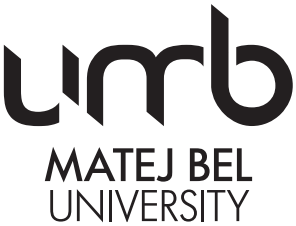

Basic algebra

for future teachers

Miroslav Haviar and Pavel Klenovčan

Second edition with answers or solutions to exercises
by Veronika Remenárová and Miroslav Haviar

Publisher of Matej Bel University in Banská Bystrica
Faculty of Natural Sciences
2020

Basic Algebra for future teachers

© Authors
prof. RNDr. Miroslav Haviar, CSc.
doc. RNDr. Pavel Klenovčan, CSc.

Reviewers
prof. RNDr. Vladimír Janiš, CSc.
doc. PaedDr. Martin Papčo, PhD.

Design
doc. Mgr. Ján Karabáš, PhD.
Typeset by LaTeX and KOMA-Script

Cover design
Mgr. art. Zuzana Ceglédyová

© Belianum, Publisher of Matej Bel University in Banská Bystrica,
Faculty of Natural Sciences

Printed by Equilibria, s.r.o., Košice

Second edition, 2020

ISBN 978-80-557-1746-3
EAN 9788055717463

Dedicated to our families

Contents

Preface to the second edition

The three parts contained in this textbook are still strongly based on the lecture notes ALGEBRA I – III published by the present authors about twenty years ago in the Slovak language [5, 7, 4]. And the textbook still presents those three volumes of lecture notes together as one unit of *Basic Algebra* intended mainly for future teachers of Mathematics.

What is new with this second edition is that answers, solutions or at least hints are provided at the end of the textbook to all 271 exercises presented in it (113 exercises in Part I, 56 exercises in Part II and 102 exercises in Part III). I believe that these answers or solutions, which of course prolonged the second edition, will be of some help to the students or other interested readers of this textbook (even more in the present times of pandemics). Since the second author of this textbook retired a few years ago and decided not be involved in preparation of this second edition, the answers or solutions to exercises at the end of the textbook were prepared together with one of our gifted present students of Mathematics, Ing. Veronika Remenárová. She is the author of the answers or solutions to exercises from Chapters 1-6 and 14-25 of this textbook (112 exercises) while I am responsible for the answers or solutions to exercises from the remaining Chapters 7-13 and 26-35 (159 exercises).

Within the time period of five years from the publication of the first edition of this textbook in January 2016, its Parts I and II have been used by myself every academic year as the primary teaching material for the existing one semester courses *Algebra I* and *Algebra II* at *Matej Bel University* in Banská Bystrica. These two courses have been aimed, at the Bc level, for future teachers of Mathematics in their third year of study as well as for students of a purely Mathematics degree in their second year of study. Part III of the textbook was used in the second semester of the last academic year for the course *Linear algebra I* for the first year students of Mathematics at Matej Bel University. Due to the pandemics, the teaching of the courses during majority of the semester at the spring 2020 had to be in online form. Since the teaching of the courses also continues online during the autumn 2020, I believe that answers, solutions or hints provided to the exercises in this textbook will assist the students as much as possible under the more difficult circumstances.

As the preparer of this second edition, I am expressing my gratitude for their comments to the two referees, prof. RNDr. Vladimír Janiš, CSc. (Banská Bystrica) and doc. PaedDr. Martin Papčo, PhD. (Ružomberok). I wish to thank colleagues doc. Mgr. Ján Karabáš, PhD. and Mgr. art. Zuzana Ceglédyová for their assistance with preparing the design of the textbook for this second edition.

I am also expressing my thanks to my former students of the courses Algebra I, Algebra II and Linear algebra I for their willingness to follow the courses in English. (At least all writings during the three courses had always been in English and followed the respective three parts of this textbook, while my explanations of the content and the communication with students had partly been in Slovak.) Teaching about a dozen of courses using the first edition of this textbook certainly helped me to estimate its value for the courses properly (and I have to admit that I liked teaching following this textbok) and to correct some typos found in the first edition. Using the first edition of the textbook in close collaboration with the students over the past five years also encouraged me to prepare this second edition of the textbook. I believe it will serve well in the above mentioned three courses of Basic Algebra at Matej Bel University in Banská Bystrica for many coming years.

Banská Bystrica, November 30, 2020 Miroslav Haviar

Notation

Throughout this textbook we use the following notation:

$\mathbb{N}$	the set of all natural numbers
$\mathbb{N}^+$	the set of all positive natural numbers, $\mathbb{N} := \mathbb{N}^+ \cup \{0\}$
$\mathbb{Z}$	the set of all integers
$\mathbb{Q}$	the set of all rational numbers
$\mathbb{R}$	the set of all real numbers
$\mathbb{C}$	the set of all complex numbers
$\mathbb{F}$	a field
$0_{\mathbb{F}}, 1_{\mathbb{F}}$	the zero resp. the unit element of a field $\mathbb{F}$
$a\|b$	the number a divides the number b
$a \equiv_m b$	a is congruent to b modulo m
$\overline{\mathbb{Z}}_m$	the set of all residue classes of integers modulo m
$\mathbb{Z}_m$	the set of all remainders of integers modulo m
a_m or $\overline{a}$	the residue class of integers modulo m represented by a
$\|S\|$	the cardinality of a set S
$\mathcal{P}(S)$	the power set of a set S
A^B	the set of all functions from a set B into a set A
id_S or i	the identity function on a set S
$[M]$	a groupoid (group, vector space) generated by a set M
$\langle M \rangle$	a ring (field) generated by a set M
S_n	the symmetric group of degree n
D_n	the dihedral group of degree n
$\mathbb{F}[x]$	the ring of polynomials in one indeterminate x over a field $\mathbb{F}$
$\mathbb{F}[x_1, \ldots, x_n]$	the ring of polynomials in indeterminates $x_1, \ldots, x_n$ over a field $\mathbb{F}$
$\mathbb{F}\langle x \rangle$	the ring of polynomial functions of one variable x over a field $\mathbb{F}$
$\mathbf{A} = [a_{ij}]$	a matrix $\mathbf{A}$ with elements a_{ij}
$\mathbf{I}_n$	the identity matrix of degree n
$M_{m,n}(\mathbb{F})$	the set of all matrices of type $m \times n$ over a field $\mathbb{F}$
$M_n(\mathbb{F})$	the set of all square matrices of degree n over a field $\mathbb{F}$
$\mathbf{A}^T$	the transpose matrix of a matrix $\mathbf{A}$
$\mathbf{A}^{-1}$	the inverse matrix of a matrix $\mathbf{A}$
$\|\mathbf{A}\|$	the determinant of a matrix $\mathbf{A}$
$V(\mathbb{F})$	a vector space over a field $\mathbb{F}$
$V_n(\mathbb{F})$	the n-dimensional vector space over a field $\mathbb{F}$
$\|\alpha\|$	the norm (length) of a vector α
$\varepsilon_1, \ldots, \varepsilon_n$	the unit vectors $(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$
$\dim(T)$	the dimension of a space T
$s(\beta, \gamma)$	a scalar product s of vectors β, γ
$T^\perp$	the orthogonal complement of a subspace T

Preface to the first edition

The three parts of this textbook are based on the lecture notes ALGEBRA I – III published by the present authors in the Slovak language [5], [7], [4]. This textbook presents those three volumes of lecture notes together as one unit of *Basic Algebra*.

It intentionally presents it in English which nowadays is the common *science* and *university* language; we believe the students these days should get used to English during their studies as soon as possible. With respect to the present intense *migration waves* into Europe we remark that it is quite possible in the coming years that some of our future teachers of mathematics reading this textbook will be these migrants or that our future teachers of mathematics might teach in their classes children arriving to Europe these days. We are therefore convinced that English has been appropriately chosen as the language here.

Parts I and II of this textbook are aimed at and can be used as the teaching material for the existing courses *Algebra I: Algebraic structures* and *Algebra II: Polynomial algebra* at *Matej Bel University* in Banská Bystrica. Part III can be used for the course *Linear algebra I* while the course *Linear algebra II* would obviously require a more advanced linear algebra content.

The textbook assumes that the students and its other possible readers have already taken at least some introductory course in mathematics. It assumes the knowledge of fundamental concepts such as *set, n-tuple, relation, function, operation* and the concepts related to operations such as *associativity, commutativity, neutral element* and *inverse element*. (At Matej Bel University this knowledge could be gained from the lecture notes *An introduction into the study of mathematics* [8] for such an introductory course.) Though the textbook is primarily intended for future teachers of mathematics, it can also be used for students of purely *mathematical degrees* at bachelor level. Comments from the students and other readers are welcomed at `miroslav.haviar@umb.sk` and `pavel.klenovcan@gmail.com`.

We are very indebted to Emeritus Professor Gareth Jones (Southampton) for his careful reading of the manuscript of this textbook and for his extremely valuable and detailed comments on the preface, the introduction and on nine chapters of the textbook (Chapters 1,2,9,13-15,25,28,35). We believe that there will be more time available before the next edition of this textbook to receive his valuable comments on the remaining chapters, too. We also express our gratitude for their comments to the other two referees, doc. RNDr. Tomáš Zdráhal, CSc. (Olomouc) and prof. RNDr. Rudolf Zimka, PhD. (Banská Bystrica), and for detailed comments to the whole text to doc. RNDr. Alfonz Haviar, CSc. We wish to thank our colleague doc. Mgr. Ján Karabáš, PhD. for his valuable help with the tables and figures and with preparing the design of this textbook and to Mgr. art. Zuzana Ceglédyová for creating the cover design. The first author also expresses his thanks for the support of the project *Mobility-Enhancing Research, Science and Education* at Matej Bel University (ITMS code 26110230082) under the Operational Programme of Education cofinanced by the European Social Foundation, and to *Christ Church College* in Oxford for its hospitality during the final stages of preparation of this textbook.

Banská Bystrica, November 17, 2015 Miroslav Haviar and Pavel Klenovčan

Introduction

Algebra is one of the oldest areas of mathematics. In the past it was understood as a discipline about calculations with *letters* representing numbers, in contrast with arithmetic which was understood as a theory about calculations with *concrete numbers*. Such an understanding is often common even nowadays in teaching *elementary* (secondary school) *algebra*.

By *modern algebra* we in present times mainly mean the theory about algebraic structures, about polynomials and algebraic equations, and about linear algebra. This textbook introduces *future teachers of mathematics* at the bachelor level of their university studies to some of the *basic* concepts, results and examples concerning the classical algebraic structures (groups, rings, integral domains and fields), then to polynomials and algebraic equations, and finally to linear algebra.

Part I concerning basic algebraic structures has thirteen chapters, starting with *the residue classes of integers* which are often used as a fundamental example of an algebraic structure throughout this textbook. The subsequent eight chapters are devoted to concepts, results and examples concerning *groups* and culminate in the classification of all finite groups of orders 1 to 15. The next three chapters are devoted to *rings, integral domains* and *fields*, and the final chapter of Part I deals with common equivalent and non-equivalent adjustments when solving algebraic equations over integral domains in *school practice*.

Part II focusing on polynomial algebra has the first eight chapters devoted to concepts, results and examples concerning polynomials and polynomial functions. Its other four chapters deal with methods of solving certain basic types of algebraic (polynomial) equations over the *school* fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ of rational, real and complex numbers, respectively and over the field $\overline{\mathbb{Z}}_p$ of residue classes of integers modulo p where p is a prime number.

Part III concerning linear algebra has the first four chapters devoted to basic methods in solving *systems of linear equations* over the fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $\overline{\mathbb{Z}}_p$. It starts with *matrices* and *elementary row operations* on them as a fundamental tool used throughout the whole exposition. The subsequent six chapters study *the algebraic structure* of the set of solutions of these systems of equations and are devoted to basic concepts, results and examples concerning *vector spaces* over *abstract fields* $\mathbb{F}$ (where, however, the students can always think of the *school* fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and of the field $\overline{\mathbb{Z}}_p$). Our aim here is to show the future teacher of mathematics a one-to-one correspondence between matrices, systems of linear equations, certain subspaces of finite-dimensional vector spaces and linear maps between these subspaces. In our final chapter we show that n-dimensional *Euclidean* vector spaces over the field $\mathbb{R}$ are *algebraically indistinguishable* from the well-known spaces $\mathbb{R}^n$ of n-tuples of real numbers.

We have aimed at achieving a transparent structure of the texbook. Items such as definitions, lemmas, propositions, theorems, corollaries and examples are numbered as $x.y$, where x is the number of chapter and y is the 'ordering' number of the item in the chapter. For example, when referring to Definition **??** (of a group) it is possible to find the required definition quickly as item number 17 in Chapter 2.

Our exposition is in each of its three parts illustrated with a great number of examples. The end of each example is marked with the symbol ■, while the end of each proof is denoted by the traditional symbol □. Since our text has been edited in *AMS–LaTeX*, we added an *Index* at the end that should enable the students to search where in the text particular concepts and results were first presented. The symbol := denotes the *defining equality* (meaning that the concept placed on its left is defined via the concepts or formulas on its right). To define a new concept outside the formal *definition environment* or to emphasize certain words (as we do already throughout the Preface and the Introduction), we use the

traditional font *italic*. To highlight an important concept inside a definition we often use the font **boldface**. Everywhere in the text expressions like $\sqrt[3]{2}$ denote the *real* cube root of 2. The composition of maps is generally written in our text as $(f \circ g)(x) = f(g(x))$, thus differing, for example, from [6].

In certain parts we present *historical notes* in footnotes which should give future teachers of mathematics a historical perspective of the development of algebra, or encourage them to study the history of algebra in more detail.

Part II
Polynomial algebra

Working with 'polynomial expressions' of the form

$$a_0 + a_1 x + \cdots + a_n x^n$$

is common already at primary and secondary schools. There such a polynomial is viewed as a function or as a certain 'algebraic expression', and a proper understanding of this second meaning is usually not achieved.

In Part II of this textbook we present a basic theory of Polynomial algebra. We introduce polynomials in one indeterminate as purely algebraic expressions and we introduce the corresponding polynomial functions of one variable. The difference between them should become understandable as well as the contexts in which both can be algebraically identified - via the concept of a 'ring isomorphism' introduced in the previous part of the textbook. Among those contexts where both can be considered the same are exactly the 'school' contexts where rings of polynomials and of polynomial functions are considered over the fields of rational, real or complex numbers, and thus are necessarily isomorphic.

In this part of the textbook we deal mainly with divisibility of polynomials, their decompositions, with roots of polynomial functions, and finally in more detail with algebraic (polynomial) equations, for which a brief introduction has already been given in the last chapter of Part I. One chapter of our exposition of polynomial algebra is devoted to polynomials in several indeterminates resp. polynomial functions of several variables. Part II of the textbook is based on the lecture notes [7].

14 Polynomials in one indeterminate

We already know that the subring $\langle M \rangle$ of a ring A' generated by a non-empty set M is the intersection of all subrings of A' which contain the set M. So it is the smallest (with respect to set inclusion) subring of A' containing M.

To present the construction of a ring of polynomials in one indeterminate we shall study the subring $\langle A \cup \{t\} \rangle$ of a ring A' generated by the set $M = A \cup \{t\}$, where A is a subring of A' and $t \in A' \setminus A$ is a selected element of A'. We remark here that the subring $\langle A \cup \{t\} \rangle$ is usually denoted by $A[t]$ in the

literature, and we introduce this more concise notation immediately after the forthcoming Theorem 14.2. We also wish to point out that all our rings considered here will be assumed to be commutative rings with unit such as the 'school' rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ and the ring of residue classes $\overline{\mathbb{Z}}_m$.

Example 14.1. We show that the set

$$A = \left\{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z} \right\}$$

is a subring of the ring $\mathbb{R}$ generated by the set $M = \mathbb{Z} \cup \left\{ \sqrt[3]{2} \right\}$. We recall that here and elsewhere in our text, expressions like $\sqrt[3]{2}$ and $\sqrt[3]{4}$ denote the *real* cube roots of 2 and 4.

First note that the set A is a subring of the ring $\mathbb{R}$ (details should be verified as an exercise).

(a) If $t \in \mathbb{Z}$, then $t \in A$ as

$$t = t + 0 \cdot \sqrt[3]{2} + 0 \cdot \sqrt[3]{4}.$$

Since

$$\sqrt[3]{2} = 0 + 1 \cdot \sqrt[3]{2} + 0 \cdot \sqrt[3]{4},$$

also $\sqrt[3]{2} \in A$. From this it follows that the subring A contains the set $\mathbb{Z} \cup \left\{ \sqrt[3]{2} \right\}$, and thus

$$\left\langle \mathbb{Z} \cup \left\{ \sqrt[3]{2} \right\} \right\rangle \subseteq A.$$

(b) Let $t \in A$ be an arbitrary element. Then there exist $a, b, c \in \mathbb{Z}$ such that $t = a + b\sqrt[3]{2} + c\sqrt[3]{4}$. Because a, b, c, $\sqrt[3]{2}$, $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$ are elements of the ring $\left\langle \mathbb{Z} \cup \left\{ \sqrt[3]{2} \right\} \right\rangle$, we also have

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \left\langle \mathbb{Z} \cup \left\{ \sqrt[3]{2} \right\} \right\rangle,$$

whence

$$A \subseteq \left\langle \mathbb{Z} \cup \left\{ \sqrt[3]{2} \right\} \right\rangle.$$

From (a) and (b) it follows that

$$A = \left\langle \mathbb{Z} \cup \left\{ \sqrt[3]{2} \right\} \right\rangle.$$

■

By an approach similar to that presented in the given example we shall prove the following statement.

Theorem 14.2. *Let $(A', +, \cdot)$ be a commutative ring with unit and let $(A, +, \cdot)$ be a subring which contains the unit. If $t \in A' \setminus A$, then*

$$\langle A \cup \{t\} \rangle = \{a_0 + a_1 t + \cdots + a_n t^n \mid a_0, a_1, \ldots, a_n \in A,\ n \in \mathbb{N}\}.$$

Proof. Let

$$B := \{a_0 + a_1 t + \cdots + a_n t^n \mid a_0, a_1, \ldots, a_n \in A,\ n \in \mathbb{N}\}.$$

The set B is closed under the operations of subtraction and multiplication (verify this in detail), hence $(B, +, \cdot)$ is a subring of the ring $(A', +, \cdot)$.

Because $A \cup \{t\} \subseteq B$ (again, verify details of this) and the subring $\langle A \cup \{t\} \rangle$ is the smallest of all subrings containing the set $A \cup \{t\}$, we have

$$\langle A \cup \{t\} \rangle \subseteq B.$$

If $b \in B$, then there exist $a_0, a_1, \ldots, a_n \in A$ and $n \in \mathbb{N}$ such that

$$b = a_0 + a_1 t + \cdots + a_n t^n.$$

Since $a_0, a_1, \ldots, a_n, t \in \langle A \cup \{t\} \rangle$, also $b \in \langle A \cup \{t\} \rangle$, from which it follows that $B \subseteq \langle A \cup \{t\} \rangle$. Therefore $\langle A \cup \{t\} \rangle = B$. □

Definition 14.3. We say that the ring $\langle A \cup \{t\} \rangle$ arises by **adjunction** of the element $t \in A' \setminus A$ to the ring A. It will be denoted by $A[t]$ and its elements will be denoted by $a(t)$, $b(t)$, $f(t)$, etc.

Example 14.4. Consider the elements $1 + 2i^2 + 3i^4$ and $3 + i^2$, where $i \in \mathbb{C}$ is the imaginary unit. These elements are, by Theorem 14.2, the elements of the ring $\mathbb{Z}[i]$ and it can easily be seen that they represent the same element, that is, $1 + 2i^2 + 3i^4 = 3 + i^2$. Further, putting $t = i$ in the expression $a(t) = -2 + x^2 + 3x^4$ gives $a(i) = 0$. Notice that in the ring $\mathbb{Z}[i]$ one can express an element via several ways and that an equation of the form $a_0 + a_1 i + \ldots a_n i^n = 0$ can hold even when the coefficients $a_0, a_1, \ldots, a_n$ are not all zero. In our case we have $a_0 = -2$, $a_1 = 0$, $a_2 = 1$, $a_3 = 0$, $a_4 = 3$. ■

We already know that every element $a(t)$ of a ring $A[t]$ can be written in the form

$$a(t) = a_0 + a_1 t + \cdots + a_n t^n, \tag{29}$$

where $a_0, a_1, \ldots, a_n \in A$, $n \in \mathbb{N}$. We now distinguish two important cases.

Definition 14.5. If, for some element $a(t) \in A[t]$, an equation $a(t) = 0_A$ holds if and only if $a_0 = a_1 = \cdots = a_n = 0_A$, we say that the element t is a **transcendental element** over the ring A. If there is an element $a(t) \in A[t]$ of the form (29) for which $a(t) = 0_A$ and at least one of the elements $a_0, a_1, \ldots, a_n$ is non-zero, we say that t is an **algebraic element** over the ring A. Algebraic elements over the rings $\mathbb{Z}$ and $\mathbb{Q}$ are also called **algebraic numbers**.

It is worth noting here that *algebraic over* $\mathbb{Z}$ and *algebraic over* $\mathbb{Q}$ are equivalent.

Example 14.6. We show that the number $\sqrt{3} - \sqrt{2}$ is an algebraic number.

Let us denote $t = \sqrt{3} - \sqrt{2}$. Then $t^2 = 5 - 2\sqrt{6}$. This gives us $t^2 - 5 = -2\sqrt{6}$. After squaring this and further adjustment we get $t^4 - 10t^2 + 1 = 0$, hence

$$(\sqrt{3} - \sqrt{2})^4 - 10(\sqrt{3} - \sqrt{2})^2 + 1 = 0.$$

This means that $\sqrt{3} - \sqrt{2}$ is an algebraic number. ■

The numbers π and e (the base of the natural logarithm) can be shown to be transcendental over the ring $\mathbb{Z}$.

When considering two algebraic elements t_1, t_2 over a ring A, the rings $A[t_1]$, $A[t_2]$ may not necessarily be isomorphic as shown by the next example.

Example 14.7. We prove that the rings $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[i]$ are not isomorphic.

The universes of the rings $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[i]$ are the sets

$$\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \text{ and } \{a + bi \mid a, b \in \mathbb{Z}\},$$

respectively (verify this in detail). Suppose, for a contradiction, that there is an isomorphism $f : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[i]$. We know that $f(1) = 1$. Hence we also have $f(2) = f(1 + 1) = f(1) + f(1) = 1 + 1 = 2$. Let $f(\sqrt{2}) = a + bi$ where $a, b \in \mathbb{Z}$. Then we have the following equality:

$$2 = f(2) = f(\sqrt{2} \cdot \sqrt{2}) = f(\sqrt{2}) \cdot f(\sqrt{2}) = (a + bi) \cdot (a + bi) = a^2 - b^2 + 2abi.$$

Since 2 is real, it follows that $a = 0$ or $b = 0$.

If $a = 0$, then $2 = -b^2$, a contradiction. If $b = 0$, then $2 = a^2$, which again is a contradiction (there is no integer whose square is 2).

Hence there is no isomorphism of the ring $\mathbb{Z}[\sqrt{2}]$ onto the ring $\mathbb{Z}[i]$. ■

The proof of the following theorem is an easy exercise and is left to the reader. We mention that a natural isomorphism to be used is the mapping

$$f : A[x] \to A[y], \quad f(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1 y + \cdots + a_n y^n.$$

Theorem 14.8. *If x, y are transcendental elements over a ring A, then the rings $A[x]$ and $A[y]$ are isomorphic.*

For every ring A (meaning, in our setting, a commutative ring with unit) there exists a ring $A' \supseteq A$ and an element $t \in A' \setminus A$, which is a transcendental element over the ring A. Thus we can always assume the existence of a transcendental element over an arbitrary ring, and it does not matter how it is denoted.

Definition 14.9. If x is a transcendental element over a ring A, then the elements of the ring $A[x]$ are called **polynomials (in one indeterminate)** over the ring A and the ring $A[x]$ is thus called the **ring of polynomials** (in one indeterminate) over the ring A. If $f(x) \in A[x]$, where

$$f(x) = a_0 + a_1 x + \dots a_n x^n,\ a_n \neq 0_A,$$

then the elements $a_0, a_1, \dots, a_n$ are called the **coefficients** of the polynomial $f(x)$. The coefficient a_n is said to be the **leading coefficient** and the number n is the **degree of the polynomial** $f(x)$. If the degree of the polynomial is n, then we write $\deg f(x) = n$. The degree of the zero polynomial is defined as $\deg 0 = -\infty$. Every non-zero element a of the ring A is a polynomial of degree $\deg a = 0$.

The definition of polynomials in one indeterminate x over a ring A means that *two polynomials are equal* if and only if they have the same degree and the same coefficients for each power of x.

From the properties of the ring operations it follows that the sum of polynomials

$$f(x) = a_0 + a_1 x + \cdots + a_r x^r, \quad g(x) = b_0 + b_1 x + \cdots + b_s x^s, \quad r \geq s,$$

is the polynomial

$$f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+\cdots+(a_s+b_s)x^s+a_{s+1}x^{s+1}+\cdots+a_r x^r \quad \text{(S)}$$

and their product is the polynomial

$$f(x) \cdot g(x) = c_0 + c_1 x + \cdots + c_{r+s} x^{r+s}, \qquad \text{(P)}$$

where

$$c_k = \sum_{i=0}^{k} a_i b_{k-i},$$

for $k \in \{0, 1, \ldots, r+s\}$.

By generalising the previous considerations we shall now analogously introduce *the ring of polynomials in several indeterminates*. Firstly, by a similar procedure to that used in Theorem 14.2 one can prove the following statement.

Theorem 14.10. *Let $(A', +, \cdot)$ be a commutative ring with unit and let $(A, +, \cdot)$ be a subring which contains the unit. If $t_1, \ldots, t_n \in A' \setminus A$, then the universe of the subring $\langle A \cup \{t_1, \ldots, t_n\}\rangle$ is the set*

$$\{a_0 t_1^{k_{01}} \ldots t_n^{k_{0n}} + \cdots + a_r t_1^{k_{r1}} \ldots t_n^{k_{rn}} \mid a_0, \ldots, a_r \in A, k_{01}, \ldots, k_{rn} \in \mathbb{N}\}.$$

The ring $\langle A \cup \{t_1, \ldots, t_n\}\rangle$ will be denoted $A[t_1, \ldots, t_n]$ and we shall say that it arises by *adjunction* of the elements $t_1, \ldots, t_n$ to the ring A. The element

$$a_0 t_1^{k_{01}} \ldots t_n^{k_{0n}} + \cdots + a_r t_1^{k_{r1}} \ldots t_n^{k_{rn}} \tag{30}$$

can contain more than one expression $a_i t_1^{k_{i1}} \ldots t_n^{k_{in}}$ with the same n-tuple of exponents $(k_{i1}, \ldots, k_{in})$. If all ordered n-tuples of exponents in the sum (30) are pairwise distinct, we say that the sum (30) is written in *canonical* form.

