretically, we could simply check by computing all possible values. On the other hand, if $K = \mathbb{Q}$ and $f \in \mathbb{Z}[T]$ is monic, every rational zero $a \in \mathbb{Q}$ already is an integer: $a \in \mathbb{Z}$ (Show that or cf. Corollary 3.41.2), dividing $a_0 = f(0)$ (using the factorization $f = (T - a)g$ with $g \in \mathbb{Z}[T]$). So there are only finitely many candidates for possible zeros, if $a_0 \neq 0$ - and that can always be assumed. But what does hold for $\deg(f) > 3$? Again there is – at least theoretically – no problem, if the field K is finite, since then there are only finitely many candidates for the polynomials g, h.

If $K = \mathbb{Q}$, we may assume that $f \in \mathbb{Q}[T]$ even has integer coefficients: $f \in \mathbb{Z}[T]$ – if not, multiply f with some natural number. Indeed, we shall see,

that if $f \in \mathbb{Z}[T]$ is not irreducible in $\mathbb{Q}[T]$, then there is even a factorization in $\mathbb{Z}[T]$. Eventually, in order to exclude that possibility, we pass to the polynomial ring $\mathbb{Z}_m[T]$ over some factor ring $\mathbb{Z}_m$: Fix a natural number $m \in \mathbb{N}_{>1}$ and consider the following ring homomorphism

$$\mathbb{Z}[T] \longrightarrow \mathbb{Z}_m[T], f = \sum_{\nu=0}^{n} a_\nu T^\nu \mapsto \tilde{f} := \sum_{\nu=0}^{n} \overline{a}_\nu T^\nu \ .$$

The polynomial $\tilde{f} \in \mathbb{Z}_m[T]$ then is called the **reduction of f mod m.**

First we show that a factorization $f = gh \in \mathbb{Z}[T]$ with polynomials $g, h \in \mathbb{Q}[T]$ of lower degree always can be realized with polynomials $g, h \in \mathbb{Z}[T]$.

Definition 3.39. *The* **content** $\mathrm{cont}(f) \in \mathbb{Q}_{>0}$ *of a polynomial* $f \in \mathbb{Q}[T]\backslash\{0\}$ *is defined as the positive rational number satisfying*

$$f = \mathrm{cont}(f)\hat{f} \quad \text{with a polynomial } \hat{f} = \sum_{\nu=0}^{n} a_\nu T^\nu \in \mathbb{Z}[T] \ ,$$

whose coefficients have greatest common divisor $\gcd(a_0, ..., a_n) = 1$.

Proposition 3.40 (Gauß' lemma). *(Carl-Friedrich Gauß, 1777-1855) The content is a multiplicative function, i.e. for two polynomials* $f, g \in \mathbb{Q}[T] \setminus \{0\}$ *we have*

$$\mathrm{cont}(fg) = \mathrm{cont}(f)\mathrm{cont}(g) \ .$$

Proof. We may assume that $\mathrm{cont}(f) = 1 = \mathrm{cont}(g)$, so in particular $f, g \in \mathbb{Z}[T]$, and have to show $\mathrm{cont}(fg) = 1$, or equivalently that in the ring $\mathbb{Z}[T]$ we have

$$p|fg \Longrightarrow p|f \text{ or } p|g$$

for all primes $p \in \mathbb{Z}$, i.e. prime numbers $p \in \mathbb{Z} \subset \mathbb{Z}[T]$ are even prime in $\mathbb{Z}[T]$! In order to see that we consider the corresponding "reduced" polynomials $\tilde{f}, \tilde{g} \in \mathbb{Z}_p[T]$. Since that ring is an integral domain, we know that $0 = \widetilde{fg} = \tilde{f}\tilde{g}$ implies $\tilde{f} = 0$ or $\tilde{g} = 0$, and that is exactly what we need. □

Corollary 3.41. *1. If* $f \in \mathbb{Z}[T]$ *can not be written as a product* $f = gh$ *of polynomials* $g, h \in \mathbb{Z}[T]$ *of lower degree, the polynomial* f *is irreducible in* $\mathbb{Q}[T]$.

2. *If $f = gh$ is a factorization of a monic polynomial $f \in \mathbb{Z}[T]$ with monic factors $g, h \in \mathbb{Q}[T]$, then we have even $g, h \in \mathbb{Z}[T]$. In particular the rational zeroes of such a polynomial $f \in \mathbb{Z}[T]$ are integers.*

Proof. 1) Assume $f \in \mathbb{Z}[T]$ is reducible (not irreducible), i.e., can be written $f = pq$ with polynomials $p, q \in \mathbb{Q}[T]$ of lower degree. Write $p = \mathrm{cont}(p)g, q = \mathrm{cont}(q)h$ with polynomials $g, h \in \mathbb{Z}[T]$. Then $\mathrm{cont}(p)\mathrm{cont}(q) = \mathrm{cont}(f) \in \mathbb{Z}$ and $f = (\mathrm{cont}(p)\mathrm{cont}(q)g)h$ is a factorization of f in $\mathbb{Z}[T]$ into polynomials of lower degree. Contradiction!
2) The content of a monic polynomial in $\mathbb{Q}[T]$ is of the form $1/m$ with a natural number $m \geq 1$. Hence, f having content $1 = \mathrm{cont}(g) \cdot \mathrm{cont}(h)$, so do g and h and thus $g, h \in \mathbb{Z}[T]$. Finally apply this to a factorization $f = (T - a)h$, if $a \in \mathbb{Q}$ is a zero of f. □

So it suffices to discuss irreducibility questions within the ring $\mathbb{Z}[T]$. Here is a sufficient criterion:

Proposition 3.42. *Let $f \in \mathbb{Z}[T] \setminus \{0\}$ be a polynomial of degree ≥ 1 and $m \in \mathbb{N}_{>1}$, such that $\deg(\tilde{f}) = \deg(f)$ for $\tilde{f} \in \mathbb{Z}_m[T]$. If then $\tilde{f}$ does not admit a factorization into polynomials of lower degree in $\mathbb{Z}_m[T]$, then f is irreducible in $\mathbb{Q}[T]$.*

Proof. Assume $f = gh$ in $\mathbb{Q}[T]$. According to 3.41 we may assume $g, h \in \mathbb{Z}[T]$. But then we have $\tilde{f} = \tilde{g}\tilde{h}$ as well with polynomials $\tilde{g}, \tilde{h} \in \mathbb{Z}_m[T]$ of lower degree. Contradiction. □

Example 3.43. Let $f = T^5 - T^2 + 1$. Take $m = 2$. We obtain $\tilde{f} = T^5 + T^2 + 1 \in \mathbb{Z}_2[T]$. Assume $\tilde{f}$ is not irreducible. Since $\tilde{f}$ has no zeroes in $\mathbb{Z}_2$, there is an irreducible (monic) polynomial of degree 2 dividing $\tilde{f}$. But the quadratic polynomials in $\mathbb{Z}_2$ are $T^2, T^2+T = T(T+1), T^2+1 = (T+1)^2$ and $T^2 + T + 1$. The last one has no zero in $\mathbb{Z}_2$ and thus is irreducible, jfr. 2.29, while the others are reducible. Now the division algorithm for polynomials 3.6 gives

$$T^5 + T^2 + 1 = (T^3 + T^2)(T^2 + T + 1) + 1 \ ;$$

so $\tilde{f}$ is not divisible with $T^2 + T + 1$ and hence irreducible. It follows that $f \in \mathbb{Q}[T]$ indeed was irreducible.

Proposition 3.44 (**Eisenstein's criterion**). *(Ferdinand Gotthold Max Eisenstein, 1823-1852)): Let $f = a_n T^n + ... + a_1 T + a_0 \in \mathbb{Z}[T]$ and p be a prime number such that*

$$p \not| a_n \ , p | a_\nu \ \forall \ \nu < n \ , p^2 \not| a_0 \ .$$

Then $f \in \mathbb{Q}[T]$ is irreducible.

Proof. Assume $f = gh$ with polynomials $g, h \in \mathbb{Q}[T]$ of lower degree, $g = \sum_{\nu=0}^{k} b_\nu T^\nu, h = \sum_{\nu=0}^{\ell} c_\nu T^\nu$ with $k + \ell = n$. According to 3.41 we may again assume $g, h \in \mathbb{Z}[T]$. We reduce mod p and obtain then

$$\overline{a}_n T^n = \tilde{f} = \tilde{g}\tilde{h} \ .$$

in the polynomial ring $\mathbb{Z}_p[T]$. Hence $\tilde{g} = \overline{b}_k T^k$ and $\tilde{h} = \overline{c}_\ell T^\ell$. But $k, \ell < n$ resp. $k, \ell > 0$, hence $\overline{b}_0 = 0 = \overline{c}_0$ resp. p divides both b_0 and c_0. Consequently $a_0 = b_0 c_0$ is divisible with p^2. Contradiction. □

Example 3.45. Let p be a prime number. We consider the polynomial

$$f = T^{p-1} + T^{p-2} + ... + T + 1 \in \mathbb{Z}[T] \ .$$

It looks like that Eisenstein's criterion is not of much use here. But we can transform the polynomial by substituting $T + 1$ for T: Every ring automorphism $\varphi : \mathbb{Q}[T] \longrightarrow \mathbb{Q}[T]$ maps irreducible polynomials onto irreducible polynomials, and according to 3.15 there is a ring homomorphism $\varphi : \mathbb{Q}[T] \longrightarrow \mathbb{Q}[T]$, which is the identity on $\mathbb{Q} \subset \mathbb{Q}[T]$ and satisfies $\varphi(T) = T + 1$. Indeed, it is an isomorphism with inverse determined by $\varphi^{-1}|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ and $\varphi^{-1}(T) = T - 1$. Hence it is sufficient to check that

$$\varphi(f) = f(T + 1) = (T + 1)^{p-1} + ... + (T + 1) + 1$$

is irreducible. But

$$T^p - 1 = (T - 1)f \Longrightarrow (T + 1)^p - 1 = ((T + 1) - 1)f(T + 1) = Tf(T + 1) \ ,$$

whence we obtain with the binomial formula

$$f(T + 1) = T^{p-1} + pT^{p-2} + ... + \binom{p}{i} T^{p-i-1} + ... + \binom{p}{p-2} T + p$$

and Eisenstein's criterion assures that $f(T + 1)$ - and thus also f itself - is irreducible.

Problems 3.46. 1. R: Check whether the following polynomials are irreducible: i) $T^4 + T + 1 \in \mathbb{Z}_2[T]$, ii) $T^3 - T - 1 \in \mathbb{Z}_3[T]$, iii) $4T^3 + 81T^2 + 8T + 32 \in \mathbb{Q}[T]$, iv) $T^5 - 4T + 2$.

2. R: Show that the polynomial $f := T^4 - 10T^2 + 1$ is irreducible. Hint: Show that f has no zeroes in $\mathbb{Z}$ resp. $\mathbb{Q}$, and that it is not the product of two quadratic polynomials. (We shall see in Problem 4.58.6 that $\tilde{f} \in \mathbb{Z}_p[T]$ is reducible for all prime numbers p.)

3. R: Factorize the polynomials $T^4 + 1, T^4 - 4, T^4 + 4$ over $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ as a product of irreducible polynomials.

4. R: The **cyclotomic polynomials** $f_d \in \mathbb{Z}[T]$, where $d \in \mathbb{N}_{>0}$, are defined by the formula $T^n - 1 = \prod_{d|n} f_d$ for all $n \in \mathbb{N}_{>0}$. Compute f_d for $d \leq 9$ and a prime number d and check whether they are irreducible.

5. R: Show that $\mathbb{Z}[T]$ is not a principal ideal domain!

6. R: Show that $\mathbb{Z}[T]$ is a factorial ring.

7. Show that Gauß' lemma 3.40 holds for a factorial ring R instead of $\mathbb{Z}$ with an appropriate(!) definition of the content. Hint: For an irreducible element $u \in R$ in a factorial ring R the factor ring $R/(u)$ is an integral domain.

8. Show: The polynomial ring over a factorial ring R is again factorial. In particular the polynomial ring $K[Y,T] := (K[Y])[T]$ is factorial.

9. Let $K(Y) := Q(K[Y])$ be the field of all rational functions in the variable Y and $g, h \in K[T]$ two relatively prime polynomials. Show that $g - Yh \in K(Y)[T]$ is irreducible. Hint: Since $K[Y]$ is factorial, it suffices to show, that it is irreducible in $(K[Y])[T] \cong (K[T])[Y]$.

4 Field Extensions and Galois Theory

4.1 Basic Definitions

Definition 4.1. *A* **field extension** *of the field K is a pair (E, φ) with a field E and a ring homomorphism $\varphi : K \longrightarrow E$.*

Remark 4.2. 1. According to Example 3.22.8 φ is automatically injective, and therefore we may identify K with $\varphi(K) \subset E$, such that we usually write $K \subset E$ or $E \supset K$ in order to denote a field extension.

2. The notion of a real or complex vector space can easily be generalized to that of a **vector space over a field** K: In the axioms we have only to replace $\mathbb{R}$ or $\mathbb{C}$ with K. In particular the following notions apply: linearly dependent resp. independent, basis, dimension, linear map, determinant of an endomorphism etc.

3. If $E \supset K$ is a field extension, then E is a K-vector space - the scalar multiplication is taken to be the field multiplication of elements in $K \subset E$ with elements in E.

As a consequence of 4.2.3 we obtain

Corollary 4.3. *For any finite field $\mathbb{F}$ its order $q := |\mathbb{F}|$ is of the form $q = p^n$ with $p := \mathrm{char}(\mathbb{F}) > 0$.*

Proof. Since $\mathbb{F}$ is finite, it has positive characteristic $p > 0$, and thus we obtain the field extension $\mathbb{F} \supset P(\mathbb{F}) \cong \mathbb{Z}_p$. In particular $\mathbb{F}$ is a finite dimensional $\mathbb{Z}_p$-vector space and hence, as vector spaces, $\mathbb{F} \cong (\mathbb{Z}_p)^n$ for $n = \dim \mathbb{F}$. Consequently $|\mathbb{F}| = p^n$. □

Indeed, in section 4.5 we shall see that for any $q = p^n$ there is, up to isomorphy, exactly one finite field $\mathbb{F}_q$ of order $|\mathbb{F}_q| = q$.

Let us now study some explicit examples:

Example 4.4. 1. Let $f \in K[T]$ be an irreducible polynomial. Then $(E := K[T]/(f), \varphi)$ is a field extension, where the ring homomorphism $\varphi : K \longrightarrow E$ is the composite of the inclusion $K \hookrightarrow K[T]$ and the quotient map $K[T] \longrightarrow K[T]/(f) = E$.

In particular let us mention:

(a) The complex numbers as an extension of the real numbers: $\mathbb{C} \supset \mathbb{R}$. Indeed $\mathbb{C} \cong \mathbb{R}[T\,]/(T^2+1)$.

(b) Let $d \in \mathbb{N}_{>0}$ be not a square. Then $\mathbb{Q}[\sqrt{d}] := \mathbb{Q} + \mathbb{Q}\sqrt{d} \supset \mathbb{Q}$ is a field extension, and $\mathbb{Q}[\sqrt{d}\,] \cong \mathbb{Q}[T]/(T^2-d)$.

(c) A finite counterpart to $\mathbb{C}$: Let p be an odd prime number $p \not\equiv 1 \bmod(4)$. Then the polynomial $f = T^2+1$ has no zeros in $K := \mathbb{F}_p := \mathbb{Z}_p$, since a zero would be an element of order 4 in $\mathbb{F}_p^*$, but the order of that group is not divisible with 4.

So we obtain a new field $\mathbb{F}_{p^2} := \mathbb{F}_p[T]/(f)$, where the element $i := \overline{T}$ satisfies $i^2 = -1$ and every element can be written uniquely in the form $a+bi; a, b \in \mathbb{F}_p$. The arithmetic in $\mathbb{F}_{p^2}$ thus is the same as that for complex numbers with the reals $\mathbb{R}$ replaced by $\mathbb{F}_p$.

2. The real numbers as an extension of the rational numbers: $\mathbb{R} \supset \mathbb{Q}$.

3. The p-adic number field as an extension of the rationals: $\mathbb{Q}_p \supset \mathbb{Q}$.

4. For a given field K we mention the extensions:

(a) $K(T) \supset K$, where

$$K(T) := Q(K[T])$$

denotes the field of fractions of the polynomial ring $K[T]$, usually called the *field of rational functions in one variable over* K;

(b) $K((T)) \supset K$, where

$$K((T)) = T^{-\mathbb{N}}K[[T]] = Q(K[[T]])$$

denotes the field of formal Laurent series with finite principal part over K, see Problem 3.9.8, and

(c) $K((T)) \supset K(T)$: The inclusion $K[T] \subset K[[T]]$ extends to an injective homomorphism $K[T]_{(T)} \hookrightarrow K[[T]]$, since $K[T] \setminus (T) \subset K[[T]]^*$. Now localization with respect to the multiplicative set $S = T^{-\mathbb{N}}$ yields a homomorphism

$$K(T) = T^{-\mathbb{N}}K[T]_{(T)} \hookrightarrow K((T)) = T^{-\mathbb{N}}K[[T]].$$

Definition 4.5. *Let $E \supset K$ be a field extension. The* **degree** $[E : K] \in \mathbb{N}_{>0} \cup \{\infty\}$ *is defined as the dimension of E as K-vector space, i.e.*

$$[E : K] := \dim_K E \ .$$

The field extension $E \supset K$ is called **finite** *iff $[E : K] < \infty$.*

Example 4.6. In Example 4.4.1 we have $[E : K] = n := \dim(f)$, since according to **??** a basis of the K-vector space E is given by $1, \vartheta := \overline{T}, ..., \vartheta^{n-1}$. In particular, the extensions $\mathbb{C} \supset \mathbb{R}$ and $\mathbb{F}_{p^2} \supset \mathbb{F}_p$ have degree 2, while the remaining extensions in 4.4.2-4 are infinite.

Remark 4.7. Let $E \supset K$ be a field extension. We take an element $a \in E$ and consider the ring homomorphism $\psi_a : K[T] \hookrightarrow E[T] \longrightarrow E, f \mapsto f(a)$, which is the restriction to $K[T] \subset E[T]$ of the evaluation homomorphism $E[T] \longrightarrow E, f \mapsto f(a)$, cf. 3.15 with $R = E$. We denote

$$K[a] := \psi_a(K[T]) = \{f(a); f \in K[T]\} \subset E,$$

its image and

$$\mathfrak{m}_a := \ker(\psi_a) = \{f \in K[T]; f(a) = 0\}$$

its kernel. As kernel of a ring homomorphism $\mathfrak{m}_a$ is an ideal, such that

$$K[a] \cong K[T]/\mathfrak{m}_a \ .$$

In fact, Prop.2.45 provides an isomorphism of the underlying additive groups, which even is a ring isomorphism.
If $\mathfrak{m}_a = \{0\}$, then $K[a] \cong K[T]$ is an infinite dimensional K-vector space. Otherwise there is according to 3.27 a polynomial $p_a \in K[T] \setminus \{0\}$ such that $\mathfrak{m}_a = (p_a)$, and we then have $\dim_K K[a] = \deg(p_a)$ according to **??**. The polynomial $p_a \in K[T]$ is determined up to a constant non-zero factor; requiring it to be monic, it becomes unique. It is irreducible, since the factor ring $K[T]/\mathfrak{m}_a \cong K[a] \subset E$ is an integral domain, indeed, even a field: Non-trivial prime ideals in the principal ideal domain $K[T]$ are maximal. So we have a field extension $K[a] \supset K$ with $[K[a] : K] = \deg(p_a)$.

Definition 4.8. *Let $E \supset K$ be a field extension. An element $a \in E$ is called*

1. **transcendent over** *K, iff ψ_a is injective, i.e., iff $\mathfrak{m}_a = \{0\}$.*

2. **algebraic over** K, *iff* $\mathfrak{m}_a \neq \{0\}$. *In that case* $\mathfrak{m}_a = (p_a)$ *with a unique monic (irreducible) polynomial* $p_a \in K[T]$, *which is called the* **minimal polynomial** *of* $a \in E$ *over* K.

Remark 4.9. 1. If $f \in K[T]$ is an irreducible monic polynomial and $a \in E \supset K$ a zero of f, then $p_a = f$.

2. In order to compute the minimal polynomial of an element $a \in E$ one considers the powers $a^0 = 1, a, a^2, ..., a^n$ for $n \in \mathbb{N}$. If they are linearly independent for all $n \in \mathbb{N}$, the element $a \in E$ is transcendent over K, otherwise choose $n \in \mathbb{N}$ minimal with $a^0 = 1, a, a^2, ..., a^n$ linearly dependent. So there is a linear combination

$$\lambda_n a^n + ... + \lambda_1 a + \lambda_0 = 0$$

with $\lambda_i \in K$ not all zero. If $\lambda_n = 0$, already $1, a, ..., a^{n-1}$ are linearly dependent, so necessarily $\lambda_n \neq 0$ according to the choice of n. Then

$$p_a = T^n + \sum_{i=0}^{n-1} \lambda_n^{-1} \lambda_i T^i$$

is the minimal polynomial of $a \in E$ over K. Hence if $a \in E \setminus K$ is the zero of a quadratic monic polynomial $f \in K[T]$, it is the minimal polynomial: $p_a = f$, e.g. the numbers $\sqrt{2}, i \in \mathbb{C} \supset \mathbb{Q}$ have the minimal polynomials $p_{\sqrt{2}} = T^2 - 2$ resp. $p_i = T^2 + 1$. In Example 4.14. we present an explicit calculation leading to $n = 4$.