If for every canonical form of the sum (30) we have

$$a_0 t_1^{k_{01}} \ldots t_n^{k_{0n}} + \cdots + a_r t_1^{k_{r1}} \ldots t_n^{k_{rn}} = 0_A$$

if and only if $a_0 = \cdots = a_r = 0_A$, we say that the elements $t_1, \ldots, t_n$ are *algebraically independent* over the ring A. If there exists a canonical form of the sum (30) equal to the zero element and at least one of the elements $a_0, \ldots, a_r$ is non-zero, we say that the elements $t_1, \ldots, t_n$ are *algebraically dependent* over the ring A.

Definition 14.11. Let $(A', +, \cdot)$ be a commutative ring with unit and let $(A, +, \cdot)$ be a subring containing the unit. Let elements $x_1, x_2, \ldots, x_n$ be algebraically independent over A. The subring $\langle A \cup \{x_1, \ldots, x_n\}\rangle$ of A' generated by the set $A \cup \{x_1, x_2, \ldots, x_n\}$ is said to be **the ring of polynomials in indeterminates $x_1, x_2, \ldots, x_n$ over the ring A**. It is denoted by $A[x_1, \ldots, x_n]$ and its elements are called **polynomials in indeterminates $x_1, x_2, \ldots, x_n$** over the ring A.

We shall deal with various aspects of polynomial algebra in more detail in the subsequent chapters.

Exercises.

Exercise 14.1. Prove that

(a) $\mathbb{Q}\left[\sqrt{8}\right] = \mathbb{Q}\left[\sqrt{2}\right]$;

(b) $\mathbb{Z}\left[\sqrt{8}\right] \neq \mathbb{Z}\left[\sqrt{2}\right]$;

(c) $\mathbb{Q}\left[1+\sqrt{3}\right] = \mathbb{Q}\left[1-\sqrt{3}\right]$.

Exercise 14.2. Prove that

(a) $\mathbb{Q}\left[i+\sqrt{2}\right] = \mathbb{Q}\left[i,\sqrt{2}\right]$;

(b) $\mathbb{Q}\left[\sqrt{2}+\sqrt{3}\right] = \mathbb{Q}\left[\sqrt{2},\sqrt{3}\right]$.

Exercise 14.3. Prove that

(a) $\mathbb{Q}\left[\sqrt{3}\right] = \left\{a+b\sqrt{3} \mid a,b \in \mathbb{Q}\right\}$;

(b) $\mathbb{Q}\left[\sqrt{2}+\sqrt{3}\right] = \left\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a,b,c,d \in \mathbb{Q}\right\}$;

(c) $\mathbb{Q}\left[\sqrt[3]{-3}\right] = \left\{a+b\sqrt[3]{-3}+c\sqrt[3]{9} \mid a,b,c \in \mathbb{Q}\right\}$;

(d) $\mathbb{Q}\left[i+\sqrt{2}\right] = \left\{a+b\sqrt{2}+ci+di\sqrt{2} \mid a,b,c,d \in \mathbb{Q}\right\}$.

Exercise 14.4. Prove that

(a) $\mathbb{Q} \subset \mathbb{Q}\left[i\right] \subset \mathbb{Q}\left[i+\sqrt{2}\right]$;

(b) $\mathbb{Q} \subset \mathbb{Q}\left[\sqrt{6}\right] \subset \mathbb{Q}\left[\sqrt{2},\sqrt{3}\right]$.

Exercise 14.5. Prove that neither

$$\mathbb{Q}\left[\sqrt{2}\right] \subseteq \mathbb{Q}\left[\sqrt{6}\right]$$

nor

$$\mathbb{Q}\left[\sqrt{6}\right] \subseteq \mathbb{Q}\left[\sqrt{2}\right].$$

Exercise 14.6. Prove that the following numbers are algebraic:
(a) $\sqrt{5}+1$; (b) $2-3i$; (c) $\sqrt{3}-\sqrt{2}$; (d) $\sqrt{2+\sqrt{2}}$; (e) $\sqrt{3}+\frac{1}{\sqrt{3}}$;
(f) $\sqrt{5}+\sqrt[4]{5}$.

Exercise 14.7. Determine the universe of the ring $\mathbb{Q}\left[\sqrt[4]{2}\right]$.

Exercise 14.8. Find out whether the rings $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ are isomorphic.

15 Polynomial functions of one variable

From now on we shall mostly deal with the ring $A[x]$ of polynomials in one indeterminate x over a ring A such that the ring A happens to be a *field*: the reader should imagine the 'school' fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and the field $\overline{\mathbb{Z}}_p$ of residue classes for a prime p. If all coefficients of a polynomial $f(x)$ are integers, we often say that $f(x)$ is a polynomial with *integer coefficients*. We similarly talk about polynomials with *rational*, *real* or *complex coefficients*. (If a polynomial is given without specifying the field, yet the coefficients are numbers, we consider it to be a polynomial over a suitable field of numbers.)

If a polynomial $f(x)$ is written in the form

$$f(x) = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n,$$

for $a_0, a_1, \ldots, a_n \in A, a_n \neq 0_A$, $n \in \mathbb{N}$ and each power x^i occurs at most once, we say that the polynomial $f(x)$ is presented in its *normal form*. A polynomial $f(x)$ in this form whose leading coefficient is $a_n = 1$ is said to be a *monic* (or *normed*) polynomial.

The properties of the sum and product of polynomials given in the previous chapter by (S) and (P) yield the following statement (verify it in details).

Lemma 15.1. *Let A be an integral domain and let $f(x), g(x) \in A[x]$. Then*

(a) $\deg(f(x) + g(x)) \leq \max(\deg f(x), \deg g(x))$*;*

(b) if $\deg f(x) \geq 0$, $\deg g(x) \geq 0$, *then*

$$\deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x).$$

Theorem 15.2.

(i) If A is an integral domain, then also $A[x]$ is an integral domain.

(ii) If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is an integral domain but it is not a field.

Proof. (i) Let $f(x), g(x) \in A[x]$ and $f(x) \neq 0, g(x) \neq 0$, i.e. $\deg f(x) \geq 0$ and $\deg g(x) \geq 0$. Then, by Lemma 15.1, $\deg(f(x) \cdot g(x)) \geq 0$, so $f(x) \cdot g(x) \neq 0$, which means that $A[x]$ is an integral domain.

(ii) Every field $\mathbb{F}$ is an integral domain and from (i) it then follows that $\mathbb{F}[x]$ is an integral domain. It is clear that $\mathbb{F}[x]$ is not a field because in $\mathbb{F}[x]$ only polynomials $f(x) = a_0$ of degree 0 have inverse elements $(f(x))^{-1} = {a_0}^{-1}$ $(a_0 \in \mathbb{F} \setminus \{0_\mathbb{F}\})$.

□

Definition 15.3. Let $\mathbb{F}$ be a field. By a **polynomial function (of one variable) over the field** $\mathbb{F}$ we mean a function $f : \mathbb{F} \to \mathbb{F}$ for which there exist $n \in \mathbb{N}$ and $a_0, a_1, \ldots, a_n \in \mathbb{F}$ such that

$$(\forall x \in \mathbb{F}) \qquad f(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

The set of all polynomial functions (of one variable) over the field $\mathbb{F}$ is denoted by the symbol $\mathbb{F}\langle x\rangle$.

Obviously, two polynomial functions $f, g \in \mathbb{F}\langle x\rangle$ are equal if and only if

$$(\forall t \in \mathbb{F}) \quad f(t) = g(t).$$

In order to distinguish the set of all polynomial functions of one variable x over a field $\mathbb{F}$ from the set of all polynomials in one indeterminate x over $\mathbb{F}$, we deliberately introduced the symbol $\mathbb{F}\langle x\rangle$ for the former set *to distinguish it* from the symbol $\mathbb{F}[x]$ for the latter set. Also to distinguish the notation from the symbols $f(x)$ used for polynomials, polynomial functions will be denoted simply by symbols f, g, h, etc. without usually writing the symbols for their variables. The symbol $f(t)$ will denote the *value* of the function f at the element t. We remark that a value $f(t)$ at the element t can only be given for a polynomial function f by substituting t for its variable while in a polynomial $f(x)$ the symbol x stands for an indeterminate (a transcendental element) and thus *no substitutions for x in polynomials $f(x)$ are possible*! We hope the student or other reader would become well aware of this *distinction* between a polynomial function $f \in \mathbb{F}\langle x\rangle$ and a polynomial $f(x) \in \mathbb{F}[x]$.

At secondary school (and this might rarely happen also here, for example, in exercises), the polynomials in one indeterminate x and the polynomial functions of one variable x are often given via the same looking 'polynomial expressions'. It should then be the (sometimes uneasy) role of the student or other reader to recognize from the context whether they are really meant only to be purely algebraic expressions (i.e. polynomials) or whether they are intended as polynomial functions.

To make the relationship and the distinction between the polynomials in one indeterminate and the polynomial functions of one variable *more precise* and *understandable*, we assign here to each polynomial $f(x)$ in one indeterminate x a unique polynomial function of one variable x as follows: if

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x],$$

then the mapping

$$\psi : \mathbb{F}[x] \to \mathbb{F}\langle x\rangle$$

has in $F\langle x\rangle$ the value $\psi(f(x)) = f : \mathbb{F} \to \mathbb{F}$ such that

$$f : t \in \mathbb{F} \mapsto f(t) = a_0 + a_1 t + \cdots + a_n t^n \in \mathbb{F}.$$

The mapping $\psi : \mathbb{F}[x] \to \mathbb{F}\langle x\rangle$ is surjective by the way that polynomial functions are defined (i.e. as functions given by a 'polynomial rule'). However, ψ is not injective in general. We illustrate this in the following example where the field $\mathbb{F}$ is finite.

Example 15.4. Let $\mathbb{F} = \mathbb{Z}_3$ and let $f(x) = x^3 + x^2$, $g(x) = x^2 + x \in \mathbb{Z}_3[x]$. We obviously have $f(x) \neq g(x)$ in $\mathbb{Z}_3[x]$, but notice that $\psi(f(x)) = \psi(g(x))$ in $\mathbb{F}\langle x\rangle$ because $f(0) = g(0) = 0$, $f(1) = g(1) = 2$ and $f(2) = g(2) = 0$.

So $x^3 + x^2$ and $x^2 + x$ understood as polynomials in one indeterminate x over the field $\mathbb{Z}_3$ are different. However if $x^3 + x^2$ and $x^2 + x$ are understood as polynomial functions of one variable x over the field $\mathbb{Z}_3$, then they are equal. ■

The sum $f+g$ and the product $f \cdot g$ of polynomial functions f, g are defined in the usual 'pointwise' manner as for all functions:

$$(\forall t \in \mathbb{F}) \quad (f+g)(t) := f(t) + g(t) \;\;\&\;\; (f \cdot g)(t) := f(t) \cdot g(t). \tag{31}$$

Let $f(x) = a_0 + a_1 x + \cdots + a_r x^r$, $g(x) = b_0 + b_1 x + \cdots + \cdots + b_s x^s$, $r \geq s$. Then

$$\begin{aligned} \psi(f(x) + g(x)) =& \psi((a_0 + b_0) + \cdots + (a_s + b_s)x^s + a_{s+1}x^{s+1} + \cdots + a_r x^r) \\ =& (a_0 + b_0) + \cdots + (a_s + b_s)x^s + a_{s+1}x^{s+1} + \cdots + a_r x^r, \\ \psi(f(x)) + \psi(g(x)) =& (a_0 + \cdots + a_r x^r) + (b_0 + \cdots + b_s x^s). \end{aligned}$$

One can easily verify (using the commutativity of the operations in $\mathbb{F}$ and the distributivity of $\cdot$ with respect to $+$) that for every $t \in \mathbb{F}$,

$$(a_0+b_0)+\cdots+(a_s+b_s)t^s+a_{s+1}t^{s+1}+\cdots+a_r t^r = (a_0+\cdots+a_r t^r)+(b_0+\cdots+b_s t^s),$$

from which it follows that

$$\psi(f(x) + g(x)) = \psi(f(x)) + \psi(g(x)). \tag{32}$$

Analogously one can show that

$$\psi(f(x) \cdot g(x)) = \psi(f(x)) \cdot \psi(g(x)). \tag{33}$$

We see that the polynomial functions of one variable can be added and multiplied just like the polynomials in one indeterminate, that is, via the rules (S)

for the sum and (P) for the product. However, their addition and multiplication just as functions via the 'pointwise rule definition' (31) is often more useful and simpler.

We leave the details of the proof of the following statement for the reader.

Theorem 15.5. *The set $\mathbb{F}\langle x\rangle$ of the polynomial functions of one variable x over a field $\mathbb{F}$ equipped with the operations of addition and multiplication of polynomial functions given by the 'pointwise' rule (31) is a commutative ring with the zero element $f \equiv 0$ (the constant function equal to zero) and with the unit element $g \equiv 1$ (the constant function equal to one).*

We remark that this theorem in ring theory also follows from the equations (32) and (33) above which say that the mapping $\psi : \mathbb{F}[x] \to \mathbb{F}\langle x\rangle$ is what is called a *ring homomorphism*; since it is surjective, ψ is even what is called a *ring epimorphism*.

We also note that we show later, in Corollary 18.6, that what Example 15.4 illustrates over a finite field $\mathbb{F}$ cannot happen over an infinite field $\mathbb{F}$, where the mapping $\psi : \mathbb{F}[x] \to \mathbb{F}\langle x\rangle$ is always injective! Hence over an infinite field $\mathbb{F}$ the ring epimorphism $\psi : \mathbb{F}[x] \to \mathbb{F}\langle x\rangle$ becomes an *isomorphism*, meaning that the ring $\mathbb{F}[x]$ of polynomials in one indeterminate x and the ring $\mathbb{F}\langle x\rangle$ of the polynomial functions of one variable x are *algebraically indistinguishable*.

Our last example shows that the finite field $\mathbb{Z}_2$ has the property that all its unary functions can be represented as polynomial functions. This property has been called 1-*functional completeness* in a modern research field of *Universal Algebra* and this property and its generalisations for general (universal) algebras have been extensively studied (also by the first author of this textbook) during the last decades.

Example 15.6. Let $\mathbb{F} = \mathbb{Z}_2$. If we denote

$$f_0(x) = 0, \quad f_1(x) = 1, \quad f_2(x) = x, \quad f_3(x) = x + 1,$$

then $\mathbb{Z}_2\langle x\rangle = \{f_0, f_1, f_2, f_3\} = \mathbb{Z}_2{}^{\mathbb{Z}_2}$. Verify it in detail (Exercise 15.5). ■

We remark that the observation presented in the previous example can be nicely generalised as follows.[1]

Example 15.7. A simple counting argument shows that if $\mathbb{F}$ is any finite field, then every function $f : \mathbb{F} \to \mathbb{F}$ is a polynomial function (of degree less than $q := |F|$).

[1] We are indebted to prof. G. Jones for this example.

There are clearly q^q functions $f \in \mathbb{F}^{\mathbb{F}}$. Notice there are also q^q polynomials

$$f(x) = a_0 + a_1x + \cdots + a_{q-1}x^{q-1} \quad (a_0, a_1, \ldots, a_{q-1} \in \mathbb{F}).$$

These polynomials $f(x) \in \mathbb{F}[x]$ induce (determine) mutually distinct functions $f : \mathbb{F} \to \mathbb{F}$: for otherwise, $f = f'$ for $f(x) = a_0 + a_1x + \cdots + a_{q-1}x^{q-1}$, $f'(x) = a_0{}' + a_1{}'x + \cdots + a_{q-1}{}'x^{q-1}$ would mean that $f(t) = f'(t)$ for all $t \in \mathbb{F}$, whence

$$0 = (f - f')(t) = (a_0 - a_0{}') + (a_1 - a_1{}')t + \cdots + (a_{q-1} - a_{q-1}{}')t^{q-1}$$

for all $t \in \mathbb{F}$. However, a polynomial function $f - f' \in \mathbb{F}\langle x\rangle$ of degree less than q cannot have q roots. (The last claim will be proved in Theorem 18.5.) ■

Exercises.

Exercise 15.1. Write the polynomial

$$f(x) = (2x + i\sqrt{3})^2(3x - i\sqrt{2})^2 - (2x - i\sqrt{3})^2(3x + i\sqrt{2})^2$$

in one indeterminate x over the field $\mathbb{C}$ in its monic (normal) form.

Exercise 15.2. Find polynomial functions $f, g \in \mathbb{C}\langle x\rangle$ of the least possible degrees such that

(a) $f(-1) = 6, \quad f(0) = 5, \quad f(1) = 4, \quad f(2) = 9;$

(b) $g(0) = 1 - i, \quad g(1 + i) = 1 + i, \quad g(1 - i) = 3 - i.$

Exercise 15.3. Find out which of the following polynomial functions of one variable over the field $\mathbb{Z}_3$ are equal: $f_1(x) = x^2 + x$, $f_2(x) = x^3 + x^2$, $f_3(x) = x^4 + 2x + 2$, $f_4(x) = 1$, $f_5(x) = x^4 + 2x^3 + x + 2$, $f_6(x) = x^3 + 2x + 1$.

Exercise 15.4. Let $f(x) = 3x^4 + 5x^3 + 2x^2 + 3x + 4, \quad g(x) = 2x^3 + 5x^2 + x + 2$ be polynomials. Find the sum $f(x) + g(x)$ and the product $f(x) \cdot g(x)$ in cases where $f(x)$, $g(x)$ belong to: (a) $\mathbb{R}[x]$, (b) $\mathbb{Z}_7[x]$, (c) $\mathbb{Z}_6[x]$.

Exercise 15.5. Show that each mapping $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ is a polynomial function.

Exercise 15.6. Write down all polynomials of the ring $\mathbb{Z}_2[x]$ of degree at most three. How many polynomials of degree at most k ($k \in \mathbb{N}^+$) can exist?

16 Divisibility of polynomials

In this chapter we study the divisibility of polynomials in one indeterminate over a field $\mathbb{F}$. Many of the statements we present here and their proofs are analogous to those concerning the divisibility of integers. We start with the fundamental theorem regarding the divisibility of polynomials with remainder.

Theorem 16.1. *Let $\mathbb{F}$ be a field, $f(x)$, $g(x) \in \mathbb{F}[x]$, $g(x) \neq 0$. Then there is a unique pair of polynomials $q(x)$ (the quotient) and $r(x)$ (the remainder) in $\mathbb{F}[x]$ such that*

$$f(x) = g(x) \cdot q(x) + r(x), \qquad \text{where } r(x) = 0 \text{ or } \deg r(x) < \deg g(x). \tag{34}$$

Proof. We start with proving *the existence* of the quotient and the remainder. If $f(x) = 0$ or $\deg f(x) < \deg g(x)$, then $q(x) = 0$ and $r(x) = f(x)$. Let us assume now that $\deg f(x) \geq \deg g(x)$. We shall proceed by induction on the degree of the polynomial $f(x)$. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$.

(a) If $n = 0$, then $f(x) = a \in \mathbb{F}$, $g(x) = b \in \mathbb{F}$ (as $\deg g(x) \leq \deg f(x)$). Then $q(x) = a \cdot b^{-1}$ and $r(x) = 0$, so the assertion holds.

(b) Let $q(x)$, $r(x)$ exist in case $\deg f(x) < n$ where $n \geq 1$ and let $g(x) = b_m x^m + \cdots + b_1 x + b_0$. Let us define the polynomial $f_1(x)$ as follows:

$$f_1(x) := f(x) - a_n \cdot b_m^{-1} \cdot g(x) \cdot x^{n-m}. \tag{35}$$

Because $\deg f_1(x) < n$, by the induction hypothesis there exist polynomials $q_1(x)$, $r(x)$, for which

$$f_1(x) = g(x) \cdot q_1(x) + r(x), \qquad \text{where } r(x) = 0 \text{ or } \deg r(x) < \deg g(x). \tag{36}$$

After substituting from (36) into (35) and an adjustment we obtain

$$f(x) = g(x) \cdot (q_1(x) + a_n \cdot b_m^{-1} \cdot x^{n-m}) + r(x).$$

If we denote $q(x) := q_1(x) + a_n \cdot b_m^{-1} \cdot x^{n-m}$, we get the equality (34).

We continue with proving *the uniqueness* of the quotient and the remainder. If $\deg f(x) < \deg g(x)$ or $f(x) = 0$, then the uniqueness is obvious. Let now $\deg f(x) \geq \deg g(x)$ and let us have two divisions of $f(x)$ by $g(x)$:

$$f(x) = g(x) \cdot q_1(x) + r_1(x), \qquad \text{where } r_1(x) = 0 \text{ or } \deg r_1(x) < \deg g(x) = m,$$
$$f(x) = g(x) \cdot q_2(x) + r_2(x), \qquad \text{where } r_2(x) = 0 \text{ or } \deg r_2(x) < \deg g(x) = m.$$

Then

$$g(x) \cdot (q_1(x) - q_2(x)) = r_2(x) - r_1(x)$$

where $r_2(x) - r_1(x) = 0$ or $\deg(r_2(x) - r_1(x)) < m$. If $q_1(x) - q_2(x) \neq 0$, then $\deg(g(x) \cdot (q_1(x) - q_2(x))) \geq m$, a contradiction. Therefore $q_1(x) = q_2(x)$, from which it follows that also $r_1(x) = r_2(x)$. So both divisions are the same. □

The polynomial $r(x)$ in (34) is called the *remainder* when dividing the polynomial $f(x)$ by the polynomial $g(x)$, and the polynomial $q(x)$ is called the *quotient*.

In a concrete calculation we always find the quotient $q(x)$ for which the difference $f(x) - g(x) \cdot q(x)$ is the remainder $r(x)$ which is either the zero polynomial or $\deg r(x) < \deg g(x)$. In practice in the process of finding $q(x)$ and $r(x)$ we gradually subtract suitable multiples of the divisor $g(x)$ from $f(x)$ (notice (35) in the proof of the previous theorem) until the degree of the difference (the remainder) is less than the degree of the polynomial $g(x)$. To illustrate it, look at the procedure in the following example.

Example 16.2. Consider the following two polynomials over the field $\mathbb{R}$:

$$f(x) = 2x^5 - 6x^4 + 3x^3 - 3x^2 - 3x + 2, \quad g(x) = 2x^3 + 2x + 1.$$

We determine the quotient $q(x)$ and the remainder $r(x)$ when dividing the polynomial $f(x)$ by the polynomial $g(x)$.

$$\begin{array}{rrrrrr|l}
(2x^5 & -6x^4 & +3x^3 & -3x^2 & -3x & +2) & : (2x^3 + 2x + 1) = x^2 - 3x + \frac{1}{2} \\
-(2x^5 & & +2x^3 & +x^2) & & & \\
\hline
& -6x^4 & +x^3 & -4x^2 & -3x & +2 & \\
& -(-6x^4 & & -6x^2 & -3x) & & \\
\hline
& & x^3 & +2x^2 & & +2 & \\
& & -(x^3 & & +x & +\frac{1}{2}) & \\
\hline
& & & 2x^2 & -x & +\frac{3}{2} &
\end{array}$$

Hence

$$q(x) = x^2 - 3x + \frac{1}{2}, \quad r(x) = 2x^2 - x + \frac{3}{2}.$$

■

Now we come to the main concept of this chapter.

Definition 16.3. Let $f(x)$, $g(x)$ be polynomials in one indeterminate over a field $\mathbb{F}$. We say that $\mathbf{g(x)}$ **divides** $\mathbf{f(x)}$ (in the ring $\mathbb{F}[x]$) and we write $g(x) \mid f(x)$ if there is a polynomial $q(x) \in \mathbb{F}[x]$ such that $f(x) = g(x) \cdot q(x)$.

We leave it to the reader to verify the following statements (similar to those for divisibility of integers).

Proposition 16.4. *Let $\mathbb{F}$ be a field and let $f(x)$, $g(x)$, $h(x) \in \mathbb{F}[x]$. Then*

(a) $1 \mid f(x)$, $f(x) \mid 0$ *and* $f(x) \mid f(x)$ *for all* $f(x) \in \mathbb{F}[x]$;

(b) if $h(x) \mid g(x)$, $g(x) \mid f(x)$, *then* $h(x) \mid f(x)$;

(c) if $h(x) \mid f(x)$, $h(x) \mid g(x)$, *then* $h(x) \mid u(x) \cdot f(x) + v(x) \cdot g(x)$ *for arbitrary* $u(x), v(x) \in \mathbb{F}[x]$.

We say that polynomials $f(x)$, $g(x)$ in one indeterminate over a field $\mathbb{F}$ are *associate* and write $f(x) \sim g(x)$, if $f(x) \mid g(x)$ and $g(x) \mid f(x)$. The next proposition characterises this property.

Proposition 16.5. *Let $f(x)$, $g(x)$ be polynomials in one indeterminate over a field $\mathbb{F}$. Then $f(x) \sim g(x)$ if and only if there is a non-zero element $c \in \mathbb{F}$ (i.e. a polynomial of zero degree) such that $f(x) = c \cdot g(x)$.*

Proof. Let $f(x) \sim g(x)$. If $f(x) = 0$, then also $g(x) = 0$ and $0 = c \cdot 0$ for any $c \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$. Let now $f(x) \neq 0$. Then (since $f(x) \sim g(x)$) $g(x) = f(x) \cdot h_1(x)$, $f(x) = g(x) \cdot h_2(x)$ for some $h_1(x), h_2(x) \in \mathbb{F}[x]$. After substitution we obtain $f(x) = f(x) \cdot h_1(x) \cdot h_2(x)$, which yields (due to the cancellation laws in integral domains) $h_1(x) \cdot h_2(x) = 1$, which means that $\deg h_1(x) = \deg h_2(x) = 0$, and thus the polynomials $h_1(x)$, $h_2(x)$ are elements of the field $\mathbb{F}$.

Conversely, let $f(x) = c \cdot g(x)$ for some $c \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$. Then $g(x) \mid f(x)$. Since $c \neq 0_{\mathbb{F}}$ and $\mathbb{F}$ is a field, we have $c^{-1} \cdot f(x) = c^{-1} \cdot c \cdot g(x)$. Hence $g(x) = c^{-1} \cdot f(x)$, which means that also $f(x) \mid g(x)$. □

Example 16.6. The polynomial $(-1 + 2i)x^2 + (1 + i)x - 2 + 3i$ and the polynomial $(2 + i)x^2 + (1 - i)x + 3 + 2i$ are associate in $\mathbb{C}[x]$ as

$$(-1 + 2i)x^2 + (1 + i)x - 2 + 3i = i \cdot ((2 + i)x^2 + (1 - i)x + 3 + 2i).$$

■

We are ready to define an important concept of the *greatest common divisor* of two polynomials.

Definition 16.7. Let $f(x)$, $g(x)$, $d(x)$ be polynomials in one indeterminate over a field $\mathbb{F}$. The polynomial $d(x)$ is called the **greatest common divisor** of the polynomials $f(x)$, $g(x)$ (in the ring $\mathbb{F}[x]$) if

(a) $d(x) \mid f(x)$, $d(x) \mid g(x)$;

(b) if $h(x) \mid f(x)$, $h(x) \mid g(x)$ for $h(x) \in \mathbb{F}[x]$, then $h(x) \mid d(x)$.

Analogously we define the concept of the *least common multiple* of two polynomials.

Definition 16.8. Let $f(x)$, $g(x)$, $m(x)$ be polynomials in one indeterminate over a field $\mathbb{F}$. The polynomial $m(x)$ is called the **least common multiple** of the polynomials $f(x)$, $g(x)$ (in the ring $\mathbb{F}[x]$) if

(a) $f(x) \mid m(x)$, $g(x) \mid m(x)$;

(b) if $f(x) \mid h(x)$, $g(x) \mid h(x)$ for $h(x) \in \mathbb{F}[x]$, then $m(x) \mid h(x)$.

The previous two definitions can be generalised for an arbitrary finite number of polynomials. The following statement can be interpreted as saying that the greatest common divisor of polynomials is (up to the identification via the relation $\sim$) unique.

Proposition 16.9. *Let $d(x) \in \mathbb{F}[x]$ be the greatest common divisor of polynomials $f(x)$, $g(x) \in \mathbb{F}[x]$. Then $h(x) \in \mathbb{F}[x]$ is the greatest common divisor of the polynomials $f(x)$, $g(x)$ if and only if $d(x) \sim h(x)$.*

Proof. Let $h(x)$ be (an another) greatest common divisor of the polynomials $f(x), g(x)$. Then since the greatest common divisor is a divisor, we have $d(x) \mid h(x)$, $h(x) \mid d(x)$, whence $d(x) \sim h(x)$.

Conversely, let $d(x) \sim h(x)$. Then $h(x) \mid f(x)$, $h(x) \mid g(x)$ (as $h(x) \mid d(x)$ and $d(x) \mid f(x)$, $d(x) \mid g(x)$), thus the condition (a) from Definition 16.7 is satisfied.

Let now $q(x) \mid f(x)$, $q(x) \mid g(x)$ for $q(x) \in \mathbb{F}[x]$. Then $q(x) \mid d(x)$ and since $d(x) \sim h(x)$, also $q(x) \mid h(x)$. Hence the condition (b) from Definition 16.7 is satisfied, too. □

Obviously, an arbitrary non-zero polynomial $g(x) = b_n x^n + \cdots + a_0$ is associate with exactly one monic polynomial $b_n^{-1} \cdot g(x)$. So if polynomials $f(x)$ and $g(x)$ of degree n with respective leading coefficients a_n and b_n are

associate, then $a_n^{-1} \cdot f(x) = b_n^{-1} \cdot g(x)$. Often polynomials which are associate are identified and instead of the symbol $\sim$ is simply used the equality symbol $=$.

The greatest common divisor $d(x)$ of polynomials $f(x)$, $g(x)$ is usually denoted by $d(x) = \gcd(f(x), g(x))$, hence this symbol denotes *any* of the greatest common divisors of the polynomials $f(x)$, $g(x)$. By the symbol $(f(x), g(x))$ we shall denote the monic greatest common divisor of the polynomials $f(x)$, $g(x)$. If $(f(x), g(x)) = 1$, we shall say that the polynomials $f(x)$, $g(x)$ are *coprime*.

When searching for the greatest common divisor of polynomials, the following two lemmas prove useful. Their proofs are left for the reader as an easy exercise.

Lemma 16.10. *Let $f(x), g(x)$ be polynomials in one indeterminate over a field $\mathbb{F}$ and let $a, b \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$. Then*

(a) $\gcd(f(x), g(x)) \sim \gcd(a \cdot f(x), b \cdot g(x))$, *whence* $(f(x), g(x)) = (a \cdot f(x), b \cdot g(x)))$;

(b) $\gcd(f(x), a) \sim a \sim 1$, *so* $(f(x), a) = 1$.

Lemma 16.11. *If $f(x) = g(x) \cdot q(x) + r(x)$ for some $q(x), r(x) \in \mathbb{F}[x]$, then*

$$\gcd(f(x), g(x)) \sim \gcd(g(x), r(x)), \text{ so } (f(x), g(x)) = (g(x), r(x))).$$

To calculate the greatest common divisor of two polynomials, there is a method called *Euclid's algorithm* since it mimics the Euclid ancient method of finding the greatest common divisor of two non-zero integers. We shall now describe this method.

Let $f(x)$, $g(x)$ be non-zero polynomials in one indeterminate over a field $\mathbb{F}$. Then, by Theorem 16.1, there exists a unique pair of polynomials $q_1(x), r_1(x)$ over $\mathbb{F}$ (resulting from the first division) such that

$$f(x) = g(x) \cdot q_1(x) + r_1(x), \quad \text{where } r_1(x) = 0 \text{ or } \deg r_1(x) < \deg g(x).$$

If $r_1(x) \neq 0$ then analogously there is a unique pair of polynomials $q_2(x), r_2(x)$ over $\mathbb{F}$ (resulting from the second division) such that

$$g(x) = r_1(x) \cdot q_2(x) + r_2(x), \quad \text{where } r_2(x) = 0 \text{ or } \deg r_2(x) < \deg r_1(x).$$

We can proceed like this further. Because the numbers

$$\deg g(x), \ \deg r_1(x), \ \deg r_2(x), \ldots$$

form a decreasing sequence of non-negative integers, after finitely many steps of our procedure some remainder, let us denote it $r_n(x)$, must become zero. Hence we have the following system of equations:

$$\begin{aligned}
f(x) &= g(x)\cdot q_1(x) + r_1(x), & \deg r_1(x) &< \deg g(x),\\
g(x) &= r_1(x)\cdot q_2(x) + r_2(x), & \deg r_2(x) &< \deg r_1(x),\\
r_1(x) &= r_2(x)\cdot q_3(x) + r_3(x), & \deg r_3(x) &< \deg r_2(x),\\
&\vdots & &\vdots\\
r_{n-3}(x) &= r_{n-2}(x)\cdot q_{n-1}(x) + r_{n-1}(x), & \deg r_{n-1}(x) &< \deg r_{n-2}(x),\\
r_{n-2}(x) &= r_{n-1}(x)\cdot q_n(x).
\end{aligned}$$

Since $r_{n-1}(x) \mid r_{n-2}(x)$, we have $\gcd(r_{n-1}(x), r_{n-2}(x)) \sim r_{n-1}(x)$ and from Lemma 16.11 we then gradually obtain

$$\gcd(f(x), g(x)) \sim \gcd(g(x), r_1(x)) \sim \cdots \sim \gcd(r_{n-2}(x), r_{n-1}(x)) \sim r_{n-1}(x).$$

Hence the greatest common divisor of two polynomials is *the last non-zero remainder* in the Euclid algorithm.

Theorem 16.12. *Let $f(x)$, $g(x)$ be polynomials in one indeterminate over a field $\mathbb{F}$. Then there are polynomials $u(x), v(x) \in \mathbb{F}[x]$ such that*

$$(f(x), g(x)) = u(x)\cdot f(x) + v(x)\cdot g(x).$$

Proof. In case $f(x) = 0$ or $g(x) = 0$ the validity of the statement is obvious. So let now $f(x)$, $g(x)$ be non-zero polynomials. We proceed by induction on the number of steps in the Euclid algorithm necessary for the calculation of the greatest common divisor of the polynomials $f(x)$, $g(x)$.

1. If only one step is needed, then $f(x) = g(x)\cdot q(x)$ for some $q(x) \in \mathbb{F}[x]$ and then $(f(x), g(x)) = c\cdot g(x) = 0\cdot f(x) + c\cdot g(x)$, where $c \in \mathbb{F}$ is such an element that $c\cdot g(x)$ is a monic polynomial.

2. Let $n > 1$ and let us assume that whenever $n-1$ steps are needed, then the statement is true. Let for $f(x), g(x)$ now n steps be necessary. By Theorem 16.1 we have

$$f(x) = g(x)\cdot q(x) + r(x), \quad \text{where} \quad \deg r(x) < \deg g(x)$$

and by Lemma 16.11 then $(f(x), g(x)) = (g(x), r(x))$, where for the calculation of $(g(x), r(x))$ only $n-1$ steps are needed. Hence by the induction

hypothesis we have $(g(x), r(x)) = v_1(x) \cdot g(x) + u_1(x) \cdot r(x)$. Now by substituting for $r(x)$ we get

$$\begin{aligned}(f(x), g(x)) =&(g(x), r(x)) = v_1(x)g(x) + u_1(x)(f(x) - g(x)q(x)) = \\ =&u_1(x)f(x) + (v_1(x) - u_1(x)q(x))g(x) = u(x)f(x) + v(x)g(x)\end{aligned}$$

as required where $u(x) := u_1(x)$ and $v(x) := v_1(x) - u_1(x) \cdot q(x)$. □

Example 16.13. We illustrate the Euclid algorithm for finding the greatest common divisor of two polynomials as well as Theorem 16.12 for the polynomials $f(x) = x^5 - x^2 - x - 1$ and $g(x) = 2x^4 - x^3 + 3x^2 - x + 1$ considered over the field $\mathbb{R}$.

We shall use the fact that (see Lemma 16.10) the polynomials $\gcd(f(x), g(x))$ and $\gcd(2f(x), g(x))$ are associate.

$$\begin{array}{llll} (2x^5 & -2x^2 & -2x-2) : (2x^4 - x^3 + 3x^2 - x + 1) = x + \frac{1}{2} \\ -(2x^5 - x^4 & +3x^3 - x^2 & +x) & \\ \hline + x^4 & -3x^3 - x^2 & -3x - 2 & \\ -(x^4 & -\frac{1}{2}x^3 + \frac{3}{2}x^2 & -\frac{1}{2}x + \frac{1}{2}) & \\ \hline & -\frac{5}{2}x^3 - \frac{5}{2}x^2 & -\frac{5}{2}x - \frac{5}{2} & \end{array}$$

Hence the first division in the Euclid algorithm is

$$2x^5 - 2x^2 - 2x - 2 = (2x^4 - x^3 + 3x^2 - x + 1) \cdot (x + \frac{1}{2}) + (-\frac{5}{2}x^3 - \frac{5}{2}x^2 - \frac{5}{2}x - \frac{5}{2}) \quad (*)$$

with the remainder $r_1(x) = -\frac{5}{2}x^3 - \frac{5}{2}x^2 - \frac{5}{2}x - \frac{5}{2}$, and by Lemmas 16.10 and 16.11 we have $\gcd(f(x), g(x)) \sim \gcd(2f(x), g(x)) \sim \gcd(g(x), r_1(x))$.

We again use that (see Lemma 16.10) $\gcd(g(x), r_1(x)) \sim \gcd(g(x), -\frac{2}{5}r_1(x))$, where $-\frac{2}{5}r_1(x) = x^3 + x^2 + x + 1$. Thus in the second division we divide the

polynomial $g(x)$ by the polynomial $x^3 + x^2 + x + 1$.

$$\begin{array}{rrrl} (2x^4 - x^3 & +3x^2 - x & +1) : (x^3 + x^2 + x + 1) = 2x - 3 \\ -(2x^4 + 2x^3 & +2x^2 + 2x) & \\ \hline \\ - 3x^3 & +x^2 - 3x & +1 \\ -(-3x^3 & -3x^2 - 3x & -3) \\ \hline \\ & 4x^2 & +4 \end{array}$$

Hence the second division is

$$2x^4 - x^3 + 3x^2 - x + 1 = (x^3 + x^2 + x + 1) \cdot (2x - 3) + (4x^2 + 4) \qquad (**)$$

with the remainder $r_2(x) = 4x^2 + 4$, and by Lemmas 16.10 and 16.11 we have $\gcd(f(x), g(x)) \sim \gcd(g(x), r_1(x)) \sim \gcd(g(x), -\frac{2}{5}r_1(x)) \sim \gcd(r_1(x), \frac{1}{4}r_2(x))$, where $\frac{1}{4}r_2(x) = x^2 + 1$. Thus in the third division we divide the polynomial $r_1(x)$ by the polynomial $x^2 + 1$.

$$\begin{array}{rrrl} (x^3 & +x^2 & +x & +1) : (x^2 + 1) = x + 1 \\ -(x^3 & & +x) & \\ \hline \\ & x^2 & & +1 \\ & -(x^2 & & +1) \\ \hline \\ & & & 0 \end{array}$$

Hence the third division is

$$x^3 + x^2 + x + 1 = (x^2 + 1) \cdot (x + 1) + 0 \qquad (***)$$

with the remainder 0, and by Lemmas 16.10 and 16.11 we have

$$\gcd(f(x), g(x)) \sim \gcd(g(x), r_1(x)) \sim \gcd(g(x), -\frac{2}{5}r_1(x)) \sim$$
$$\gcd(r_1(x), \frac{1}{4}r_2(x)) \sim \gcd(\frac{1}{4}r_2(x), 0) \sim x^2 + 1.$$

Thus the polynomial $x^2 + 1$ as the last non-zero remainder in the Euclid algorithm is the demanded greatest common divisor of the polynomials $f(x)$ and $g(x)$.

Now we illustrate how to express the greatest common divisor of the polynomials $f(x)$ and $g(x)$ in the form presented in Theorem 16.12. We shall firstly use the division (**) to substitute for the remainder $r_2(x) = 4x^2 + 4$ and then we use the division (*) to substitute for the remainder $r_1(x) = -\frac{5}{2}x^3 - \frac{5}{2}x^2 - \frac{5}{2}x - \frac{5}{2}$:

$$\begin{aligned}
\gcd(f(x), g(x)) &= x^2 + 1 \\
&= \frac{1}{4} \cdot (4x^2 + 4) \\
&= \frac{1}{4} \cdot [2x^4 - x^3 + 3x^2 - x + 1 - (x^3 + x^2 + x + 1) \cdot (2x - 3)] \\
&= \frac{1}{4} \cdot [g(x) - \frac{2}{5} r_1(x) \cdot (2x - 3)] \\
&= \frac{1}{4} \cdot g(x) - \frac{1}{10}[(2x^5 - 2x^2 - 2x - 2) - g(x) \cdot (x + \frac{1}{2})] \cdot (2x - 3) \\
&= \frac{1}{4} \cdot g(x) - \frac{1}{10} 2f(x) \cdot (2x - 3) + \frac{1}{10} g(x) \cdot (x + \frac{1}{2}) \cdot (2x - 3) \\
&= (-\frac{2}{5}x + \frac{3}{5}) \cdot f(x) + (\frac{1}{5}x^2 - \frac{1}{5}x + \frac{1}{10}) \cdot g(x) \\
&= u(x) \cdot f(x) + v(x) \cdot g(x),
\end{aligned}$$

where $u(x) = -\frac{2}{5}x + \frac{3}{5}$ and $v(x) = \frac{1}{5}x^2 - \frac{1}{5}x + \frac{1}{10}$. ■

Exercises.

Exercise 16.1. Find the quotient and the remainder when dividing the polynomial $f(x)$ by the polynomial $g(x)$ over the field $\mathbb{C}$:

(a) $f(x) = x^4 + x^3 - 5x^2 + x - 6, \quad g(x) = x^3 - 8x^2 + x - 8;$

(b) $f(x) = x^3 - 8x^2 + x - 7, \quad g(x) = x^2 + 1;$

(c) $f(x) = x^5 + 15x^2 - 31x + 15, \quad g(x) = x^2 + 2x - 3;$

(d) $f(x) = x^5 + 2ix^4 + (3 - i)x^3 + 2ix^2 - 4x - 6i, \quad g(x) = x^2 + 2ix - 3;$

(e) $f(x) = 5x^6 + 4x^5 + 3x^2 + 2x + 1, \quad g(x) = 7x^4 + 2x^2 - 3x + 2.$

Exercise 16.2. Find the quotient and the remainder when dividing the polynomial $f(x)$ by the polynomial $g(x)$ over the field $\mathbb{Z}_5$:

(a) $f(x) = 4x^3 + x^2 + x + 3, \quad g(x) = 2x + 1;$

(b) $f(x) = x^5 + 2x^4 + 4x^3 + x^2 + 2x + 2, \quad g(x) = 3x^3 + 2x + 1;$

(c) $f(x) = x^5 + 3x^3 + 4x^2 + 3, \quad g(x) = x^3 + 2x^2 + 4x + 1;$

(d) $f(x) = 4x^3 + 4, \quad g(x) = 2x^2 + 3x + 2.$

Exercise 16.3. Determine $a, b \in \mathbb{R}$ such that $g(x) \mid f(x)$ in the ring $\mathbb{R}[x]$:

(a) $f(x) = 6x^5 + 11x^4 + 5x^3 + 5x^2 + ax + b, \quad g(x) = x^2 + 1;$

(b) $f(x) = x^3 + 8x^2 + 5x + a, \quad g(x) = x^2 + 3x + b.$

Exercise 16.4. Find $a, b, c \in \mathbb{Z}$ such that the polynomial $f(x)$ is divisible by the polynomial $g(x)$:

(a) $f(x) = x^3 + 2x^2 + ax - 3, \quad g(x) = x^2 + bx + c;$

(b) $f(x) = x^3 + ax^2 + 3x + b, \quad g(x) = x^2 + cx + 2.$

Exercise 16.5. Find $\gcd(f(x), g(x))$ over the field $\mathbb{Q}$:

(a) $f(x) = x^4 + x^3 - 5x^2 + x - 6, \quad g(x) = x^3 - 8x^2 + x - 8;$

(b) $f(x) = x^5 + 1, \quad g(x) = x^2 + 1;$

(c) $f(x) = x^4 + x^3 - 3x^2 - 4x - 1, \quad g(x) = x^3 + x^2 - x - 1;$

(d) $f(x) = x^6 + 3x^5 + 3x^4 + 3x^3 + 4x^2 + 6x + 4, \quad g(x) = x^4 + x^3 - 3x^2 - x + 2;$

(e) $f(x) = x^5 - 2x^4 + x^3 + 7x^2 - 12x + 10, \quad g(x) = 3x^4 - 6x^3 + 5x^2 + 2x - 2.$

Exercise 16.6. Find $\gcd(f(x), g(x))$ over the field $\mathbb{Z}_5$:

(a) $f(x) = x^4 + 4x^3 + 1, \quad g(x) = x^3 + 3x^2 + 1;$

(b) $f(x) = x^4 + x^3 + 2x^2 + x + 4, \quad g(x) = x^3 + x^2 + 4x + 4.$

Exercise 16.7. Find a condition for $a, b \in \mathbb{R}$ such that $\gcd(f(x), g(x))$ is a polynomial of at least degree 1 provided $f(x) = 3x^3 + 3ax + 3b, g(x) = 3x^2 + a.$

17 Decompositions of polynomials

The Fundamental Theorem of Arithmetic says that every $n \in N, n \geq 2$ can be decomposed into a product of prime factors and that this decomposition is unique up to the order of factors. In this chapter we derive an analogue of this theorem for polynomials in one indeterminate over a field $\mathbb{F}$.

In arithmetic *trivial divisors* of $n \in N^+$ are the number 1 and n itself. The next definition gives an analogue for polynomials.

Definition 17.1. Let $f(x), g(x)$ be polynomials in one indeterminate over a field $\mathbb{F}$. The polynomial $g(x)$ is called a **trivial divisor** of the polynomial $f(x)$ (in the ring $\mathbb{F}[x]$) if $\deg g(x) = 0$ or $g(x) \sim f(x)$.

Again, in arithmetic numbers $n \in N, n \geq 2$ having only trivial divisors are the *prime* numbers while numbers having also non-trivial divisors are *compound* numbers. Analogues for polynomials are the *irreducible* and the *reducible* polynomials, respectively.

Definition 17.2. Let $f(x)$ be a polynomial in one indeterminate over a field $\mathbb{F}$ of degree at least 1. The polynomial $f(x)$ is said to be **irreducible** (in the ring $\mathbb{F}[x]$) if $f(x)$ has in $\mathbb{F}[x]$ only trivial divisors. Otherwise $f(x)$ is called a **reducible** polynomial (in the ring $\mathbb{F}[x]$).

Hence if a polynomial $f(x)$ is reducible in $\mathbb{F}[x]$, there exist polynomials $g(x)$, $q(x)$ whose degrees are smaller than $\deg f(x)$ and $f(x) = g(x) \cdot q(x)$. The reader will recognize that the next lemma is an analogue of a well-known statement from arithmetic.

Lemma 17.3. *Let $p(x), f(x), g(x)$ be polynomials in one indeterminate over a field $\mathbb{F}$. If the polynomial $p(x)$ is irreducible and $p(x) \mid f(x) \cdot g(x)$, then $p(x) \mid f(x)$ or $p(x) \mid g(x)$.*

Proof. If $p(x)$ is irreducible , then the greatest common divisor of the polynomials $p(x)$, $f(x)$ is either $p(x)$ or 1. In the first case $p(x) \mid f(x)$, in the second case, by Theorem 16.12, $1 = u(x) \cdot p(x) + v(x) \cdot f(x)$ for some $u(x), v(x) \in \mathbb{F}[x]$. After multiplying both sides of this equality by the polynomial $g(x)$ we obtain

$$g(x) = u(x) \cdot p(x) \cdot g(x) + v(x) \cdot f(x) \cdot g(x),$$

from which it follows that $p(x) \mid g(x)$. □

Now we present the promised analogue of The Fundamental Theorem of Arithmetic for polynomials in one indeterminate over a field $\mathbb{F}$.

Theorem 17.4. *Every polynomial $f(x) \in \mathbb{F}[x]$ of degree at least 1 over a field $\mathbb{F}$ can be decomposed into a product of irreducible polynomials, and this product is unique up to the order of the factors and their substitution by their associate polynomials.*

Proof. We proceed by induction on the degree n of the polynomial $f(x)$.

1. For $n = 1$ we have that the polynomial $f(x)$ is irreducible and so its decomposition is unique.

2. Assume that $n \geq 2$ and the statement holds for every polynomial of degree less than n. Let $f(x)$ be a polynomial of degree n. If it is irreducible, then $f(x) = f(x)$ is the required 'decomposition' of $f(x)$ into irreducible polynomials. If $f(x)$ is reducible, then there are polynomials $h(x)$, $g(x)$ with $\deg h(x) < n, \deg g(x) < n$ such that $f(x) = h(x) \cdot g(x)$. By the induction hypothesis there are decompositions

$$h(x) = p_1(x) \cdot \cdots \cdot p_k(x), \quad g(x) = q_1(x) \cdot \cdots \cdot q_l(x),$$

where $p_i(x)$ for $i \in \{1, \ldots, k\}$ and $q_j(x)$ for $j \in \{1, \ldots, l\}$ are irreducible polynomials. From that we have

$$f(x) = p_1(x) \cdot \cdots \cdot p_k(x) \cdot q_1(x) \cdot \cdots \cdot q_l(x).$$

It remains to prove the uniqueness of this decomposition. We again can proceed by induction on the number of irreducible factors. For one factor the statement is true. We assume that every polynomial that is the product of less than n irreducible factors has a unique decomposition ($n \geq 2$). Let us consider the decompositions into irreducible polynomials

$$p_1(x) \cdot \cdots \cdot p_{n-1}(x) \cdot p_n(x) = f(x) = q_1(x) \cdot \cdots \cdot q_m(x).$$

The irreducible polynomial $p_n(x)$ divides the left-hand side of this equality, so it divides the right-hand side. Consequently, by Lemma 17.3, it must divide some of the factors on the right-hand side, e.g. $q_j(x)$. Since $p_n(x)$, $q_j(x)$ are irreducible, we get $p_n(x) \sim q_j(x)$, whence $q_j(x) = c \cdot p_n(x)$ for some $c \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$. After substitution and cancellation we obtain

$$p_1(x) \cdot \cdots \cdot p_{n-1}(x) = c \cdot q_1(x) \cdot \cdots \cdot q_{j-1}(x) \cdot q_{j+1}(x) \cdot \cdots \cdot q_m(x).$$

We now can use the induction hypothesis and this completes the proof. □

By this theorem, every polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$ can be written in a unique (up to the order of the factors and their substitution by their associate polynomials) form

$$f(x) = q_1(x) \cdot q_2(x) \cdot \cdots \cdot q_m(x), \tag{37}$$

where $q_1(x), \ldots, q_m(x)$ are irreducible polynomials. Every polynomial $q_i(x)$ is associate with a unique monic polynomial $p_i(x)$, $i \in \{1, \ldots, m\}$. Hence for every $i \in \{1, \ldots, m\}$ we have $q_i(x) = c_i \cdot p_i(x)$ where $c_i \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$. After substituting into (37) we obtain

$$f(x) = c_1 \cdot \cdots \cdot c_m \cdot p_1(x) \cdot \cdots \cdot p_m(x). \tag{38}$$

The product of monic polynomials is again a monic polynomial and we have $c_1 \cdot \cdots \cdot c_m = a_n$. This and Theorem 17.4 yield the following statement.

Corollary 17.5. *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial of degree at least 1 over a field $\mathbb{F}$. Then there are monic irreducible polynomials $p_1(x), \ldots, p_m(x)$ such that*

$$f(x) = a_n \cdot p_1(x) \cdot \cdots \cdot p_m(x). \tag{39}$$

The decomposition (39) is unique up to the order of the factors.