3. **Transcendent numbers**: A complex number is called algebraic resp. transcendent, if it is algebraic resp. transcendent over $\mathbb{Q}$. The set $\mathbb{Q}_a \subset \mathbb{C}$ of all algebraic numbers is countable, since $\mathbb{Q}[T]$ is countable, while $\mathbb{C}$ itself is uncountable: So the vast majority of all complex numbers numbers is transcendent, but nevertheless it is not easy to show that a specific number is transcendent. For example one knows that each number e^a with an algebraic number $a \in \mathbb{C}$ is transcendent - conclude that both e (Charles Hermite, 1822-1901) and π (cf. Problem 4.15.2) (Carl Louis Ferdinand von Lindemann, 1852-1939) are transcendent! - or that irrational numbers $a \in \mathbb{R} \setminus \mathbb{Q}$ are transcendent, if they can be approximated "very well" by rational numbers (if one compares the error in relation to the size of the denominators of the approximating rational numbers). It is even known that e^π is transcendent, but what about $e + \pi, e\pi, \pi^e$?

But here we are essentially interested in algebraic or even finite extensions:

Definition 4.10. *A field extension $E \supset K$ is called algebraic, if every element $a \in E$ is algebraic over K.*

Proposition 4.11. *A finite field extension is algebraic.*

Proof. Let $E \supset K$ be finite and $a \in E$. Since $K[a] \subset E$ is a vector subspace, we have $\dim_K K[a] \leq \dim_K E < \infty$. Now use 4.7! □

Proposition 4.12. *Let $L \supset E$ and $E \supset K$ be field extensions. If they are algebraic resp. finite, the composite field extension $L \supset K$ is as well.*

Furthermore, in the finite case, the degree is multiplicative, i.e.

$$[L : K] = [L : E] \cdot [E : K] \ .$$

Before we prove 4.12, we extend the notation $K[a]$:

Notation: Let $E \supset K$ be a field extension, $a_1, ..., a_r \in E$. Then we define

$$K[a_1, ..., a_r] := \left\{ \sum_{(\nu_1,...,\nu_r) \in \mathbb{N}^r} b_{\nu_1,...,\nu_r} a_1^{\nu_1} \cdot ... \cdot a_r^{\nu_r}; b_{\nu_1,...,\nu_r} \in K \text{ almost all } = 0 \right\} \subset E \ ,$$

where "almost all" means "all except finitely many". With other words: All our sums are finite.
For $r = 1$ this is our old definition, and furthermore for $r > 1$:

$$K[a_1, ..., a_r] = (K[a_1, ..., a_{r-1}])[a_r] \ .$$

Proof of 4.12. The case of finite extensions together with the degree formula follows from the following observation: If $u_1, ..., u_n$ is a basis of the K-vector space E and $v_1, ..., v_m$ a basis of the E-vector space L, then the products $u_i v_j, 1 \leq i \leq n, 1 \leq j \leq m$, form a basis of L as K-vector space - the details are left to the reader.
Let us now consider the algebraic case. Given an element $a \in L$ we construct a finite extension $L_0 \supset K$ containing it, thus proving that it is algebraic over K. First of all: If $a_1, ..., a_r \in L$ are algebraic, then $K[a_1, ..., a_r] \supset K$ is a finite field extension. To see that use remark 4.7 and induction on r as well as what we just have noticed. Consider now the minimal polynomial $p_a = T^m + b_{m-1}T^{m-1} + ... + b_1 T + b_0 \in E[T]$ of a over E and take $E_0 := K[b_0, ..., b_{m-1}], L_0 := E_0[a]$. Then $E_0 \supset K$ (since $b_0, ..., b_{m-1}$ are algebraic over K) as well as $L_0 \supset E_0$ are finite extensions; so $L_0 \supset K$ is as well. □

Remark 4.13. If $E \supset K$ is a field extension, the elements in E, which are algebraic over K, constitute a subfield $E_a \subset E$, i.e. E_a endowed with E:s field operations is itself a field. For that we have to show $b, c \in E_a \Longrightarrow b + c, bc, b^{-1} \in E_a$, where $b \neq 0$ in the last case. But that is evident since $K[b, c] \supset K$ is a finite field extension and thus $K[b, c] \subset E_a$.

Example 4.14. We know already that $\sqrt{2}, i \in \mathbb{C}$ are algebraic over $\mathbb{Q}$ and thus also $a := \sqrt{2} + i$. We compute its minimal polynomial $p_a \in \mathbb{Q}[T]$: First we consider the field $E := \mathbb{Q}[\sqrt{2}, i] \ni a$. Since $\sqrt{2}$ has minimal polynomial $T^2 - 2$ over $\mathbb{Q}$ and i has minimal polynomial $T^2 + 1$ over $\mathbb{Q}[\sqrt{2}]$, it folllows that $[E : \mathbb{Q}] = [\mathbb{Q}[\sqrt{2}][i] : \mathbb{Q}[\sqrt{2}]] \cdot [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2 \cdot 2 = 4$ and that a basis of the $\mathbb{Q}$-vector space E is given by $1, \sqrt{2}, i, i\sqrt{2}$.
Since $\deg(p_a) = [\mathbb{Q}[a] : \mathbb{Q}]$ divides $[E : \mathbb{Q}] = 4$, the minimal polynomial has either degree $1, 2$ or 4. But $1, a = \sqrt{2} + i, a^2 = 1 + 2 \cdot i\sqrt{2}$ are obviously linearly independent, so we obtain the degree 4, in particular $E = \mathbb{Q}[\sqrt{2}+i]$. Furthermore $a^3 = -\sqrt{2}+5i$ and $a^4 = -7+4\cdot i\sqrt{2} = 2(1+2\cdot i\sqrt{2})-9 = 2a^2-9$. Hence $p_a = T^4 - 2T^2 + 9$.

Problems 4.15.

1. R: Let $E \supset K$ be a finite field extension and $a \in E$. Show: The K-vector space endomorphism $\mu_a : E \longrightarrow E, x \mapsto ax$, has characteristic polynomial $(p_a)^s$ with $s := [E : K[a]]$.

2. R: Show: The number $\pi \in \mathbb{R}$ is transcendent, using the fact that e^a is transcendent for any algebraic number $a \in \mathbb{C}$.

3. Let $K(X) = Q(K[X])$ be the field of all rational functions in one variable X over K (the letter X replacing our usual T in order to reserve the latter for polynomials over $K(X)$). Show that the extension $K(X) \supset K$ is purely transcendent, i.e. $K(X)_a = K$. Hint: Take $f = g/h \in K(X)_a$ with relatively prime polynomials $g, h \in K[X]$ and consider the equation $p_f(gh^{-1})h^n = 0$, where $n := \deg(p_f)$ with the minimal polynomial $p_f \in K[T]$ of f over K.

4. Let $K(Y) = Q(K[Y])$ and $K(X) = Q(K[X])$ be two copies of the field of all rational functions in one variable Y resp. X over K. If $f := g/h \in K(X) \setminus K$, where $g, h \in K[X]$ are relatively prime, the ring homomorphism $\sigma : K[Y] \longrightarrow K(X)$ with $\sigma|_K = \mathrm{id}_K, \sigma(Y) = f$ is injective and can therefore uniquely be extended to a homomorphism $\hat{\sigma} : K(Y) \longrightarrow K(X)$. Show that the field extension $(K(Y), \hat{\sigma})$ has degree $\max(\deg(g), \deg(h))$! Hint: The minimal polynomial of X over $K(Y) \cong \hat{\sigma}(K(Y))$ is up to a constant factor $\in K^* \cup K^*Y \subset K(Y)^*$ the polynomial $g(T) - Yh(T) \in K(Y)[T]$. Here $g(T), h(T) \in K[T]$ denote the polynomials obtained from $g, h \in K[X]$ by substituting T for X!

5. R: Let K be a field and $f = f_1^{k_1} \cdot \ldots \cdot f_r^{k_r}$ the factorization of the polynomial $f \in K[T]$ as product of irreducible polynomials. Show an analogue of the Chinese Remainder

Theorem:

$$K[T]/(f) \cong \prod_{i=1}^{r} K[T]/(f_i^{k_i}) \ .$$

Show that the summands are local rings, with their nilradical as the maximal ideal. Hint: Compare the dimensions of the underlying K-vector spaces!

6. Let $K[\vartheta] = K[T]/(f)$ with $\vartheta := \overline{T}$. Determine the matrix of the K-linear map $\mu_\vartheta : K[\vartheta] \longrightarrow K[\vartheta]$ given by $\mu_\vartheta(x) := \vartheta x$ with respect to the basis $1, \vartheta, ..., \vartheta^{n-1}$, where $n = \deg(f)$. Show: $K[A] \cong K[\vartheta]$.

7. **Algebraic integers:** A complex number $\lambda \in \mathbb{C}$ is called an **algebraic integer** if it is the zero of a monic polynomial $f \in \mathbb{Z}[T]$. Show:

   (a) A rational algebraic integer (sometimes simply called a "rational integer") is a usual integer.

   (b) A complex number $\lambda \in \mathbb{C}$ is an algebraic integer iff there is an $n \in \mathbb{N}$ and a square matrix $A \in \mathbb{Z}^{n,n}$, i.e. with integer entries, having λ as an eigenvalue.

   (c) The algebraic integers form a subring of $\mathbb{C}$. (For this part you need to know the notion of the tensor product $V \otimes W$ of two K-vector spaces V and W.)

   (PS: We shall see in Problam 4.46.6 that we also could have required for $\lambda \in \mathbb{Q}_a$ to be an algebraic integer that $p_\lambda \in \mathbb{Z}[T]$ holds for the minimal polynomial p_λ of λ over $\mathbb{Q}$.)

4.2 Automorphism Groups

The modern formulation of Galois theory has been created in the 1920-ies by Emil Artin (1898-1962). The central notion is that of a field automorphism.

Definition 4.16. *Let $E \supset K$ and $L \supset K$ be field extensions of the same field K. A K-***morphism** *(or simply* **morphism***, if it is clear, which field K has to be taken) between the field extensions $E \supset K$ and $L \supset K$ is a ring homomorphism*

$$\sigma : E \longrightarrow L \ ,$$

such that $\sigma|_K = \mathrm{id}_K$.

Two extensions $E \supset K$ and $L \supset K$ of a given field are called **isomorphic***, if there is a K-morphism $\sigma : E \longrightarrow L$, which is a (ring) isomorphism.*
*If $L = E$ such a σ is called a K-***automorphism** *(or simply an* **automorphism***) of the field extension $E \supset K$.*

The set

$$\mathrm{Aut}_K(E) := \{\sigma : E \longrightarrow E \ K-\text{automorphism}\}$$

constitutes a subgroup of the permutation group $\mathbb{S}(E)$ *and is called the* **automorphism group** *of the extension* $E \supset K$.

Example 4.17. 1. The identity id_E is in any case an automorphism of the field extension $E \supset K$.

2. Complex conjugation $\sigma : \mathbb{C} \longrightarrow \mathbb{C}, z \mapsto \bar{z}$, is an automorphism of the extension $\mathbb{C} \supset \mathbb{R}$.

3. Let $d \in \mathbb{N}_{>0}$ not be a square. Then $\mathbb{Q}[\sqrt{d}\,] \supset \mathbb{Q}$ is a field, and beside $\mathrm{id}_{\mathbb{Q}}$ we have the automorphism $\sigma : a + b\sqrt{d} \mapsto a - b\sqrt{d}$, where $a, b \in \mathbb{Q}$.

   A "non-algebraic" observation: The automorphism σ is not continuous (with respect to the topology on $\mathbb{Q}[\sqrt{d}\,] \subset \mathbb{R}$ as subset of the reals): Take a sequence $(x_\nu) \subset \mathbb{Q}$ converging to $\sqrt{d} \in \mathbb{R}$. Then $x_\nu - \sqrt{d}$ tends to 0, but $\sigma(x_\nu - \sqrt{d}) = x_\nu + \sqrt{d}$ does not converge to $\sigma(0) = 0$, but to $2\sqrt{d}$.

4. We have $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R}) = \{\mathrm{id}_{\mathbb{R}}\}$ according to 4.20.3.

5. In striking contrast the automorphism group $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$ is quite large: Every automorphism $\sigma : K \longrightarrow K$ of some subfield $K \subset \mathbb{C}$ can be extended to an automorphism $\hat{\sigma} : \mathbb{C} \longrightarrow \mathbb{C}$, cf. Problem 5.11.3. But the only continuous ones are the identity or complex conjugation, cf. Problem 4.20.4.

6. Let E be a field with $\mathrm{char}(E) = p > 0$. Then $E \supset P(E) \cong \mathbb{Z}_p$ is a field extension, and $\sigma : E \longrightarrow E, x \mapsto x^p$, is a $\mathbb{Z}_p$-morphism: Obviously $\sigma(xy) = \sigma(x)\sigma(y)$, while

$$\sigma(x+y) = (x+y)^p = x^p + \sum_{\nu=1}^{p-1} \binom{p}{\nu} x^\nu y^{p-\nu} + y^p = x^p + y^p = \sigma(x) + \sigma(y)\ ,$$

   since for $1 \leq \nu \leq p-1$ the binomial coefficients $\binom{p}{\nu} = \frac{p!}{\nu!(p-\nu)!}$ are divisible by p (p being a prime) and therefore $= 0$ in the field E. Furthermore $x^p = x^{p-1}x = x$ for $x \in \mathbb{Z}_p$ according to Lagrange's theorem 2.38 applied to $\mathbb{Z}_p^*$. It is even surjective and thus an automorphism, if E is a finite field, an injective map from a finite set to itself being surjective as well. It is called **Frobenius homomorphism** resp. - if it is even surjective - **Frobenius automorphism** (Georg Frobenius, 1849-1917).

The next proposition describes $\mathrm{Aut}_K(E)$ for $E = K[a]$ as a set. But for technical reasons the formulation is slightly more general: We consider a (ring) isomorphism $\varphi : K \longrightarrow K'$ between two fields K and K'. It induces an isomorphism of the corresponding polynomial rings

$$K[T] \longrightarrow K'[T], f = \sum a_\nu T^\nu \mapsto f^\varphi := \sum \varphi(a_\nu) T^\nu \ .$$

Then we have:

Proposition 4.18. *1. Let $\varphi : K \longrightarrow K'$ be a ring isomorphism between the fields K and K', $E = K[a] \supset K$ and $E' \supset K'$ field extensions, $[E : K] < \infty$ and $p_a \in K[T]$ the minimal polynomial of a over K. Then there is a bijective correspondence between the ring homomorphisms*

$$\sigma : E = K[a] \longrightarrow E'$$

extending φ, and the zeroes of the polynomial p_a^φ in the field E', given by

$$\sigma \mapsto \sigma(a) \ .$$

2. If $E' = E = K[a]$, then

$$\mathrm{Aut}_K(E) \longrightarrow N_E(p_a), \sigma \mapsto \sigma(a)$$

is a bijection. Here for a polynomial $f \in K[T]$ we denote

$$N_E(f) := \{b \in E; f(b) = 0\}$$

the set of all zeroes of f in E.

Proof. i) Let $\sigma : E \longrightarrow E'$ be an extension of $\varphi : K \longrightarrow K'$. Then for any polynomial $f \in K[T]$ we have

$$\sigma(f(a)) = f^\varphi(\sigma(a)) \ .$$

Now every element in $K[a]$ is of the form $f(a)$, hence the above formula shows that σ is uniquely determined by $\sigma(a)$.
On the other hand, taking $f = p_a$ we see that $p_a^\varphi(\sigma(a)) = \sigma(p_a(a)) = \sigma(0) = 0$. It remains to show that every zero of p_a^φ can be realized as $\sigma(a)$: The ring isomorphism

$$K[T] \longrightarrow E, f \mapsto f(a)$$

induces an isomorphism $K[T]/(p_a) \cong K[a] = E$, while according to 3.15, there is for every $b \in E'$ a ring homomorphism

$$\varphi_b : K[T] \longrightarrow E'$$

with $\varphi_b|_K = \varphi$ and $\varphi_b(T) = b$ – here we regard φ as a ring homomorphism $K \longrightarrow E'$. If now b is a zero of p_a^φ, we have $\varphi_b(p_a) = p_a^\varphi(b) = 0$. Hence $(p_a) \subset \ker(\varphi_b)$, and therefore φ_b factors through $K[T]/(p_a) \cong K[a] = E$, the second factor being the looked for map σ with $\sigma(a) = b$.
ii) Apply i) with $K' = K$ and $\varphi = \mathrm{id}_K$, using the fact that a K-morphism of a finite field extension $E \supset K$ to itself automatically is an automorphism, as an injective endomorphism of the finite dimensional K-vector space E. □

Let us now compute some automorphism groups:

Example 4.19. 1. $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}_{\mathbb{C}}, \sigma\} \cong \mathbb{Z}_2$ with the complex conjugation $\sigma : z \mapsto \bar{z}$. Apply 4.18.ii) to $\mathbb{C} = \mathbb{R}[i], p_i = T^2 + 1$.

2. Let $d \in \mathbb{N}_{>0}$ be not a square. Then $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sqrt{d}]) = \{\mathrm{id}_{\mathbb{C}}, \sigma\} \cong \mathbb{Z}_2$ with $\sigma : a + b\sqrt{d} \mapsto a - b\sqrt{d}$. Apply 4.18.ii) to $\mathbb{Q}[\sqrt{d}\,] \supset \mathbb{Q}, p_{\sqrt{d}} = T^2 - d$.

3. Consider a monic polynomial $f \in \mathbb{Q}[T]$ of degree $\deg(f) = 3$ without zero in $\mathbb{Q}$. (So it is irreducible over $\mathbb{Q}$). Then f has at least one real zero $a \in \mathbb{R}$, since the polynomial function $\mathbb{R} \longrightarrow \mathbb{R}, x \mapsto f(x)$, is continuous and $\lim_{x\to\infty} f(x) = \infty, \lim_{x\to-\infty} f(x) = -\infty$ (apply the theorem on intermediate values). We investigate the extension $E := \mathbb{Q}[a] \supset \mathbb{Q}$:

   First of all write $f = (T-a)g$ with a quadratic polynomial $g \in E[T] \subset \mathbb{R}[T]$. Since any quadratic polynomial $g \in \mathbb{R}[T]$ has complex zeroes, we may write $g = (T-b)(T-c)$ with complex numbers $b, c \in \mathbb{C}$. Now there are two possibilities:

   1.) Either $b \notin E$ (and then $c \notin E$ as well), e.g. if $b, c \in \mathbb{C} \setminus \mathbb{R}$ as in the case $f = T^3 - 2$, where we have $a = \sqrt[3]{2}, b = a\varepsilon, c = a\varepsilon^2$ with the third root of unity $\varepsilon = \frac{1}{2}(-1 + i\sqrt{3})$. Then obviously $\mathrm{Aut}_{\mathbb{Q}}(E) = \{\mathrm{id}_E\}$. Or

   2.) $b \in E$ (and then $c \in E$ as well). The real zeroes a, b, c are pairwise different: Regard f as function $f : \mathbb{R} \longrightarrow \mathbb{R}$. Since f is the minimal polynomial of its zeroes, its derivative f' as a polynomial of degree $2 < 3 = \deg(f)$ has none of them as a zero, i.e. f has only simple and hence 3 pairwise different zeroes.

Then there are unique automorphisms $\sigma, \tau \in \mathrm{Aut}_{\mathbb{Q}}(E)$ with $\sigma(a) = b, \tau(a) = c$, and $\mathrm{Aut}_{\mathbb{Q}}(E) = \{\mathrm{id}_E, \sigma, \tau\}$. Hence $|\mathrm{Aut}_{\mathbb{Q}}(E)| = 3$, and since a group of prime order is cyclic, it is generated by σ or τ and $\tau = \sigma^2, \sigma = \tau^2$.

As an example of such a polynomial f we can take $f = T^3 - 3T + 1$. Indeed, the identity

$$f(T^2-2) = T^6-6T^4+9T^2-1 = (T^3-3T-1)(T^3-3T+1) = (T^3-3T-1)\cdot f$$

implies that $b := a^2 - 2 \neq a$ (the elements $1, a, a^2$ constitute a basis of the $\mathbb{Q}$-vector space E) is another zero of f. In fact, we can give a zero of f explicitly, namely the real number $a := 2\cos(2\pi/9) = \zeta + \overline{\zeta} = \zeta + \zeta^{-1}$ with $\zeta := e^{2\pi i/9}$: Since ζ^3 is a third root of unity, we get $(\zeta^3)^2 + \zeta^3 + 1 = 0$, whence:

$$f(a) = (\zeta+\zeta^{-1})^3 - 3(\zeta+\zeta^{-1}) + 1 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} - 3(\zeta+\zeta^{-1}) + 1$$

$$= \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} - 3(\zeta + \zeta^{-1}) + 1 = \zeta^3 + \zeta^6 + 1 = 0 \ .$$

4. Finally we consider the extension $E = \mathbb{Q}[\sqrt{2}, i] \supset \mathbb{Q}$. We know already that $E = \mathbb{Q}[\sqrt{2} + i]$ and

$$p_{\sqrt{2}+i} = T^4-2T^2+9 = (T-(\sqrt{2}+i))(T-(\sqrt{2}-i))(T+(\sqrt{2}+i))(T+(\sqrt{2}-i)) \ .$$

In particular $p_{\sqrt{2}+i}$ has 4 pairwise distinct zeroes in E, so there are 4 automorphisms as well. It remains to determine the group structure: There are exactly two non-isomorphic groups of order 4, namely $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$, cf. Problem 2.6.4.