It is possible that some factors are repeated in the product (39) (i.e. in the product (37) some factors are associate). In such case the product (39) can be adjusted and written in the form

$$f(x) = a_n \cdot p_1(x)^{\alpha_1} \cdot \cdots \cdot p_r(x)^{\alpha_r}, \tag{40}$$

where $p_1(x), \ldots, p_r(x)$ are pairwise distinct monic irreducible polynomials and $\alpha_1, \ldots, \alpha_r \in N^+$. The form (40) is called the *canonical decomposition* of the polynomial $f(x)$ (in the ring $\mathbb{F}[x]$). If we allow zero exponents in the decomposition (40), then we talk about a *generalised decomposition* of the polynomial $f(x)$.

The existence of canonical decompositions of polynomials leads to the following (theoretical) criterion of divisibility of one polynomial by the other.

Theorem 17.6. *Let $f(x) = a \cdot p_1(x)^{\alpha_1} \cdot \cdots \cdot p_n(x)^{\alpha_n}$ be the canonical decomposition of a polynomial $f(x)$ over a field $\mathbb{F}$. Then a polynomial $g(x)$ divides the polynomial $f(x)$ if and only if the polynomial $g(x)$ can be written in the form*

$$g(x) = b \cdot p_1(x)^{\beta_1} \cdot \cdots \cdot p_n(x)^{\beta_n}, \tag{41}$$

where $0 \leq \beta_i \leq \alpha_i$ for every $i \in \{1, \ldots, n\}$.

Proof. To show the necessity, assume that $g(x) \mid f(x)$. Then there is a polynomial $h(x)$ such that $f(x) = g(x) \cdot h(x)$. If the polynomial $g(x)$ contains (in its decomposition (41)) an irreducible monic factor which is not present in the

canonical decomposition of the polynomial $f(x)$ or $g(x)$ contains some factor in a greater power than is present in the canonical decomposition of the polynomial $f(x)$, then this would contradict the uniqueness of the decomposition of $f(x)$.

Conversely, let $g(x)$ has a decomposition of the form (41). Then

$$\begin{aligned} f(x) &= a \cdot p_1(x)^{\alpha_1} \cdot \dots \cdot p_n(x)^{\alpha_n} \\ &= a \cdot p_1(x)^{\beta_1+\alpha_1-\beta_1} \cdot \dots \cdot p_n(x)^{\beta_n+\alpha_n-\beta_n} \\ &= a \cdot b \cdot b^{-1} \cdot p_1(x)^{\beta_1} \cdot \dots \cdot p_n(x)^{\beta_n} \cdot p_1(x)^{\alpha_1-\beta_1} \cdot \dots \cdot p_n(x)^{\alpha_n-\beta_n} \\ &= b \cdot p_1(x)^{\beta_1} \cdot \dots \cdot p_n(x)^{\beta_n} \cdot a \cdot b^{-1} \cdot p_1(x)^{\alpha_1-\beta_1} \cdot \dots \cdot p_n(x)^{\alpha_n-\beta_n} \\ &= g(x) \cdot h(x), \end{aligned}$$

where we have denoted $h(x) := a \cdot b^{-1} \cdot p_1(x)^{\alpha_1-\beta_1} \cdot \dots \cdot p_n(x)^{\alpha_n-\beta_n}$. Hence we have $g(x) \mid f(x)$. □

Assume that we know the canonical decompositions of polynomials $f(x)$ and $g(x)$. (We warn that finding them might sometimes be hard or even impossible although their existence in theory is guaranteed.) We can then use Theorem 17.6 for finding their greatest common divisor and their least common multiple:

Theorem 17.7. *Assume that*

$$\begin{aligned} f(x) &= a \cdot p_1(x)^{k_1} \cdot \dots \cdot p_n(x)^{k_n}, \\ g(x) &= b \cdot p_1(x)^{l_1} \cdot \dots \cdot p_n(x)^{l_n} \end{aligned}$$

are generalised decompositions of polynomials $f(x)$, $g(x)$ over a field $\mathbb{F}$. Then

$$\gcd(f(x), g(x)) = p_1(x)^{r_1} \cdot \dots \cdot p_n(x)^{r_n}, \quad \textit{where} \quad r_i = \min(k_i, l_i) \tag{42}$$

and

$$\operatorname{lcm}(f(x), g(x)) = p_1(x)^{s_1} \cdot \dots \cdot p_n(x)^{s_n}, \quad \textit{where} \quad s_i = \max(k_i, l_i), \tag{43}$$

for every $i \in \{1, \dots, n\}$.

Proof. By Theorem 17.6, the polynomial on the right-hand side of (42) divides $f(x)$ and $g(x)$, hence condition (a) from Definition 16.7 is satisfied. Let $h(x) \mid f(x)$, $h(x) \mid g(x)$. Then again by Theorem 17.6,

$$h(x) = a \cdot p_1(x)^{t_1} \cdot \dots \cdot p_n(x)^{t_n}, \quad \text{where} \quad 0 \le t_i \le k_i \text{ and } 0 \le t_i \le l_i$$

for every $i \in \{1, \ldots, n\}$. This means that $0 \leq t_i \leq \min(k_i, l_i) = r_i$, hence $h(x) \mid p_1(x)^{r_1} \cdot \cdots \cdot p_n(x)^{r_n}$ and so also condition (b) from Definition 16.7 is satisfied.

One can analogously prove the formula (43). □

Example 17.8. Let

$$f(x) = 2(x-2)^3(x-1)(x^2+1), \quad g(x) = (x-2)^2(x+1)(x^2+1)^2$$

be polynomials over the field $\mathbb{R}$. (One can verify that the given decompositions are canonical.) We shall apply the formulas (42) and (43) to find the greatest common divisor and the least common multiple of the given polynomials.

First we present the polynomials $f(x)$, $g(x)$ in their 'uniform' generalised forms. We have

$$f(x) = 2(x-2)^3(x-1)^1(x+1)^0(x^2+1),$$
$$g(x) = (x-2)^2(x-1)^0(x+1)^1(x^2+1)^2.$$

By applying Theorem 17.7 we now obtain

$$\gcd(f(x), g(x)) = (x-2)^2(x-1)^0(x+1)^0(x^2+1)^1 = (x-2)^2(x^2+1),$$
$$\operatorname{lcm}(f(x), g(x)) = (x-2)^3(x-1)(x+1)(x^2+1)^2.$$

■

Exercises.

Exercise 17.1. Show that the polynomial $x^2 + 4$ is in $\mathbb{R}[x]$ irreducible.

Exercise 17.2. Find in $\mathbb{R}[x]$ the canonical decomposition of the polynomial:

(a) $f(x) = x^4 + 1$;

(b) $g(x) = x^4 - x^2 + 1$.

Exercise 17.3. Using the canonical decompositions find $\gcd(f(x), g(x))$ and $\operatorname{lcm}(f(x), g(x))$ in $\mathbb{R}[x]$ provided $f(x) = x^3 - 8$, $g(x) = x^4 + 2x^3 + 3x^2 - 2x - 4$.

Exercise 17.4. Using the canonical decompositions find $\gcd(f(x), g(x))$ and $\operatorname{lcm}(f(x), g(x))$ in $\mathbb{C}[x]$ provided $f(x) = x^4 + 2x^2 + 1$, $g(x) = x^2 + (1+i)x + i$.

18 Roots of polynomial functions

In this chapter we mainly deal with polynomial functions of one variable over a field $\mathbb{F}$. We shall denote the zero element $0_{\mathbb{F}}$ of the field $\mathbb{F}$ simply 0.

Definition 18.1. Let $f \in \mathbb{F}\langle x\rangle$ be a polynomial function of one variable over a field $\mathbb{F}$. An element $c \in \mathbb{F}$ is called a **root of the polynomial function** f if $f(c) = 0$.

Each root of a polynomial function f is also called a **root of the algebraic equation** $f(x) = 0$ or a **solution** of $f(x) = 0$.

Proposition 18.2. *If a field $\mathbb{F}$ is finite then the ring $\mathbb{F}\langle x\rangle$ has proper divisors of zero.*

Proof. Let $\mathbb{F} = \{a_1, a_2, \ldots, a_n\}$, $n \in \mathbb{N}$ and let us take the polynomials $f(x) = x - a_1$ and $g(x) = (x - a_2)(x - a_3)\ldots(x - a_n)$ in the ring $\mathbb{F}[x]$. Then neither $f = \psi(f(x))$ nor $g = \psi(g(x))$ are zero functions since $f(a_2) = a_2 - a_1 \neq 0$ and $g(a_1) = (a_1 - a_2)\ldots(a_1 - a_n) \neq 0$. But for the polynomial $f(x) \cdot g(x) = (x-a_1)(x-a_2)\ldots(x-a_n)$ its corresponding function $\psi(f(x)\cdot g(x))$ is obviously the zero function. □

The following 'divisibility criterion' for an element of a field to be a root of a given polynomial function is called *Bézout Theorem* and it will be of a primary importance within our subsequent study.

Theorem 18.3 (**Bézout Theorem**). *Let $f \in \mathbb{F}\langle x\rangle$ for a field $\mathbb{F}$. An element $c \in \mathbb{F}$ is a root of the polynomial function f if and only if $x - c$ divides $f(x)$ in $\mathbb{F}[x]$.*

Proof. To prove the necessity, let c be a root of f, thus $f(c) = 0$. By Theorem 16.1, for the polynomials $f(x)$ and $x - c$ in $\mathbb{F}[x]$ there exist polynomials $q(x)$ (the quotient) and $r(x)$ (the remainder) such that

$$f(x) = (x - c)q(x) + r(x), \qquad \text{where } r(x) = 0 \text{ or } \deg r(x) < \deg(x - c).$$

We shall show that the case $r(x) \neq 0$ cannot happen. Indeed, suppose for contradiction that $r(x) \neq 0$. Since $\deg(x - c) = 1$ and $\deg r(x) < \deg(x - c)$, we get $r(x) = z \in \mathbb{F} \setminus \{0\}$. By assumption $0 = f(c) = (c - c)q(c) + z = 0 + z$, whence $z = 0$, a contradiction. Hence indeed for the remainder $r(x)$ we have $r(x) = 0$. This implies $f(x) = (x - c)q(x)$, thus $x - c \mid f(x)$ in $\mathbb{F}[x]$.

To prove the sufficiency, let $x - c \mid f(x)$ in $\mathbb{F}[x]$. Then $f(x) = (x - c)q(x)$ and $f(c) = (0 - 0)q(c) = 0$, whence c is a root of f. □

The proof of the following statement is easy and thus left for the reader.

Lemma 18.4. *Let $f(x)$, $g(x)$, $h(x) \in \mathbb{F}[x]$ be polynomials over a field $\mathbb{F}$ and let $f(x) = g(x) \cdot h(x)$. Then c is a root of the polynomial function $f = \psi(f(x))$ if and only if c is a root of the polynomial function $g = \psi(g(x))$ or c is a root of the polynomial function $h = \psi(h(x))$.*

The next result is an important consequence of Bézout Theorem 18.3 and the previous lemma.

Theorem 18.5. *Let $\mathbb{F}$ be an arbitrary field and let $f(x) \in \mathbb{F}[x]$ be a polynomial of degree n ($n \in \mathbb{N}$). Then the corresponding polynomial function $f \in \mathbb{F}\langle x \rangle$ has in $\mathbb{F}$ at most n roots.*

Proof. We proceed by induction on the degree n of the polynomial $f(x)$.

1. If $n = 0$, then $f(x) = a_0 \neq 0$ and the corresponding polynomial function $f = \psi(f(x))$ has 0 roots. So the statement is true.

2. Assume that the statement is valid for all polynomials $f(x) \in \mathbb{F}[x]$ of degrees $n - 1$ where $n \geq 1$. Let $f(x) \in \mathbb{F}[x]$ be a polynomial of degree n and let $c \in \mathbb{F}$ be a root of the corresponding polynomial function $f = \psi(f(x))$. Then by Bézout Theorem 18.3, $f(x) = (x - c)q(x)$ in $\mathbb{F}[x]$, where $q(x)$ is a polynomial of degree $n - 1$. By the induction hypothesis, the polynomial function $q = \psi(q(x))$ in $\mathbb{F}\langle x \rangle$ corresponding to $q(x)$ has at most $n - 1$ roots. From the previous lemma it follows that the only roots of the polynomial function f are the element c and the roots of the polynomial function q (and no other roots). Hence the polynomial function f has at most n roots. □

The next corollary characterises in (E) the equality of polynomial functions in $\mathbb{F}\langle x \rangle$ over an infinite field $\mathbb{F}$. It says that over infinite fields, like the 'school' fields $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ of rational, real and complex numbers, respectively, two polynomial functions f and g are equal if and only if their corresponding polynomials $f(x)$ and $g(x)$ are equal. This means that they must have the same degree and the same coefficients for each power of x and so they must look the same. (We recall that, as Example 15.4 showed, the situation is different over finite fields.)

Corollary 18.6. *Let $\mathbb{F}$ be an infinite field and let $f(x) = a_0 + a_1 x + \cdots + a_r x^r$, $g(x) = b_0 + b_1 x + \cdots + b_s x^s$ be polynomials in one indeterminate over the field $\mathbb{F}$. Let $f = \psi(f(x))$ and $g = \psi(g(x))$ be the polynomial functions in $\mathbb{F}\langle x \rangle$ corresponding to the polynomials $f(x)$ and $g(x)$. Then*

$$f = g \text{ in } \mathbb{F}\langle x \rangle \quad \textit{iff} \quad r = s \quad \& \quad (\forall i \in \{0, 1, \ldots, r\})\ a_i = b_i. \tag{E}$$

Proof. If $r = s$ and the corresponding coefficients are equal, then obviously for every $t \in \mathbb{F}$ we have $f(t) = g(t)$, which means that $f = g$ in $\mathbb{F}\langle x\rangle$.

Conversely, suppose by contradiction that $f = g$ in $\mathbb{F}\langle x\rangle$ but $r \neq s$ or $a_i \neq b_i$ for some i. Then $f(x) - g(x)$ is a polynomial of degree n for a suitable $n \in \mathbb{N}$ in $\mathbb{F}[x]$ and every element of the field $\mathbb{F}$ is the root of the corresponding polynomial function $f - g = \psi(f(x) - g(x))$ in $\mathbb{F}\langle x\rangle$. Since the field $\mathbb{F}$ is infinite, this contradicts Theorem 18.5. □

Hence if $\mathbb{F}$ is an infinite field, then Corollary 18.6 yields that the mapping $\psi : \mathbb{F}[x] \to \mathbb{F}\langle x\rangle$ is injective and so in such case the rings $\mathbb{F}[x]$ of polynomials and $\mathbb{F}\langle x\rangle$ of polynomial functions are isomorphic, and so can be *algebraically identified*. Therefore over the 'school' fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ it indeed does not matter much if at secondary schools teachers and students talk about polynomials in one indeterminate or they talk about polynomial functions of one variable over these fields.

The calculations of the quotients and remainders when dividing a given polynomial by a polynomial $x - c$ are usually performed via *Horner's scheme* (or *Horner's method*) which is due to **William George Horner**.[1] The calculations via this scheme are based on the following results.

Proposition 18.7. *Let $f(x) \in \mathbb{F}[x]$ be a polynomial over a field $\mathbb{F}$ and let $c \in \mathbb{F}$. Then there exists a polynomial $q(x) \in \mathbb{F}[x]$ such that*

$$f(x) = (x - c)q(x) + f(c).$$

Proof. By Theorem 16.1 we have $f(x) = (x - c)q(x) + z$ for some $z \in \mathbb{F}$ and a polynomial $q(x) \in \mathbb{F}[x]$. For the polynomial function $f = \psi(f(x))$ in $\mathbb{F}\langle x\rangle$ corresponding to $f(x)$ we then obtain $f(c) = (c - c)q(c) + z$, whence $z = f(c)$. □

Corollary 18.8 (Horner's scheme). *Assume that when dividing a polynomial $f(x) = a_n x^n + \cdots + a_0$ by a polynomial $x - c$ over a field $\mathbb{F}$ ($c \in \mathbb{F}$) we*

[1] William George Horner (1786-1837) was a British mathematician. He was a schoolmaster, headmaster and schoolkeeper, proficient in classics as well as mathematics, who wrote extensively on functional equations, number theory and approximation theory, but also on optics. His contribution to approximation theory is honoured in the designation Horner's method, in particular respect of a paper in Philosophical Transactions of the Royal Society of London for 1819. The modern invention of the zoetrope, under the name Daedaleum in 1834, has been attributed to him.

Horner died comparatively young, before the establishment of specialist, regular scientific periodicals. So, the way others have written about him has tended to diverge, sometimes markedly, from his own prolific, if dispersed, record of publications and the contemporary reception of them. [14]

obtain the quotient $q(x) = b_{n-1}x^{n-1} + \cdots + b_1x + b_0$ *and the remainder* $f(c)$. *Then*

$$\begin{aligned} b_{n-1} &= a_n, \\ b_{n-2} &= a_{n-1} + c \cdot b_{n-1}, \\ &\vdots \\ b_0 &= a_1 + c \cdot b_1, \\ f(c) &= a_0 + c \cdot b_0. \end{aligned} \tag{H}$$

Proof. By Proposition 18.7, $f(x) = (x-c)q(x) + f(c)$, hence

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = (x-c)(b_{n-1}x^{n-1} + \cdots + b_1x + b_0) + f(c).$$

From this by comparing the coefficients we get that

$$\begin{aligned} a_n &= b_{n-1}, \\ a_{n-1} &= b_{n-2} - c \cdot b_{n-1}, \\ a_{n-2} &= b_{n-3} - c \cdot b_{n-2}, \\ &\vdots \\ a_1 &= b_0 - c \cdot b_1, \\ a_0 &= f(c) - c \cdot b_0, \end{aligned}$$

and this gives us (H). □

Based on this corollary we built Horner's scheme as follows. Into the first row we write all (thus also zero) coefficients of the polynomial $f(x)$. Into the second and the third lines we then gradually write the elements b_{n-1}, $c \cdot b_{n-1}$, b_{n-2}, $c \cdot b_{n-2}$, b_{n-3}, etc. (see the following table).

	a_n	a_{n-1}	a_{n-2}	$\ldots$	a_1	a_0
c		$c \cdot b_{n-1}$	$c \cdot b_{n-2}$	$\ldots$	$c \cdot b_1$	$c \cdot b_0$
	b_{n-1}	b_{n-2}	b_{n-3}	$\ldots$	b_0	$f(c)$

Example 18.9. We determine via Horner's scheme the quotient and the remainder when dividing the polynomial $f(x) = x^5 - 3x^4 + 2x - 7$ by $x + 2$.

In this case we have the root $c = -2$ of the polynomial function $h = \psi(h(x))$ corresponding to the polynomial $h(x) = x + 2$ and so Horner's scheme has the form

	1	-3	0	0	2	-7
-2		-2	10	-20	40	-84
	1	-5	10	-20	42	-91

hence $x^5-3x^4+2x-7 = (x+2)(x^4-5x^3+10x^2-20x+42)-91$, $f(-2) = -91$. ■

Definition 18.10. Let $f \in \mathbb{F}\langle x\rangle$ be a polynomial function of degree $n \geq 2$ over a field $\mathbb{F}$ and $k \in N^+$. An element $c \in \mathbb{F}$ is said to be a **k-root** of the polynomial function f if $f(x) = (x-c)^k g(x)$ and $g(c) \neq 0$ for some polynomial $g(x) \in \mathbb{F}[x]$ and the polynomial function $g = \psi(g(x))$ corresponding to the polynomial $g(x)$.

If $k = 1$ we usually call the k-root a *simple root* and if $k \geq 2$ then we talk about a *multiple root*. For example, if $f(x) = (x-i)(x+2)^3$ then i is a simple root of f and -2 is a multiple root, more precisely, a 3-root of f.

Definition 18.11. A field $\mathbb{F}$ is said to be **algebraically closed** if every polynomial function $f \in \mathbb{F}\langle x\rangle$ of degree $n \geq 1$ has in $\mathbb{F}$ at least one root.

The field of rational numbers $\mathbb{Q}$ is not algebraically closed because for instance the polynomial function $x^2 - 2$ has no rational roots. Similarly, the field of real numbers $\mathbb{R}$ is not algebraically closed because for instance the polynomial function $x^2 + 1$ has no real roots. The question for the field $\mathbb{C}$ of complex numbers is addressed by *The Fundamental Theorem of Algebra* which will be presented here without its proof (the proof would require at least a semester course using complex analysis).

Theorem 18.12 (**The Fundamental Theorem of Algebra**). *The field $\mathbb{C}$ of complex numbers is algebraically closed, that is, every polynomial function $f \in \mathbb{C}\langle x\rangle$ of degree $n \geq 1$ has at least one complex root.*

Exercises.

Exercise 18.1. Determine via Horner's scheme the quotient and the remainder when dividing the polynomial $2x^5 + 3x^4 - 13x^3 + 31x - 15$ by

(a) $x - 1$;

(b) $x + 3$.

Exercise 18.2. The polynomial function $3x^5 - 16x^4 + 25x^3 - 6x^2 - 4x - 8$ has a root 2. Determine the greatest k such that 2 is a k-root.

Exercise 18.3. For the polynomial function $f(x) = x^7 + 2x^6 + x^4 - 5x^3 + 3x^2 + 1$ determine $f(-2)$ by (a) substitution, (b) Horner's scheme.

Exercise 18.4. Determine number a such that the polynomial $x^3 + 2x^2 + ax + 24$ is divisible by $x + 3$ by (a) Bézout Theorem 18.3, (b) Horner's scheme.

Exercise 18.5. Determine via Horner's scheme the quotient and the remainder when dividing the polynomial $x^6 + (2 - 2i)x^5 + (1 + i)x^3 - (1 + i)x^2 + 2i$ by the polynomial $x + 1 - i$.

Exercise 18.6. Determine $a, b \in \mathbb{R}$ such that the polynomial $2x^{35} - 18x^{33} - 5x^{15} + 45x^{13} + ax^2 + bx - 3$ is divisible by $x^2 - 4x + 3$.

Exercise 18.7. Determine $a, b, c \in \mathbb{R}$ such that the number -2 is at least a 3-root of the polynomial function $x^4 + ax^3 + bx^2 + cx - 24$.

19 Polynomial functions with complex, real and integer coefficients

In this chapter we study polynomial functions over the algebraically closed field $\mathbb{C}$ of complex numbers with a particular focus on polynomial functions with real and integer coefficients. We start with a consequence (in fact, an equivalent) of The Fundamental Theorem of Algebra.

Theorem 19.1. *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial of degree $n \geq 1$ over the field $\mathbb{C}$. There are complex numbers $c_1, c_2, \ldots, c_n$ such that*

$$f(x) = a_n(x - c_1)(x - c_2)\ldots(x - c_n). \tag{44}$$

Hence the corresponding polynomial function $f = \psi(f(x))$ in $\mathbb{C}\langle x\rangle$ has exactly n roots $c_1, c_2, \ldots, c_n$ in $\mathbb{C}$.

Proof. We proceed by induction on the degree n of $f(x)$.

1. For $n = 1$ we have $f(x) = a_1 x + a_0 = a_1(x + \frac{a_0}{a_1})$, hence $c_1 = -\frac{a_0}{a_1}$, and the statement is true.

2. Let the statement be valid for all polynomials of degree n over the field $\mathbb{C}$ where $n \geq 1$ and let $f(x) = a_{n+1}x^{n+1} + a_n x^n + \cdots + a_1 x + a_0$ be a polynomial of degree $n+1$. By The Fundamental Theorem of Algebra 18.12 (notice this is the place where our proof relies heavily on it), the corresponding polynomial function $f = \psi(f(x))$ in $\mathbb{C}\langle x\rangle$ has some root $c_1 \in \mathbb{C}$. Now by Bézout Theorem 18.3, $f(x) = (x - c_1)g(x)$ where $g(x)$ is a polynomial of degree n with the leading coefficient a_{n+1}. By the induction hypothesis, there are numbers $c_2, \ldots, c_{n+1} \in \mathbb{C}$ such that

$$g(x) = a_{n+1}(x - c_2) \ldots (x - c_{n+1}).$$

After substituting from this we obtain

$$f(x) = a_{n+1}(x - c_1)(x - c_2) \ldots (x - c_{n+1}).$$

as required.

It follows for the corresponding polynomial function $f = \psi(f(x))$ that $f(c) = 0$ if and only if $c \in \{c_1, \ldots, c_n\}$, hence f has exactly the roots c_1, c_2, $\ldots$, c_n in $\mathbb{C}$. □

The *linear* (i.e. of degree 1) polynomials $x - c_1, \ldots x - c_n$ are said to be the *root factors* of the polynomial $f(x)$ and (44) is called a *decomposition into root factors* of the polynomial $f(x)$. Because the linear factors are necessarily irreducible, the decomposition (44) is unique up to the order of factors. It can further be adjusted into the form

$$f(x) = a_n(x - c_1)^{k_1} \ldots (x - c_r)^{k_r}, \tag{45}$$

where the factors $x - c_1, \ldots, x - c_r$ are pairwise distinct and the exponents $k_1, \ldots, k_r \in N^+$ with $k_1 + \cdots + k_r = n$. This decomposition is in fact the canonical decomposition. Also note that if $f(x)$ has the canonical decomposition (45), then c_1 is a k_1-root of the polynomial function f, etc., c_r is a k_r-root of f.

We remark that the theorem above is often presented as a version of the Fundamental Theorem of Algebra itself since the proof we have just given shows that it is equivalent to it. We also emphasize that while the theorem guarantees the existence of n complex roots of each polynomial function of degree n over the field $\mathbb{C}$ of complex numbers, this is far from meaning that such roots can in practice be calculated.

Here we should come back to and mention again (we did so the first time in Chapter **??**) the two young 'romantic heroes' of modern algebra and so of

the whole modern mathematics, **Henrik Abel**[1] and **Évariste Galois**[2] (For more details on their lives see for instance a well-written account of their lives and the influence on modern algebra by M. Ronan [12].) It is due to them that for general polynomials of degree $n \geq 5$ over a field $\mathbb{C}$ there is no formula expressing the roots of the corresponding polynomial functions from their coefficients by using the basic arithmetic operations of addition, subtraction, multiplication, division and the nth roots ($n \geq 2$) such as the *quadratic formula* is widely known for expressing this way (we say, *in radicals*) the roots of polynomial functions of degree 2. The theory showing that there is no algorithm for determining the roots for general polynomial functions of degree $n \geq 5$ over a field $\mathbb{C}$, **Galois theory**, is one of the most beautiful parts of mathematics. The reader is strongly encouraged to become familiar with it, for example, via the famous book *A survey of modern algebra* by G. Birkhoff and S. Mac Lane [2].

The following statement is now an immediate corollary of the previous theorem (and yet another equivalent of The Fundamental Theorem of Algebra).

Corollary 19.2. *Every polynomial function f of degree $n \geq 1$ with complex coefficients has exactly n roots in the field $\mathbb{C}$ of complex numbers (where each k-root is counted k times).*

For polynomial functions with real coefficients the following result is of primary importance.

---

[1] Niels Henrik Abel (1802-1829) was a Norwegian mathematician who made pioneering contributions in several fields of mathematics. His most important result is the first complete proof demonstrating the impossibility of solving the general quintic equation in radicals. This question was one of the most famous open problems of his day, and had been unresolved for 250 years. He was also an innovator in the field of elliptic functions, namely a discoverer of so-called *Abelian functions*. Despite his great achievements, Abel was largely unrecognized during his lifetime; he made his discoveries while living in poverty and died at the age of 26.

Most of his work was done in six or seven years of his working life. Regarding Abel, the French mathematician Charles Hermite said: "Abel has left mathematicians enough to keep them busy for five hundred years." Another French mathematician, Adrien-Marie Legendre, said: "quelle tete celle du jeune Norvégien!" ("what a head the young Norwegian has!") [14]

[2] Évariste Galois (1811-1832) was a French mathematician born in Bourg-la-Reine. While still in his teens, he was able to determine a necessary and sufficient condition for a polynomial to be solvable by radicals, thereby solving a problem standing for hundreds years. His work laid the foundations for what is called today *Galois theory* and for the group theory, two major branches of abstract algebra, and the subfield of *Galois connections*. He died at age 20 from wounds suffered in a duel. [14]

Theorem 19.3. *If a polynomial function $f \in \mathbb{R}\langle x\rangle$ with real coefficients has a k-root $c = a + bi$, then it also has a k-root $\overline{c} = a - bi$ which is a complex conjugate to c.*

Proof. (a) We firstly prove that if a polynomial function $f(x) = a_n x^n + \cdots + a_0$ with real coefficients has a root $a+bi$, then it also has the root $a-bi$. We shall use that for arbitrary complex numbers $c_1, c_2, \ldots, c_n$ the following formulas hold (verify them in detail):

$$\overline{c}_1 + \overline{c}_2 + \cdots + \overline{c}_n = \overline{c_1 + c_2 + \cdots + c_n},$$
$$\overline{c}_1 \cdot \overline{c}_2 \cdot \cdots \cdot \overline{c}_n = \overline{c_1 \cdot c_2 \cdot \cdots \cdot c_n}.$$

Let $a + bi$ be a root of the polynomial $f(x)$ i.e. $f(a + bi) = 0$. Then

$$\begin{aligned} f(\overline{a+bi}) &= a_n(\overline{a+bi})^n + \cdots + a_1(\overline{a+bi}) + a_0 = \\ &= a_n\overline{(a+bi)^n} + \cdots + a_1\overline{(a+bi)} + a_0 = \\ &= \overline{a_n}\overline{(a+bi)^n} + \cdots + \overline{a_1}\overline{(a+bi)} + \overline{a_0} = \\ &= \overline{a_n(a+bi)^n} + \cdots + \overline{a_1(a+bi)} + \overline{a_0} = \\ &= \overline{a_n(a+bi)^n + \cdots + a_1(a+bi) + a_0} = \overline{f(a+bi)} = \overline{0} = 0, \end{aligned}$$

which means that also $\overline{a+bi} = a - bi$ is the root of f.

(b) Now by induction on the degree n of the polynomial function f we prove that if f has a k-root $c = a + bi$, then it also has a k-root $\overline{c} = a - bi$ $(k \geq 2)$.

1. If $n = 1$ then the function $f(x) = a_1 x + a_0$ has the unique root $-\frac{a_0}{a_1}$ in $\mathbb{R}$, hence the statement is true.

2. Assume that the statement is valid for all polynomial functions with real coefficients of degrees less than n where $n \geq 2$. Let a polynomial function f of degree n has a k-root $a + bi$. By the part (a) then f also has a root $a - bi$. By Bézout Theorem 18.3, the polynomial $f(x)$ is divisible by pairwise coprime root factors $x - a - bi$ and $x - a + bi$. Hence there is a polynomial $g(x)$ such that

$$f(x) = (x - a - bi)(x - a + bi)g(x) = (x^2 - 2ax + a^2 + b^2)g(x).$$

Because $f(x)$ and also $x^2 - 2ax + a^2 + b^2$ are polynomials with real coefficients (here we rely heavily on this assumption), the quotient $g(x)$ arising when dividing $f(x)$ by $x^2 - 2ax + a^2 + b^2$ has real coefficients, too. The polynomial function g is of degree $n - 2$, it has a $k - 1$-root $a + bi$ and thus, by the induction hypothesis, it also has a $k - 1$-root $a - bi$. This means that the polynomial function f has a k-root $a - bi$. □

Corollary 19.4. *The irreducible polynomials in* $\mathbb{R}[x]$ *are the polynomials of degree* 1 *and the polynomials* $ax^2 + bx + c$ *of degree* 2 *with a negative discriminator* $b^2 - 4ac < 0$.

Corollary 19.5. *Every polynomial function with real coefficients of an odd degree has at least one real root.*

The next theorem from the 19th century is due to yet another 'young heroe' **Ferdinand Gotthold Max Eisenstein**[3] and it gives a necessary condition for a polynomial function with integer coefficients to have a rational root. By using this theorem one can find in finitely many steps all rational roots of a given polynomial function with integer coefficients provided such roots exist.

Theorem 19.6 (**Eisenstein's criterion for rational roots**). *Let* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *be a polynomial with integer coefficients* $a_n, \ldots, a_0 \in \mathbb{Z}$. *If the corresponding polynomial function* $f \in \mathbb{Z}\langle x \rangle$ *has a rational root* $\frac{p}{q}$, *where* p, q *are coprime, then*

$$p \mid a_0 \quad \textit{and} \quad q \mid a_n.$$

Proof. Let $\frac{p}{q}$ be a root of the polynomial function f and let p, q be coprime. Then

$$a_n \left(\frac{p}{q}\right)^n + \cdots + a_1 \left(\frac{p}{q}\right) + a_0 = 0.$$

By multiplying both sides of this equality by q^n we obtain

$$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0. \tag{46}$$

After putting all members containing p on the left-hand side we get

$$p(a_n p^{n-1} + \cdots + a_1 q^{n-1}) = -a_0 q^n.$$

Since p divides the left-hand side of this equality, it must divide its right-hand side, and because p, q are coprime, we obtain $p \mid a_0$.

[3] Ferdinand Gotthold Max Eisenstein (1823-1852) was a German mathematician. He specialized in number theory and analysis, and proved several results that eluded even Gauss. Like Galois and Abel before him, Eisenstein died before the age of 30. He was born and died in Berlin, Prussia.

The following autobiographical statement from his "Autobiography" (1843) was written when Eisenstein was 20: "As a boy of six I could understand the proof of a mathematical theorem more readily than that meat had to be cut with one's knife, not one's fork." And the following quote is due to Carl Friedrich Gauss, one of the greatest mathematicians of all times. "There have been only three epoch-making mathematicians: Archimedes, Newton, and Eisenstein." [14]

Similarly, after putting all members in (46) containing q on the left-hand side we have

$$q(a_{n-1}p^{n-1} + \cdots + a_1pq^{n-2} + a_0q^{n-1}) = -a_np^n.$$

Since now q divides the left-hand side of the equality, it must divide its right-hand side, and again, since p, q are coprime, we obtain $q \mid a_n$ as required. □

Example 19.7. Using Eisenstein's criterion we find all rational roots of the polynomial function $f(x) = 24x^3 + 2x^2 - 11x - 3$.

If f has a rational root $\frac{p}{q}$, then by Theorem 19.6, $p \mid -3$, $q \mid 24$. This means that

$$p \in \{1, 3, -1, -3\},$$
$$q \in \{1, 2, 3, 4, 6, 8, 12, 24, -1, -2, -3, -4, -6, -8, -12, -24\}.$$

Hence the polynomial function f can only have rational roots from the set

$$\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{6}, \frac{1}{8}, \frac{1}{12}, \frac{1}{24}, 3, \frac{3}{2}, \frac{3}{4}, \frac{3}{8}\} \cup$$
$$\cup \{-1, -\frac{1}{2}, -\frac{1}{3}, -\frac{1}{4}, -\frac{1}{6}, -\frac{1}{8}, -\frac{1}{12}, -\frac{1}{24}, -3, -\frac{3}{2}, -\frac{3}{4}, -\frac{3}{8}\}.$$

One can verify, for example via Horner's scheme, that the only rational roots of f are the numbers $\frac{3}{4}$, $-\frac{1}{2}$, $-\frac{1}{3}$ which are the simple roots. ■

Exercises.

Exercise 19.1. Find all roots of the polynomial function $f(x) = x^4 - 4x^2 + 8x - 4$ if you know that one of its roots is $1 + i$.

Exercise 19.2. Construct a polynomial function of the least degree with real coefficients which has the following roots: the number 1 as a 2-root and the numbers $1 - i$ and -2 as simple roots.

Exercise 19.3. Find all rational roots of the following polynomial functions:

(a) $x^3 - 6x^2 + 11x - 6$;

(b) $2x^3 + 3x^2 - 3x - 2$;

(c) $4x^4 - 7x^2 - 5x - 1$.

Exercise 19.4. Find the root decomposition of the polynomial $16x^4 - 8x + 3$.

20 Derivatives of polynomials

In mathematical analysis a *derivative* of a function $f : \mathbb{R} \to \mathbb{R}$ is defined as a certain limit. In algebra a derivative of a polynomial (a polynomial function) is defined over an arbitrary field $\mathbb{F}$, so the traditional concept of a limit cannot be used.

Definition 20.1. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ be a polynomial in one indeterminate over a field $\mathbb{F}$ where $n \in \mathbb{N}^+$. Then the polynomial

$$(f(x))' = f'(x) := n \times a_n x^{n-1} + (n-1) \times a_{n-1}x^{n-2} + \cdots + 2 \times a_2 x + a_1 \quad (47)$$

is called the (first) **derivative** of the polynomial $f(x)$. For polynomials $f(x) = a_0$ of degree 0 ($a_0 \in \mathbb{F} \setminus \{0\}$) we have $f'(x) := 0$.

Let us recall that if $k \in \mathbb{N}^+$ and a is an element of some field $(\mathbb{F}, +, \cdot)$, then the symbol $k \times a$ means $(a + \cdots + a)_{k-\text{times}}$.

Example 20.2. If $f(x) = 2x^5 + 3x^4 + 4x^2 + 3x + 2$ is a polynomial over $\mathbb{Z}_5$, then

$$f'(x) = 5 \times 2x^4 + 4 \times 3x^3 + 2 \times 4x + 3 = 2x^3 + 3x + 3.$$

■

From the previous example we see that if $f(x)$ is a polynomial over a field of finite characteristics and $\deg f(x) = n \geq 1$, then the degree of the derivative $f'(x)$ does not need to be $n-1$. However, if $f(x)$ is a polynomial over a field of characteristics ∞ and $\deg f(x) = n \geq 1$, then its derivative obviously is a a polynomial of degree $n-1$.

If no confusion arises, instead of $k \times a$ we shall simply write $k \cdot a$ (or only ka). The equality (47) can thus be written in a simpler form

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1.$$

We see that although in algebra the derivative of a polynomial is defined via a certain 'mechanical manipulation' with its coefficients and exponents, it has an analogous form as the derivative of a real (polynomial) function of a real variable known from mathematical analysis. Analogous rules also hold for derivatives of the sum and the product of polynomials as the following theorem shows.

Theorem 20.3. *Let $f(x)$, $g(x)$ be polynomials over a field $\mathbb{F}$. Then*

$$(f(x)+g(x))' = f'(x)+g'(x), \tag{48}$$
$$(f(x)\cdot g(x))' = f'(x)\cdot g(x)+f(x)\cdot g'(x), \tag{49}$$
$$(\forall m\in\mathbb{N}^+)\quad ((x-c)^m)' = m(x-c)^{m-1}. \tag{50}$$

Proof. In proving the equality (48) we assume for simplicity that

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$
$$g(x) = b_n x^n + \cdots + b_1 x + b_0.$$

Then

$$f(x)+g(x) = (a_n+b_n)x^n + \cdots + (a_1+b_1)x + (a_0+b_0).$$

The derivative of the sum $f(x)+g(x)$ then gives us

$$\begin{aligned}(f(x)+g(x))' &= n(a_n+b_n)x^{n-1} + \cdots + (a_1+b_1)\\ &= (na_n x^{n-1} + \cdots + a_1) + (nb_n x^{n-1} + \cdots + b_1)\\ &= f'(x)+g'(x),\end{aligned}$$

hence the equality (48) holds. It can also be extended by induction for the sum of any finite number of polynomials.

For proving (49) we denote

$$f(x) = a_m x^m + \cdots + a_1 x + a_0 = \sum_{i=0}^{m} a_i x^i,$$
$$g(x) = b_n x^n + \cdots + b_1 x + b_0 = \sum_{j=0}^{n} b_i x^i.$$

The product of polynomials $f(x)$, $g(x)$ contains only members of the form

$$a_i x^i b_j x^j, \quad \text{where} \quad i\in\{1,\ldots,m\},\ j\in\{1,\ldots,n\}.$$

The derivative of such a member is

$$\begin{aligned}(a_i x^i b_j x^j)' &= (a_i b_j x^{i+j})' = (i+j)a_i b_j x^{i+j-1}\\ &= i a_i x^{i-1}\cdot b_j x^j + a_i x^i \cdot j b_j x^{j-1}\\ &= (a_i x^i)'\cdot(b_j x^j) + (a_i x^i)\cdot(b_j x^j)'.\end{aligned}$$

By adjustments we then obtain

$$\begin{aligned}
(f(x)\cdot g(x))' &= \left(\sum_{i=0}^{m} a_i x^i \cdot \sum_{j=0}^{n} b_j x^j\right)' \\
&= \left(\sum_{i=0}^{m}\sum_{j=0}^{n} a_i x^i b_j x^j\right)' \\
&= \sum_{i=0}^{m}\sum_{j=0}^{n} \left(a_i x^i b_j x^j\right)' \\
&= \sum_{i=0}^{m}\sum_{j=0}^{n} \Big(\left(a_i x^i\right)'\cdot\left(b_j x^j\right) + \left(a_i x^i\right)\cdot\left(b_j x^j\right)'\Big) \\
&= \sum_{i=0}^{m} \left(a_i x^i\right)' \cdot \sum_{j=0}^{n} b_j x^j + \sum_{i=0}^{m} a_i x^i \cdot \sum_{j=0}^{n} \left(b_j x^j\right)' \\
&= \left(\sum_{i=0}^{m} a_i x^i\right)' \cdot \sum_{j=0}^{n} b_j x^j + \sum_{i=0}^{m} a_i x^i \cdot \left(\sum_{j=0}^{n} b_j x^j\right)' \\
&= f'(x)\cdot g(x) + f(x)\cdot g'(x),
\end{aligned}$$

hence the equality (49) holds.

The equality (50) will be proved by induction on m.

1. For $m = 1$ we have $((x-c)^1)' = 1$ and $1\cdot(x-c)^0 = 1$.
2. We assume that

$$((x-c)^m)' = m(x-c)^{m-1}$$

for $m \geq 1$. We show that then

$$((x-c)^{m+1})' = (m+1)(x-c)^m.$$

By adjustments and using the induction hypothesis we obtain

$$\begin{aligned}
((x-c)^{m+1})' &= ((x-c)^m(x-c))' = m(x-c)^{m-1}(x-c) + (x-c)^m(x-c)^0 \\
&= m(x-c)^m + (x-c)^m = (m+1)(x-c)^m.
\end{aligned}$$

Hence the equality (50) holds. □

Next we inductively define *derivatives of higher orders.*

Definition 20.4. Let $f(x) \in \mathbb{F}[x]$ be a polynomial over a field $\mathbb{F}$ and let $k \in \mathbb{N}^+$. Then the k**th derivative** $f^{(k)}(x)$ of the polynomial $f(x)$ is

$$f^{(1)}(x) := f'(x),$$
$$f^{(k+1)}(x) := \left(f^{(k)}(x)\right)'.$$

For example, for the polynomial $f(x) = 4x^3 - 2x + 1$ we have $f'(x) = 12x^2 - 2$, $f''(x) := f^{(2)}(x) = 24x$, $f'''(x) := f^{(3)}(x) = 24$ and $f^{(4)}(x) = 0$.

From now on we shall only focus on polynomials over the field $\mathbb{C}$ of complex numbers (without explicitly saying so in statements below). We shall study the relationship between the derivatives of the polynomials and the multiple roots of their corresponding polynomial functions.

Theorem 20.5. *If c is a k-root of a polynomial function f, then c is a $(k-1)$-root of the polynomial function f'.*

Proof. Let c be a k-root ($k \geq 1$) of a polynomial function f. Then

$$f(x) = (x-c)^k \cdot g(x), \quad \text{where} \quad g(c) \neq 0$$

and

$$f'(x) = k(x-c)^{k-1} \cdot g(x) + (x-c)^k \cdot g'(x) =$$
$$= (x-c)^{k-1} \cdot (kg(x) + (x-c) \cdot g'(x)).$$

Since for the polynomial function $h(x) := kg(x) + (x-c) \cdot g'(x)$ we have

$$h(c) = kg(c) + (c-c) \cdot g'(c) = kg(c) \neq 0,$$

we see that c is a $(k-1)$-root of the polynomial function f'. □

Theorem 20.6. *Let $f(x) \in \mathbb{C}[x]$ be a polynomial of degree $n \geq 2$. Then c is a k-root of the corresponding polynomial function $f \in \mathbb{C}\langle x \rangle$ if and only if*

$$f(c) = 0, f'(c) = 0, \ldots, f^{(k-1)}(c) = 0, f^{(k)}(c) \neq 0. \tag{51}$$

Proof. Let c be a k-root of the polynomial function f. Then, by Theorem 20.5, c is a $(k-1)$-root of the polynomial function f', $(k-2)$-root of the polynomial function f'', etc. $(k-(k-1))$-root (i.e. simple root) of the polynomial function $f^{(k-1)}$ and it is not a root of the polynomial function $f^{(k)}$. Hence (51) holds.

Conversely, assume that (51) holds, so c is a root of f.

If c is an ℓ-root and $\ell < k$, then $f^{(\ell)}(c) \neq 0$, which contradicts (51).

If c is an ℓ-root and $\ell > k$, then $f^{(k)}(c) = 0$, which again contradicts (51).

So we must have that c is a k-root of the polynomial function f. □

Example 20.7. We determine $a, b \in \mathbb{R}$ such that the polynomial function

$$f(x) = x^3 + ax^2 + bx + 1$$

has a 2-root $c = -2$.

We calculate $f'(x)$, $f(-2)$, $f'(-2)$:

$$\begin{aligned} f'(x) &= 3x^2 + 2ax + b, \\ f(-2) &= -8 + 4a - 2b + 1, \\ f'(-2) &= 12 - 4a + b. \end{aligned}$$

By the previous theorem we must have $f(-2) = f'(-2) = 0$, i.e.

$$\begin{aligned} 4a - 2b - 7 &= 0, \\ -4a + b + 12 &= 0. \end{aligned}$$

This gives us $a = \frac{17}{4}$, $b = 5$. Since $f''(x) = 6x + 2a$ and $f''(-2) \neq 0$, we have that -2 is a 2-root of the polynomial function f. ■

Corollary 20.8. *A polynomial function $f \in \mathbb{C}\langle x \rangle$ has at least one multiple root if and only if the polynomials $f(x)$, $f'(x)$ have a common divisor of degree at least* 1.

Proof. Assume that a polynomial function $f \in \mathbb{C}\langle x \rangle$ has a k-root c ($k \geq 2$). Then, by Theorem 20.6, $f(c) = f'(c) = 0$. This by Bézout Theorem 18.3 means that $x - c$ divides the polynomials $f(x)$ and $f'(x)$, and so they have a common divisor of degree at least 1.

Conversely, let $d(x)$ be a a common divisor of the polynomials $f(x)$, $f'(x)$ and let $\deg d(x) \geq 1$. Then there are polynomials $g(x)$, $q(x)$ such that

$$f(x) = d(x) \cdot g(x), \qquad f'(x) = d(x) \cdot q(x).$$

By The Fundamental Theorem of Algebra 18.12, the polynomial function $d(x)$ has a root $c \in \mathbb{C}$, hence $d(c) = 0$. Then $f(c) = 0$ and $f'(c) = 0$. This by Theorem 20.6 means that the element c is at least a 2-root of the polynomial function $f(x)$. □

Theorem 20.9. *Let $f(x) \in \mathbb{C}[x]$ be a polynomial of degree $n \geq 1$. Let $d(x) := (f(x), f'(x))$ and let $F(x) \in \mathbb{C}[x]$ be a polynomial such that $f(x) = d(x) \cdot F(x)$. Then the corresponding polynomial function $F \in \mathbb{C}\langle x \rangle$ has the same roots as the polynomial function $f \in \mathbb{C}\langle x \rangle$ but all of them are simple.*

Proof. Let the function f have a k-root c. Then the canonical decomposition of the polynomial $f(x)$ has $(x-c)^k$ as a factor and the canonical decomposition of the polynomial $f'(x)$ has, by Theorem 20.5, the polynomial $(x-c)^{k-1}$ as a factor. Thus the canonical decomposition of the polynomial $d(x) = (f(x), f'(x))$ has, by Theorem 17.7, the polynomial $(x-c)^{k-1}$ as a factor. Hence the canonical decomposition of the polynomial $F(x)$ has, by Corollary 17.5, the polynomial $(x-c)^1$ as a factor. This means that c is a simple root of the polynomial function $F(x)$. □

The construction of the polynomial $F(x)$ described in the previous theorem is said to be a *separation of roots* or a *removal of multiple roots.*

Example 20.10. We find the roots of the polynomial function

$$f(x) = x^5 - 6x^4 + 16x^3 - 24x^2 + 20x - 8.$$

This polynomial function has a unique rational root 2. Therefore

$$f(x) = (x-2)(x^4 - 4x^3 + 8x^2 - 8x + 4).$$

Now it suffices to find the roots of $f(x) = x^4 - 4x^3 + 8x^2 - 8x + 4$. This polynomial function does not have rational roots. We check if it has multiple roots. The greatest common divisor of the polynomials $f(x)$, $f'(x)$ is the polynomial $d(x) = x^2 - 2x + 2$ (verify this in detail). From this it follows that also $F(x) = x^2 - 2x + 2$. The roots of the polynomial function F are the numbers $1+i$ and $1-i$. The polynomial function f thus has the following roots: a simple root 2 and double roots $1+i$ and $1-i$. ■

Sometimes, for example when decomposing a polynomial into so-called *partial fractions*, it is useful to express a polynomial in an other form. One of such options will be described in the following theorem.

Theorem 20.11. *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ be a polynomial of degree $n \geq 1$ and let $c \in \mathbb{C}$. Then there are unique elements $b_0, b_1, \ldots, b_n \in \mathbb{C}$ such that*

$$f(x) = b_n(x-c)^n + b_{n-1}(x-c)^{n-1} + \cdots + b_2(x-c)^2 + b_1(x-c) + b_0. \quad (52)$$

Proof. We proceed by induction on n.

1. Let $n = 1$. Then by Lemma 18.7 we have $f(x) = q(x)(x-c) + f(c)$, where the polynomial $q(x)$ is of degree 0, i.e. $q(x) = b_1 \in \mathbb{C}$. If we denote $f(c) = b_0$, then $f(x) = b_1(x-c) + b_0$. From Theorem 16.1 it follows that the elements b_1, b_0 are unique.

2. Assume that the statement is valid for every polynomial of degree less than n where $n \geq 2$. By Lemma 18.7 again, for the polynomials $f(x)$ and $x-c$ we get $f(x) = (x-c)q(x)+f(c)$, where the polynomial $q(x)$ is of degree $n-1$. By the induction hypothesis there are elements $d_0, \ldots, d_{n-1} \in \mathbb{C}$ such that

$$q(x) = d_{n-1}(x-c)^{n-1} + \cdots + d_1(x-c) + d_0.$$

After substituting and adjustments we obtain

$$f(x) = d_{n-1}(x-c)^n + \cdots + d_1(x-c)^2 + d_0(x-c) + f(c).$$

If we denote $b_0 = f(c)$ and $b_i = d_{i-1}$ for every $i \in \{1, \ldots, n\}$, we obtain (52).

We now show the uniqueness of our form. Assume we have an other expression of the polynomial $f(x)$ in the form

$$f(x) = k_m(x-c)^m + \cdots + k_2(x-c)^2 + k_1(x-c) + k_0.$$

Since the polynomial $f(x)$ is of degree n, we have $m = n$. Let us adjust both expressions of the polynomial $f(x)$:

$$f(x) = (x-c)(b_n(x-c)^{n-1} + \cdots + b_2(x-c) + b_1) + b_0,$$
$$f(x) = (x-c)(k_n(x-c)^{n-1} + \cdots + k_2(x-c) + k_1) + k_0.$$

From this, by Theorem 16.1, it follows that

$$b_0 = k_0 \quad \text{and} \quad b_n(x-c)^{n-1} + \cdots + b_2(x-c) + b_1 = k_n(x-c)^{n-1} + \cdots + k_2(x-c) + k_1.$$

Now by the induction hypothesis we obtain

$$b_1 = k_1, b_2 = k_2, \ldots, b_n = k_n,$$

and this completes the proof. □

The expression of a polynomial $f(x)$ in the form (52) is called a *Taylor's series* or a *Taylor's polynomial formula* for the polynomial $f(x)$ *near* c (or *with center* c, or *at point* c) due to **Brook Taylor**.[1] The elements $b_0, \ldots, b_n$

[1] Brook Taylor FRS (1685-1731) was an English mathematician who is best known for Taylor's theorem and the Taylor series. Taylor was elected a fellow of the Royal Society early in 1712, and in the same year sat on the committee for adjudicating the claims of Sir Isaac Newton and Gottfried Leibniz, and acted as secretary to the society from January 1714 to October 1718. From 1715 his studies took a philosophical and religious bent. As a mathematician, he was the only Englishman after Sir Isaac Newton and Roger Cotes capable of holding his own with the Bernoullis, but a great part of the effect of his demonstrations was lost through his failure to express his ideas fully and clearly. [14]

are called *coefficients of the Taylor series*. It can be shown that

$$b_i = \frac{f^{(i)}(c)}{i!}, \quad \text{for every} \quad i \in \{1, \ldots, n\},$$

where $f^{(0)}(c) = f(c)$, $0! = 1$.