Now for every automorphism $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(E)$ we have $\sigma(\sqrt{2})^2 = \sigma(\sqrt{2}^2) = \sigma(2) = 2$ and $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$. Hence $\sigma(\sqrt{2}) = \pm\sqrt{2}, \sigma(i) = \pm i$, and any distribution of signs can be realized, since there really are 4 automorphisms and each of them is uniquely determined by its values $\sigma(\sqrt{2}), \sigma(i)$. In particular $\sigma^2 = \mathrm{id}_E$ for all automorphisms, i.e. there is no element of order 4, whence $\mathrm{Aut}_{\mathbb{Q}}(E) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Problems 4.20. 1. R: For a field K and $n \in \mathbb{N}$ set $C_n(K) := \{a \in K; a^n = 1\} \subset K^*$, the subgroup of K^* of all n-th roots of unity in K (so $C_n = C_n(\mathbb{C})$). An element $\zeta \in C_n(K)$ of order n is called a primitive n-th root of unity. Let $F := K[\zeta] \supset K$

with a primitive n-th root of unity $\zeta \in C_n(F)$. Show: $\mathrm{Aut}_K(F)$ is isomorphic with a subgroup of the group of units $\mathbb{Z}_n^*$ of the ring $\mathbb{Z}_n$. Hint: Every automorphism $\sigma \in \mathrm{Aut}_K(F)$ induces a group automorphism $\sigma|_{C_n(F)} : C_n(F) \longrightarrow C_n(F)$, and Problem 2.39.6.

2. Let K be a field containing all n-th roots of unity, i.e. the polynomial $T^n - 1 \in K[T]$ can be factorized as a product of linear polynomials, and $E := K[b] \supset K$ a field extension, where $b^n = a \in K$. Show that $\mathrm{Aut}_K(E)$ is isomorphic with a subgroup of the group $C_n(K) \subset K^*$ of all n-th roots of unity in K, hence in particular a cyclic group. Furthermore: If $n = p$ is a prime number, either $E = K$ or $T^p - a$ is the minimal polynomial $p_b \in K[T]$ of $b \in E$ over K.

3. R: Show: $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R}) = \{\mathrm{id}_{\mathbb{R}}\}$. Hint: $\mathbb{R}_{\geq 0} = \{x^2; x \in \mathbb{R}\}$.

4. R: Show: Any continuous automorphism $\sigma : \mathbb{C} \longrightarrow \mathbb{C}$ is the identity or complex conjugation.

5. Let $E \supset K$ be a field extension. Show: A family of pairwise distinct automorphisms $\sigma_1, ..., \sigma_n \in \mathrm{Aut}_K(E) \subset \mathrm{End}_K(E)$ is linearly independent over K, where $\mathrm{End}_K(E)$ denotes the K-vector space of all endomorphisms of the K-vector space E. Hint: Induction on n; if $\lambda_1\sigma_1 + ... + \lambda_n\sigma_n = 0$ is a non-trivial relation, we may assume $\lambda_1 \neq 0$ and choose $y \in E$ with $\sigma_1(y) \neq \sigma_n(y)$. Let $x \in E$ be arbitrary. Replace x with yx in the above relation and get a new relation $\lambda_1\sigma_1(y)\sigma_1 + ... + \lambda_n\sigma_n(y)\sigma_n = 0$, multiply the old one with $\sigma_n(y)$ and subtract them. One obtains a non-trivial relation for $\sigma_1, ..., \sigma_{n-1}$.

6. Show: $\mathrm{Aut}_K(K(X)) \cong GL_2(K)/K^*E$, where K^*E denotes the subgroup of all matrices $\lambda E, \lambda \in K^*$, i.e. being scalar multiples of the unit matrix $E \in K^{2,2}$. Hint: Every K-morphism $\sigma : K(X) \longrightarrow K(X)$ is uniquely determined by its value $f := \sigma(X) \in K(X)$. It is surjective and thus an automorphism iff $f = g/h$ with non-proportional linear polynomials $g, h \in K[X]$ – to see that use Problem 4.15.4. Then one defines a homomorphism

$$GL_2(K) \longrightarrow \mathrm{Aut}_K(K(X)),\ A \longrightarrow \sigma_{A^{-1}}\ ,$$

where the automorphism $\sigma_A : K(X) \longrightarrow K(X)$ for a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$$

is determined by

$$\sigma_A(X) = \frac{aX + b}{cX + d}\ .$$

Check first that $\sigma_{AB} = \sigma_B \circ \sigma_A$! (The group $PGL_n(K) := GL_n(K)/K^*E$ is called the **projective linear group** (of size n) over K.). Cf. Problem 3.19.6, where we saw that $\mathrm{Aut}_K(K[X]) \cong \mathrm{Aff}(K)$.

4.3 Formal Derivatives and Multiplicities

In Prop. 4.18 we have seen that in order to determine the order $|\mathrm{Aut}_K(E)|$ of the automorphism group of an extension $E \supset K$, it is important to know how many zeros an irreducible polynomial $f \in K[T]$ may have. An upper bound is its degree $\deg(f)$. But is there always an extension $E \supset K$ with $|N_E(f)| = \deg(f)$? In that case every zero of f in E has **multiplicity** 1:

Definition 4.21. *The multiplicity of a zero $a \in K$ of a polynomial $f \in K[T] \setminus \{0\}$ is the unique number $\ell \in \mathbb{N}$, such that*

$$f = (T-a)^\ell h \quad \text{with some } h \in K[T],\ h(a) \neq 0\ .$$

Remark 4.22. Let $f \in K[T]$ be an irreducible polynomial and $a \in E \supset K$ and $b \in L \supset K$ be zeros of f. Then the multiplicities of $f \in E[T]$ at a and $f \in L[T]$ at $b \in L$ coincide: The factorizations $f = (T-a)^\ell h$ resp. $f = (T-b)^k g$ as in Def. 4.21 are in fact already over the isomorphic subfields $K[a\,] \subset E$ resp. $K[b\,] \subset L$: We have $\mathfrak{m}_a = (f) = \mathfrak{m}_b$ and thus $K[a\,] \cong K[T]/(f) \cong K[b\,]$. Consequently $k = \ell$.

For a more detailed investigation the notion of the formal derivative of a polynomial $f \in K[T]$ plays an important rôle:

Definition 4.23. *The* **formal derivative** *of a polynomial $f \in K[T], f = \sum_{\nu=0}^{n} a_\nu T^\nu$, is defined as the polynomial*

$$f' := \sum_{\nu=1}^{n} \nu a_\nu T^{\nu-1} \in K[T]\ .$$

Proposition 4.24. *The formal derivative*

$$K[T] \longrightarrow K[T], f \mapsto f'\ ,$$

*is a K-linear map, satisfying the "Leibniz rule", (*Gottfried Wilhelm Leibniz, 1646-1716*):*

$$(fg)' = f'g + fg'\ ,$$

as well as the chain rule:

$$g(f)' = g'(f) \cdot f'.$$

Furthermore for $\mathrm{char}(K) = 0$*:*

$$f' = 0 \Longleftrightarrow f = a_0 \in K \ ,$$

while for $\mathrm{char}(K) = p > 0$*:*

$$f' = 0 \Longleftrightarrow f \in K[T^p] \ .$$

Proof. We comment on the Leibniz rule and the chain rule: Both the left and the right hand side of the Leibniz rule define bilinear maps $K[T] \times K[T] \longrightarrow K[T]$, so it suffices to check it for the polynomials $1, T, T^2, ...$ (which constitute a base of the K-vector space $K[T]$). But for $f = T^m, g = T^n$ it holds obviously. The chain rule is linear in g, hence we may assume $g = T^n$ - and then it follows from a repeated application of the Leibniz rule. □

Corollary 4.25. *A zero* $a \in K$ *of the polynomial* $f \in K[T]$ *is simple iff* $f'(a) \neq 0$*.*

Proof. We may assume $f \neq 0$ and write $f = (T-a)^\ell h$ with a polynomial $h \in K[T], h(a) \neq 0$. Then we have $f' = \ell(T-a)^{\ell-1}h + (T-a)^\ell h'$ and hence $f'(a) = 0$ iff $\ell > 1$. □

Now we are able to show:

Proposition 4.26. *Let* $f \in K[T]$ *be an irreducible polynomial. Then*

1. *If* $f' \neq 0$*, so in particular if* $\mathrm{char}(K) = 0$*, every zero of* f *in some extension* $E \supset K$ *is simple.*

2. *If* $\mathrm{char}(K) = p > 0$*, we may write*

$$f = g(T^{p^n})$$

with an irreducible polynomial $g \in K[T]$ *with* $g' \neq 0$ *and hence only simple zeros in any extension* $E \supset K$*. In particular all zeros of* f *in any extension* $E \supset K$ *have multiplicity* p^n*.*

Proof. We may assume that f is monic.
i) We show, that $f(a) = 0$ implies $f'(a) \neq 0$. Otherwise $f' \in \mathfrak{m}_a = (f)$ – since f as a monic irreducible polynomial is the minimal polynomial p_a of

its zero $a \in E$ – hence $f|f'$. Since $\deg(f) > \deg(f')$ that implies $f' = 0$. Contradiction!
ii) Choose $n \in \mathbb{N}$ maximal, such that all the exponents of the monomials in the polynomial f are divisible with p^n. Then $f = g(T^{p^n})$, where $g \in K[T], g' \neq 0$. Since f is irreducible, g is as well. Let now $a \in E$ be a zero of f. Then $b = a^{p^n}$ is a simple zero of g according to the first part, i.e. $g = (T-b)h$, where $h(b) \neq 0$. Finally $f = (T^{p^n} - b)h(T^{p^n}) = (T-a)^{p^n} h(T^{p^n})$ with $h(a^{p^n}) \neq 0$, i.e., a has multiplicity p^n. □

The fields K where all irreducible polynomials have automatically only simple zeros get a name:

Definition 4.27. A field K is called **perfect** if either $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p > 0$ and the Frobenius homomorphism $\sigma : K \longrightarrow K, x \mapsto x^p$, is surjective.

Example 4.28.
1. A finite field $\mathbb{F}$ is perfect: The Frobenius homomorphism $\mathbb{F} \longrightarrow \mathbb{F}$ being an injective map from a finite set to itself is also surjective.

2. Let $\mathrm{char}(K) = p > 0$. Then $K(T) = Q(K[T])$ is not perfect, since the indeterminate T is not a p-th power.

Remark 4.29.
1. An irreducible polynomial over a perfect field K has only simple zeros: Write $f = g(T^{p^n})$ as in 4.26, with $g = \sum_\nu a_\nu T^\nu$. Since K is perfect there are (unique) p^n-th roots $c_\nu \in K$ of the coefficients a_ν, i.e. $(c_\nu)^{p^n} = a_\nu$. Then for $h = \sum_\nu c_\nu T^\nu$ we obtain $f = h^{p^n}$, and thus, f being irreducible, we find $n = 0$ and $f = g$.

2. On the other hand, if K is not perfect, there is an irreducible polynomial with multiple roots: Choose an element $a \in K$, which is not a p-th power: Then $f := T^p - a \in K[T]$ is an irreducible polynomial. Assume $h|f$ with an irreducible polynomial $h \in K[T]$. Take an extension $E \supset K$, such that $f(b) = 0$ for some $b \in E$. Then $f = (T-b)^p$ and $h = (T-b)^\ell$ with $2 \leq \ell \leq p$, the ring $E[T]$ being factorial. But according to Prop. 4.26 the multiplicity ℓ is a p-power. Since on the other hand $b \notin K$, we have $\ell = p$, and $f = h$ is irreducible.

For later use we mention the following consequence:

Corollary 4.30. *Let* $\mathrm{char}(K) = p > 0$ *and* $E \supset K$ *be a finite purely inseparable extension, i.e., such that for every* $x \in E$ *there is some* $s \in \mathbb{N}$ *with* $x^{p^s} \in K$ *. Then* $[E : K] = p^\ell$ *for some* $\ell \in \mathbb{N}$.

Proof. We do induction on the extension degree $[E : K]$. Take some $b \in E \backslash K$ with $a = b^p \in K$. Then according to remark 4.29 we have $p_b = T^p - a$ and thus $[K[b] : K] = p$. Since on the other hand $[E : K[b]]$ is a p-power by induction hypothesis, we obtain that $[E : K]$ is as well. □

Problems 4.31.

1. Show Hensels lemma: Let $f \in \hat{\mathbb{Z}}_p[T]$ be a monic polynomial over the ring $\hat{\mathbb{Z}}_p$ of p-adic integers, denote $\tilde{f} \in \mathbb{Z}_p[T] \cong (\hat{\mathbb{Z}}_p/(p))[T]$ the induced polynomial. Show: A simple zero $\xi \in \mathbb{Z}_p$ of $\tilde{f}$ has a unique lift $a = (\xi, \xi_2, \xi_3, ...) \in \hat{\mathbb{Z}}_p$ to a zero of f in $\hat{\mathbb{Z}}_p$. Hint: Construct inductively the components $\xi_n \in \mathbb{Z}_{p^n}$! If $\xi_n = c + (p^n)$, then $\xi_{n+1} = c + tp^n + (p^{n+1})$, where $0 \leq t < p$. Consider the expansion $f(T + c) = f(c) + f'(c)T + ...$

2. Let $r \in \mathbb{N}_{>0}$, relatively prime to both p and $p - 1$. Show for the "sphere"

$$\hat{\mathbb{Z}}_p^* = \{x \in \mathbb{Q}_p; |x| = 1\} \subset \mathbb{Q}_p$$

the following characterization

$$\hat{\mathbb{Z}}_p^* = \{x \in \mathbb{Q}_p^*; x \text{ is an } r^n\text{-th power in } \mathbb{Q}_p \text{ for all } n \in \mathbb{N}\}.$$

Hint: For the inclusion "$\subset$" it is sufficient to see that any $x \in \hat{\mathbb{Z}}_p^*$ is an r-th power (why?), then use the previous problem with the polynomial $f = T^r - x$.

3. Show $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}_p) = \{\mathrm{id}_{\mathbb{Q}_p}\}$. Hint: Use the previous problem in order to see that $\sigma(\hat{\mathbb{Z}}_p^*) \subset \hat{\mathbb{Z}}_p^*$ for any automorphism $\sigma : \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$. As a consequence, σ is an isometry, and thus, $\mathbb{Q}$ being dense in $\mathbb{Q}_p$, the identity.

4. For the ring $K[[X]]$ of formal power series over a field K and the factor ring $K[[T]]/(T) \cong K$ formulate and show Hensels lemma, cf. the first problem of this section 4.31 as well as Problem 3.38.10.

5. Let K be a field and

$$K((X)) = Q(K[[X]]) = K[[X]] \oplus \bigoplus_{n=1}^{\infty} KX^{-n}$$

the field of fractions of the ring $K[[X]]$ of formal power series over K, furthermore $r \neq \mathrm{char}(K)$ a prime number. Show:

$$K[[X]]^* = K^* + XK[[X]]$$

$$= K^* \cdot \{f \in K((X))^*; f \text{ is an } r^n\text{-th power in } K((X)) \text{ for all } n \in \mathbb{N}\}.$$

6. Show that for $\sigma \in \mathrm{Aut}_K(K((X)))$ we have $\sigma(K[[X]]) \subset K[[X]]$. (Hint: Use the previous problem in order to see $\sigma(K[[X]]^*) \subset K[[X]]^*$.) Hence $\sigma : K((X)) \longrightarrow K((X))$ is the unique extension of a substitution automorphism $\hat{\psi}_g : K[[X]] \longrightarrow K[[X]], f \mapsto f(g)$, with a series $g \in K^*X + K[[X]]X^2$, cf. Problem 3.19.7.

7. Show $\mathrm{Aut}_{K(X)}(K((X))) = \{\mathrm{id}_{K((X))}\}$.

4.4 Splitting Fields

The example 4.19.3 suggests that a field extension $E \supset K$ has a big automorphism group, if it has the following form:

Definition 4.32. *1. A finite field extension $E \supset K$ is called* **normal** *iff there is a polynomial $f \in K[T]$, such that*

$$f = (T - a_1) \cdot ... \cdot (T - a_r)$$

with elements $a_1, ..., a_r \in E$ and

$$E = K[a_1, ..., a_r] \ .$$

In that case E is called a **splitting field** *(rotkropp) of the polynomial $f \in K[T]$.*

2. A normal extension $E \supset K$ is called a **Galois extension** *or* **galois** *(*Évariste Galois, 1811-1832*) if we can choose the elements $a_1, ..., a_r \in E$ pairwise distinct, i.e. such that f only has simple zeroes (or "roots") in E, and the automorphism group $\mathrm{Aut}_K(E)$ then also is called the* **Galois group** *of the extension $E \supset K$.*

Example 4.33. 1. All field extensions $E \supset K$ with $[E : K] = 2$ are normal. Why?

2. $E = \mathbb{Q}[\sqrt{2}, i] \supset \mathbb{Q}$ is normal, in fact even a Galois extension, since E is the splitting field of the polynomial $T^4 - 2T^2 + 9$ or $(T^2 - 2)(T^2 + 1)$, both having 4 distinct zeros.

Proposition 4.34. *For every polynomial $f \in K[T]$ there is an extension $E \supset K$, such that E is a splitting field of f. If $F \supset K$ is another splitting field of $f \in K[T]$, then the extensions $E \supset K$ and $F \supset K$ are isomorphic, but note that there are in general several isomorphisms $E \xrightarrow{\cong} F$.*

Proof. Existence: Induction on $\deg(f)$. For $\deg(f) = 1$ take $E := K$. Now we assume the existence of a splitting field $E \supset K$ for any polynomial $f \in K[T]$ with $\deg(f) < n$ and any field K. Consider then a polynomial $f \in K[T]$ with $\deg(f) = n$. According to 3.33 there is an extension $E \supset K$, such that f has a zero $a \in E$. We may even assume $E = K[a]$ - the element $a \in E$ is algebraic over K and $K[a]$ thus a field.
Now write $f = (T - a)g$ with a polynomial $g \in E[T]$. Since $\deg(g) = n - 1$ there is an extension $L \supset E = K[a]$, such that L is a splitting field of $g \in E[T]$. But then L is also a splitting field of $f = (T - a)g \in K[T]$.
Uniqueness: Apply the below proposition. □

Proposition 4.35. *Let $\varphi : K \longrightarrow F$ be a ring homomorphism between the fields K and F, and let $E \supset K$ be a splitting field of $f \in K[T]$. Assume that $f^\varphi \in F[T]$ is "split", i.e., can be factorized as a product of linear polynomials.*

1. *There is an extension of $\varphi : K \longrightarrow F$ to a ring homomorphism $\sigma : E \longrightarrow F$. The number of such extensions equals $[E : K]$, if f has only simple zeros or if K is perfect, while for a non-perfect field K it is of the form $p^{-\ell}[E : K]$ with $p := \mathrm{char}(K)$ and some $\ell \in \mathbb{N}$.*

2. *If $g \in K[T]$ is an irreducible polynomial dividing f and $a \in N_E(g), b \in N_F(g^\varphi)$, we can even require $\sigma(a) = b$.*

3. *If $F \supset L := \varphi(K)$ is a splitting field of f^φ all extensions $\sigma : E \longrightarrow F$ are isomorphisms.*

Proof. 1.) We do induction on $[E : K]$: For $[E : K] = 1$ we have $E = K$ and $\sigma = \varphi$.
Now assume that for every extension $E \supset K$ as above with $[E : K] < n$ and any $\varphi : K \longrightarrow F$ the statement *1.)* holds.
Let now $[E : K] = n$. Take an element $a \in N_E(f) \setminus K$ and let $g := p_a \in K[T]$. According to 4.18.ii) with $E' = F, K' := \varphi(K)$ there is for every $b \in N_F(g^\varphi)$ precisely one extension $\psi : K[a] \longrightarrow F$ with $\psi(a) = b$, and $N_F(g^\varphi) \neq \emptyset$, since g^φ divides f^φ. Because of $[E : K[a]] < n$ we know according to the induction hypothesis that every ψ can be extended to some $\sigma : E \longrightarrow F$. If f has only simple zeros, so does g as well as g^φ and thus there are $\deg(g^\varphi) = \deg(g) = [K[a] : K]$ different choices for ψ. On the other hand, by induction hypothesis every ψ admits $[E : K[a]]$ different extensions $\sigma : E \longrightarrow F$. Altogether

$\varphi : K \longrightarrow F$ can be extended exactly in $[E : K[a]][K[a] : K] = [E : K]$ different ways.
If K is perfect we may replace f with a polynomial $\tilde{f}$ with only simple zeros: Denote $f_1, ..., f_r$ the (pairwise distinct) monic irreducible divisors of f, then set $\tilde{f} = f_1 \cdot ... \cdot f_r$.
Finally if K is not perfect and $\mathrm{char}(K) = p > 0$, write $f_i = g_i(T^{p^{s_i}})$ with an irreducible polynomial $g_i \notin K[T^p]$ as in Prop. 4.26 and denote $E_0 \subset E$ the splitting field of $g_1 \cdot ... \cdot g_r$. Then we have $x \in E_0 \Longrightarrow x^{p^s} \in E_0$ with $s = \max(s_1, ..., s_r)$, since that holds for all $x \in N_E(f)$. Now there are $[E_0 : K]$ different extensions $\sigma_0 : E_0 \longrightarrow F$ of φ, while for every σ_0 there is only one $\sigma : E \longrightarrow F$ extending σ_0, the Frobenius homomorphism being injective. Since on the other hand $[E : E_0] = p^\ell$ with some $\ell \in \mathbb{N}$ according to Cor. 4.30, we are done.
2.) is an immediate consequence of the above argument, if $a \notin K$, while the case $a \in K$ is trivial.
3.) Applying i) with the ring homomorphism $\varphi^{-1} : L := \varphi(K) \longrightarrow K$ we obtain an extension $\tau : F \longrightarrow E$. The homomorphisms $\tau \circ \sigma : E \longrightarrow E$ and $\sigma \circ \tau : F \longrightarrow F$ then are necessarily automorphisms as injective endomorphisms of finite dimensional K- resp. L-vector spaces. In particular σ is an isomorphism. □

Remark 4.36.
1. For every finite extension $E \supset K$ there is an extension $L \supset E$ such that $L \supset K$ is normal: Write $E = K[a_1, ..., a_r]$ and set $f := p_{a_1} \cdot ... \cdot p_{a_r} \in K[T]$, where $p_{a_i} \in K[T]$ is the minimal polynomial of a_i over K. Let $L \supset E$ be the splitting field of the polynomial $f \in E[T]$. Obviously it is also the splitting field of $f \in K[T]$.