However, the coefficients $b_0, b_1, \ldots, b_n$ can be easier calculated via Horner's scheme. A hint is given already by the previous theorem. The equality (52) can be adjusted to the form

$$f(x) = (x - c)(b_n(x - c)^{n-1} + \cdots + b_2(x - c) + b_1) + b_0.$$

The element b_0 is the remainder obtained when dividing the polynomial $f(x)$ by $x - c$ (this can be done via Horner's scheme). If we denote

$$q_1(x) = b_n(x - c)^{n-1} + \cdots + b_2(x - c) + b_1,$$

then by adjustments we have

$$q_1(x) = (x - c)(b_n(x - c)^{n-2} + \cdots + b_2) + b_1$$

and we again see that the element b_1 is the remainder obtained when dividing the polynomial $q_1(x)$ by $x - c$. We can proceed further in this way so that the partial quotients will be $q_1(x), q_2(x), \ldots, q_n(x)$ and b_i will be the remainder obtained when dividing the polynomial $q_i(x)$ by the polynomial $x - c$ for $i \in \{1, 2, \ldots, n\}$.

The calculation of the coefficients of the Taylor series of a polynomial via Horner's scheme will be illustrated in the following example.

Example 20.12. We find the Taylor series of the polynomial

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

near 2.

The coefficients b_0, b_1, b_2, b_3, b_4 can be found by a gradual process of divi-

sions as described above.

	1	3	−2	3	1	
2		2	10	16	38	
	1	5	8	19	⌊39	$= b_0$
2		2	14	44		
	1	7	22	⌊63	$= b_1$	
2		2	18			
	1	9	⌊40	$= b_2$		
2		2				
	1	⌊11	$= b_3$			
2		2				
	⌊1	$= b_4$				

Hence the Taylor series of a given polynomial with center 2 is

$$f(x) = 39 + 63(x-2) + 40(x-2)^2 + 11(x-2)^3 + (x-2)^4.$$

■

Exercises.

Exercise 20.1. Find $a \in \mathbb{R}$ such that the polynomial function given by $f(x) = x^3 - 5x^2 + 3x + a$ has a 2-root. Determine the third root.

Exercise 20.2. Find the Taylor series of the polynomial

$$g(x) = x^4 + 11x^3 + 45x^2 + 81x + 55$$

near -3.

Exercise 20.3. Find the coefficients of the polynomial

$$h(x) = (x-2)^4 + 4(x-2)^3 + 6(x-2)^2 + 10(x-2) + 20.$$

21 Polynomials in several indeterminates

The ring of polynomials in indeterminates $x_1, \ldots, x_n$ over a ring A is the ring $A[x_1, \ldots, x_n]$ that arises by adjunction of algebraically independent elements (over A) to the ring A as it was explained in Chapter 14. The elements of the ring $A[x_1, \ldots, x_n]$ are called *polynomials in indeterminates* $x_1, \ldots, x_n$ *over* A and these are expressions of the form

$$a_0 x_1^{k_{01}} \cdot \cdots \cdot x_n^{k_{0n}} + a_1 x_1^{k_{11}} \cdot \cdots \cdot x_n^{k_{1n}} + \cdots + a_r x_1^{k_{r1}} \cdot \cdots \cdot x_n^{k_{rn}}, \qquad (53)$$

where $a_1, \ldots, a_r \in A$ and $k_{ij} \in \mathbb{N}$ for $i \in \{0, \ldots, r\}$ and $j \in \{1, \ldots, n\}$. The elements $a_0, \ldots, a_r$ are called *coefficients* and the expressions

$$a_0 x_1^{k_{01}} \cdot \cdots \cdot x_n^{k_{0n}},\ a_1 x_1^{k_{11}} \cdot \cdots \cdot x_n^{k_{1n}},\ \ldots,\ a_r x_1^{k_{r1}} \cdot \cdots \cdot x_n^{k_{rn}}$$

are said to be the *members* of the polynomial (53). Analogously as for polynomials in one indeterminate one can show that if $\mathbb{F}$ is a field then the ring $\mathbb{F}[x_1, \ldots, x_n]$ is an integral domain. The polynomials in indeterminates $x_1, \ldots, x_n$ will usually be denoted by $f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_n)$, etc. For example,

$$f(x_1, x_2, x_3) = x_1^4 + x_1^3 x_2 x_3 + x_3^2, \quad g(x_1, x_2, x_3) = 2x_1 + x_3^4, \quad h(x_1, x_2, x_3) = 5$$

are polynomials of three indeterminates (and can be considered over the field $\mathbb{Q}$). From now on the ring A will always be considered to be a field $\mathbb{F}$.

If every two of the n-tuples $[k_{01}, \ldots, k_{0n}], \ldots, [k_{r1}, \ldots, k_{rn}]$ are pairwise distinct, we say that the polynomial (53) is written in its *normed* form. By a *degree of a member* $ax_1^{r_1} \cdot \cdots \cdot x_n^{r_n}$ $(a \neq 0)$ we mean the number $r_1 + \cdots + r_n$ and the *degree of a polynomial* written in its monic form is the maximal of degrees of its members. The ordered n-tuple $[r_1, \ldots, r_n]$ is said to be the *height* of the member $ax_1^{r_1} \cdot \cdots \cdot x_n^{r_n}$. Such a member is called the *leading member* of a polynomial if its height is the greatest in the sense that comparing it to the height $[k_1, \ldots, k_n]$ of any other distinct member of the polynomial the first non-zero number in the sequence $r_1 - k_1, \ldots, r_n - k_n$ is positive. The height of the leading member of the polynomial is said to be the *height of the polynomial*.

A permutation $\varphi = \left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{smallmatrix}\right)$ of the set $\{1, \ldots, n\}$ will simply be written as $(i_1, i_2, \ldots, i_n)$. By a *permutation of a polynomial* $f(x_1, \ldots, x_n)$ we shall mean the polynomial $f(x_{i_1}, \ldots, x_{i_n})$ obtained from $f(x_1, \ldots, x_n)$ by swapping the indeterminates x_1 and x_{i_1}, then x_2 and x_{i_2}, etc., and finally x_n and x_{i_n}. From this it follows that an expression $ax_1^{r_1} \cdot \cdots \cdot x_n^{r_n}$ is a member of a polynomial $f(x_1, \ldots, x_n)$ if and only if $ax_{i_1}^{r_1} \cdot \cdots \cdot x_{i_n}^{r_n}$ is a member of the polynomial

$f(x_{i_1}, \ldots, x_{i_n})$. For example, if

$$f(x_1, x_2, x_3) = x_1^2 x_2 + x_1 x_2 x_3 + x_3,$$

then

$$f(x_2, x_3, x_1) = x_2^2 x_3 + x_2 x_3 x_1 + x_1.$$

Notice that $f(x_1, x_2, x_3) \neq f(x_2, x_3, x_1)$.

Definition 21.1. A polynomial $f(x_1, \ldots, x_n)$ over a field $\mathbb{F}$ is called **symmetric** if $f(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$ for every permutation $(i_1, \ldots, i_n)$ of the set $\{1, \ldots, n\}$.

It can easily be shown that the set of all symmetric polynomials in indeterminates $x_1, \ldots, x_n$ over an integral domain A is a subring of the integral domain $A[x_1, \ldots, x_n]$ which again is an integral domain.

Example 21.2. The polynomial

$$\begin{aligned} f(x_1, x_2, x_2) =& x_1^2 x_2 + x_1^2 x_3 + x_2^2 x_1 + x_2^2 x_3 + x_3^2 x_1 + x_3^2 x_2 + \\ & x_1^3 x_2 x_3 + x_1 x_2^3 x_3 + x_1 x_2 x_3^3 \end{aligned}$$

is symmetric. ■

Notice that if a symmetric polynomial $f(x_1, x_2, x_3)$ contains e.g. $x_1^2 x_2$ as a member, then it must also contain as members $x_1^2 x_3$, $x_2^2 x_1$, $x_2^2 x_3$, $x_3^2 x_1$ and $x_3^2 x_2$, and if it contains e.g. $x_1 x_2^3 x_3$ as a member, then it must also contain as members $x_1^3 x_2 x_3$ and $x_1 x_2 x_3^3$. By generalising this observation, we shall present and prove the following theoretical characterisation of symmetric polynomials.

Theorem 21.3. *Let a polynomial $f(x_1, \ldots, x_n)$ be written in its monic form. Then $f(x_1, \ldots, x_n)$ is symmetric if and only if it contains, with each of its members $a x_1^{r_1} \cdot \cdots \cdot x_n^{r_n}$ and with each of the permutations φ of the set $\{1, \ldots, n\}$, also the members $a x_{\varphi(1)}^{r_1} \cdot \cdots \cdot x_{\varphi(n)}^{r_n}$.*

Proof. Let a polynomial $f(x_1, \ldots, x_n)$ be symmetric and let $a x_1^{r_1} \cdot \cdots \cdot x_n^{r_n}$ be its member. Then $a x_{\varphi(1)}^{r_1} \cdot \cdots \cdot x_{\varphi(n)}^{r_n}$ is a member of the polynomial

$$f(x_{\varphi(1)}, \ldots, x_{\varphi(n)}) = f(x_1, \ldots, x_n).$$

Conversely, let a polynomial $f(x_1, \ldots, x_n)$ contain, with each of its non-zero members $a x_1^{r_1} \cdot \cdots \cdot x_n^{r_n}$ and with each of the permutations φ of the set $\{1, \ldots, n\}$, also the members $a x_{\varphi(1)}^{r_1} \cdot \cdots \cdot x_{\varphi(n)}^{r_n}$. We prove that

$$f(x_1, \ldots, x_n) = f(x_{\varphi(1)}, \ldots, x_{\varphi(n)}),$$

i.e. that $f(x_1, \ldots, x_n)$ is symmetric. It suffices to show that the polynomials $f(x_1, \ldots, x_n)$ and $f(x_{\varphi(1)}, \ldots, x_{\varphi(n)})$ contain the same members.

(a) Let $ax_1^{r_1} \cdot \cdots \cdot x_n^{r_n}$ be a member of the polynomial $f(x_1, \ldots, x_n)$, let φ be an arbitrary permutation of $\{1, \ldots, n\}$ and let ψ be its inverse permutation. Then by assumption, $ax_{\psi(1)}^{r_1} \cdot \cdots \cdot x_{\psi(n)}^{r_n}$ is a member of the polynomial $f(x_1, \ldots, x_n)$ and

$$ax_{\varphi(\psi(1))}^{r_1} \cdot \cdots \cdot x_{\varphi(\psi(n))}^{r_n} = ax_1^{r_1} \cdot \cdots \cdot x_n^{r_n}$$

is a member of the polynomial $f(x_{\varphi(1)}, \ldots, x_{\varphi(n)})$.

(b) Let $bx_{\varphi(1)}^{k_1} \cdot \cdots \cdot x_{\varphi(n)}^{k_n}$ be a member of the polynomial $f(x_{\varphi(1)}, \ldots, x_{\varphi(n)})$. Then $bx_1^{k_1} \cdot \cdots \cdot x_n^{k_n}$ is a member of the polynomial $f(x_1, \ldots, x_n)$ and by assumption, also $bx_{\varphi(1)}^{k_1} \cdot \cdots \cdot x_{\varphi(n)}^{k_n}$ is a member of the polynomial $f(x_1, \ldots, x_n)$.

From (a) and (b) it follows that $f(x_1, \ldots, x_n) = f(x_{\varphi(1)}, \ldots, x_{\varphi(n)})$. □

A symmetric polynomial that is the sum of all pairwise distinct members $ax_{i_1}^{r_1} \cdot \cdots \cdot x_{i_n}^{r_n}$, where $(i_1, \ldots, i_n)$ is a permutation of the set $\{1, \ldots, n\}$, is said to be a *simple symmetric polynomial* given by the member $ax_1^{r_1} \cdot \cdots \cdot x_n^{r_n}$. It will be briefly written in the form $\sum ax_1^{r_1} \cdot \cdots \cdot x_n^{r_n}$. From Theorem 21.3 it follows that every symmetric polynomial is the sum of simple symmetric polynomials. The symmetric polynomial from Example 21.2 can thus be briefly written as

$$f(x_1, x_2, x_3) = \sum x_1^2 x_2 + \sum x_1^3 x_2 x_3.$$

The simple symmetric polynomials of the form

$$\begin{aligned} \sigma_1(x_1, \ldots, x_n) &= \sum x_1, \\ \sigma_2(x_1, \ldots, x_n) &= \sum x_1 x_2, \\ &\vdots \\ \sigma_n(x_1, \ldots, x_n) &= \sum x_1 x_2 \ldots x_n, \end{aligned}$$

are called *basic symmetric polynomials*. A basic symmetric polynomial is such simple symmetric polynomial in which all indeterminates occur in the first power. For example, the basic symmetric polynomials in four indeterminates

x_1, x_2, x_3, x_4 are

$$\begin{aligned}
\sigma_1(x_1, x_2, x_3, x_4) &= x_1 + x_2 + x_3 + x_4,\\
\sigma_2(x_1, x_2, x_3, x_4) &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4,\\
\sigma_3(x_1, x_2, x_3, x_4) &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4,\\
\sigma_4(x_1, x_2, x_3, x_4) &= x_1x_2x_3x_4.
\end{aligned}$$

Let $f(x)$ be a monic polynomial over the field $\mathbb{C}$. We shall henceforth present it in the form

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \tag{54}$$

that will best serve our needs. Let us denote the roots of the polynomial function f by $x_1, x_2, \ldots, x_n$. Then the decomposition of the polynomial $f(x)$ into root factors is

$$f(x) = (x - x_1)(x - x_2)\ldots(x - x_n). \tag{55}$$

If we multiply the root factors in (55) and we compare the forms (54) and (55) of the polynomial $f(x)$, we obtain

$$\begin{aligned}
-a_1 &= x_1 + x_2 + \cdots + x_n = \sigma_1(x_1, \ldots, x_n),\\
a_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = \sigma_2(x_1, \ldots, x_n),\\
-a_3 &= x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n = \sigma_3(x_1, \ldots, x_n),\\
&\vdots\\
(-1)^n a_n &= x_1x_2\ldots x_n = \sigma_n(x_1, \ldots, x_n).
\end{aligned} \tag{56}$$

The formulas in (56) enable us to calculate the roots of the polynomial function f provided some further relationship between the roots is given. The equalities (56) are known as *Vieta's formulae* due to **Francois Viéte**.[1]

If no confusion arises, we write σ_i instead of $\sigma_i(x_1, \ldots, x_n)$ from now on.

Example 21.4. We find roots of the polynomial function

$$f(x) = x^3 - \sqrt{2}x^2 - 5x + 5\sqrt{2},$$

[1]Francois Viéte (Latin: Franciscus Vieta) (1540 - 1603) was a French mathematician whose work on new algebra was an important step towards modern algebra, due to its innovative use of letters as parameters in equations. He was a lawyer by trade, and served as a privy councillor to both Henry III and Henry IV. Vieta created many innovations: the binomial formula, which would be taken by Pascal and Newton, and the link between the roots and coefficients of a polynomial, called Vieta's formulae.

knowing that two of these roots are opposite numbers.

We denote the roots of the polynomial function by x_1, x_2, x_3. Then from (56) we obtain

$$\begin{aligned} x_1 + x_2 + x_3 &= \sqrt{2}, \\ x_1x_2 + x_1x_3 + x_2x_3 &= -5, \\ x_1x_2x_3 &= -5\sqrt{2}. \end{aligned}$$

The opposite roots will be denoted by x_1, x_2. Then $x_2 = -x_1$ and from the first equation we get that $x_3 = \sqrt{2}$. After substituting into the second equation and after adjustment we have $x_1^2 = 5$, i.e. $x_1 = \sqrt{5}$ or $x_1 = -\sqrt{5}$.

If $x_1 = \sqrt{5}$, then $x_2 = -\sqrt{5}$, $x_3 = \sqrt{2}$.

If $x_1 = -\sqrt{5}$, then $x_2 = \sqrt{5}$, $x_3 = \sqrt{2}$.

By the test of validity we verify that these numbers also satisfy the third equation. The roots of the polynomial function f are thus the numbers $\sqrt{5}$, $-\sqrt{5}$, $\sqrt{2}$. ■

Let $f(x_1, x_2) = x_1^2 + x_2^2$. This simple symmetric polynomial can easily be expressed via the basic symmetric polynomials. After an easy adjustment we have

$$f(x_1, x_2) = x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2 = \sigma_1^2 - 2\sigma_2.$$

Analogously one can express every simple symmetric polynomial and so also every symmetric polynomial.

Theorem 21.5. *To every symmetric polynomial $f(x_1, \ldots, x_n)$ there exists a unique polynomial $g(y_1, \ldots, y_n)$ such that*

$$f(x_1, \ldots, x_n) = g(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)).$$

The polynomial $g(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n))$ essentially is a polynomial of n indeterminates where the indeterminates are the basic symmetric polynomials $\sigma_1, \ldots, \sigma_n$. A formal proof of Theorem 21.5 will be skipped but we shall present an example illustrating the procedures for proving Theorem 21.5.

Example 21.6. We shall express the simple symmetric polynomial

$$f(x_1, x_2, x_3) = x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2 = \sum x_1^2x_2$$

via the basic symmetric polynomials.

The leading member of the polynomial $\sum x_1^2 x_2$ is $x_1^2 x_2$. This member is also the leading member of the product $\sigma_1\sigma_2$. By calculating the difference $\sum x_1^2 x_2 - \sigma_1\sigma_2$ we obtain

$$\sum x_1^2 x_2 - \sigma_1\sigma_2 = \sum x_1^2 x_2 - (\sum x_1^2 x_2 - 3\sigma_3)$$

(verify this in detail) which yields

$$f(x_1, x_2, x_3) = \sum x_1^2 x_2 = \sigma_1\sigma_2 + 3\sigma_3.$$

■

We proceed similarly in more complicated situations. Every symmetric polynomial is the sum of simple symmetric polynomials. To each simple symmetric polynomial we find the product of basic symmetric polynomials such that the leading member of it will be the leading member of a given simple symmetric polynomial. Their difference then obviously has the leading member of smaller degree. We proceed this way until we obtain only basic symmetric polynomials.

Example 21.7. We find a polynomial whose roots are squares of the roots of the polynomial $f(x) = x^3 - x^2 + 2x - 1$.

For the roots c_1, c_2, c_3 of the polynomial $f(x)$ we have

$$\begin{aligned}\sigma_1 &= c_1 + c_2 + c_3 = 1,\\ \sigma_2 &= c_1c_2 + c_1c_3 + c_2c_3 = 2,\\ \sigma_3 &= c_1c_2c_3 = 1.\end{aligned}$$

We determine the polynomial $g(x) = x^3 + b_1x^2 + b_2x + b_3$ such that the roots of the corresponding polynomial function g will be the numbers c_1^2, c_2^2, c_3^2. From the formulas (56) we obtain

$$\begin{aligned}b_1 &= -(c_1^2 + c_2^2 + c_3^2),\\ b_2 &= c_1^2c_2^2 + c_1^2c_3^2 + c_2^2c_3^2,\\ b_3 &= -c_1^2c_2^2c_3^2.\end{aligned}$$

The simple symmetric polynomials $\sum c_1^2$, $\sum c_1^2c_2^2$, $\sum c_1^2c_2^2c_3^2$ will be expressed via the basic symmetric polynomials:

$$\sum c_1^2 - \sigma_1^2 = \sum c_1^2 - (\sum c_1^2 + 2\sum c_1c_2) = -2\sigma_2,$$

hence $\sum c_1^2 = \sigma_1^2 - 2\sigma_2$. Further,

$$\sum c_1^2 c_2^2 - \sigma_2^2 = \sum c_1^2 c_2^2 - (\sum c_1^2 c_2^2 + 2\sum c_1^2 c_2 c_3) = -2\sum c_1^2 c_2 c_3 = -2\sigma_1\sigma_3,$$

hence $\sum c_1^2 c_2^2 = \sigma_2^2 - 2\sigma_1\sigma_3$. Finally, $\sum c_1^2 c_2^2 c_3^2 = \sigma_3^2$. For the coefficients b_1, b_2, b_3 we thus obtain

$$\begin{aligned} b_1 &= -(\sigma_1^2 - 2\sigma_2) = -(1^2 - 2\cdot 2) = 3, \\ b_2 &= \sigma_2^2 - 2\sigma_1\sigma_3 = 2^2 - 2\cdot 1\cdot 1 = 2, \\ b_3 &= -\sigma_3^2 = -1^2 = -1. \end{aligned}$$

Hence $g(x) = x^3 + 3x^2 + 2x - 1$. ■

If a polynomial $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$ has roots $x_1, x_2, \ldots, x_n$, then the element

$$D_n = \begin{matrix} (x_1 - x_2)^2 (x_1 - x_3)^2 & \ldots\ldots\ldots & (x_1 - x_n)^2 \\ (x_2 - x_3)^2 & \ldots\ldots\ldots & (x_2 - x_n)^2 \\ & & \vdots \\ & (x_{n-2} - x_{n-1})^2 (x_{n-2} - x_n)^2 & \\ & & (x_{n-1} - x_n)^2 \end{matrix}$$

is said to be the *discriminator of the polynomial* $f(x)$. The discriminator D_n can also be viewed as a symmetric polynomial of n indeterminates.

The *quadratic* polynomial $f(x) = x^2 + a_1 x + a_2$ with roots x_1, x_2 thus has the discriminator $(x_1 - x_2)^2$. If we express it via the basic symmetric polynomials and employ the formulas (56), we obtain

$$D_2 = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = (-a_1)^2 - 4a_2 = a_1^2 - 4a_2.$$

Similarly, for a *cubic* polynomial $f(x) = x^3 + a_1 x^2 + a_2 x + a_3$, its discriminator can be expressed via its coefficients in the form

$$D_3 = a_1^2 a_2^2 - 4a_1^3 a_3 - 4a_2^3 + 18a_1 a_2 a_3 - 27a_3^2.$$

Notice that the discriminator of a polynomial is non-zero if and only if there are no multiple roots of the corresponding polynomial function.

Theorem 21.8. *Let $f(x)$ be a polynomial with real coefficients such that the corresponding polynomial function $f \in \mathbb{R}\langle x\rangle$ has no multiple roots. The*

discriminator of the polynomial $f(x)$ is positive if and only if the number of pairs of conjugate imaginary complex roots is an even number, and it is negative if and only if the number of pairs of conjugate imaginary complex roots is an odd number.

Proof. Since $f(x)$ is a polynomial with real coefficients, by Theorem 19.3 the corresponding polynomial function $f \in \mathbb{R}\langle x\rangle$ has with every root $c \in \mathbb{C} \setminus \mathbb{R}$ also its conjugate complex root $\overline{c}$. For an arbitrary pair of roots c_i, c_j then one of the following situations must occur: both roots are real, one is real while the other is imaginary, both are imaginary but are not conjugate, they are conjugate of each other.

1. If c_i, c_j are real, then $(c_i - c_j)^2 > 0$.
2. If c_i is real and c_j is imaginary, then $(c_i - c_j)^2(c_i - \overline{c_j})^2 > 0$.
3. If c_i, c_j are imaginary but are not conjugate, then $(c_i - c_j)^2(\overline{c_i} - \overline{c_j})^2 > 0$.
4. If c_i, c_j are conjugate of each other, then $(c_i - c_j)^2 < 0$.

From 1. – 4. the statement of the theorem follows. □

Corollary 21.9. *A cubic polynomial with real coefficients has three pairwise distinct real roots if and only if its discriminator is positive. It has one real and two imaginary (conjugate) roots if and only if its discriminator is negative.*

Exercises.

Exercise 21.1. Let the (complex) roots of the polynomial function $f(x) = x^3 - 3x^2 - 2x - 1$ be denoted c_1, c_2, c_3. Calculate the values of the expressions:

(a) $c_1^2 + c_2^2 + c_3^2$;

(b) $\frac{1}{c_1^2} + \frac{1}{c_2^2} + \frac{1}{c_3^2}$;

(c) $(c_1 - c_2)^2 + (c_1 - c_3)^2 + (c_2 - c_3)^2$.

Exercise 21.2. Let c_1, c_2, c_3 be the (complex) roots of the polynomial function $g(x) = x^3 - 2x^2 + x + 1$. Find a polynomial which has the roots:

(a) $c_1 + 2, \quad c_2 + 2, \quad c_3 + 2$;

(b) $c_1c_2, \quad c_1c_3, \quad c_2c_3$;

(c) $c_1 + c_2, \quad c_1 + c_3, \quad c_2 + c_3$;

(d) $c_1^2, \quad c_2^2, \quad c_3^2$.

Exercise 21.3. Using Vieta's formulae solve the following systems of equations over $\mathbb{C}$:

(a)

$$\begin{aligned} x + y &= 1 \\ xy &= -2; \end{aligned}$$

(b)

$$\begin{aligned} x^2 + y^2 &= 13 \\ xy &= 6; \end{aligned}$$

(c)

$$\begin{aligned} x + y + z &= -3 \\ xy + xz + yz &= -1 \\ xyz &= 3; \end{aligned}$$

(d)

$$\begin{aligned} x + y + z &= 2 \\ x^2 + y^2 + z^2 &= 6 \\ x^3 + y^3 + z^3 &= 8. \end{aligned}$$

22 Solving binomial equations

We dealt with basic concepts and facts concerning algebraic equations over integral domains in Chapter **??**. In this and the subsequent chapters we focus on particular types of algebraic equations over the field $\mathbb{C}$ of complex numbers. We start our study with *binomial equations*.

Definition 22.1. By a **binomial equation** we mean an algebraic equation $x^n - a = 0$ of degree n over the field $\mathbb{C}$ of complex numbers, where $a \in \mathbb{C} \setminus \{0\}$. It is usually presented in the form

$$x^n = a. \tag{57}$$

If c is a root of the binomial equation (57), we sometimes write $c = \sqrt[n]{a}$ and we say that c is the **nth complex root of a**.

If a is a non-negative real number, then the usual meaning of the symbol $\sqrt[n]{a}$ is to denote the nth *real* root of a, i.e. a non-negative real number b such that $b^n = a$. Such a meaning is common at secondary schools and used also always in this text unless stated otherwise. The symbol $\sqrt[n]{a}$ therefore denotes the nth complex root of a, i.e. one of the solutions of the binomial equation (57), only if such meaning of $\sqrt[n]{a}$ is said explicitly.

In the next theorem we present so-called *goniometrical solution* of the binomial equation.

Theorem 22.2. *The roots of the binomial equation*

$$x^n = a, \quad \textit{where} \quad a = |a|(\cos\alpha + i\sin\alpha) \in \mathbb{C} \setminus \{0\}, \tag{58}$$

are the complex numbers

$$c_k = \sqrt[n]{|a|}\left(\cos\frac{\alpha+2k\pi}{n} + i\sin\frac{\alpha+2k\pi}{n}\right) \quad \textit{for} \quad k \in \{0,\dots,n-1\}. \tag{59}$$

Proof. Let $c = |c|(\cos\varphi + i\sin\varphi)$ is a root of the equation (57). Then $c^n = a$ and after substitution and calculating the power via *Moivre's theorem* we obtain

$$|c|^n(\cos n\varphi + i\sin n\varphi) = |a|(\cos\alpha + i\sin\alpha).$$

The complex numbers are equal if and only if they have the same *absolute value* (it is called also *modulus* or *magnitude*) and they differ in their *argument* (it is called also *phase* or *angle*) by an integer multiple of 2π. Hence

$$|c|^n = |a| \quad \text{and} \quad n\varphi = \alpha + 2k\pi, \quad k \in \mathbb{Z}.$$

From this it follows that

$$|c| = \sqrt[n]{|a|} \quad \text{and} \quad \varphi = \frac{\alpha+2k\pi}{n}, \quad k \in \mathbb{Z}.$$

So if c is a root of the equation (58), then

$$c = c_k = \sqrt[n]{|a|}\left(\cos\frac{\alpha+2k\pi}{n} + i\sin\frac{\alpha+2k\pi}{n}\right), \quad k \in \mathbb{Z}.$$

By the test of validity one can show that for every $i \in \mathbb{Z}$, c_k is a root of (58). We know that an equation of the nth degree has in $\mathbb{C}$ exactly n roots. Let us consider the roots $c_0,\dots,c_{n-1}$. We show that for $k,l \in \{0,\dots,n-1\}$ and $k \neq l$ we have $c_k \neq c_l$. Let us assume that $c_k = c_l$, i.e.

$$\sqrt[n]{|a|}\left(\cos\frac{\alpha+2k\pi}{n} + i\sin\frac{\alpha+2k\pi}{n}\right) = \sqrt[n]{|a|}\left(\cos\frac{\alpha+2l\pi}{n} + i\sin\frac{\alpha+2l\pi}{n}\right).$$

Then

$$\frac{\alpha+2k\pi}{n}=\frac{\alpha+2l\pi}{n}+2m\pi \quad (m\in\mathbb{Z}).$$

This after an adjustment yields $k-l=m\cdot n$. Therefore n divides $k-l$, which implies (since $0\leq|k-l|<n$) that $k-l=0$, i.e. $k=l$. The set $\{c_0,\ldots,c_{n-1}\}$ is thus the set of all solutions of the binomial equation (58). □

Each of the roots c_k of the equation (58) can be, by using the Moivre's theorem, expressed in the form

$$c_k=\sqrt[n]{|a|}\left(\cos\frac{\alpha}{n}+i\sin\frac{\alpha}{n}\right)\cdot\left(\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}\right).$$

We denote $\varepsilon_k=\left(\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}\right)$. In fact the set $K_n=\{\varepsilon_0,\ldots,\varepsilon_{n-1}\}$ is the set of all solutions of the binomial equation $x^n=1$, i.e. the set of all nth complex roots of one. The set K_n equipped with the operation of multiplication of complex numbers is a cyclic group (see Chapter **??**). Every element of the group $(K_n,\cdot)$ which generates K_n will be called a *primitive nth root of one* or a *primitive root of the equation* $x^n=1$. If ε is a primitive nth root of one, then $K_n=\{1,\varepsilon,\ldots,\varepsilon^{n-1}\}$ (see again Chapter **??**). Since for every $k\in\{0,\ldots,n-1\}$ we have

$$\varepsilon_k=\left(\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}\right)=\left(\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}\right)^k=\varepsilon_1^k,$$

ε_1 is a generator of K_n, hence a primitive nth root of one.

Theorem 22.3. *Let c be a root of the binomial equation $x^n=a$ for $a\in\mathbb{C}\backslash\{0\}$ and let ε is a primitive nth root of one. Then $\{c,c\varepsilon,\ldots,c\varepsilon^{n-1}\}$ is the set of all solutions of the equation $x^n=a$.*

Proof. Since c is a root of the equation $x^n=a$ and ε is a primitive root of the equation $x^n=1$, we have for every $k\in\{0,\ldots,n-1\}$,

$$(c\cdot\varepsilon^k)^n=c^n\cdot(\varepsilon^k)^n=c^n\cdot(\varepsilon_k)^n=c^n\cdot 1=c^n=a,$$

which means that also $c\varepsilon^k$ is a root of the equation $x^n=a$. As ε is a primitive nth root of one, the numbers $1=\varepsilon^0,\varepsilon^1,\ldots,\varepsilon^{n-1}$ are pairwise distinct and so (since $c\neq 0$) the numbers $c,c\varepsilon,\ldots,c\varepsilon^{n-1}$ are pairwise distinct. □

Example 22.4. We find the canonical decomposition of the polynomial $f(x)=x^6+1$ over the field $\mathbb{R}$ of real numbers.

For every $x \in \mathbb{R}$ we have $x^6 + 1 > 0$, i.e. f has no real roots. Because $f(x)$ is a polynomial with real coefficients, it must have three pairs of imaginary complex conjugate roots. By solving the binomial equation $x^6 = -1$ we find all of them. We first write $-1 = \cos\pi + i\sin\pi$. Then

$$\begin{aligned}
c_0 &= \cos\frac{\pi}{6} + i\sin\frac{\pi}{6} = \frac{\sqrt{3}}{2} + i\frac{1}{2},\\
c_1 &= \cos\frac{\pi+2\pi}{6} + i\sin\frac{\pi+2\pi}{6} = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = i,\\
c_2 &= \cos\frac{\pi+4\pi}{6} + i\sin\frac{\pi+4\pi}{6} = \cos\frac{5\pi}{6} + i\sin\frac{5\pi}{6} = -\frac{\sqrt{3}}{2} + i\frac{1}{2},\\
c_3 &= \cos\frac{\pi+6\pi}{6} + i\sin\frac{\pi+6\pi}{6} = \cos\frac{7\pi}{6} + i\sin\frac{7\pi}{6} = -\frac{\sqrt{3}}{2} - i\frac{1}{2},\\
c_4 &= \cos\frac{\pi+8\pi}{6} + i\sin\frac{\pi+8\pi}{6} = \cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2} = -i,\\
c_5 &= \cos\frac{\pi+10\pi}{6} + i\sin\frac{\pi+10\pi}{6} = \cos\frac{11\pi}{6} + i\sin\frac{11\pi}{6} = \frac{\sqrt{3}}{2} - i\frac{1}{2}.
\end{aligned}$$

For the roots $c_0, c_1, c_2, c_3, c_4, c_5$ we have $c_0 = \overline{c_5}$, $c_1 = \overline{c_4}$, $c_2 = \overline{c_3}$. If we now calculate the products of root factors containing the complex conjugate roots, we obtain quadratic polynomials irreducible over the field $\mathbb{R}$:

$$\begin{aligned}
(x - c_0)(x - c_5) &= x^2 - \sqrt{3}x + 1,\\
(x - c_1)(x - c_4) &= x^2 + 1,\\
(x - c_2)(x - c_3) &= x^2 + \sqrt{3}x + 1.
\end{aligned}$$

The canonical decomposition of the polynomial $f(x) = x^6 + 1$ over the field $\mathbb{R}$ is thus $x^6 + 1 = (x^2 - \sqrt{3}x + 1)(x^2 + 1)(x^2 + \sqrt{3}x + 1)$. ■

Exercises.

Exercise 22.1. Find all solutions of the binomial equations over the field $\mathbb{C}$:

(a) $x^6 = 1$;

(b) $x^4 = \frac{1}{16}$;

(c) $x^8 = 625$;

(d) $x^3 = i$.

Exercise 22.2. Find the canonical decompositions of the polynomials $f(x)$ into irreducible polynomials over the field $\mathbb{R}$ in cases:

(a) $f(x) = x^6 - 1$;

(b) $f(x) = x^8 + 1$;

(c) $f(x) = x^4 + 2$.

23 Quadratic and cubic equations over $\mathbb{C}$

The equation

$$ax^2 + bx + c = 0, \tag{60}$$

where $a, b, c \in \mathbb{C}$ and $a \neq 0$, is said to be a *quadratic equation over* $\mathbb{C}$. In case its coefficients are real numbers we know the formula for its roots already from secondary school. We show in this chapter that an analogous formula is valid for the roots of a quadratic equation whose coefficients are complex numbers.

To present the roots satisfactorily also in this case, one needs to be able to express a square root of a complex number as a complex number in its traditional algebraic form $a + bi$. We show here how to do it and so the reader should be able to find full solutions to quadratic equations over the field $\mathbb{C}$. We also show the reader how to solve, over $\mathbb{C}$, algebraic equations of degrees three called *cubic equations*. Solving equations of degrees four in general will be skipped throughout this textbook, we just notice that *solving them in radicals* is possible. On the other hand, solving algebraic equations of degrees five or more *in radicals is not possible* in general as we mentioned in Chapter 19 with respect to the 'romantic heroes' of modern algebra, Henrik Abel and Evariste Galois. However, there are procedures for solving *very special* algebraic equations of degrees five and more and we present this in the next chapter.

Lemma 23.1. *For every complex number $a + bi$ there is its square complex root*

$$x = \pm\left(\sqrt{\frac{1}{2}\left(\sqrt{a^2+b^2}+a\right)} + i\delta\sqrt{\frac{1}{2}\left(\sqrt{a^2+b^2}-a\right)}\right), \tag{61}$$

where $\delta = 1$ for $b > 0$ and $\delta = -1$ for $b < 0$.

Proof. If x is the square complex root of the number $a+bi$, then $x^2 = a+bi$. The number x is complex thus $x = u+vi$, whence $(u+vi)^2 = a+bi$. After an adjustment we obtain

$$u^2 - v^2 + 2uvi = a + bi,$$

and this gives us the system of two equations with two real unknowns u, v:

$$\begin{aligned} u^2 - v^2 &= a, \\ 2uv &= b. \end{aligned}$$

By squaring both equations and by taking their sum we get

$$(u^2+v^2)^2 = a^2 + b^2.$$

Now because $a^2+b^2 \geq 0$, we have

$$u^2 + v^2 = \sqrt{a^2+b^2}.$$

From the equations $u^2 - v^2 = a$, $u^2 + v^2 = \sqrt{a^2+b^2}$ it follows that

$$u = \pm\sqrt{\frac{1}{2}\left(\sqrt{a^2+b^2}+a\right)}, \qquad v = \pm\sqrt{\frac{1}{2}\left(\sqrt{a^2+b^2}-a\right)}.$$

The equation $2uv = b$ yields that $b > 0$ if and only if both numbers u, v are either positive or negative and $b < 0$ if and only if one of u, v is positive and the other is negative. Now (61) follows.

By a straightforward calculation one can verify that the complex numbers given by (61) satisfy $x^2 = a+bi$, thus they are indeed the square complex roots of $a+bi$. □

We now present the solution to the quadratic equation (60). Notice that (60) is equivalent to the monic equation

$$x^2 + \frac{b}{a}x + \frac{c}{a} = 0.$$

We gradually adjust the polynomial $x^2 + \frac{b}{a}x + \frac{c}{a}$ to the form

$$\begin{aligned} x^2 + \frac{b}{a}x + \frac{c}{a} &= x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} + \frac{c}{a} - \frac{b^2}{4a^2} \\ &= \left(x + \frac{b}{2a}\right)^2 - \frac{b^2-4ac}{4a^2} = \left(x+\frac{b}{2a}\right)^2 - \left(\frac{\sqrt{b^2-4ac}}{2a}\right)^2 \\ &= \left(x + \frac{b-\sqrt{b^2-4ac}}{2a}\right) \cdot \left(x + \frac{b+\sqrt{b^2-4ac}}{2a}\right), \end{aligned}$$

which in fact is its decomposition into the product of root factors. Here $\sqrt{b^2-4ac}$ is one concretely chosen square complex root of the number b^2-4ac which is called the *quadratic discriminant*. Hence we obtain the following theorem:

Theorem 23.2. *The roots of the quadratic equation (60) are the complex numbers*

$$x_1 = \frac{-b+\sqrt{b^2-4ac}}{2a}, \qquad x_2 = \frac{-b-\sqrt{b^2-4ac}}{2a},$$

where the symbol $\sqrt{b^2-4ac}$ denotes one chosen square complex root of the quadratic discriminant b^2-4ac.

Example 23.3. We solve the quadratic equation $x^2-(5+4i)x+6+8i=0$.
In this case $a=1$, $b=-(5+4i)$, $c=6+8i$. Then

$$\sqrt{b^2-4ac} = \sqrt{-15+8i} = \pm(1+4i).$$

We choose $\sqrt{-15+8i} = 1+4i$ and we get

$$x_1 = 3+4i, \qquad x_2 = 2.$$

■

In the rest of this chapter we deal with cubic equations over the field $\mathbb{C}$. These are equations of the form

$$ax^3+bx^2+cx+d=0$$

where $a,b,c,d \in \mathbb{C}$ and $a \neq 0$. Each such equation can be adjusted to its equivalent monic form

$$x^3+a_2x^2+a_1x+a_0=0. \tag{62}$$

After using the substitution $x = y-\frac{a_2}{3}$ we obtain the cubic equation

$$y^3+py+q=0, \tag{63}$$

where $p = a_1-\frac{{a_2}^2}{3}$ and $q = \frac{2{a_2}^3}{27}-\frac{a_1a_2}{3}+a_0$. This is called a *reduced cubic equation*, meaning that the coefficient for y^2 is 0. We employ an another substitution $y=u+v$. Then we get

$$(u+v)^3+p(u+v)+q=0,$$

and after an adjustment,

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0.$$

If u, v are chosen such that $3uv + p = 0$, i.e. $uv = -\frac{p}{3}$, then

$$u^3 + v^3 = -q \qquad \text{and} \qquad u^3 v^3 = -\frac{p^3}{27}.$$

In this case we can consider u^3, v^3 to be the roots of the quadratic equation

$$z^2 + qz - \frac{p^3}{27} = 0,$$

which is called the *quadratic resolvent* of the cubic equation (63). Its roots are

$$z_1 = u^3 = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} = -\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3},$$
$$z_2 = v^3 = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} = -\frac{q}{2} - \frac{1}{18}\sqrt{-3D_3},$$

where $D_3 = -4p^3 - 27q^2$ is the discriminant of the reduced cubic equation (63).

For expressing the number $y = u + v$ we thus have nine possibilities. If

$$u_1 = \sqrt[3]{-\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3}}$$

is one of the (three) third complex roots of $-\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3}$, then v_1 can be calculated (uniquely) from the equality $uv = -\frac{p}{3}$ (i.e. $v_1 = -\frac{p}{3u_1}$) and we denote it as

$$v_1 = \sqrt[3]{-\frac{q}{2} - \frac{1}{18}\sqrt{-3D_3}}.$$

After denoting one of the third complex roots of the number $\sqrt[3]{-\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3}}$ by u_1, the other two third complex roots are, by Theorem 24.3, $u_2 = \varepsilon u_1$ and $u_3 = \varepsilon^2 u_1$. Here ε is a primitive root of the equation $x^3 = 1$, i.e. $\varepsilon = -\frac{1}{2} + \frac{1}{2}i\sqrt{3}$. The corresponding numbers v_2, v_3 can be determined from the equality $uv = -\frac{p}{3}$:

$$v_2 = -\frac{p}{3u_2} = -\frac{p}{3u_1\varepsilon} = \frac{v_1}{\varepsilon} = v_1\varepsilon^2,$$
$$v_3 = -\frac{p}{3u_3} = -\frac{p}{3u_1\varepsilon^2} = \frac{v_1}{\varepsilon^2} = v_1\varepsilon.$$

For y_1, y_2, y_3 we thus have

$$\begin{aligned} y_1 &= u_1 + v_1, \\ y_2 &= u_1\varepsilon + v_1\varepsilon^2, \\ y_3 &= u_1\varepsilon^2 + v_1\varepsilon. \end{aligned} \tag{64}$$

From this, using the substitution $x = y - \frac{a_2}{3}$, we can calculate the roots x_1, x_2, x_3 of the equation (61). By the test of validity one can verify that the numbers y_1, y_2, y_3 are the roots of the equation (62), resp. the numbers x_1, x_2, x_3 are the roots of the equation (61).

We formulate the obtained results (for a reduced cubic equation of the form (63)) in the following theorem:

Theorem 23.4. *A cubic equation $y^3 + py + q = 0$ over $\mathbb{C}$ has solutions*

$$\begin{aligned} y_1 &= \sqrt[3]{-\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3}} + \sqrt[3]{-\frac{q}{2} - \frac{1}{18}\sqrt{-3D_3}}, \\ y_2 &= \varepsilon\sqrt[3]{-\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3}} + \varepsilon^2\sqrt[3]{-\frac{q}{2} - \frac{1}{18}\sqrt{-3D_3}}, \\ y_3 &= \varepsilon^2\sqrt[3]{-\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3}} + \varepsilon\sqrt[3]{-\frac{q}{2} - \frac{1}{18}\sqrt{-3D_3}}, \end{aligned}$$

where $D_3 = -4p^3 - 27q^2$ is the discriminant of this equation and ε is a primitive third root of one.

The above formulas for solving cubic equations are called *Cardano formulas* (though **Gerolamo Cardano**[1] was not the one who discovered them,

[1] Gerolamo Cardano (1501-1576) was an Italian mathematician, physician, astrologer, philosopher and gambler, best known as the earliest founder of probability and the establisher of the binomial coefficients and the binomial theorem, which was comprised in his book, *Opus novum de proportionibus*. He wrote more than 200 works on medicine, mathematics, physics, philosophy, religion, and music.

Cardano partially invented and described several mechanical devices including the combination lock, the gimbal consisting of three concentric rings allowing a supported compass or gyroscope to rotate freely, and the Cardan shaft with universal joints, which allows the transmission of rotary motion at various angles and is used in vehicles to this day. He studied hypocycloids, published in de proportionibus 1570. The generating circles of these hypocycloids were later named Cardano circles or cardanic circles and were used for the construction of the first high-speed printing presses.

Today, he is well-known for his achievements in algebra. He made the first systematic use of negative numbers, published with attribution the solutions of other mathematicians for the cubic and quartic equations, and acknowledged the existence of imaginary numbers. [14]

see again [12]). To use these formulas is not always useful as the following example shows.

Example 23.5. One can easily check that the roots of the cubic equation

$$x^3 - 3x^2 + x + 5 = 0$$

are the numbers -1, $2+i$, $2-i$. By substitution $x = y+1$ the equation can be adjusted to a reduced cubic equation $y^3 - 2y + 4 = 0$. Its roots are the numbers -2, $1+i$, $1-i$ (verify this). By using the Cardano formulas we get

$$\begin{aligned}
y_1 &= \sqrt[3]{-2 + \frac{10}{9}\sqrt{3}} + \sqrt[3]{-2 - \frac{10}{9}\sqrt{3}},\\
y_2 &= \varepsilon\sqrt[3]{-2 + \frac{10}{9}\sqrt{3}} + \varepsilon^2\sqrt[3]{-2 - \frac{10}{9}\sqrt{3}},\\
y_3 &= \varepsilon^2\sqrt[3]{-2 + \frac{10}{9}\sqrt{3}} + \varepsilon\sqrt[3]{-2 - \frac{10}{9}\sqrt{3}}.
\end{aligned}$$

Since y_1 is a real number, we have $y_1 = 2$, however, this is not immediately visible from the given expression (try to find an approximate calculation of the roots y_1, y_2, y_3). ■

The situation is even more difficult when the cubic equation has all three roots real, that is, when $D_3 > 0$. In this case the real roots are expressed via the Cardano formulas in their complex form (since $\sqrt{-3D_3}$ is an imaginary number). The presented Cardano procedure is thus not always useful in practice. It has mainly a theoretical and historical importance because searching for solutions to cubic equations (see again [12] for more details) contributed to creating the theory of complex numbers.

Exercises.

Exercise 23.1. Solve the following quadratic equations over the field $\mathbb{C}$:

(a) $x^2 - (2+i)x + 7i - 1 = 0$;

(b) $(2+i)x^2 - (5-i)x + 2 - 2i = 0$;

(c) $x^2 - (6-4i)x + 5 - 12i = 0$.

Exercise 23.2. Decompose the polynomial $x^4 - 3x^2 + 4$ into

(a) root factors over $\mathbb{C}$;

(b) irreducible polynomials over $\mathbb{R}$.

Exercise 23.3. Find the decomposition of the polynomial $x^4+6x^3+9x^2+100$ into irreducible polynomials in $\mathbb{R}[x]$.

Exercise 23.4. Find all (complex) roots of the polynomial $x^4+2x^2-24x+72$.

Exercise 23.5. Using the Cardano formulas solve the following cubic equations over the field $\mathbb{C}$:

(a) $x^3 - 9x^2 + 36x - 28 = 0$;

(b) $x^3 - 15x + 22 = 0$;

(c) $x^3 + x + 10$.

24 Reciprocal equations

Some algebraic equations over the field $\mathbb{C}$ can be solved such that we diminish their degree via a suitable substitution. A simple example is given by biquadratic equations, that is, equations of the form

$$x^4 + px^2 + q = 0, \quad p,\, q \in \mathbb{C},$$

which we solve via the substitution $y = x^2$. In general, from the equation

$$a_{kn}x^{kn} + a_{k(n-1)}x^{k(n-1)} + \cdots + a_k x^k + a_0 = 0 \tag{65}$$

over $\mathbb{C}$ we obtain via the substitution $y = x^k$ the equation

$$a_{kn}y^n + a_{k(n-1)}y^{n-1} + \cdots + a_k y + a_0 = 0. \tag{66}$$

One can show that every solution $\alpha \in \mathbb{C}$ of the equation (65) is a solution of some binomial equation $x^k = \beta$, where $\beta \in \mathbb{C}$ is a suitable solution of the equation (66).

Example 24.1. We find all solutions of the equation $x^6 - 5x^3 - 14 = 0$ over the field $\mathbb{C}$.

If we use the substitution $y = x^3$, we obtain the equation $y^2 - 5y - 14 = 0$. The roots of this equation are $y_1 = 7$, $y_2 = -2$. By solving the binomial equations

$$x^3 = 7 \qquad \text{a} \qquad x^3 = -2$$

we obtain all six roots of the original equation:

$$x_1 = \sqrt[3]{7}, \qquad x_2 = \sqrt[3]{7}\left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right), \qquad x_3 = \sqrt[3]{7}\left(-\frac{1}{2} - \frac{i\sqrt{3}}{2}\right),$$
$$x_4 = -\sqrt[3]{2}, \qquad x_5 = \sqrt[3]{2}\left(\frac{1}{2} - \frac{i\sqrt{3}}{2}\right), \qquad x_6 = \sqrt[3]{2}\left(\frac{1}{2} + \frac{i\sqrt{3}}{2}\right).$$

(Perform all necessary calculations in detail.) ■

In the rest of this chapter we focus on very special algebraic equations over the field $\mathbb{C}$ called *reciprocal equations* that can be solved in spite of having degrees higher than four. These equations are 'symmetric' and their degree can also be diminished via a suitable substitution.

Definition 24.2. A polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0,\ n \geq 1,$$

over the field $\mathbb{C}$ is said to be a **positively reciprocal polynomial** if

$$a_i = a_{n-i}, \quad \text{for every} \quad i \in \{0, 1, \ldots, n\}.$$

If $f(x)$ is a positively reciprocal polynomial over $\mathbb{C}$, then for the corresponding polynomial function $f \in \mathbb{C}\langle x\rangle$ the equation $f(x) = 0$ is said to be a **positively reciprocal equation** over $\mathbb{C}$.

The next theorem provides a certain characterisation of positively reciprocal polynomials which highlights their internal symmetry.