2. If $L \supset E \supset K$ is a field extension and $L \supset K$ is normal, so is $L \supset E$. Furthermore if both $L \supset E$ and $E \supset K$ are normal, then $L \supset K$ is normal, if $L \supset E$ is the splitting field of a polynomial $\in K[T] \subset E[T]$, but otherwise it may happen that $L \supset K$ is not normal any longer, cf. Example 4.41.2.

A natural question now arises: Is it possible to find a (not necessarily finite) algebraic extension $E \supset K$, such that every polynomial $f \in K[T]$ can be written as a product of linear polynomials in $E[T]$? A possible construction could be like this:

We assume that the irreducible monic polynomials in $K[T]$ of degree > 1 can be arranged in a sequence $(f_n)_{n\in\mathbb{N}^+}$ – for $K = \mathbb{Q}$ this applies since $\mathbb{Q}[T] = \bigcup_{n=1}^{\infty} \mathbb{Q}[T]_{\leq n}$ itself is countable (where $K[T]_{\leq n} := K \oplus KT \oplus ... \oplus KT^n$). Then we define inductively an increasing sequence of extensions $(E_n)_{n\in\mathbb{N}}$: Set $E_0 := K$ and for $n \geq 1$ define $E_n \supset E_{n-1}$ to be a splitting field of $f_n \in K[T] \subset E_{n-1}[T]$ and take $E := \bigcup_{n=1}^{\infty} E_n$ as their union.

In the general case we have to apply Zorns lemma, cf. 5.4 and 5.8. In any case the field E deserves a name:

Definition 4.37. *1. Let $E \supset K$ be an algebraic extension, such that every polynomial $f \in K[T]$ can be written as a product of linear polynomials in $E[T]$. Then E is called an* **algebraic closure** *of the field K.*

2. A field K is called **algebraically closed***, iff it is its own algebraic closure, i.e., iff every polynomial in $K[T]$ can be written in $K[T]$ as a product of linear polynomials.*

In fact two algebraic closures $E \supset K$ and $L \supset K$ of a given field K are isomorphic, cf. 5.8. Algebraically closed fields are characterized in:

Proposition 4.38. *For a field K the following statements are equivalent:*

1. K is algebraically closed.

2. There are no non-trivial finite extensions $E \supset K$ (i.e., such that $E \neq K$).

3. Every irreducible polynomial $\in K[T]$ is a linear polynomial.

We leave the easy proof as an exercise to the reader.

Example 4.39. 1. The field $\mathbb{C}$ of all complex numbers is algebraically closed, cf. 4.66.

2. The algebraic closure $E \supset K$ of a field K is algebraically closed: Otherwise there is a non-trivial finite extension $L \supset E$. The composite extension $L \supset K$ is algebraic; take an element $a \in L \setminus E$ and consider its minimal polynomial $p_a \in K[T]$ over K. It can be factorized into linear polynomials over E and hence $a \in E$. Contradiction!

3. The set
$$\mathbb{Q}_a := \{z \in \mathbb{C}; z \text{ algebraic over } \mathbb{Q}\} \subset \mathbb{C} ,$$
of all algebraic complex numbers constitutes a field, cf. 4.13, the algebraic closure of $\mathbb{Q}$. Note that it is much smaller than $\mathbb{C}$, more precisely: $\mathbb{Q}_a$ is countable, but $\mathbb{C}$ is not.

Let us return to finite extensions! The next proposition characterizes splitting fields:

Proposition 4.40. *For a finite field extension $E \supset K$ the following conditions are equivalent:*

1. *The extension $E \supset K$ is normal.*
2. *If an irreducible polynomial $g \in K[T]$ has a zero in E, then it can already be factorized into linear polynomials in $E[T]$.*
3. *If $L \supset E$ is another finite field extension, then $\sigma(E) = E$ for all automorphisms $\sigma \in \mathrm{Aut}_K(L)$.*

Before we prove 4.40, let us discuss some examples:

Example 4.41.
1. The extension $\mathbb{Q}[\sqrt[3]{2}] \supset \mathbb{Q}$ is not normal, since the irreducible polynomial $f = T^3 - 2$ has a zero in $\mathbb{Q}[\sqrt[3]{2}]$, but can not be written as a product of linear polynomials in $(\mathbb{Q}[\sqrt[3]{2}])[T]$.
2. A warning: If $L \supset E$ and $E \supset K$ are normal extensions, the composite extension $L \supset K$ need not be normal: Consider $L = \mathbb{Q}[\sqrt[4]{2}], E = \mathbb{Q}[\sqrt{2}], K = \mathbb{Q}$: The extensions $L \supset E$ and $E \supset K$ have degree 2 and hence are normal, but $L \supset K$ is not: The irreducible polynomial $T^4 - 2 \in \mathbb{Q}[T]$ has the zeros $\pm\sqrt[4]{2} \in E$, but is not the product of linear polynomials $\in L[T]$, since $L \subset \mathbb{R}$, while $T^4 - 2$ has the non-real zeros $\pm i\sqrt[4]{2} \in \mathbb{C}$.

Proof. "i) $\Longrightarrow$ iii)": Assume that E is the splitting field of the polynomial $f \in K[T]$ and $\sigma : L \longrightarrow L$ is a K-automorphism. Let $N(f) = N_L(f) = \{a_1, ..., a_r\}$. Since $f(\sigma(a_i)) = \sigma(f(a_i)) = \sigma(0) = 0$, we have $\sigma(N(f)) \subset N(f)$ resp. $\sigma(N(f)) = N(f)$ ($N(f)$ is finite and σ injective) and thus $\sigma(E) = E$ for $E = K[a_1, ..., a_r]$.
"iii) $\Longrightarrow$ ii)": Assume that the irreducible polynomial $g \in K[T]$ has the zero $a \in E$. According to 4.35 there is an extension $F \supset E$ such that F is the

splitting field of some polynomial $h \in K[T]$. Now let $L \supset F$ be the splitting field of $g \in K[T]$; then $L \supset K$ is the splitting field of $f = gh \in K[T]$.
We have to show that $N_L(g) \subset E$. Take $b \in N_L(g)$. According to 4.18 with the inclusion $K \hookrightarrow E$ as φ there is an automorphism $\sigma \in \mathrm{Aut}_K(L)$ with $b = \sigma(a)$. But then $b \in \sigma(E) = E$.
"ii) $\Longrightarrow$ i)" : Write $E = K[a_1, ..., a_r]$. Then E is the splitting field of the polynomial $p_{a_1} \cdot ... \cdot p_{a_r} \in K[T]$. □

Let us briefly recall the facts we know about the automorphism group $\mathrm{Aut}_K(E)$ of a normal extension $E \supset K$:

Theorem 4.42. *Let $E \supset K$ be a normal extension, the splitting field of the polynomial $f \in K[T]$. Then*

1. *If $g \in K[T]$ is irreducible, the automorphism group $\mathrm{Aut}_K(E)$ acts transitively on the (possibly empty) set $N_E(g) := \{a \in E; g(a) = 0\}$ of zeros of g, i.e., for arbitrary $a, b \in N_E(g)$ there is an automorphism $\sigma \in \mathrm{Aut}_K(E)$ with $\sigma(a) = b$.*

2. *We have*
$$|\mathrm{Aut}_K(E)| = [E : K],$$
if $E \supset K$ is galois, e.g. if K is perfect. In the general case we have
$$[E : K] = p^\ell \cdot |\mathrm{Aut}_K(E)|$$
for $p = \mathrm{char}(K)$ and some $\ell \in \mathbb{N}$.

3. *The map $\sigma \mapsto \sigma|_{N_E(f)}$ defines an injective group homomorphism*
$$\mathrm{Aut}_K(E) \hookrightarrow \mathbb{S}(N_E(f))$$
from the automorphism group of the extension $E \supset K$ to the group of permutations of the set $N_E(f)$ of zeros of the polynomial f in E. If $f_1, ..., f_r \in K[T]$ are the pairwise distinct irreducible monic divisors of f, then the above homomorphism can be factorized:
$$\mathrm{Aut}_K(E) \hookrightarrow \mathbb{S}(N_E(f_1)) \times ... \times \mathbb{S}(N_E(f_r)) \subset \mathbb{S}(N_E(f)).$$

Proof. i) According to 4.40 we have either $N_E(g) = \emptyset$ or g can be written as a product of linear polynomials in $E[T]$. In the first case there is nothing to be shown, while in the second case we may assume that g divides the polynomial giving rise to E as its splitting field - if not, we may multiply it with g - the splitting field remains the same. Now apply 4.35.2.
ii) is nothing but 4.35.i) with $F = E$ and the inclusion $\varphi : K \hookrightarrow E$.
iii) follows from the fact that $E = K[a_1, ..., a_r]$, where $N_E(f) = \{a_1, ..., a_r\}$, and that a K-automorphism is uniquely determined by its values $\sigma(a_i) \in N_E(f), 1 \leq i \leq r$. □

Remark 4.43. Let us briefly recall the explicit construction of automorphisms $\sigma : E = K[a_1, ..., a_r] \longrightarrow E$ for a normal extension $E \supset K$: Every automorphism $\sigma \in \mathrm{Aut}_K(E)$ is obtained in the following way: Let $E_i := K[a_1, ..., a_i]$. We have in any case $\sigma|_{E_0} = \mathrm{id}_{E_0}$. If $\sigma|_{E_i}$ already is given, we may choose $\sigma(a_{i+1})$ freely in the (non-empty) zero set $N_E(g^\sigma)$, where $g \in E_i[T]$ is the minimal polynomial of $a_{i+1} \in E$ over E_i. Indeed, the minimal polynomial $h := p_{a_{i+1}} \in K[T]$ of a_{i+1} over K is split over E, and $g|h$ implies $g^\sigma|h^\sigma = h$.

Example 4.44.

1. Take the polynomial $f = T^3 - 2 \in \mathbb{Q}[T]$, cf. 4.19 3.1. Its splitting field is $E := \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}\varepsilon, \sqrt[3]{2}\varepsilon^2] = \mathbb{Q}[\sqrt[3]{2}, \varepsilon]$ with the third root of unity $\varepsilon := \frac{1}{2}(-1 + i\sqrt{3})$. We have $E_1 = \mathbb{Q}[\sqrt[3]{2}]$ and there are three different $\mathbb{Q}$-morphisms $\psi_\nu : E_1 \longrightarrow E; 0 \leq \nu \leq 2$, with $\psi_\nu(\sqrt[3]{2}) = \sqrt[3]{2}\varepsilon^\nu$. Each $\psi_\nu : E_1 \longrightarrow E$ in turn may be extended in two ways: The minimal polynomial $g \in E_1[T]$ of ε is $g = (T-\varepsilon)(T-\varepsilon^{-1}) = T^2+T+1$, lying even in $\mathbb{Q}[T]$; hence $g^{\psi_\nu} = g$ for $\nu = 0, 1, 2$, and ψ_ν extends to the automorphisms $\sigma_\nu^\pm : E \longrightarrow E$ with $\sigma_\nu^\pm(\varepsilon) = \varepsilon^{\pm 1}$. Note that any permutation of $N_E(f)$ is realized by some automorphism.

2. The situation is more interesting for the polynomial $f = T^4 - 2 \in \mathbb{Q}[T]$. The splitting field is $E := \mathbb{Q}[\sqrt[4]{2}, i]$ with the fourth root of unity i, and we could argue as in the first case. Instead we consider the representation $E = \mathbb{Q}[\sqrt{2}, i, \sqrt[4]{2}]$ and discuss the step from $E_2 =: L$ to $E_3 = E$. The intermediate field $L = \mathbb{Q}[\sqrt{2}, i]$ is the splitting field of $(T^2-2)(T^2+1)$, cf. 4.19 iv). Since $L \supset \mathbb{Q}$ is normal, we have $\sigma(L) = L$ for every $\sigma \in \mathrm{Aut}_\mathbb{Q}(E)$. The minimal polynomial $g \in L[T]$ of $\sqrt[4]{2}$ is $T^2 - \sqrt{2}$ and $g^\sigma = T^2 \mp \sqrt{2}$. Depending on the sign ± 1 necessarily $\sigma(\sqrt[4]{2}) = \pm\sqrt[4]{2}$ or $\sigma(\sqrt[4]{2}) = \pm\sqrt[4]{2}i$. In contrast to the situation in i) not

every permutation of $N_E(f)$ is the restriction of some automorphism, cf. Problem 4.46.2.

The case where the splitting field $E \supset K$ is of maximal size is characterized by:

Proposition 4.45. *Let $E \supset K$ be the splitting field of $f \in K[T], n := \deg(f)$. Then we have $[E : K] \leq n!$. Furthermore for $n \geq 3$, equality $[E : K] = n!$ holds if and only if $|N_E(f)| = n$ and the homomorphism $\mathrm{Aut}_K(E) \hookrightarrow \mathbb{S}(N_E(f)), \sigma \mapsto \sigma|_{N_E(f)}$, is an isomorphism.*

Proof. The degree estimate is shown by induction on n.
" $\Longrightarrow$ ": If $r := |N_E(f)| < n$, there is a multiple root a of f, i.e. such that $f = (T-a)^2 g$. But then we obtain $E \supset L := K[a]$ as splitting field of $g \in L[T]$ and $[E : K] = [E : L][L : K] \leq (n-2)! \cdot n < n!$. Contradiction!. So f has n pairwise distinct zeros and the extension $E \supset K$ is galois, hence $|\mathrm{Aut}_K(E)| = [E : K] = n!$ and the injective homomorphism $\mathrm{Aut}_K(E) \hookrightarrow \mathbb{S}(N_E(f))$ is even an isomorphism.
" $\Longleftarrow$ ": Because of $|N_E(f)| = n$ the polynomial f has no multiple roots; thus $E \supset K$ is galois. We have then $[E : K] = |\mathrm{Aut}_K(E)| = n!$. □

Problems 4.46.

1. R: Let K be a field of characteristic $p > 0$ and $E \supset K$ a splitting field of $T^p - T - c \in K[T]$. Show, that either $E = K$ or $E \supset K$ is Galois with $[E : K] = p$ and cyclic Galois group $\mathrm{Aut}_K(E)$! What can be said, if $K = \mathbb{Z}_p$? Hint: If $a \in E \supset K$ is a zero of f, compute $f(a+n)$!
2. R: Let $E \supset \mathbb{Q}$ be the splitting field of the polynomial $T^4 - 2$. Show that $\mathrm{Aut}_{\mathbb{Q}}(E) \cong D_4$, where D_4 denotes the dihedral group. Hint: Consider the square with vertices $\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i$!
3. R: Compute the splitting field $E \supset \mathbb{Q}$ of $f := T^4 - 10T^2 + 1$. Determine $\mathrm{Aut}_{\mathbb{Q}}(E)$! Hint: Consider the splitting field F of the polynomial $T^2 - 10T + 1$? Then try to compute the square roots of its zeros in F - that is not possible since there is missing what in F?
4. Let $f \in \mathbb{Q}[T]$ be an irreducible polynomial whose degree is a prime p and which has exactly two (simple) non-real roots. Show that its splitting field $E \supset \mathbb{Q}$ satisfies $\mathrm{Aut}_{\mathbb{Q}}(E) \cong \mathbb{S}_p$. Hint: Apply Problem 2.39.5.
5. Show that the polynomial $f := T^5 - 4T + 2$ satisfies the conditions in the preceding problem. Hint: Apply real analysis: Determine the real zeros of its derivative f' and the sign of the corresponding value of f. Then one can apply which theorem?
6. Show: An algebraic number $\lambda \in \mathbb{Q}_a$ is an algebraic integer iff its minimal polynomial $p_\lambda \in \mathbb{Q}[T]$ has integer coefficients: $p_\lambda \in \mathbb{Z}[T]$. Hint: Consider a splitting field $E \supset \mathbb{Q}$ containing λ; if λ is an algebraic integers its "conjugates" $\sigma(\lambda) \in E, \sigma \in \mathrm{Aut}_{\mathbb{Q}}(E)$, are algebraic integers as well. Cf. also Problem 4.15.7.

4.5 Finite Fields

The aim of this section is the complete classification of all finite fields. We start our investigations with the following general result about finite subgroups of the multiplicative group K^* of any field K:

Proposition 4.47. *Any finite subgroup of the multiplicative group K^* of a field K is cyclic. In particular, the multiplicative group $\mathbb{F}^*$ of a finite field $\mathbb{F}$ is cyclic*

Proof. Denote $G \subset K^*$ a finite subgroup of the multiplicative group K^* of our field K. Since G is abelian, there is according to 2.84 an isomorphism $G \cong \mathbb{Z}_{q_1}^{n_1} \times ... \times \mathbb{Z}_{q_r}^{n_r}$ - (with the right hand side additively written!) - where $q_1, ..., q_r$ are pairwise distinct prime powers and $n_i \in \mathbb{N}_{>0}$. Then the least common multiple $q := \text{lcm}(q_1, ..., q_r)$ satisfies $a^q = 1$ for all $a \in G$, i.e., the zero set of the polynomial $T^q - 1 \in K[T]$ contains the entire group G. A polynomial of degree q over an integral domain has at most q zeros, cf. 3.17, hence $q_1^{n_1} \cdot ... \cdot q_r^{n_r} = |G| \leq q$.
But that is possible only if the numbers $q_1, ..., q_r$ are pairwise relatively prime and $n_1 = ... = n_r = 1$. In that case $(\overline{1}, ..., \overline{1})$ has order $q_1 \cdot ... \cdot q_r = q = |\mathbb{Z}_{q_1} \times ... \times \mathbb{Z}_{q_r}|$, so G is a cyclic group. □

To every prime power $q = p^n$ we associate a finite field $\mathbb{F}_q$:

Definition 4.48. *Let $q = p^n$ with a prime number p and $n \in \mathbb{N}_{>0}$. We denote $\mathbb{F}_q \supset \mathbb{Z}_p$ a splitting field of the polynomial $T^q - T \in \mathbb{Z}_p[T]$.*

Remark 4.49.

1. For $n = 1$ we have $\mathbb{F}_p = \mathbb{Z}_p$, while $\mathbb{F}_{p^n} \ncong \mathbb{Z}_{p^n}$ for $n > 1$, since the ring $\mathbb{Z}_{p^n}$, containing non-zero nilpotent elements, neither is a field nor an integral domain.

2. There is a further difference between the definition of $\mathbb{Z}_q$ and that of $\mathbb{F}_q$: While the first one is well defined even as a set, the latter has as a set no natural realization, though all constructions lead to isomorphic fields, cf. 4.34. Hence from the point of view of algebra, the choices entering in a concrete realization are not really interesting, and one usually refers to **the** field $\mathbb{F}_q$. For example given a generator $a \in \mathbb{F}_q^*$ of its multiplicative group, we find $\mathbb{F}_q \cong \mathbb{Z}_p[T]/(p_a)$, where p_a is the minimal polynomial of the generator a, but unfortunately the polynomial p_a in general really depends on the choice of that generator.

The main result of this section is

Theorem 4.50. *1. We have* $|\mathbb{F}_{p^n}| = p^n$ *resp.* $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

2. Every finite field is isomorphic to a field $\mathbb{F}_{p^n}$.

3. The field $\mathbb{F}_{p^m}$ *is isomorphic to a subfield of* $\mathbb{F}_{p^n}$*, iff* m *is a divisor of* n*. (But note that for* $m > 1$ *there are then several ring homomorphisms* $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$*, two such homomorphisms differing by an automorphism* $\in \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^m})$*!)*

4. The extension $\mathbb{F}_{p^n} \supset \mathbb{F}_p$ *is a Galois extension, and* $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ *is a cyclic group of order* n*, generated by the Frobenius automorphism* $\sigma : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}, x \mapsto x^p$.

Remark 4.51. The field $\mathbb{F}_{p^n}$ is also called the **field with** p^n **elements**. A more old fashioned notation for it is $GF(p^n)$, where GF is the abbreviation for "Galois field". This is also the reason why in English the word "field" is used in general, while in most other languages the corresponding translation of "kropp" applies, as introduced by Bourbaki, a group of french mathematicians which beginning in the 1930ies tried to modernize and systematize mathematics.

Proof. i) The polynomial $f := T^{p^n} - T$ has derivative $f' = -1$ and hence only simple zeros, and thus $|N_{\mathbb{F}_{p^n}}(f)| = p^n$. But on the other side we may interpret that zero set as the fixed point set of the n-th iterate σ^n of the Frobenius automorphism $\sigma : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}, x \mapsto x^p$, i.e.:

$$N_{\mathbb{F}_{p^n}}(f) = \mathrm{Fix}(\sigma^n) := \{x \in \mathbb{F}_{p^n}; x = \sigma^n(x) = x^{p^n}\}$$

and hence is in particular itself a field! Since $\mathbb{F}_{p^n}$ is the smallest extension of $\mathbb{F}_p$, over which f is split, it follows $\mathbb{F}_{p^n} = \mathrm{Fix}(\sigma^n)$.
ii) According to Corollary 4.3 we already know $|\mathbb{F}| = p^n$ with some $n \in \mathbb{N}_{>0}$. On the other hand Corollary 2.38 tells us that $x^{p^n-1} = x^{|\mathbb{F}^*|} = 1$ holds for all $x \in \mathbb{F}^*$ resp. $x^{p^n} = x$ for all $x \in \mathbb{F}$. So the polynomial $f := T^{p^n} - T$ has the entire field $\mathbb{F}$ as its zero set, in particular

$$T^{p^n} - T = \prod_{a \in \mathbb{F}} (T - a),$$

both sides being monic polynomials with the same (simple) zeroes. With other words, the field $\mathbb{F}$ is a splitting field of $f \in \mathbb{Z}_p[T] = \mathbb{F}_p[T]$.

iii) "$\Longrightarrow$": Assume $\varphi : \mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$ is a ring homomorphism (it is not unique for $m > 1$). Then $\mathbb{F}_{p^n}$ is a $\mathbb{F}_{p^m}$-vector space, whence $\mathbb{F}_{p^n} \cong (\mathbb{F}_{p^m})^r$ with $r = \dim_{\mathbb{F}_{p^m}} \mathbb{F}_{p^n}$ resp. $p^n = (p^m)^r = p^{mr}$ resp. $n = mr$.
"$\Longleftarrow$": Let $n = mr$. Since $\mathbb{F}_{p^m}$ is the splitting field of $T^{p^m-1}-1$, it is sufficient to show:

$$(T^{p^m-1} - 1) \text{ divides } (T^{p^n-1} - 1) \ .$$

In any case $T - 1$ divides $T^r - 1$, and after substitution of T by T^m we see that $T^m - 1$ divides $T^n - 1$. In particular the number $p^m - 1$ divides $p^n - 1$, and finally, with $p^m - 1$ and $p^n - 1$ instead of m and n we arrive at our claim.
iv) The extension $\mathbb{F}_{p^n} \supset \mathbb{F}_p = \mathbb{Z}_p$ is galois, since $T^{p^n} - T$ only has simple zeros. If we can show, that the Frobenius automorphism $\sigma : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ has order n, we are done, since the automorphism group $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ has order n according to 4.42. But $\sigma^k = \mathrm{id}_{\mathbb{F}_{p^n}}$ is equivalent to $x^{p^k-1} = 1$ for all $x \in \mathbb{F}_{p^n}^*$. Since $\mathbb{F}_{p^n}^*$ is cyclic and thus there is an element $x \in \mathbb{F}_{p^n}^*$ of order $p^n - 1$, we see that $\sigma^k \neq \mathrm{id}_{\mathbb{F}_{p^n}}$ för $k < n$. □

Remark 4.52. Let us give here an explicit description of an algebraic closure $\overline{\mathbb{F}}_p \supset \mathbb{F}_p$ of the finite field $\mathbb{F}_p$. Take $E_n := \mathbb{F}_{p^{n!}}$ and choose ring homomorphisms $\varphi_n : E_n \hookrightarrow E_{n+1}$. Then, interpreting φ_n as an inclusion $E_n \subset E_{n+1}$ we may define

$$\overline{\mathbb{F}}_p := \bigcup_{n=1}^{\infty} E_n.$$

4.5.1 Digression 1: Quadratic reciprocity

As an application of finite fields we shall give a proof of the law of quadratic reciprocity. In order to formulate it we need the Legendre symbol (André Marie Legendre, 1752 - 1833):

Definition 4.53. Denote $P_{>2}$ the set of all odd primes. The Legendre symbol is the map

$$\left(\frac{-}{-}\right) : \mathbb{Z} \times P_{>2} \longrightarrow \{0, \pm 1\}, (a, p) \mapsto \left(\frac{a}{p}\right),$$

where

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & , \text{ if } \overline{a} \in \mathbb{F}_p^* \text{ is a square} \\ -1 & , \text{ if } \overline{a} \in \mathbb{F}_p^* \text{ is not a square} \\ 0 & , \text{ if } \overline{a} = 0 \in \mathbb{F}_p \end{cases} .$$

Remark 4.54. 1. The Legendre symbol depends only on $\overline{a} \in \mathbb{F}_p$, so for convenience we define

$$\left(\frac{\overline{a}}{p}\right) := \left(\frac{a}{p}\right)$$

for $\overline{a} \in \mathbb{F}_p$.

2. If $c \in \mathbb{F}_p^*$ is a generator of the (cyclic) multiplicative group $\mathbb{F}_p^*$, i.e., $\mathbb{F}_p^* = c^{\mathbb{Z}}$, we have

$$\left(\frac{c^\nu}{p}\right) = (-1)^\nu.$$

3. $\{0, \pm 1\} \subset K$ for any field K with $\mathrm{char}(K) \neq 2$.

4. With that convention we have

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \in \mathbb{F}_p$$

for all $a \in \mathbb{F}_p$.

5. The Legendre symbol is multiplicative in the upper variable:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

for $a, b \in \mathbb{Z}$ as well as $a, b \in \mathbb{Z}_p$. In particular it is sufficient to compute the Legendre symbol for a being a prime as well.

Theorem 4.55. *Let $p \in P_{>2}$ be an odd prime.*

1. *We have*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & , \quad \text{if } p \equiv \pm 1 \mod (8) \\ -1 & , \quad \text{if } p \equiv \pm 3 \mod (8) \end{cases},$$

or, more briefly

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

2. *The law of quadratic reciprocity: For a prime $q \in P_{>2}$ different from p we have*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Proof. 1.) The field $\mathbb{F}_{p^2} \supset \mathbb{F}_p$ contains an element ζ of order 8, since the order $p^2 - 1$ of the cyclic group $(\mathbb{F}_{p^2})^*$ is divisible by 8.

Now for $\beta := \zeta + \zeta^{-1}$ we have

$$\beta^2 = \zeta^2 + 2 + \zeta^{-2} = \zeta^2 + 2 - \zeta^2 = 2,$$

since $\zeta^4 = -1$. As a consequence 2 is a square in $\mathbb{F}_p$ iff $\beta \in \mathbb{F}_p \subset \mathbb{F}_{p^2}$ iff $\beta = \beta^p$. Now

$$\beta^p = \zeta^p + \zeta^{-p} = \zeta^s + \zeta^{-s},$$

where $p = 8d + r$. Thus for $r = \pm 1$ we find $\beta^p = \beta$, while $r = \pm 3$ yields $\beta^p = -\beta$.

2.) We do computations in the splitting field $E \supset \mathbb{F}_p$ of the polynomial $T^q - 1 \in \mathbb{F}_p[T]$, denote $\eta \in E \setminus \{1\}$ a root of it and use the notation

$$\chi(a) := \left(\frac{a}{q}\right) \in \{0, \pm 1\} \subset E.$$

We need the following auxiliary lemma:

Lemma 4.56. *The square of the* Gauß' sum

$$\gamma := \sum_{i=0}^{q-1} \chi(i)\eta^i$$

satisfies

$$\gamma^2 = \chi(-1)q \in \mathbb{F}_p^* \subset E.$$

Let us first finish the proof of the theorem: We apply the Frobenius map $E \longrightarrow E, x \mapsto x^p$, to our Gauß' sum:

$$\gamma^p = \sum_{i=0}^{q-1} \chi(i)^p \eta^{ip} = \sum_{i=0}^{q-1} \chi(i)\eta^{ip}$$

$$= \sum_{i=0}^{q-1} \chi(p^2 i)\eta^{ip} = \chi(p) \sum_{i=0}^{q-1} \chi(ip)\eta^{ip} = \chi(p)\gamma,$$

using $\chi(i)^p = \chi(i) = \chi(p^2 i)$ and the fact that $\mathbb{Z}_q \longrightarrow \mathbb{Z}_q, i \mapsto ip$, is a bijection. Since $\gamma \neq 0$, we may conclude

$$\left(\frac{p}{q}\right) = \gamma^{p-1} = (\gamma^2)^{\frac{p-1}{2}} = (\chi(-1)q)^{\frac{p-1}{2}}$$

$$= ((-1)^{\frac{q-1}{2}})^{\frac{p-1}{2}} q^{\frac{p-1}{2}} = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{q}{p}\right),$$

where we have used Remark 4.54.4 with respect to $a = -1$ and the prime q as well as $a = q$ and the prime p. □

Proof of the lemma. First of all we may understand the exponents of η as well as the argument of χ as elements in $\mathbb{Z}_q$. Using that convention we remark the following identities:

$$\sum_{i \in \mathbb{Z}_q} \chi(i) = 0, \ \sum_{i \in \mathbb{Z}_q} \eta^i = 0.$$

The first one follows from the fact that $\chi(0) = 0$ and there are $\frac{q-1}{2}$ quadratic residues as well as $\frac{q-1}{2}$ quadratic non-residues in $\mathbb{Z}_q$, for the second one notes that the sum not changing when multiplied by η has to be $= 0$.

Now

$$\begin{aligned} \gamma^2 &= \sum_{(i,j) \in (\mathbb{Z}_q)^2} \chi(i)\chi(j)\eta^{i+j} \\ &= \sum_{\ell \in \mathbb{Z}_q} \Big(\sum_{i+j=\ell} \chi(i)\chi(j) \Big) \eta^\ell. \end{aligned}$$

Let us now compute the inner sums. The case $\ell = 0$ yields

$$\sum_{i+j=0} \chi(i)\chi(j) = \sum_{i \in \mathbb{Z}_q} \chi(i)\chi(-i) = \sum_{i \in \mathbb{Z}_q} \chi(-i^2) = \chi(-1)(q-1),$$

since $\chi(-i^2) = \chi(i^2)\chi(-1) = \chi(-1)$ for $i \neq 0$, while $\chi(-0^2) = 0$.

Finally we treat the case $\ell \neq 0$ and get

$$\begin{aligned}\sum_{i+j=\ell} \chi(i)\chi(j) &= \sum_{i\in\mathbb{Z}_q^*} \chi(i)\chi(\ell-i) \\ &= \sum_{i\in\mathbb{Z}_q^*} \chi(i^{-1})\chi(\ell-i) \\ &= \sum_{i\in\mathbb{Z}_q^*} \chi(\ell i^{-1}-1) \\ &= \sum_{i\in\mathbb{Z}_q\setminus\{-1\}} \chi(i) = -\chi(-1),\end{aligned}$$

since $\chi(0) = 0, \chi(i^{-1}) = \chi(i)$ and $\{\ell i^{-1} - 1; i \in \mathbb{Z}_q^*\} = \mathbb{Z}_q \setminus \{-1\}$. Hence

$$\gamma^2 = \chi(-1)(q-1) - \chi(-1)\sum_{\ell\in\mathbb{Z}_q^*} \eta^\ell$$

$$= \chi(-1)(q-1) - \chi(-1)\cdot(-1) = \chi(-1)q.$$

□

4.5.2 Digression 2: Further Simple Groups

Finite fields may be used to give further examples of simple groups. First of all note that we may define the general linear group $GL_n(K)$ and the special linear group $SL_n(K)$ of 2.4.5 and 2.24.2 for any field K, in particular for finite fields $K = \mathbb{F}$.

The general linear group acts in a natural way on the projective space $\mathbb{P}_{n-1}(K)$, the set of all lines (:= one dimensional subspaces) in K^n, cf. Problems 2.18.11 and 4.20.6. The kernel of the corresponding group homomorphism $GL_n(K) \longrightarrow \mathbb{S}(\mathbb{P}_{n-1}(K))$ is K^*E, the subgroup of all non-zero multiples of the unit matrix $E = (\delta_{ij})$. So the *projective (general) linear group*

$$PGL_n(K) := GL_n(K)/K^*E$$

can be understood as a group of projective transformations, i.e. permutations of $\mathbb{P}_{n-1}(K)$, usually called *projective linear transformations*.

Restricting everything to $SL_n(K) \trianglelefteq GL_n(K)$ we obtain the *projective special linear group*

$$PSL_n(K) := SL_n(K)/C_n(K)E$$

with the group

$$C_n(K) := \{a \in K^*; a^n = 1\}$$

of n-th roots of unity in the field K. We note that $K^*E \trianglelefteq GL_n(K)$ and $C_n(K) \cdot E \trianglelefteq SL_n(K)$ are nothing but the centers of the general resp. special linear group of size n. Obviously

$$PSL_n(K) \trianglelefteq PGL_n(K),$$

with factor group

$$PGL_n(K)/PSL_n(K) \cong GL_n(K)/K^*SL_n(K)$$

$$\cong K^*/\det(K^*E) = K^*/p_n(K^*)$$

with the n-th power map $p_n : K^* \longrightarrow K^*, x \mapsto x^n$.

The central result of this digression is:

Theorem 4.57. *Let K be a field. The group $PSL_n(K)$ is simple for $n > 2$ and for $n = 2, |K| > 3$.*

Proof. Since the inverse image of a normal subgroup with respect to a group homomorphism itself is normal, it suffices to show the following: Any normal subgroup $N \trianglelefteq SL_n(K)$ containing the center $C_n(K)E$ as a proper subgroup coincides with $SL_n(K)$.

The strategy is as follows: We show

1. The group $G := SL_n(K)$ is generated by "elementary matrices".
2. If $N \trianglelefteq G$ is a normal subgroup containing the center $C_n(K)E$ as proper subgroup, then the factor group G/N is abelian.
3. If $n > 2$ or $n = 2$ and $|K| > 3$ any elementary matrix can be written as a "commutator" $ABA^{-1}B^{-1}$ with matrices $A, B \in G$.

By 2) every commutator $ABA^{-1}B^{-1}$ belongs to the subgroup $N \subset G$, and then 1) and 3) tell us that $N = G$.

Generators for $SL_n(K)$: We identify a matrix $A \in GL_n(K)$ freely with the corresponding linear map $K^n \longrightarrow K^n, x \mapsto Ax$, and denote $e_1, ..., e_n$ the

standard base of the vector space K^n. Denote $E = (\delta_{ij})$ the unit matrix and $E_{k\ell} = (\delta_{ik}\delta_{j\ell})$, i.e.

$$E_{k\ell}\, e_i = \begin{cases} e_k & , \text{ if } i = \ell \\ 0 & , \text{ otherwise} \end{cases},$$

whence $E_{k\ell}E_{rs} = \delta_{\ell r}E_{ks}$. An elementary matrix now is a matrix

$$Q_{ij}(\lambda) := E + \lambda E_{ij},\ i \neq j, \lambda \in K^*.$$

Note that $K \longrightarrow SL_n(K), \lambda \mapsto Q_{ij}(\lambda)$ is a group homomorphism:

$$Q_{ij}(\lambda + \mu) = Q_{ij}(\lambda)Q_{ij}(\mu),$$

and that for $n > 2$ all $Q_{ij}(\lambda)$ for fixed $\lambda \in K^*$ belong to the same conjugacy class in $SL_n(K)$: There is some $P \in SL_n(K)$ with $Pe_1 = e_i, Pe_2 = e_j$, whence

$$PQ_{12}(\lambda)P^{-1} = Q_{ij}(\lambda).$$

For $n = 2$ we take P with $Pe_1 = e_2, Pe_2 = -e_1$ and find

$$PQ_{12}(\lambda)P^{-1} = Q_{21}(-\lambda).$$

¿From linear algebra it is well known that $GL_n(K)$ is generated by the following three groups of matrices:

- The elementary matrices $Q_{ij}(\lambda), i \neq j, \lambda \in K^*$,
- the "transposition matrices" $T_{k\ell}, k < \ell$, satisfying

$$T_{k\ell}\, e_i = \begin{cases} e_k & , \text{ if } i = \ell \\ e_\ell & , \text{ if } i = k \\ e_i & , \text{ otherwise} \end{cases},$$

  and

- the diagonal matrices.

More precisely, any matrix $A \in GL_n(K)$ is of the form $A = A_0TD$, where A_0 is a product of elementary matrices, T a product of transposition matrices and D a diagonal matrix (the matrix TD having in every row and column exactly one nonzero entry). In order to get generators of $SL_n(K)$ we have to modify the matrices of the second and third kind: We claim that

- the elementary matrices $Q_{ij}(\lambda), i \neq j, \lambda \in K^*$,
- the special transposition matrices $P_{k\ell}, k < \ell$, with

$$P_{k\ell}\ e_i = \begin{cases} e_k & , \text{ if } i = \ell \\ -e_\ell & , \text{ if } i = k \\ e_i & , \text{ otherwise} \end{cases},$$

and

- the special diagonal matrices, i.e. the diagonal matrices

$$D_1(\lambda_1)D_2(\lambda_2) \cdot ... \cdot D_{n-1}(\lambda_{n-1})$$

with (unique) $\lambda_1, ..., \lambda_{n-1} \in K^*$, where $D_k(\lambda), k < n$, is defined by

$$D_k(\lambda)\ e_i = \begin{cases} \lambda e_k & , \text{ if } i = k \\ \lambda^{-1} e_{k+1} & , \text{ if } i = k+1 \\ e_i & , \text{ otherwise} \end{cases},$$

together generate $SL_n(K)$: Let $A \in SL_n(K), A = A_0TD$ as above. If we replace T, a product of matrices $T_{k\ell}$ with P, the corresponding product of the matrices $P_{k\ell}$, we have $A = A_0P\tilde{D}$ with a diagonal matrix $\tilde{D}$, whose entries coincide with those of D up to sign. Since A_0, P are special matrices, $\tilde{D}$ is special as well.

1.) The elementary matrices generate $SL_n(K)$: We show that the matrices $P_{k\ell}, k < \ell \leq n$, and $D_k(\lambda), k = 1, ..., n-1$, are products of elementary matrices. In fact

$$P_{k\ell} = Q_{\ell k}(-1)Q_{k\ell}(1)Q_{\ell k}(-1),$$

and for the $D_k(\lambda)$ we may assume $n = 2$ and find for $D(\lambda) := D_1(\lambda)$ that

$$D(\lambda) = Q_{12}(-\lambda)Q_{21}(\lambda^{-1})Q_{12}(-\lambda)P_{12},$$

which yields the desired result, since we already know that P_{12} is a product of elementary matrices.

2.) Abelian Factor group: The stabilizer

$$U := SL_n(K)_L = \{A \in SL_n(K); A(L) = L\}$$

of the line $L := Ke_1 \in \mathbb{P}_{n-1}(K)$ satisfies

$$A \in U \Longleftrightarrow A = \begin{pmatrix} \lambda & b \\ 0 & C \end{pmatrix} \text{ with } \lambda \in K^*, b^T, 0 \in K^{n-1}, C \in K^{n-1.n-1}, \lambda \det C = 1.$$

Consider the kernel $U_0 \trianglelefteq U$ of the natural group homomorphism

$$U \longrightarrow GL(L) \times GL(K^n/L), A \mapsto (A|_L, \overline{A}),$$

where $\overline{A} : K^n/L \longrightarrow K^n/L$ is the linear map $x + L \mapsto Ax + L$. In fact,

$$A \in U_0 \Longleftrightarrow A = \begin{pmatrix} 1 & b \\ 0 & E \end{pmatrix} \text{ with } b^T, 0 \in K^{n-1}, E = (\delta_{ij}) \in K^{n-1.n-1},$$

and

$$K^{n-1} \longrightarrow U_0, \ y \mapsto \begin{pmatrix} 1 & y^T \\ 0 & E \end{pmatrix}$$

is a group isomorphism; in particular, U_0 is abelian. –

We have

$$SL_n(K) = NU,$$

since $U = SL_n(K)_L$ is the stabilizer of $L \in \mathbb{P}_{n-1}(K)$ in $SL_n(K)$ and the subgroup $N \trianglelefteq SL_n(K)$ acts transitively on $\mathbb{P}_{n-1}(K)$: Take a line $Ky \neq L$. Since $N \supsetneqq C_n(K) \cdot E$, there is some $B \in N \setminus K^*E$. Hence we can find $x \in K^n$, such that $x, Bx \in K^n$ are linearly independent and choose $C \in SL_n(K)$ with $Cx = e_1, CBx = \lambda y$ for some $\lambda \in K^*$. Then $A := CBC^{-1} \in N$ satisfies $Ae_1 = \lambda y$, in particular $Ky = A(L)$.

Now we show that even

$$SL_n(K) = NU_0.$$

First of all, $NU_0 \trianglelefteq NU = SL_n(K)$ is a normal subgroup. To see that we have to show $CNU_0 = NU_0C$ for all $C \in SL_n(K) = NU$. We may assume $C \in N$ or $C \in U$. For $C \in U$ that is obvious since both $U_0 \trianglelefteq U$ and $N \trianglelefteq G$ are normal subgroups. For $C \in N$ we find $CN = N = NC$ and $NU_0 = U_0N$, hence $CNU_0 = NU_0 = U_0N = U_0NC$.

Now $Q_{12}(\pm\lambda) \in U_0 \leq NU_0 \trianglelefteq SL_n(K)$ for any $\lambda \in K^*$. Since $Q_{ij}(\lambda)$ is conjugate to $Q_{12}(\lambda)$ or $Q_{12}(-\lambda)$, all the generators $Q_{ij}(\lambda)$ of $SL_n(K)$ are contained in NU_0, hence NU_0 coincides with $SL_n(K)$.

Finally we see that

$$SL_n(K)/N = (NU_0)/N = (U_0N)/N \cong U_0/(U_0 \cap N)$$

is isomorphic to a factor group of the abelian group U_0 and hence itself abelian.

3.) Commutators: For $n \geq 3$, given two distinct indices i, j choose a third index $\ell \neq i, j$. Then

$$Q_{ij}(\lambda) = Q_{i\ell}(-\lambda)Q_{\ell j}(-1)Q_{i\ell}(\lambda)Q_{\ell j}(1)$$

is a commutator because of $Q_{rs}(\mu)^{-1} = Q_{rs}(-\mu)$. For $n = 2$ and $|K| > 3$ choose $\mu \in K \setminus \{0, \pm 1\} \neq \emptyset$. Then with the diagonal matrix

$$D(\mu) := \begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix}$$

we get

$$D(\mu)Q_{12}(\lambda)D(\mu^{-1})Q_{12}(-\lambda) = Q_{12}((\mu^2 - 1)\lambda).$$

Hence because of $\mu^2 - 1 \neq 0$, any elementary matrix is again a commutator. □

Problems 4.58.

1. R: Show that $\mathbb{Z}_{p^n}^*$ is a cyclic group for any prime $p > 2$. Furthermore the residue class of an integer $k \in \mathbb{Z} \setminus \mathbb{Z}p$ generates $\mathbb{Z}_{p^2}^*$ if and only if it generates $\mathbb{Z}_{p^n}^*$ for all $n \in \mathbb{N}_{>0}$. Hint: According to Problem 2.62.7 the subgroup $U(p^n) \subset \mathbb{Z}_{p^n}^*$ is cyclic.

2. R: Let $\mathrm{char}(K) = p > 0$. Assume $a \in E \supset K$ with $b := a^{p^r} \in K, a^{p^{r-1}} \notin K$. Show: $T^{p^r} - b$ is the minimal polynomial p_a of a over K. Hint: Consider first the case $r = 1$ and show then by induction $[K[a] : K] = p^r$.

3. R: Determine all generators of the cyclic group $\mathbb{F}_9^*$ and their minimal polynomials over $\mathbb{F}_3$! Hint: Example 4.4 c).

4. R: Find a concrete realization of the field $\mathbb{F}_{p^p}$, i.e. an isomorphism $\mathbb{F}_{p^p} \cong \mathbb{Z}_p[T]/(f)$, where $f = ...$? Same question for $\mathbb{F}_{16}$, cf. Problems 4.46.1 and 3.46.1.

5. R: Let K be an algebraically closed field. Determine the order $|C_n(K)|$ of the group $C_n(K) \subset K^*$ of n-th roots of unity in K.

6. Show the converse of 4.47: If K is a field and K^* cyclic, then K is finite. Hint: Assume $K^* =< a >$ and $|K| = \infty$. Then K has characteristic $\mathrm{char}(K) = 2$ - why? - and a is transcendent over $\mathbb{F}_2 \cong P(K) \subset K$ resp. $K = Q(\mathbb{F}_2[a]) \cong \mathbb{F}_2(T)$.

7. Let $\mathbb{F}$ be a finite field. Show for $a, b \in \mathbb{F}$: If ab is not a square in $\mathbb{F}$, one of the factors is a square in $\mathbb{F}$ and the other is not. Assume now that p is an odd prime and 6 not a square in $\mathbb{F}_p$. Then $\mathbb{F}_{p^2} = \mathbb{F}_p[\beta]$ with an element $\beta \in \mathbb{F}_{p^2}, \beta^2 = 6$. Show that the number $5 + 2\beta \in \mathbb{F}_{p^2}$ is a square in $\mathbb{F}_{p^2}$.

8. Let $f := T^4 - 10T^2 + 1 \in \mathbb{Z}[T]$. Show that the reduced polynomial $\tilde{f} \in \mathbb{Z}_p[T] = \mathbb{F}_p[T]$ is reducible for all primes p. Hint: The case $p = 2$ is easy. Otherwise write $f = (T^2 - 5)^2 - 24$. If 6 is a square in $\mathbb{F}_p$, we are done. Otherwise $\mathbb{F}_{p^2} = \mathbb{F}_p[\beta]$ with an element $\beta \in \mathbb{F}_{p^2}, \beta^2 = 6$. Then $f = ((T^2 - 5) - 2\beta)((T^2 - 5) + 2\beta)$. Use now the preceding problem 4.58.5 in order to factorize f as product of linear polynomials over $\mathbb{F}_{p^2}$. They can be paired together to quadratic polynomials $\in \mathbb{F}_p[T]$.

9. R: Let $\mathbb{F} := \mathbb{F}_q$ be the finite field with $q = p^r$ element. Show: The ring homomorphism $\mathbb{F}[T] \longrightarrow \mathbb{F}^{\mathbb{F}}, f \mapsto \hat{f}$, cf. Remark 3.16, is surjective with kernel $(T^q - T)$.

10. Compute the orders of the groups $GL_n(\mathbb{F}_q), SL_n(\mathbb{F}_q), PGL_n(\mathbb{F}_q), PSL_n(\mathbb{F}_q)$!

11. Show $PSL_2(\mathbb{F}_2) = PGL_2(\mathbb{F}_2) \cong \mathbb{S}_3$. Hint: $|\mathbb{P}_2(\mathbb{F}_2)| = 3$, Problem 2.18.12.

12. Show $PGL_2(\mathbb{F}_3) \cong \mathbb{S}_4$ and $PSL_2(\mathbb{F}_3) \cong \mathbb{A}_4$. Hint: $|\mathbb{P}_2(\mathbb{F}_3)| = 4$.

4.6 Galois Theory

The fundamental theorem of Galois theory explains the "structure" of a Galois extension $E \supset K$ in terms of its automorphism group (Galois group) $\mathrm{Aut}_K(E)$.

Definition 4.59. *An* **intermediate field** *L of an extension $E \supset K$ is a subfield $L \subset E$ containing K, i.e. $K \subset L \subset E$.*

Theorem 4.60 (Fundamental Theorem of Galois Theory). *Let $E \supset K$ be a Galois extension and let $G := \mathrm{Aut}_K(E)$ be its Galois group. Then there is a bijection*

$$\{L \text{ intermediate fields of the extension } E \supset K\} \longrightarrow \{H \subset G \text{ subgroup}\}$$

between the set of all intermediate fields of the extension $E \supset K$ and the set of all subgroups of $G = \mathrm{Aut}_K(E)$, defined as follows

$$E \supset L \mapsto H := \mathrm{Aut}_L(E) \subset G$$

resp. in the reverse direction:

$$G \supset H \mapsto L := \mathrm{Fix}(H) := \{a \in E; \sigma(a) = a \ , \forall \ \sigma \in H\} \ .$$

It satisfies

$$|\mathrm{Aut}_L(E)| = [E : L] \ , \ |H| = [E : \mathrm{Fix}(H)] \ ,$$

and $H = \mathrm{Aut}_L(E)$ *is a normal subgroup of* $G = \mathrm{Aut}_K(E)$*, iff the extension* $L \supset K$ *is normal. In that case the restriction*

$$G = \mathrm{Aut}_K(E) \longrightarrow \mathrm{Aut}_K(L) \ , \ \sigma \mapsto \sigma|_L \ ,$$

induces an isomorphism

$$G/H \cong \mathrm{Aut}_K(L) \ .$$

Example 4.61. The splitting field of $f := T^3 - 2 \in \mathbb{Q}[T]$ is $E = \mathbb{Q}[\sqrt[3]{2}, \varepsilon]$ with the third root of unity $\varepsilon := \frac{1}{2}(-1+i\sqrt{3})$, cf. Example 4.44.1. We already know the automorphisms $\sigma, \tau \in G := \mathrm{Aut}_{\mathbb{Q}}(E)$ with $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\varepsilon, \sigma(\varepsilon) = \varepsilon, \tau(\sqrt[3]{2}) = \sqrt[3]{2}, \tau(\varepsilon) = \varepsilon^2$. In fact $\mathrm{Aut}_{\mathbb{Q}}(E) \cong \mathbb{S}(N_E(f)) \cong \mathbb{S}_3 \cong D_3$.
The automorphism σ has order 3 and τ order 2 and $\mathrm{id}_E, \sigma, \sigma^2, \tau, \tau \circ \sigma, \tau \circ \sigma^2$ constitute the entire Galois group; they have order 1,3,3,2,2,2.
Let us now determine the non-trivial subgroups: The possible orders being 2 and 3, such a subgroup is cyclic. Hence we find $< \sigma >=< \sigma^2 >, < \tau >$, $< \tau \circ \sigma >, < \tau \circ \sigma^2 >$. If we use that always

$$|H| = [E : \mathrm{Fix}(H)] = 6/[\mathrm{Fix}(H) : \mathbb{Q}]$$

we obtain the following table of subgroups and corresponding fixed fields:

H	$\mathrm{Fix}(H)$
G	$\mathbb{Q}[\sqrt[3]{2}, \varepsilon]$
$< \sigma >$	$\mathbb{Q}[\varepsilon]$
$< \tau >$	$\mathbb{Q}[\sqrt[3]{2}]$
$< \tau \circ \sigma >$	$\mathbb{Q}[\sqrt[3]{2}\varepsilon]$
$< \tau \circ \sigma^2 >$	$\mathbb{Q}[\sqrt[3]{2}\varepsilon^2]$
$< \mathrm{id}_E >$	E

Proof. We have to show that the given maps are inverse one to another, i.e.:

$$\mathrm{Fix}(\mathrm{Aut}_L(E)) = L \ , \ \mathrm{Aut}_{\mathrm{Fix}(H)}(E) = H$$

for every intermediate field L of $E \supset K$ and every subgroup $H \subset G$. Since $E \supset L$ resp. $E \supset \mathrm{Fix}(H)$ are again Galois extensions, we may assume $L = K$ resp. $\mathrm{Fix}(H) = K$ and show then for a Galois extension $E \supset K$ the propositions 4.62 and 4.64.

Proposition 4.62. *For a Galois extension $E \supset K$ we have*

$$\mathrm{Fix}(\mathrm{Aut}_K(E)) = K \ .$$

Proof. The inclusion $K \subset F := \mathrm{Fix}(\mathrm{Aut}_K(E))$ is obvious. On the other side we have $\mathrm{Aut}_F(E) = \mathrm{Aut}_K(E)$ and therefore (see 4.42):

$$[E : F] = |\mathrm{Aut}_F(E)| = |\mathrm{Aut}_K(E)| = [E : K] \ ,$$

whence $F = K$. □

Before we come to the second proposition, we need an auxiliary result telling us when an extension is of the form $K[a] \supset K$:

Theorem 4.63. *(***Primitive Element Theorem)** *A finite field extension $E \supset K$ admits a* **primitive element** *$a \in E$, i.e., such that $E = K[a]$, iff there are only finitely many intermediate fields for the extension $E \supset K$. That condition is satisfied, if $E \supset K$ can be extended to a Galois extension, in particular if $\mathrm{char}(K) = 0$ or more generally, if K is perfect.*

Proof. Since both conditions are satisfied if K (and with K also E) are finite (according to 4.47 we have $E^* =< a >$, whence $E = K[a]$), we may assume that K is infinite.
"$\Longleftarrow$": We do induction on $n := [E : K]$, the case $n = 1$ being trivial.
Let now $n > 1$. Choose an element $b \notin K$. Then $E \supset K[b]$ satisfies $[E : K[b]] < n$ and has as well only finitely many intermediate fields, hence admits according to the induction hypothesis a primitive element $c \in E$, i.e., $E = (K[b])[c] = K[b, c]$. Now we consider the intermediate fields $K[b + \lambda c], \lambda \in K$. Since there are only finitely many intermediate fields and $|K| = \infty$, we find two elements $\lambda_1, \lambda_2 \in K$ with $K[b+\lambda_1 c] = K[b+\lambda_2 c] =: L$. But then we have even $b, c \in L$ resp. $E = K[b, c] \subset L$ resp. $E = L = K[a]$ with $a := b + \lambda_1 c$.
"$\Longrightarrow$": Assume now $E = K[a]$. To every intermediate field L we can associate the minimal polynomial $p_L \in L[T]$ of our primitive element a over L. The map $L \mapsto p_L \in L[T] \subset E[T]$ is injective: If $n = [E : L]$ and $p_L = T^n + \sum_{\nu=0}^{n-1} \lambda_\nu T^\nu$, we have $L = K[\lambda_0, ..., \lambda_{n-1}]$, i.e. we may reconstruct L from p_L. Let $F := K[\lambda_0, ..., \lambda_{n-1}]$. In any case we have $F \subset L$, but on the other hand $[F : K] = [L : K]$ because of

$$n[F : K] = [E : F][F : K] = [E : K] = [E : L][L : K] = n[L : K] \ .$$

Consequently $L = F$.
Now every polynomial p_L is a divisor of the minimal polynomial p_K in the ring $E[T]$. Write then p_K as a product of (finitely many) monic irreducible polynomials $\in E[T]$, cf. 3.33. Any polynomial p_L is then a product of certain of these polynomials (here we use again the unique factorization property 3.33!), and there are of course only finitely many possibilities.
It remains to show that a Galois extension $E \supset K$ satisfies the given condition, but Prop. 4.62 with a subfield L instead of K means that $L \mapsto \mathrm{Aut}_L(E) \subset G$ is injective, and G has of course only finitely many subgroups. □

Proposition 4.64. *Let $E \supset K$ be a Galois extension and $H \subset \mathrm{Aut}_K(E)$ a subgroup with $\mathrm{Fix}(H) = K$. Then we have*

$$H = \mathrm{Aut}_K(E) = \mathrm{Aut}_{\mathrm{Fix}(H)}(E).$$

Proof. Let $G := \mathrm{Aut}_K(E)$. It suffices to show $|G| = [E : K] \leq |H|$. According to 4.63 we may write $E = K[a]$ with a primitive element $a \in E$. We consider the polynomial

$$f := \prod_{b \in Ha} (T - b) \in E[T] \ .$$

Here Ha denotes the H-orbit of $a \in E$, i.e.

$$Ha = \{\sigma(a); \sigma \in H\} \subset E.$$

Every automorphism $\sigma \in H$ induces a permutation $\sigma|_{Ha} \in \mathbb{S}(Ha)$, therefore we obtain $f^\sigma = f$ for all automorphisms $\sigma \in H$, with other words $f \in \mathrm{Fix}(H)[T] = K[T]$ and thus, since the minimal polynomial $p_a \in K[T]$ of a over K is a divisor of f because of $f(a) = 0$, we have
$[E : K] = [K[a] : K] = \deg(p_a) \leq \deg(f) = |H|$. □

We continue the proof of 4.60: The Galois group acts on the set of intermediate field of $[E : K]$ by $(\sigma, L) \mapsto \sigma(L)$, and on the set of subgroups of G by conjugation $(\sigma, H) \mapsto \sigma H \sigma^{-1}$, such that

$$\mathrm{Aut}_{\sigma(L)}(E) = \sigma \mathrm{Aut}_L(E) \sigma^{-1} \ .$$

Hence we can conclude that $H = \mathrm{Aut}_L(E) \subset G$ is a normal subgroup iff $\sigma(L) = L$ for all automorphisms $\sigma \in G$. But that is equivalent to $L \supset K$

being normal: For "$\Longleftarrow$" we may refer to 4.40, while "$\Longrightarrow$" is not difficult either: Again according to 4.40 it is sufficient to show that every irreducible polynomial $g \in K[T]$ with a zero $a \in L$ is split over L. Since $E \supset K$ is normal, that is true over E and we have to show $N_E(g) \subset N_L(g)$. So let $b \in N_E(g)$. From 4.42.i) we know that there is an automorphism $\sigma \in G = \mathrm{Aut}_K(E)$ with $\sigma(a) = b$. Consequently $b \in \sigma(L) = L$.
In particular we see that in this situation the group homomorphism

$$G = \mathrm{Aut}_K(E) \longrightarrow \mathrm{Aut}_K(L)\ ,\ \sigma \mapsto \sigma|_L\ ,$$

is well defined, since $\sigma(L) = L$ for all automorphisms $\sigma \in \mathrm{Aut}_K(E)$. Its kernel is $H := \mathrm{Aut}_L(E)$, and being surjective according to 4.35, it induces an isomorphism $G/H \cong \mathrm{Aut}_K(L)$.

This finishes the proof of Theorem 4.60. □

Problems 4.65.

1. R: Determine all intermediate fields of the extension $\mathbb{Q}[\sqrt[4]{2}, i] \supset \mathbb{Q}$. Which of them are normal? Cf. Problem 4.46.2.

2. Let $\mathrm{char}(F) = p$ and $F[X,Y] := (F[X])[Y]$ be the polynomial ring over F in the variables X, Y and $F(X,Y) := Q(F[X,Y])$. Compute the degree $[E : K]$ of the field extension $E := F(X,Y) \supset K := F(X^p, Y^p)$ and show that there is no primitive element $a \in E$, i.e. such that $E = K[a]$ holds.

3. R: Let $E \supset K$ be a finite field extension and $p := \mathrm{char}(K) > 0$. An element $a \in E$ is called **separable** over K, if $p_a \in K[T]$ has only simple zeros and **purely inseparable** over K, if there is an $r \in \mathbb{N}$ with $a^{p^r} \in K$. We denote $E_s \subset E$ resp. $E_{in} \subset E$ the set of all separable resp. purely inseparable elements. The extension $E \supset K$ is called separable resp. purely inseparable iff $E = E_s$ resp. $E = E_{in}$.

   (a) Show: A finite extension $E \supset K$ is galois, if $|\mathrm{Aut}_K(E)| = [E : K]$. Hint: If the latter is satisfied, we have $E_{in} = K$ (why?) and E can be written $E = K[a]$.

   (b) Show: The sets $E_s, E_{in} \subset E$ äre intermediate fields. (Hint: Assume first that $E \supset K$ is normal and use the fact that $E_{in} = K$ for a Galois extension $E \supset K$). The intermediate field $E_s \supset K$ is also called the separable hull of K in E. Show that $E \supset E_s$ is purely inseparable, and that $E \supset E_{in}$ separable for a normal extension $E \supset K$.

4. Let $E \supset K$ be a Galois extension with Galois group $G := \mathrm{Aut}_K(E)$. Show that the **trace** $\mathrm{Tr} : E \longrightarrow K, \mathrm{Tr}(x) := \sum_{\sigma \in G} \sigma(x)$ and the **norm** $N : E^* \longrightarrow K^*, N(x) := \prod_{\sigma \in G} \sigma(x)$ define homomorphisms between the additive resp. multiplicative groups of E and K. Let $a \in E$ and $n := [E : K], s := [E : K[a]]$. Show that $(p_a)^s = T^n + \mathrm{Tr}(a)T^{n-1} + ... + (-1)^n N(a)$. Indeed $(p_a)^s$ is the characteristic polynomial of the multiplication $\mu_a \in \mathrm{End}_K(E)$.

(a) Let p be a prime and K a field with $\mathrm{char}(K) \neq p$. Show: If $a \notin K^p$, then the polynomial $f = T^p - a \in K[T]$ is irreducible. Hint: We may assume $p > 2$. Let $E \supset K$ be the splitting field of f. It is a Galois extension because of $\mathrm{char}(K) \neq p$. If f would be reducible, then $n := [E : K]$ is not divisible with p. Take $b \in E$ with $b^p = a$. Then $N(b)^p = N(b^p) = N(a) = a^n$. Consequently $a^n \in K^p$ resp. $a \in K^p$ (why?), a contradiction.

(b) Let p be an odd prime and $f_r := T^{p^r} - a \in K[T]$ with a field K of characteristic $\mathrm{char}(K) \neq p$. Show: f_r is irreducible iff $a \notin K^p$. Hint for the non-trivial implication: According to a) the polynomial $f := T^p - a \in K[T]$ is irreducible, hence $[K[b] : K] = p$, where $b^p = a$. If b is not a p-th power in $K[b]$ we may use the induction hypothesis and obtain that $T^{p^{r-1}} - b \in K[b][T]$ is irreducible, resp. that $[K[c] : K[b]] = p^{r-1}$, if $b = c^{p^{r-1}}$. Altogether $[K[c] : K] = p^r$, i.e. $T^{p^r} - a \in K[T]$ is irreducible. Otherwise take $c \in K[b]$ with $c^p = b$ and let $E \supset K[b]$ be the splitting field of f with corresponding norm $N : E^* \longrightarrow K^*$. As in a) we get the Galois extension $E \supset K$, where $s := [E : K[b]]$ is not divisible with p. Then with $n := [E : K]$ we find $(-1)^s a^s = (-1)^n N(b) = (-1)^n N(c^p) = (-1)^n N(c)^p$, and since p is odd and relatively prime to s, that implies $a \in K^p$, a contradiction!

(c) Take now $p = 2$ in b). Show: $f_r := T^{2^r} - a \in K[T]$ is irreducible iff $a \notin K^2, \notin -4K^4$. Hint: Reason as before and exclude the possibility $b = c^2$ with some $c \in K[b]$.

(d) Show that the polynomial $f := T^n - a \in K[T]$, where the exponent n is not divisible with $\mathrm{char}(K)$, is irreducible, iff $a \notin K^p$ for all primes p dividing n, and if $a \notin -4K^4$ in case $4|n$.

5. In the two last problems we investigate Galois extensions $E \supset K$, whose Galois group $\mathrm{Aut}_K(E) =< \sigma >$ is cyclic of prime order and look for a primitive element $a \in E$, i.e. $E = K[a]$, with a minimal polynomial of "standard form". The element $a \in E$ is characterized by the fact that $\sigma(a)$ should be of a special form, either $\sigma(a) = \zeta a$ with a primitive p-th root of unity or $\sigma(a) = a + 1$.

(a) Let $E \supset K$ be a Galois extension, with its degree $[E : K] = p$ being a prime number. Show: If K contains a primitive p-th root of unity $\zeta \in K$ (this implies $\mathrm{char}(K) \neq p$), we can write $E = K[a]$ with an element $a \in E$, such that $b := a^p \in K$, or, with other words, the minimal polynomial $p_a \in K[T]$ of a over K is $p_a = T^p - b$. In that case $E \supset K$ is also called a simple radical extension. Hint: The Galois group is cyclic and generated by any automorphism $\sigma \neq \mathrm{id}_E$. The element $a \in E$ can be found as an eigenvector of the K-linear map $\sigma : E \longrightarrow E$ belonging to the eigenvalue $\zeta \in K$: In fact, it has characteristic polynomial $\chi_\sigma = p_\sigma = f := T^p - 1 \in K[T]$, since $f(\sigma) = 0$ because of $\sigma^p = \mathrm{id}_E$, while $\mathrm{id}_E, \sigma, ..., \sigma^{p-1}$ are linearly independent according to Problem 4.20.5.

(b) Let $E \supset K$ be a Galois extension with cyclic Galois group $\mathrm{Aut}_K(E) =< \sigma >$ and $[E : K] = p = \mathrm{char}(K)$. Show:There is an element $a \in E$ with minimal

polynomial $p_a = T^p - T - c \in K[T]$, cf. problems 4.46.1 and 4.58.2. Hint: Consider $\tau := \sigma - \mathrm{id}_E \in \mathrm{End}_K(E)$ (τ is not an automorphism!). Show: $\tau^p = 0 \neq \tau^{p-1}$ - if already $\tau^{p-1} = 0$ choose integers r, s with $rp + s(p-1) = 1$ and conclude $\tau = 0$. Hence $\dim \ker(\tau) = 1$ resp. $\ker(\tau) = K \subset E$. But τ being nilpotent, we have $\ker(\tau) \cap \tau(E) \neq \{0\}$ resp. $K \subset \tau(E)$. Take now $a \in E$ with $\tau(a) = 1$ resp. $\sigma(a) = a + 1$. Finally $\sigma(a^p - a) = a^p - a$ and thus $c := a^p - a \in K$.

4.7 The Fundamental Theorem of Algebra

As an application of the Fundamental Theorem of Galois Theory 4.60 we show

Theorem 4.66. (Fundamental Theorem of Algebra) *The field $\mathbb{C}$ of all complex numbers is algebraically closed.*

Proof. According to Proposition 4.38 it suffices to prove that there are no non-trivial finite extensions $E \supset \mathbb{C}$. In any case the degree $[E : \mathbb{C}]$ of such an extension is a 2-power: It is a divisor of $[E : \mathbb{R}]$ and there we have:

Proposition 4.67. *The degree of a finite extension $E \supset \mathbb{R}$ is a power of 2, i.e., $[E : \mathbb{R}] = 2^r$ with some $r \in \mathbb{N}$.*

Proof. We may assume that $E \supset \mathbb{R}$ is normal: Otherwise there is an extension $L \supset E$, such that $L \supset \mathbb{R}$ is normal, see 4.36.1. But $[E : \mathbb{R}]$ is a divisor of $[L : \mathbb{R}]$ by 4.12. So let us consider a normal extension $E \supset \mathbb{R}$. It is then automatically galois, and we choose a 2-Sylow subgroup $H \subset G := \mathrm{Aut}_{\mathbb{R}}(E)$. Now it suffices to show: $F := \mathrm{Fix}(H) = \mathbb{R}$, since that implies according to 4.60 $H = G$ and $[E : \mathbb{R}] = |G| = |H| = 2^r$ with some $r \in \mathbb{N}$.
Because of $[E : F] = |H|$ and $|G| = [E : \mathbb{R}] = [E : F][F : \mathbb{R}]$, the extension degree $[F : \mathbb{R}]$ is odd; in particular every element $a \in F$ has a minimal polynomial $p_a \in \mathbb{R}[T]$ of odd degree, but on the other hand every polynomial $\in \mathbb{R}[T]$ of odd degree has a real zero.
Thus the irreducible polynomial p_a has degree 1 and $a \in \mathbb{R}$. So we have seen $F \subset \mathbb{R}$ resp. $F = \mathbb{R}$ and are done. □

Let us now go on with the proof of 4.66: The extension $E \supset \mathbb{C}$ has degree $[E : \mathbb{C}] = 2^s$ with some $s \in \mathbb{N}$. We show that for $s \geq 1$ there is a subgroup $H \subset G := \mathrm{Aut}_{\mathbb{C}}(E)$ of index $(G : H) = 2$. Taking that for granted, $\mathrm{Fix}(H) \supset \mathbb{C}$ is an extension of degree 2 and thus $\mathrm{Fix}(H) = \mathbb{C}[a]$ with some element a whose

minimal polynomial $p_a \in \mathbb{C}[T]$ has degree 2. But every quadratic polynomial $\in \mathbb{C}[T]$ has a zero in $\mathbb{C}$, in particular it is reducible. Contradiction!
Existence of the subgroup $H \subset G$: We show that every p-group G has a subgroup H of index $(G : H) = p$. If $|G| = p$, take $H := \{e\}$. Let $\varrho : G \longrightarrow G/Z(G)$ be the quotient projection. According to 2.32 we have $|G/Z(G)| < |G|$, and now may assume, that we already have found a subgroup $H_0 \subset G/Z(G)$ of index p. Finally take $H := \varrho^{-1}(H_0)$. □

Problems 4.68. 1. Show: If K has characteristic $\mathrm{char}(K) = 0$ and $E \supset K$ is a finite extension with an algebraically closed field E, then either $E = K$ or $E = K[i]$ with an element $i \in E$, $i^2 = -1$. Hint: Since $i \in E$, we may replace K with $K[i]$ resp. assume $i \in K$ and have to show $E = K$. In any case $E \supset K$ is galois. Take a prime number p dividing $[E : K] = |\mathrm{Aut}_K(E)|$ and an automorphism $\sigma \in \mathrm{Aut}_K(E)$ of order p and let $F \subset E$ be its fixed field. We then have $[E : F] = p$ and all non-linear irreducible polynomials $\in F[T]$ have degree p. In particular the p-th roots of unity belong to F - their minimal polynomial being of degree $< p$, while all element $\in F \setminus E$ have a minimal polynomial of degree p. According to Problem 4.65.5 c) we may write $E = F[a]$, where $b := a^p \in F$. In particular $b \notin F^p$ and, for $p = 2$, nor $b \in -4F^4$ - otherwise a would be a square in F because of $i \in F$. So the polynomial $T^{p^2} - b \in F[T]$ is irreducible according to Problem 4.65.4 c). Contradiction!

4.8 Cyclotomic Extensions

The finite field $\mathbb{F}_{p^n}$ is the splitting field of the polynomial $T^{p^n-1} - 1 \in \mathbb{F}_p[T]$ and has cyclic Galois group. In this section we investigate the splitting field $E_n \supset \mathbb{Q}$ of $f = T^n - 1 \in \mathbb{Q}[T]$. Indeed, $E_n = \mathbb{Q}[\zeta_n]$ with $\zeta_n := e^{\frac{2\pi i}{n}}$, it is called the **$n$-th cyclotomic field**, since the n-th roots of unity $1, \zeta_n, ..., \zeta_n^{n-1}$ divide the unit circle into n sectors of the same size. ($\kappa\upsilon\kappa\lambda o\varsigma$ = circle, $\tau\varepsilon\mu\nu\varepsilon\iota\nu$ = to cut).
We determine first the minimal polynomial $p_{\zeta_n} \in \mathbb{Q}[T]$ of ζ_n. Recall that $\zeta_n^k, k \in \mathbb{Z}$, only depends on the residue class $\bar{k} \in \mathbb{Z}_n$ of k modulo n.

Definition 4.69. *The n-th* **cyclotomic polynomial** $f_n \in \mathbb{C}[T]$ *is the polynomial*

$$f_n := \prod_{\bar{k} \in \mathbb{Z}_n^*} (T - \zeta_n^k) \ , n \geq 2,$$

while $f_1 := T - 1$.

Remark 4.70. 1. We have $\deg(f_n) = \varphi(n)$ with Euler's φ-function, cf. Example 3.8.5.

2. Let $\mathbf{S}^1 := \{z \in \mathbb{C}; |z| = 1\}$ be the unit circle. Then

$$f_n = \prod_{a \in \mathbf{S}^1, \mathrm{ord}(a)=n} (T - a)$$

and thus:

$$T^n - 1 = \prod_{a \in C_n} (T - a) = \prod_{d|n} \big(\prod_{a \in \mathbf{S}^1, \mathrm{ord}(a)=d} (T - a) \big) = \prod_{d|n} f_d \ .$$

Using that formula we can compute the cyclotomic polynomials inductively, cf. Problem 3.46.4. For example for a prime p we obtain $T^p - 1 = (T - 1)f_p$, and the division algorithm for polynomials yields

$$f_p = T^{p-1} + T^{p-2} + ... + T + 1 \ ,$$

while $T^4 - 1 = f_1 f_2 f_4 = (T - 1)(T + 1)f_4$, whence $f_4 = T^2 + 1$ (of course $f_4 = (T - i)(T + i)$ as well), and

$$T^6 - 1 = f_1 f_2 f_3 f_6 = (T - 1)(T + 1)(T^2 + T + 1)f_6$$

leads to $f_6 = T^2 - T + 1$. Eventually $T^8 - 1 = (T - 1)(T + 1)(T^2 + 1)f_8$, such that $f_8 = T^4 + 1$ etc..

In any case we see that the cyclotomic polynomials have integral coefficients:

$$f_n \in \mathbb{Z}[T] \ .$$

The n-th root of unity ζ_n being a zero of f_n, its minimal polynomial p_{ζ_n} is a divisor of f_n. In fact

Proposition 4.71. *The n-th cyclotomic polynomial $f_n \in \mathbb{Z}[T]$ is irreducible. In particular, it agrees with the minimal polynomial $p_{\zeta_n} \in \mathbb{Q}[T]$ of $\zeta_n = e^{2\pi i/n}$, i.e.*

$$p_{\zeta_n} = f_n \ .$$

Proof. Denote $f := p_{\zeta_n} \in \mathbb{Q}[T]$ the minimal polynomial of ζ_n over $\mathbb{Q}$. Since $f | f_n$ and f_n only has simple zeros, it is sufficient to show that $f := p_{\zeta_n} \in \mathbb{Q}[T]$ and f_n have the same zeros, i.e., we have to see that $f(\zeta_n^k) = 0$ for all $k \in \mathbb{N}$ relatively prime to n.

Writing a given k as a product of primes, we see that we are done if for all $a \in C_n$ and primes p not dividing n, we can prove the implication:

$$f(a) = 0 \Longrightarrow f(a^p) = 0 \ . \tag{3}$$

The polynomial f is a divisor of $T^n - 1$, say $T^n - 1 = fh$. Gauß' lemma 3.40 tells us $1 = \mathrm{cont}(f)\mathrm{cont}(h)$, but with f also h is a monic polynomial, and the content of a monic polynomial is a number of the form $1/m, m \in \mathbb{N}_{>0}$. Hence necessarily $\mathrm{cont}(f) = \mathrm{cont}(h) = 1$, in particular $f, h \in \mathbb{Z}[T]$.

So let us fix a prime p with $p \not| n$. Assume $f(a) = 0$ and $f(a^p) \neq 0$. Since $a \in C_n$, we see $0 = (a^n)^p - 1 = (a^p)^n - 1 = f(a^p)h(a^p)$. Thus, if not $f(a^p) = 0$, we must have $h(a^p) = 0$. That can also be formulated in a more sophisticated way, by saying: The polynomial $h(T^p)$ has a as a zero. But then f, being the minimal polynomial of a, divides $h(T^p)$ in $\mathbb{Q}[T]$ resp. $\mathbb{Z}[T]$. For the modulo p reduced polynomials $\tilde{f}, \tilde{h}(T^p) = \tilde{h}^p \in \mathbb{Z}_p[T]$ we have the same divisibility relation $\tilde{f}|\tilde{h}(T^p) = \tilde{h}^p$. But that implies that every zero $b \in N_{\mathbb{F}}(\tilde{f})$ of $\tilde{f} \in \mathbb{Z}_p[T]$ in some extension $\mathbb{F} \supset \mathbb{Z}_p$ is also a zero of $\tilde{h}^p$ resp. of $\tilde{h}$ itself. We choose $\mathbb{F}$ as splitting field of the polynomial $g := T^n - 1 = \tilde{f}\tilde{h} \in \mathbb{Z}_p[T]$. In $\mathbb{F}$ there is of course such a zero b, which then is at least a double zero of g. But since $g' = nT^{n-1}$ and $p \not| n$, we have $g'(b) \neq 0$. Contradiction. □

Let us now determine the Galois group of $\mathbb{Q}[\zeta_n] \supset \mathbb{Q}$:

Theorem 4.72. *For the cyclotomic extension $\mathbb{Q}[\zeta_n] \supset \mathbb{Q}$ we have*

1. *Its degree satisfies $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \varphi(n)$ with Eulers' φ-function $\varphi : \mathbb{N}_{>0} \longrightarrow \mathbb{N}$.*

2. *Let $C_n \subset \mathbb{Q}[\zeta_n]$ denote the group of all n-th roots of unity. Then the restriction map*

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n]) \longrightarrow \mathrm{Aut}(C_n), \sigma \mapsto \sigma|_{C_n}$$

is an isomorphism. Here $\mathrm{Aut}(C_n) \cong \mathbb{Z}_n^*$ is the automorphism group of the group C_n. So altogether

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n]) \cong \mathbb{Z}_n^*.$$

Proof. The degree equality is an immediate consequence of 4.71, while the restriction map in the second part is injective, an automorphism σ being determined by its value $\sigma(\zeta_n)$, and surjective, since the Galois group acts transitively on the roots of the irreducible polynomial f_n. Finally remember the isomorphism

$$\mathbb{Z}_n^* \xrightarrow{\cong} \mathrm{Aut}(C_n), \overline{k} \mapsto p_k$$

with the k-th power map $p_k : C_n \longrightarrow C_n, a \mapsto a^k$. □

Remark 4.73. Since the automorphism group of a cyclotomic extension is abelian, every intermediate field L of $\mathbb{Q}[\zeta_n] \supset \mathbb{Q}$ provides a Galois extension $L \supset \mathbb{Q}$ with abelian Galois group. A deep result of Leopold Kronecker (1823-1891) assures that (up to isomorphy) every Galois extension $E \supset \mathbb{Q}$ with abelian Galois group $\mathrm{Aut}_{\mathbb{Q}}(E)$ is obtained in that way. We only discuss an example:

Example 4.74. We consider the real part of the n-th cyclotomic field:

$$L_n := \mathbb{Q}[\zeta_n] \cap \mathbb{R} = \mathrm{Fix}(\tau) = \mathbb{Q}[a]$$

with the complex conjugation $\tau : z \mapsto \overline{z}$ and $a := \zeta_n + \overline{\zeta}_n = 2\cos(\frac{2\pi}{n})$. (Note that $\tau|_{C_n} = p_{-1}$.)

We find $[\mathbb{Q}[\zeta_n] : L_n] = 2$, since ζ_n is a root of the quadratic polynomial $T^2 - aT + 1 \in L_n[T]$, and thus $[L_n : \mathbb{Q}] = \varphi(n)/2$ for $n > 2$. Obviously $L_n \supset \mathbb{Q}[a]$, while equality follows from the fact, that even $T^2 - aT + 1 \in (\mathbb{Q}[a])[T]$. The case $n = 9$ has already been discussed, see Example 4.19.2).

Problems 4.75.

1. Let $E \supset \mathbb{Q}$ be the splitting field of the polynomial $T^n - a$, where $a \in \mathbb{Q}^*$. Show that $\mathbb{Q}[\zeta_n] \subset E$ and $\mathrm{Aut}(E) := \mathrm{Aut}_{\mathbb{Q}}(E)$ is isomorphic to a subgroup of the semidirect product $C_n \times_\sigma \mathbb{Z}_n^*$ with the homomorphism $\sigma : \mathbb{Z}_n^* \longrightarrow \mathrm{Aut}(C_n), \overline{k} \mapsto p_k$. Let now $n = p$ be a prime number and $a \in \mathbb{Z}$ not a p-th power. Show that in this case $\mathrm{Aut}(E) \cong C_n \times_\sigma \mathbb{Z}_n^*$. Hint: The polynomial $T^p - a$ is irreducible over $\mathbb{Q}$, cf. Problem 4.65.4. Conclude that p divides $[E : \mathbb{Q}] = \varphi(n)k$ and thus $p|k$ because of $\gcd(p, \varphi(p)) = 1$ resp. even $p = k$.

2. Show that, with the notation of the previous problem: $C_n \times_\sigma \mathbb{Z}_n^* \cong \mathrm{Aff}(\mathbb{Z}_n)$, cf. Problem 3.9.8.

4.9 Solvability by Radicals

In the final section we explain how Galois theory leads to a solution of our problem to decide when a polynomial equation over a field K of characteristic $\mathrm{char}(K) = 0$ can be "solved by radicals". First of all we have to make precise that notion. We begin with

Definition 4.76. *An extension $E \supset K$ is called a* **simple radical extension***, if it can be written $E = K[a]$ with a primitive element $a \in E$, such that $a^m \in K$ for some exponent $m > 0$.*

Remark 4.77. Given a simple radical extension, the polynomial $T^m - b \in K[T]$ with $b = a^m$ is not necessarily the minimal polynomial $p_a \in K[T]$ of a over K (even if $m > 0$ is minimal with $a^m \in K$). But in any case p_a is of course a divisor of $T^m - b$.

Example 4.78. Let $\zeta_m \in \mathbb{C}$ be the m-th root of unity $\zeta_m := \exp(\frac{2\pi i}{m})$. Then $\mathbb{Q}[\zeta_m] \supset \mathbb{Q}$ is a simple radical extension. Another example is $\mathbb{Q}[\sqrt[3]{2}] \supset \mathbb{Q}$.

Let us now discuss the automorphism group $\mathrm{Aut}_K(E)$ for a simple radical extension $E = K[a] \supset K$ with $b = a^m \in K$.

Proposition 4.79. *The automorphism group $\mathrm{Aut}_K(E)$ of a simple radical extension $E = K[a] \supset K$ (with, say, $a^m \in K$) is solvable.*

Proof. Consider the group $C_m(E) \subset E^*$ of m-th roots of unity in E, a cyclic group (cf. Prop. 4.47) whose order $\ell := |C_m(E)|$ divides m (with $\ell = m$ for $\mathrm{char}(K) = 0$) and the intermediate field $L = K[C_m(E)]$, obtained from K by adjoining the elements in $C_m(E)$, the splitting field of the polynomial $T^m - 1$. Then the normal series

$$\{\mathrm{id}_E\} \trianglelefteq \mathrm{Aut}_L(E) \trianglelefteq \mathrm{Aut}_K(E)$$

has abelian factors: The automorphism group $\mathrm{Aut}_L(E)$ is isomorphic to a subgroup of $C_m(E)$, the group homomorphism

$$\mathrm{Aut}_L(E) \longrightarrow C_m(E), \sigma \mapsto \sigma(a)a^{-1}$$

being injective. On the other hand

$$\mathrm{Aut}_K(E)/\mathrm{Aut}_L(E) \cong \mathrm{Aut}_K(L) \hookrightarrow \mathrm{Aut}(C_m(E)), \sigma \mapsto \sigma|_{C_m(E)},$$

with the abelian group $\mathrm{Aut}(C_m(E)) \cong \mathbb{Z}_\ell^*$, where a residue class $\overline{k}$ corresponds to the k-th power map $p_k : C_m(E) \longrightarrow C_m(E), a \mapsto a^k$. □

Definition 4.80. *An extension $E \supset K$ is called a* **radical extension**, *if it is the composite of finitely many simple radical extensions $E_i \supset E_{i-1}, i = 1, ..., r$, (often also called a "tower"):*

$$K = E_0 \subset E_1 \subset ... \subset E_r = E \ .$$

Eventually we can define "solvability by radicals":

Definition 4.81. *Let $f \in K[T]$ be an irreducible polynomial. We say that the equation $f(x) = 0$ is solvable with radicals, if there is a radical extension $L \supset K$, such that f has a zero in L.*

Example 4.82. As we shall see later on the radical extension $L \supset K$ can always be taken as an extension $L \supset E$ of the splitting field $E \supset K$ of $f \in K[T]$, but it may happen that we can not actually choose $L = E$. For example consider $f = T^3 - 3T + 1 \in \mathbb{Q}[T]$. Its splitting field is $E := \mathbb{Q}[a]$ with $a := \zeta_9 + \zeta_9^{-1} = 2\cos(\frac{2\pi}{9})$ and we choose $L := \mathbb{Q}[\zeta_9] \supset E$; so the equation $f(x) = 0$ is solvable with radicals. Now the extension $E \supset \mathbb{Q}$ has degree $[E : \mathbb{Q}] = 3$ and hence no proper intermediate fields, and it is itself not a simple radical extension: We have $E \subset \mathbb{R}$ and thus $|C_m(E)| \leq 2$ and $\mathrm{Aut}(C_m(E)) = \{\mathrm{id}\}$; so, if $E \supset \mathbb{Q}$ would be a simple radical extension, its automorphism group had at most two elements. But we have already seen that it is cyclic of order 3.

Here is the central result characterizing polynomials solvable by radicals:

Theorem 4.83. *Let* $\mathrm{char}(K) = 0$ *and $f \in K[T]$ be an irreducible polynomial. Then the equation $f(x) = 0$ is solvable with radicals, iff its Galois group, i.e. the automorphism group* $\mathrm{Aut}_K(E)$ *of its splitting field $E \supset K$, is solvable.*

Proof. "$\Longleftarrow$": Let $n := [E : K]$ and $L \supset E$ be the splitting field of the polynomial $T^{n!} - 1 \in E[T]$. Then $L \supset K$ is the splitting field of $(T^{n!} - 1)f \in K[T]$ and thus a Galois extension because of $\mathrm{char}(K) = 0$. Furthermore its Galois group $\mathrm{Aut}_K(L)$ is solvable, since both, $\mathrm{Aut}_E(L) \subset \mathrm{Aut}_K(L)$ and $\mathrm{Aut}_K(L)/\mathrm{Aut}_E(L) \cong \mathrm{Aut}_K(E)$ are solvable: The extension $L \supset E$ is a simple radical extension: $L = E[\zeta]$ with a primitive $n!$-th root of unity ζ, and $\mathrm{Aut}_K(E)$ is solvable by assumption. We take now $L_0 := K, L_1 := K[\zeta]$. The Galois group $\mathrm{Aut}_{L_1}(L) \subset \mathrm{Aut}_K(L)$ is also solvable. We have now

$[L : L_1] \leq [E : K]$, since we may write $E = K[a]$ with some primitive element $a \in E$. Then $L = L_1[a]$, and the minimal polynomial $p_a \in K[T]$ of a over K is divisible with the minimal polynomial $q_a \in L_1[T]$ of a over L_1. And $[E : K] = \deg(p_a)$ as well as $[L : L_1] = \deg(q_a)$.

It remains to show that $L \supset L_1$ is a radical extension. In order to simplify notation we replace L_1 with K and L with E, where we may assume that $C_n(K)$ with $n := [E : K]$ has order n, i.e. all n-th roots of unity lie already in the base field K. Take now a normal series

$$G_0 = G := \mathrm{Aut}_K(E) \trianglerighteq G_1 \trianglerighteq ... \trianglerighteq G_r := \mathrm{Aut}_E(E) = \{\mathrm{id}_E\}$$

with cyclic factors G_i/G_{i+1} of prime order and consider the corresponding tower of intermediate fields

$$K = L_0 \subset L_1 \subset .... \subset L_r = E \ .$$

Then $L_{i+1} \supset L_i$ is a Galois extension with cyclic Galois group $\mathrm{Aut}_{L_i}(L_{i+1}) \cong G_i/G_{i+1}$ of prime order. The extension degree $p := [L_{i+1} : L_i]$ divides $n = [E : K]$ and hence $C_p(L_i) \subset C_n(L_i) = C_n(K)$ has order p, i.e., all p-th roots of unity belong to L_i. Problem 4.65.5 a) with $K = L_i$ and $E = L_{i+1}$ gives us, that we really have a simple radical extension.

"$\Longrightarrow$": We take a radical extension $L \supset K$, such that f has a zero in L and construct an extension $F \supset L$, such that $F \supset K$ is a Galois extension with solvable Galois group $\mathrm{Aut}_K(F)$. This yields the result, since the splitting field $E \supset K$ of f then is isomorphic to an intermediate field of $F \supset K$. Take a tower

$$L_0 := K \subset L_1 \subset ... \subset L_r = L$$

of simple radical extensions $L_{i+1} \supset L_i$, say $L_i = L_{i-1}[a_i]$, where $b_i := a_i^{m_i} \in L_{i-1}$. Let $m := m_1 \cdot ... \cdot m_r$. Then we take $F \supset K$ as splitting field of $(T^m - 1)g \in K[T]$, where $g = p_a$ is the minimal polynomial over K of some primitive element $a \in L$ for the field extension $L \supset K$, i.e., $L = K[a]$. Hence we may regard L as intermediate field of the extension $F \supset K$. On the other hand

$$F = K[\zeta, \sigma(a); \sigma \in \mathrm{Aut}_K(F)] = K[\zeta, \sigma(a_i); i = 1, ..., r, \sigma \in \mathrm{Aut}_K(F)]$$

with a primitive m-th root of unity $\zeta \in F$. Let

$$\mathrm{Aut}_K(F) = \{\sigma_1 := \mathrm{id}_F, \sigma_2, ..., \sigma_n\} \ .$$

Now consider the tower

$$F_0 := K \subset F_1 := K[\zeta] \subset F_2 := F_1[a_2] \subset ... \subset F_{1+nr}$$

with

$$F_{1+(j-1)r+i} := K[\zeta, a_1, ..., a_r, \sigma_2(a_1), ..., \sigma_{j-1}(a_r), \sigma_j(a_1), ..., \sigma_j(a_i)] \ ,$$

where $j = 1, ..., n$ and $i = 1, ..., r$. Then it is sufficient to show that $F_\ell \supset F_{\ell-1}$ is a Galois extension with abelian Galois group: That extension is the splitting field of $T^m - 1 \in F_0[T] = K[T]$ for $\ell = 1$ and of $T^{m_i} - \sigma_j(b_i) \in F_{\ell-1}[T]$ for $\ell = 1 + (j-1)r + i$, since $F_{\ell-1}$ contains all m_i-th roots of unity. As above we see that $\mathrm{Aut}_{F_{\ell-1}}(F_\ell) \subset C_{m_i}(F_{\ell-1})$ is cyclic. □

5 Annex: Zorns Lemma

If in algebra infinite or even uncountable sets are involved, it can be useful to know about the existence of certain objects even if there is no constructive method to create them: A generally accepted tool in this context is "Zorns lemma", which we shall discuss in this annex.

Definition 5.1. *A* **partial order** *on a set M is a relation "$\preceq$", which is reflexive, antisymmetric and transitive, i.e.*

1. $\forall\ x \in M :\ x \preceq x$,
2. $\forall\ x, y \in M :\ x \preceq y \wedge y \preceq x \Longrightarrow x = y$ *and*
3. $\forall\ x, y, z \in M : x \preceq y \wedge y \preceq z \Longrightarrow x \preceq z$.

Such a relation is sometimes simply called an order (relation) on M. A **total** *or* **linear** *order is a partial order, where any two elements $x, y \in M$ are related:*

$$\forall\ x, y \in M :\ x \preceq y \vee y \preceq x \ .$$

A **well ordering** *on M is a linear order, such that every non-empty subset $M_0 \subset M$ has a first element (with respect to $\preceq$), i.e.,*

$$\forall\ M_0 \subset M\ \exists\ a \in M_0 : \forall\ x \in M_0\ :\ a \preceq x \ .$$

An element $a \in M$ is called **maximal** *(w.r.t. the order $\preceq$), iff*

$$\forall\ x \in M :\ a \preceq x \Longrightarrow a = x,$$

i.e., there are no elements bigger than a.

Example 5.2. In many applications the set M is realized as a subset $M \subset \mathcal{P}(U)$ of the power set of some set U (the "universe") with the inclusion as order relation

$$A \preceq B \Longleftrightarrow A \subset B.$$

Remark 5.3. 1. If $x \preceq a$ for all $x \in M$, the element a is obviously maximal, but in general that need not hold for a maximal element: It is allowed for a maximal element $a \in M$, that there are elements in M not related to a.

2. The set $\mathbb{N} = \{0, 1, 2, ...\}$ of all natural numbers, endowed with the natural order, is well ordered, but $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$ are not. The set $\mathbb{N}^2$, endowed with the **lexicographic order**

$$(x, y) \preceq (x', y') \Longleftrightarrow x < x' \vee (x = x' \text{ and } y \leq y') \ .$$

is well ordered. A subset of a well ordered set has by definition a unique first element, but in general no last element, and every element has an immediate successor - the first element of the set of all elements after the given one, but not necessarily an immediate predecessor. An **initial segment** M_0 of a linearly ordered set M is a subset $M_0 \subset M$ satisfying $M \ni y \preceq x \in M_0 \Longrightarrow y \in M_0$, i.e., with an element $x \in M_0$ all elements $y \preceq x$ before x belong to M_0. If M is well ordered, such an initial segment satisfies either $M_0 = M$ or $M_0 = M_{\prec a} := \{x \in M; x \prec a\}$. Namely, given an initial segment $M_0 \neq M$, choose a as the first element in the complement $M \setminus M_0$.

Theorem 5.4. (Zorns lemma) *(Max August Zorn, 1906-1993): Let M be a set with the partial order $\preceq$. If for every (w.r.t. $\preceq$) linearly ordered subset $T \subset M$ there is an upper bound $b \in M$, i.e. such that $t \preceq b$ for all $t \in T$ (written briefly as $T \preceq b$), then there are maximal elements in M.*

Example 5.5. If $M \subset \mathcal{P}(U)$ as in Example 5.2, the upper bound B of a linearly ordered subset $T \subset M \subset \mathcal{P}(U)$ usually is taken as the union $B := \bigcup_{A \in T} A$ of all sets $A \in T$, and it remains to check that in fact $B \in M$.

Before we prove Zorns lemma we present the most important applications. The first one is basic for Linear Algebra:

Theorem 5.6. *Every K-vector space V has a basis.*

Proof. Take $M \subset \mathcal{P}(V)$ as the set of all linearly independent subsets of V. We can apply Zorns lemma as in Example 5.5. So there is a maximal linearly independent set $B \in M$, indeed B is a basis: We have to show that any vector $v \in V$ is a finite linear combination of vectors in B. So let $v \in V$. If $v \in B$, we are done, otherwise $B \cup \{v\} \notin M$ – the set $B \in M$ being maximal in M – and hence there is a non-trivial relation

$$0 = \lambda v + \lambda_1 v_1 + ... + \lambda_r v_r$$

with $v_1, ..., v_r \in B$ and $\lambda, \lambda_1, ..., \lambda_r \in K$. But $\lambda \neq 0$, since the vectors $v_1, ..., v_r$ are linearly independent, i.e., we may solve for $v \in V$. □

Theorem 5.7. *Every proper ideal $\mathfrak{a} \subset R$ in a (commutative) ring (with 1) is contained in a maximal ideal $\mathfrak{m} \subset R$.*

Proof. Take $M \subset \mathcal{P}(R)$ as the subset of all proper ideals in R containing $\mathfrak{a}$. Since an ideal $\mathfrak{a}$ is proper iff $1 \notin \mathfrak{a}$, it is obvious that the union of a linearly ordered set of proper ideals again is a proper ideal. □

As a corollary of Theorem 5.7 we obtain:

Theorem 5.8. *Every field K has an algebraic closure $E \supset K$, and any two algebraic closures are isomorphic as K-extensions.*

Proof. **Existence**: First we make the field K perfect, if $\mathrm{char}(K) = p > 0$: The pair $(E := K, \sigma)$ with the Frobenius homomorphism $\sigma : K \longrightarrow E = K$ defines a field extension $\sqrt[p]{K} \supset K$, where every element $x \in K$ has a p-th root. We may iterate that procedure and obtain after n steps the field $\sqrt[p^n]{K} \supset K$. Since for $m \geq n$ there is a unique (injective) morphism $\sqrt[p^n]{K} \hookrightarrow \sqrt[p^m]{K}$ of K-extensions, we may treat it is an inclusion and define

$$K_\infty := \bigcup_{n=0}^{\infty} \sqrt[p^n]{K} \ ,$$

which obviously is a perfect field.

A more explicit construction of K_∞ is as follows:

$$K_\infty := \left(\bigcup_{n=0}^{\infty} K \times \{n\} \right) / \sim \ ,$$

where for $m \geq n$, we have $(x,n) \sim (y,m)$ iff $y = \sigma^{m-n}(x)$, and $K \hookrightarrow K_\infty$ is given by $x \mapsto [(x,0)]$:=the equivalence class of $(x,0)$. We leave it to the reader to define the addition and multiplication of equivalence classes. Thus it remains to find an algebraic closure of K_∞.

So, from now on we may assume that K is perfect. Then we construct a field $E \supset K$, such that every irreducible polynomial $f \in K[T]$ has a zero in E and use

Proposition 5.9. *Let $E \supset K$ be an algebraic extension of the perfect field K, such that every irreducible polynomial $f \in K[T]$ has a zero in E. Then $E \supset K$ is an algebraic closure of K.*

Proof. We have to show that every irreducible polynomial $f \in K[T]$ is split over E. Consider a splitting field $L \supset K$ of f. Since K is perfect, we can write $L = K[a]$ according to the Primitive Element Theorem 4.63. But the minimal polynomial $p_a \in K[T]$ is irreducible and thus has a zero $b \in E$. Therefore f is split over $E \supset K[b] \cong L$. □

The extension $E \supset K$ satisfying the assumptions of Proposition 5.9 is obtained as follows: Index the irreducible monic polynomials $\in K[T]$ as $f_\alpha, \alpha \in A$, with some index set A, and consider the polynomial ring $K[T_A]$ of all polynomials in the variables $T_\alpha, \alpha \in A$, every individual polynomial depending only on finitely many variables. To be more precise: The polynomial ring $K[T_1, ..., T_n]$ may be defined inductively:

$$K[T_1, ..., T_{n+1}] := (K[T_1, ..., T_n])[T_{n+1}].$$

Now for a finite subset $A_0 \subset A$, say $A_0 = \{\alpha_1, ..., \alpha_n\}$, we set

$$K[T_{A_0}] := K[T_{\alpha_1}, ..., T_{\alpha_n}] \ ,$$

and finally

$$K[T_A] := \bigcup_{A_0 \subset A,\ |A_0| < \infty} K[T_{A_0}] \ .$$

Now let

$$g_\alpha := f_\alpha(T_\alpha) \in K[T_\alpha] \subset K[T_A],$$

i.e. every polynomial f_α gets its own variable T_α! Let now $\mathfrak{a} \subset K[T_A]$ be the ideal generated by the g_α, i.e.,

$$\mathfrak{a} = \left\{ \sum_{i=1}^{r} h_{\alpha_i} g_{\alpha_i}; h_{\alpha_i} \in K[T_A], r \in \mathbb{N}, \alpha_1, ..., \alpha_r \in A \right\} \ .$$

Indeed $\mathfrak{a}$ is a proper ideal: Otherwise we can write

$$1 = \sum_{i=1}^{n} h_{\alpha_i} g_{\alpha_i} \ .$$

Now take a finite set $A_0 \subset A$ with $h_{\alpha_i}, g_{\alpha_i} \in K[T_{A_0}]$ for $i = 1, ..., n$. In order to simplify notation write h_i, g_i instead of $h_{\alpha_i}, g_{\alpha_i}$ and $A_0 = \{1, ..., m\}$ with some $m \geq n$. So we have the equality

$$1 = \sum_{i=1}^{n} h_i g_i$$

in the ring $K[T_1, ..., T_m]$. Now consider a splitting field $F \supset K$ of $f := f_1 \cdot ... \cdot f_n$ and substitute $x = (x_1, ..., x_n, 0, ..., 0) \in F^m$, where $x_i \in F$ is a zero of f_i: Since $g_i(x) = f_i(x_i) = 0$ for $i = 1, ..., n$, we obtain that $1 = 0$ holds in F. Contradiction!

Eventually Theorem 5.7 provides a maximal ideal $\mathfrak{m} \supset \mathfrak{a}$, and we may set $E := K[T_A]/\mathfrak{m}$. Obviously $K \longrightarrow K[T_A]/\mathfrak{m}$ is a field extension, where $f_\alpha \in K[T]$ has the zero $x_\alpha := T_\alpha + \mathfrak{m}$. In particular $E \supset K$ is algebraic.
Uniqueness: Let $E \supset K$ and $F \supset K$ be two algebraic closures. Consider the set M of all pairs (L, σ), where L is an intermediate field of $E \supset K$ and $\sigma : L \longrightarrow F$ a morphism of K-extensions; furthermore we define

$$(L, \sigma) \preceq (L', \sigma') \Longleftrightarrow L \subset L' \ \text{ and } \sigma = \sigma'|_L \ .$$

Let now $\{(L_i, \sigma_i), i \in I\}$ be a linearly ordered subset. The upper bound we are looking for can be taken as (L_∞, σ), where

$$L_\infty := \bigcup_{i \in I} L_i \ , \ \sigma|_{L_i} := \sigma_i \ .$$

According to Zorns lemma there is a maximal element (L, σ) and it remains to show $L = E$ and $\sigma(E) = F$. If $L \neq E$, take an element $a \in E \setminus L$, denote $p_a \in L[T]$ its minimal polynomial over L. Since F is algebraically closed, the polynomial $p_a^\sigma \in \sigma(L)[T]$ has a zero $b \in F$. Then we have $(L[a], \hat{\sigma}) \succ (L, \sigma)$, if $\hat{\sigma}|_L = \sigma, \hat{\sigma}(a) = b$. So necessarily $L = E$. But E being algebraically closed, $\sigma(E)$ is algebraically closed as well, in particular $\sigma(E)$ has no non-trivial finite or algebraic extensions, i.e. $F = \sigma(E)$. $\square$

Proof of Th.5.4. We assume that there is no maximal element in M, but that every linearly ordered subset $T \subset M$ has an upper bound $\gamma(T) \in M$. So there is a function

$$\gamma : \mathrm{Lin}(M) \longrightarrow M$$

from the set $\mathrm{Lin}(M) \subset \mathcal{P}(M)$ of all subsets linearly ordered with respect to $\preceq$, such that $T \preceq \gamma(T)$. We may even assume that $\gamma(T)$ is a strict upper bound: $T \prec \gamma(T)$ or, equivalently $\gamma(T) \notin T$. If only $\gamma(T) \in T$ is possible, the element $\gamma(T)$ would be a maximal element for the entire set M.

Then we use the function γ in order to produce recursively a linearly ordered, indeed even well ordered, subset not admitting an upper bound, contrary to our hypothesis. We take $x_1 := \gamma(\emptyset)$ as its first element. If $x_1, ..., x_n$ are found one defines $x_{n+1} := \gamma(\{x_1, ..., x_n\})$. In this way we obtain a sequence $(x_n)_{n\in\mathbb{N}}$ with $x_1 \prec x_2 \prec ...$, but the chain $\{x_n; n \in \mathbb{N}\}$ can be extended further: Take $y_1 := \gamma(\{x_n; n \in \mathbb{N}\})$, $y_2 := \gamma(\{y_1, x_n; n \in \mathbb{N}\})$.

In order to make sure that this idea really works, we introduce the concept of a "γ-chain": We shall call a subset $K \subset M$ a γ-chain, if $(K, \preceq)$ is well ordered and for any $y \in K$ the initial segment $K_{\prec y} := \{x \in K;\ x \prec y\}$ satisfies

$$y = \gamma(K_{\prec y}) \ .$$

We shall see that given two γ-chains K, L one of them is an initial segment of the other. Taking this for granted the set

$$T := \bigcup_{K\ \gamma\text{-chain}} K$$

is obviously a maximal γ-chain. On the other hand $\hat{T} := T \cup \{\gamma(T)\}$ is γ-chain as well, so $\hat{T} \subset T$ resp. $\gamma(T) \in T$ – a contradiction!

It remains to show that of two γ-chains K, L one is an initial segment of the other: Denote $K_0 = L_0$ the union of all sets which are initial segments of both K and L. Obviously it is an initial segment of both K and L. If $K_0 = K$ or $L_0 = L$, we are done; otherwise $K_0 = K_{\prec a}$ and $L_0 = L_{\prec b}$. In that case we have

$$a = \gamma(K_{\prec a}) = \gamma(L_{\prec b}) = b \in L \ ,$$

i.e., $K_{\preceq a} = L_{\preceq b}$ is an initial segment of both K and L, a contradiction! $\square$

Remark 5.10. The above proof of Zorns lemma is a naive one. The most problematic part is the existence of the function

$$\gamma : \mathrm{Lin}(M) \longrightarrow M,$$

since in general there is no recipe for an explicit construction, the set $\mathrm{Lin}(M)$ being quite big. Instead one has to derive it from the

Axiom of Choice: *Given a family $(A_i)_{i\in I}$ of pairwise disjoint subsets $A_i \subset M$ of a set M, there is a set $A \subset M$ containing precisely one element out of each set $A_i, i \in I$, i.e., it has the form $A = \{x_i; i \in I\}$ with $x_i \in A_i$ for all $i \in I$.*

The axiom of choice, though looking quite harmless, has striking consequences, as for example the fact, that every set admits a well ordering, cf. Problem 5.11.4. Indeed, no human being has up to now succeeded in well ordering the set of all real numbers.

Problems 5.11.

1. Let $S \subset R \setminus \{0\}$ be a multiplicative subset in the ring R. Show: There is a maximal ideal $\mathfrak{a} \subset R$ in the set of all ideals not intersecting S. If $S = \{1\}$, it is a maximal ideal in the sense of Def. 3.23, but otherwise not necessarily. But in any case it is a prime ideal!

2. Show that
$$\bigcap_{\mathfrak{p}\subset R \text{ prime ideal}} \mathfrak{p} \quad = \sqrt{\{0\}}\,.$$
Hint: Use Problem 4.75.1! Here we denote $\sqrt{\{0\}} := \{x \in R; \exists\, n \in \mathbb{N} : x^n = 0\}$ the nilradical of the ring R.

3. Let $K \subset \mathbb{C}$ be a subfield. Show: Every automorphism $\sigma : K \longrightarrow K$ can be extended to an automorphism $\hat{\sigma} : \mathbb{C} \longrightarrow \mathbb{C}$! Note that the corresponding statement for $\mathbb{R}$ instead of $\mathbb{C}$ is wrong! (Cf. Problem 4.20.3)

4. Show: Every set M admits a well ordering. Hint: Choose a map $\gamma : \mathcal{P}(M)\backslash\{M\} \longrightarrow M$ with $\gamma(A) \in M \setminus A$ for all proper subsets $A \subset M$. Then argue as in the proof of Zorns lemma!

References

[1] Cohn, Paul Moritz: *Classic Algebra*, John Wiley & Sons, 2000.

[2] Ebbinghaus, Hans Dieter; Hermes, Hans; Hirzebruch, Friedrich; Koecher, Max; Mainzer, Klaus; Prestel, Alexander and Remmert, Reinhold: *Zahlen*, Springer 1983.

[3] Gorenstein, Daniel; Lyons, Richard and Solomon, Ronald: *The Classification of the Finite Simple Groups*, Math. Surveys and Monographs, AMS, Providence, Rhode Island.

[4] Grillet, Pierre Antoine: *Abstract Algebra*, GTM 242, Springer, 2006.

[5] Hasse, Helmut: *Höhere Algebra I/II*, Sammlung Göschen Bd.931/932, 1969/1967.

[6] Lang, Serge: *Algebra*, Addison Wesley 1965.

[7] Reiffen, Hans-Jörg; Scheja, Günter and Vetter, Udo: *Algebra*, BI Hochschultaschenbücher 110/110a.

[8] Ringel, Claus-Michael: *Leitfaden zur Algebra I*, SS 2001, Homepage Universität Bielefeld.

[9] Rotman, Joseph: *Galois Theory*, Springer 1998.

[10] Scharlau, Winfried, and Opolka, Hans: *Von Fermat bis Minkowski*, Springer 1980.

[11] van der Waerden, Bartel Ludwig: *Algebra I/II*; Springer, Heidelberger Taschenbücher 12/13 (8th edition of his classical book "Moderne Algebra").

[12] Willems, Wolfgang: *Codierungstheorie*; Walter de Gruyter 1999.

[13] Zariski, Oscar and Samuel, Pierre: *Commutative Algebra I/II*, GTM 28/29, Springer.