Theorem 24.3. *A polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ is positively reciprocal if and only if for the corresponding polynomial function $f \in \mathbb{C}\langle x\rangle$ the following holds:*

$$(\forall x \neq 0)\ f(x) = x^n f\left(\frac{1}{x}\right). \tag{67}$$

Proof. If $f(x)$ is a positively reciprocal polynomial over $\mathbb{C}$, then it can be written as

$$f(x) = a_o x^n + a_1 x^{n-1} + \cdots + a_1 x + a_0.$$

From this, for the corresponding polynomial function $f \in \mathbb{C}\langle x\rangle$ and $x \neq 0$ by adjustments we obtain

$$f(x) = x^n \left(a_0 + a_1\left(\frac{1}{x}\right) + \cdots + a_1\left(\frac{1}{x}\right)^{n-1} + a_0\left(\frac{1}{x}\right)^n\right),$$

that is,

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

Conversely, let $x \neq 0$ and $f(x) = x^n f\left(\frac{1}{x}\right)$ for $f \in \mathbb{C}\langle x\rangle$. Then

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = x^n \left(a_n \left(\frac{1}{x}\right)^n + a_{n-1}\left(\frac{1}{x}\right)^{n-1} + \cdots + a_0\right).$$

By comparing the left- and right-hand sides for the corresponding polynomials of the unknown x, we obtain that for all $i \in \{0, 1, \ldots, n\}$, $a_i = a_{n-i}$. □

Corollary 24.4. *If a positively reciprocal equation $f(x) = 0$ over $\mathbb{C}$ has a root $\alpha \in \mathbb{C}$, then it also has the root $\frac{1}{\alpha}$ which is the inverse element to α in the field $\mathbb{C}$.*

Proof. Since a positively reciprocal equation $f(x) = 0$ has a coefficient $a_n \neq 0$ and $a_n = a_0$, every its (complex) root is non-zero. If $\alpha \in \mathbb{C}$ is a root, i.e. $f(\alpha) = 0$, then from the previous theorem we get that $\alpha^n f\left(\frac{1}{\alpha}\right) = 0$, hence also $f\left(\frac{1}{\alpha}\right) = 0$. This means that $\frac{1}{\alpha}$ is a root of the positively reciprocal equation $f(x) = 0$. □

Corollary 24.5. *Let $f(x)$ be a positively reciprocal polynomial of an odd degree over $\mathbb{C}$. Then $f(x) = (x+1)g(x)$, where $g(x)$ is a positively reciprocal polynomial of an even degree over $\mathbb{C}$.*

Proof. By substituting -1 into (67) we obtain $(-1)^n f(-1) = f(-1)$. After an adjustment we have $f(-1) = 0$, so -1 is a root of the corresponding polynomial function f. By Bézout Theorem 18.3 we get $f(x) = (x+1)g(x)$, where $g(x)$ is a polynomial of an even degree. From the last equation we obtain that for every $x \neq 0$, $f\left(\frac{1}{x}\right) = \left(\frac{1}{x} + 1\right) g\left(\frac{1}{x}\right)$. If we substitute from the last two equations $f(x)$ and $f\left(\frac{1}{x}\right)$ into (67), we obtain after an adjustment

$$(\forall x \neq -1)\ g(x) = x^{n-1} g\left(\frac{1}{x}\right).$$

One can easily check that this also holds for $x = -1$. From Theorem 24.3 it then follows that $g(x)$ is a positively reciprocal polynomial of an even degree $n-1$ over $\mathbb{C}$. □

Definition 24.6. A polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0,\ n \geq 1,$$

over the field $\mathbb{C}$ is said to be a **negatively reciprocal polynomial** if

$$a_i = -a_{n-i}, \quad \text{for every} \quad i \in \{0, 1, \ldots, n\}.$$

If $f(x) \in \mathbb{C}[x]$ is a negatively reciprocal polynomial, then then for the corresponding polynomial function $f \in \mathbb{C}\langle x \rangle$ the equation $f(x) = 0$ is said to be a **negatively reciprocal equation** over $\mathbb{C}$.

Analogously as we proved Theorem 24.3 and the Corollaries 24.4 and 24.5, one can also prove the following three statements (write down their proofs in detail). The first theorem characterises negatively reciprocal polynomials over $\mathbb{C}$.

Theorem 24.7. *A polynomial* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ *is negatively reciprocal if and only if for the corresponding polynomial function* $f \in \mathbb{C}\langle x \rangle$ *the following holds:*

$$(\forall x \neq 0)\ f(x) = -x^n f\left(\frac{1}{x}\right).$$

Corollary 24.8. *If a negatively reciprocal equation* $f(x) = 0$ *over* $\mathbb{C}$ *has a root* $\alpha \in \mathbb{C}$*, then it also has the root* $\frac{1}{\alpha}$.

Corollary 24.9. *Let* $f(x)$ *be a negatively reciprocal polynomial over* $\mathbb{C}$*. Then* $f(x) = (x-1)g(x)$ *where* $g(x)$ *is a positively reciprocal polynomial over* $\mathbb{C}$.

From Corollaries 24.5 and 24.9 it follows that when studying reciprocal equations over $\mathbb{C}$ one can focus only on the positively reciprocal equations of even degrees. Such equations can be expressed in the form

$$a_0 x^{2m} + a_1 x^{2m-1} + \cdots + a_1 x + a_0 = 0. \tag{68}$$

If such an equation is multiplied by $\frac{1}{x^m}$, then after an adjustment we obtain

$$a_0\left(x^m + \frac{1}{x^m}\right) + a_1\left(x^{m-1} + \frac{1}{x^{m-1}}\right) + \cdots + a_{m-1}\left(x + \frac{1}{x}\right) + a_m = 0. \tag{69}$$

Let us use the substitution

$$x + \frac{1}{x} = y. \tag{70}$$

By gradually powering and adjusting (70) we obtain

$$\begin{aligned} x^2 + \frac{1}{x^2} &= y^2 - 2, \\ x^3 + \frac{1}{x^3} &= y^3 - 3y, \\ x^4 + \frac{1}{x^4} &= y^4 - 4y^2 + 2, \\ &\vdots \end{aligned}$$

After substituting these expressions into (69) we obtain an equation of degree m:

$$b_m y^m + \cdots + b_0 = 0. \tag{71}$$

After solving it (if we can) and after substituting its roots into (70) we finish the task by solving the m quadratic equations over $\mathbb{C}$. Their solutions are the solutions of the original equation (68).

Example 24.10. We find all roots of the polynomial function

$$f(x) = x^6 + 2x^5 - 2x^4 + 2x^2 - 2x - 1 \tag{72}$$

over $\mathbb{C}$.

The polynomial $f(x)$ is negatively reciprocal. Hence the function f has the number 1 as its root, thus

$$f(x) = (x-1)g(x),$$

where

$$g(x) = x^5 + 3x^4 + x^3 + x^2 + 3x + 1$$

is a positively reciprocal polynomial of an odd degree. This means that the function g has -1 as its root. Hence

$$g(x) = (x+1)h(x),$$

where

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

is a positively reciprocal polynomial of an even degree. So it remains to solve the positively reciprocal equation

$$x^4 + 2x^3 - x^2 + 2x + 1 = 0. \tag{73}$$

If we multiply this equation with $\frac{1}{x^2}$ and adjust it, we get

$$\left(x^2 + \frac{1}{x^2}\right) + 2\left(x + \frac{1}{x}\right) - 1 = 0.$$

By using the substitution $y = x + \frac{1}{x}$ we obtain the quadratic equation

$$y^2 + 2y - 3 = 0, \tag{74}$$

which has roots $y_1 = 1$ and $y_2 = -3$. Hence for x we have

$$x + \frac{1}{x} = 1, \qquad x + \frac{1}{x} = -3,$$

which yields two quadratic equations

$$x^2 - x + 1 = 0, \qquad x^2 + 3x + 1 = 0.$$

By solving them we obtain all solutions of the equation (73):

$$x_{1,2} = \frac{1 \pm i\sqrt{3}}{2}, \qquad x_{3,4} = \frac{-3 \pm \sqrt{5}}{2}.$$

The polynomial function (72) thus has these roots:

$$1, \quad -1, \quad , \frac{1 + i\sqrt{3}}{2}, \quad \frac{1 - i\sqrt{3}}{2}, \quad \frac{-3 + \sqrt{5}}{2}, \quad \frac{-3 - \sqrt{5}}{2}.$$

■

The substitution $y = x + \frac{1}{x}$ enables us to diminish the degree of a positively reciprocal equation of an even degree to its half and so to transfer the problem of solving the reciprocal equation over the field $\mathbb{C}$ into a problem of solving an another equation over $\mathbb{C}$. However, in general it is possible to aim for solving algebraically over the field $\mathbb{C}$ positively reciprocal equations of degrees at most nine (as they have -1 as a root) and negatively reciprocal equations of degrees at most ten (they have 1 and -1 as their roots).

Exercises.

Exercise 24.1. Solve the equation $x^4 + x^2 + 1 = 0$ over $\mathbb{C}$ as

(a) a biquadratic equation;

(b) a reciprocal equation.

Exercise 24.2. Solve the equation $x^5 - 1 = 0$ over $\mathbb{C}$ as

(a) a binomial equation;

(b) a reciprocal equation.

Exercise 24.3. Solve the equations over $\mathbb{C}$:

(a) $x^4 - 2x^3 - x^2 - 2x + 1 = 0$;

(b) $x^4 + 2x^3 + x^2 + 2x + 1 = 0$;

(c) $x^6 + x^4 + x^2 + 1 = 0$;

(d) $4x^6 + x^4 + x^3 + x^2 - 3x + 1 = 0$.

25 Numerical methods for solving algebraic equations

As demonstrated so far, by algebraic methods we can solve only certain types of algebraic equations such as all binomial equations, all equations of degrees at most four and all reciprocal equations of degrees up to ten. However, in general there are no algorithms for finding all solutions of algebraic equations of degree more than four.

Nevertheless, for all algebraic equations there have been many *numerical methods* developed which give algorithms for calculating all solutions with an almost arbitrarily small error prescribed in advance. Some of these methods can be used both for algebraic equations $f(x) = 0$ as well as for equations of the form $f(x) = g(x)$ where $f, g \in \mathbb{R}\langle x \rangle$ are real functions of a real variable x. These methods are used also in the computer software *Mathematica* - A System for Doing Mathematics by Computer. In Chapter 5.2 of [10] one can read:

If equations contain only linear functions or polynomial functions of small degrees, we can use for their numerical solutions the tool `NSolve`*, which does not require putting a starting value and can calculate all solutions. Yet if the equation contains more complicated functions, then to solve, the system Mathematica must search for a numerical method for solving non-linear equations. Here we must use the tool* `FindRoot`*, in which we always put a starting value*

of the variable. Even if the equation has several solutions, the tool FindRoot always returns only one solution, namely the one it finds as the first one. If we want to find further solutions, we must change the starting value of the variable. The tool `FindRoot` *is able to find also a complex root if the starting value of the variable is a complex number. If we provide only one starting value of the variable, FindRoot uses the Newton method for finding the root. If we provide two starting values of the variable, FindRoot uses the bisection method.*[1] *Both methods are very sensitive with respect to the starting value(s) of the variable. When choosing bad starting value(s) of the variable, too far from a root, the methods will be divergent.*

In this chapter we briefly present the background for two methods, the Newton method and the secant method. As usually, the set of all points in the plane whose coordinates x, y satisfy the equation $y = f(x)$ will be called the *graph of the function* $f(x)$.

We assume that in the interval $[a, b]$ there is exactly one root c of the function $f(x)$ and that in this interval the function is either increasing or decreasing and that it is convex or concave. For example, let the function $f(x)$ be increasing in the interval $[a, b]$ (i.e. for every $x \in [a, b]$ we have $f'(x) > 0$) and convex (i.e. for every $x \in [a, b]$ we have $f''(x) > 0$). We construct a tangent to the graph of f at the point $B = (b, f(b))$ (see Figure 25.1). The intersection of this tangent with the x-axis is a point $(b_1, 0)$. For the slope (gradient) of tangent line we have

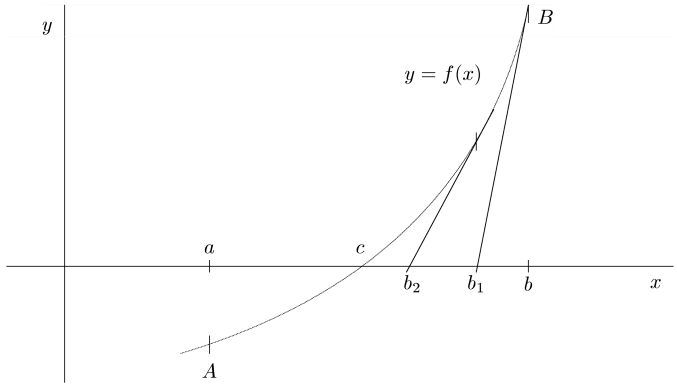

Figure 25.1

[1] We explain a related *secant method.*

$$f'(b) = \frac{f(b)}{b - b_1},$$

from which it follows that

$$b_1 = b - \frac{f(b)}{f'(b)}.$$

If we again construct a tangent to the graph of f at the point $(b_1, f(b_1))$, then analogously for the coordinate b_2 of the intersection $(b_2, 0)$ of the tangent with the x-axis we obtain

$$b_2 = b_1 - \frac{f(b_1)}{f'(b_1)}.$$

This procedure is repeated and we get a sequence (in this case decreasing)

$$b_0,\ b_1,\ b_2,\ \ldots$$

where

$$b_0 = b, \qquad b_{k+1} = b_k - \frac{f(b_k)}{f'(b_k)}, \quad k \in N, \tag{75}$$

which can be shown to converge to the root c of the function $f(x)$.

This method of finding a root (more precisely, its approximate value) is called *Newton's method* or the *method of tangents*. (It is also sometimes called the *Newton-Raphson method*.) Notice that it is necessary to choose the endpoint of an interval in which we start to construct the tangent. It is that endpoint of the interval $[a, b]$ in which the values of a given function and of its second derivative have the same sign (in our case it has been the endpoint b). The next example illustrates when the described Newton's method may fail.[2]

[2] We are indebted to prof. G. Jones for this example and Figure 25.2.

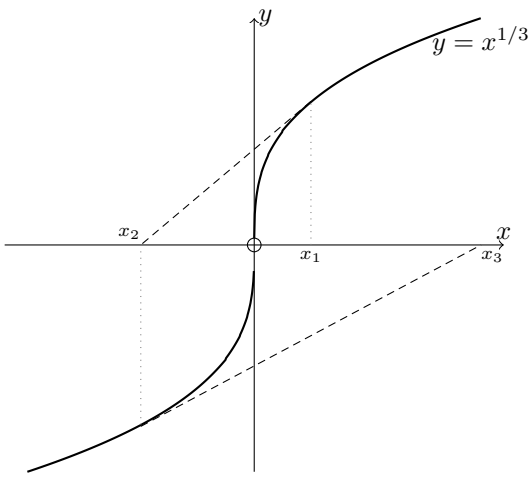

Figure 25.2

Example 25.1. We show that if f and f'' have opposite signs then Newton's method may fail, either by oscillating between two approximations either side of the root, or by diverging away from the root.

We consider the function $f(x) = x^{\frac{1}{3}}$, or more generally, $f(x) = x^{\frac{1}{k}}$ for odd $k \geq 3$. A simple calculation (we leave it as an exercise for the reader) shows that

$$x_{n+1} = -2x_n \quad \text{or more generally,} \quad x_{n+1} = (1-k)x_n.$$

So successive approximations oscillate away from the unique root at 0 (see Figure 25.2).

Of course, no one would try to solve $x^{1/k} = 0$ by this method, but it is easy to believe that if a function has a similar graph then the presented method will fail. ■

The second method for calculating the approximate value of the root c is the *secant method*, or *false position method* (known also as *regula falsi method*). Let us construct the line joining the points $A = (a, f(a))$ and $B = (b, f(b))$. This line intersects the x-axis at a point $(a_1, 0)$. The slope (gradient) of this line is (see Figure 25.3)

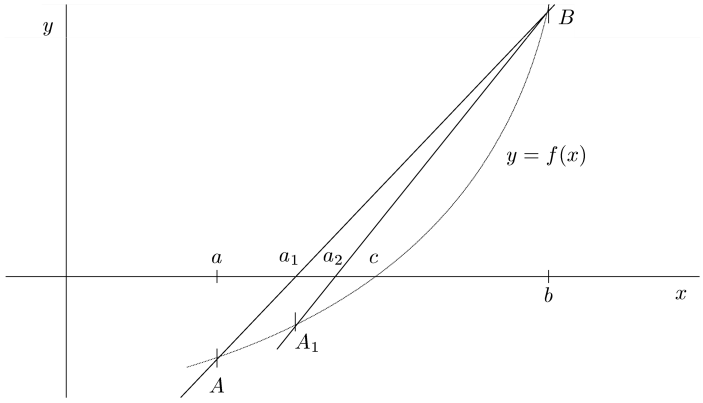

Figure 25.3

$$k = \frac{f(b) - f(a)}{b - a}.$$

If we express it via the points $(a, f(a))$ and $(a_1, 0)$, then we have

$$k = \frac{0 - f(a)}{a_1 - a} = \frac{-f(a)}{a_1 - a},$$

hence

$$\frac{-f(a)}{a_1 - a} = \frac{f(b) - f(a)}{b - a}.$$

After adjustments we obtain

$$a_1 = a - \frac{b - a}{f(b) - f(a)} \cdot f(a).$$

Similarly, the line joining the points $A_1 = (a_1, f(a_1))$ and B intersects the x-axis at a point $(a_2, 0)$, where

$$a_2 = a_1 - \frac{b - a_1}{f(b) - f(a_1)} \cdot f(a_1).$$

If we repeat this procedure, we get the sequence (in this case an increasing one)

$$a_0,\ a_1,\ a_2,\ \ldots$$

where

$$a_0 = a, \qquad a_{k+1} = a_k - \frac{b - a_k}{f(b) - f(a_k)} \cdot f(a_k), \quad k \in N, \tag{76}$$

which can be shown to converge to the root c of the function $f(x)$.

We also proceed analogously in other cases when the given function is increasing and concave or is decreasing and convex or is decreasing and concave (sketch these three cases separately).

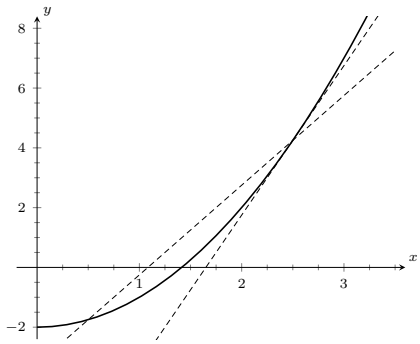

Figure 25.4

Example 25.2. We find an approximate value of the positive root of the polynomial function $f(x) = x^2 - 2$ (i.e. an approximate value of the number $\sqrt{2}$) by both the Newton and the secant methods.

We know this value quite well (the approximate value of $\sqrt{2}$ expressed to eight decimal places is 1.41421356). So we shall be able to compare how quickly we obtain this value by the applied methods. For the calculation we use the 'table editor' Excel.

Consider for example the interval $[0.5, 2.5]$ in which the given function is increasing and convex and in which its positive root lies (see Figure 25.4). In the Table 25.1 we present the values

$$b = b_0 = 2.5,\ b_1,\ b_2,\ \ldots,\ b_{16}$$

for the Newton method and the values

$$a = a_0 = 0.5,\ a_1,\ a_2, \ldots,\ a_{16}$$

for the secant method (in both cases we stopped when both algorithms gave successive approximations agreeing in the first eight decimal places). In our

case (75) has the form

$$b_0 = b = 2.5, \qquad b_{k+1} = b_k - \frac{b_k^2 - 2}{2b_k}, \quad k \in N$$

and (76) has the form

$$a_0 = a = 0.5, \qquad a_{k+1} = a_k - \frac{2.5 - a_k}{6.25 - a_k^2} \cdot (a_k^2 - 2), \quad k \in N$$

(verify it in detail).

One can show (in this particular case we see it from the table) that the Newton method is faster than the secant method. For every $i \in \{1, 2, \ldots, 16\}$ we have determined the interval $[a_i, b_i]$ in which the root lies, that is, we know the root with a maximal error $b_i - a_i$ (it is also given in Table 25.1). ■

Iteration	Newton method	Secant method	Difference
i	b_i	a_i	$\lvert a_i - b_i \rvert$
0	2,50000000	0,50000000	2,00000000
1	1,65000000	1,08333333	0,56666667
2	1,43106061	1,31395349	0,11710712
3	1,41431273	1,38567073	0,02864200
4	1,41421357	1,40623774	0,00797583
5	1,41421356	1,41199659	0,00221698
6	1,41421356	1,41359823	0,00061533
7	1,41421356	1,41404285	0,00017072
8	1,41421356	1,41416620	0,00004736
9	1,41421356	1,41420043	0,00001314
10	1,41421356	1,41420992	0,00000364
11	1,41421356	1,41421255	0,00000101
12	1,41421356	1,41421328	0,00000028
13	1,41421356	1,41421348	0,00000008
14	1,41421356	1,41421354	0,00000002
15	1,41421356	1,41421356	0,00000001
16	1,41421356	1,41421356	0,00000000

Table 25.1

If we use the software *Mathematica* for finding the roots, we can depict the graph of a given function and find the roots for instance via the commands *NSolve* or *FindRoot* mentioned above. In doing so, it is useful to know an

interval containing all real roots of a given function. In case of a polynomial function one can utilise the following statement.

Lemma 25.3. *Let $f(x)$ be a polynomial with real coefficients and let c be a positive real number. If all the coefficients in its Taylor series (see Theorem 20.11 and Example 20.12)*

$$f(x) = b_0 + b_1(x-c) + \cdots + b_n(x-c)^n$$

near c are positive, then every real root of the polynomial function f is less than c.

Proof. If $x \geq c$ then obviously $f(x) > 0$, which means that there is no root of f greater than or equal to c. □

Example 25.4. Using the software *Mathematica* we depict the graph of the polynomial function

$$f(x) = 11x^6 - 7x^5 - 10x^4 + 29x^3 - 26x^2 + 9x - 1 \tag{77}$$

and we find its real roots. We first find an interval containing all real roots of a given function. Using Horner's method we find the Taylor series of the polynomial $f(x)$ near 1. We obtain

$$f(x) = 11(x-1)^6+59(x-1)^5+120(x-1)^4+139(x-1)^3+96(x-1)^2+35(x-1)+5.$$

By Lemma 25.3 all the roots of the polynomial function f are less than 1. A lower bound for real roots of the polynomial function f is found if we substitute $x = -y$ into (77). We get the polynomial

$$g(y) = f(-y) = 11y^6 + 7y^5 - 10y^4 - 29y^3 - 26y^2 - 9y - 1. \tag{78}$$

We find an upper bound c for the real roots of the polynomial function (78). The number $-c$ is then obviously a lower bound for the real roots of the polynomial function (77). By a straightforward calculation we obtain $g(1) = -57$. By Horner's method we find that $g(2) = 413$ (see Table 25.2).

11	7	−10	−29	−26	−9	−1
	22	58	96	134	216	414
11	29	48	67	108	207	413

Table 25.2

Since all the numbers in the last row are positive, the coefficients

$$b_0 = g(2),\ b_1,\ b_2,\ b_3,\ b_4,\ b_5,\ b_6$$

of the Taylor series of the polynomial $g(y)$ near 2 are also positive, which means (by Lemma 25.3) that the number 2 is an upper bound for the roots of the polynomial function (78) and hence the number -2 is obviously a lower bound for the roots of the polynomial function (77). All real roots of the polynomial function (77) thus lie in the interval $[-2, 1]$. If we depict the graph of this polynomial function via the system *Mathematica* for instance in the interval $[-2, 2]$ (see Figure 25.5), we see that at least one of the roots lies in the interval $[-2, -1.5]$. How to *separate* the other roots, i.e. to determine the intervals in which exactly one root lies, cannot yet be seen from the given figure. If we depict the graph of this function for instance in the interval $[-0.1, 0.8]$ (see Figure 25.6) we see that one of the other roots lies in the interval $[0.2, 0.3]$, the next one in the interval $[0.4, 0.5]$ and the last one in the interval $[0.6, 0.7]$. Thus we have found four real roots. Since f(x) has degree 6, exactly two roots are imaginary.

(a) If in *Mathematica* we use the command

$$\texttt{FindRoot}[f[x] == 0, \{x, b_0\}],$$

for the polynomial function (77), then *Mathematica* finds the root via the Newton method and it uses as the starting value the number b_0. For $b_0 = 0.7$ we get the root $x = 0.618034$ as the output:

$$\texttt{FindRoot}[f[x] == 0, x, 0.7],$$

```
x -> 0.618034.
```

(b) If in *Mathematica* we use the command

$$\texttt{FindRoot}[f[x] == 0, \{x, \{a_0, b_0\}\}],$$

then *Mathematica* finds the root via the secant method and it uses as the starting values a_0 and b_0. For $a_0 = 0.6$, $b_0 = 0.7$ we get $x = 0.618033$ as the output:

$$\texttt{FindRoot}[f[x] == 0, x, 0.6, 0.7],$$

```
x -> 0.618033.
```

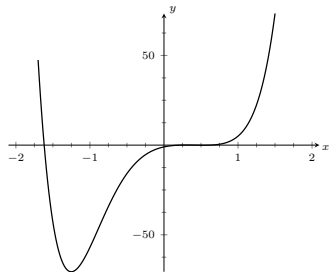

Figure 25.5

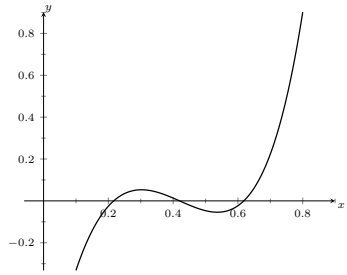

Figure 25.6

(c) In a simple case as is for *Mathematica* our polynomial function (77), *Mathematica* is able to find the roots via the command *NSolve* without giving some starting values and it will present also the imaginary roots. In this case we obtain as the output the following:

$$\texttt{NSolve}[f[x] == 0, x],$$

```
x -> -1.61803, x -> 0.216542, x -> 0.419821,
x -> 0.5 - 0.866025 I, x -> 0.5 + 0.866025 I, x -> 0.618034.
```

Hence the roots of the polynomial function $f(x)$ given in (77) are (correct to six decimal places):

$$x_1 = -1.61803, \quad x_2 = 0.216542, \quad x_3 = 0.419821, \quad x_4 = 0.618034,$$

$$x_5 = 0,5 - 0.866025\, i, \quad x_6 = 0,5 + 0.866025\, i.$$

■

Exercises.

Exercise 25.1. Solve the following equation in *Mathematica* using the command `NSolve`:

$$x^2 + 7x - 3 = 0.$$

Exercise 25.2. Solve the following equation in *Mathematica* using the command `NSolve`:

$$x^5 + 7x + 1 = 0.$$

Exercise 25.3. Solve the following equation in *Mathematica* using the command `NSolve`:

$$x^4 + 3x - 1 = 0.$$

Exercise 25.4. Solve the following equation in *Mathematica* using the command `NSolve`:

$$x^5 - 2x + 3 = 0.$$

Part IV
Answers or solutions to exercises

Chapters 14-25 (Veronika Remenárová)

14 Polynomials in one indeterminate

Exercise 14.1: We shall utilize Theorem 14.2. Let $(A', +, \cdot)$ be a commutative ring with unit element and let $(A, +, \cdot)$ be a subring which contains the unit $1_{A'}$. Let $t \in A' - A$, then

$$\langle A \cup \{t\}\rangle = \{a_0 + a_1 t + \cdots + a_n t^n \mid a_0, a_1, \ldots, a_n \in A, n \in \mathbb{N}\}.$$

(a) We want to prove that $\langle \mathbb{Q} \cup \{\sqrt{8}\}\rangle = \langle \mathbb{Q} \cup \{\sqrt{2}\}\rangle$.
(i) First, we need to prove $\mathbb{Q}[\sqrt{8}] \subseteq \mathbb{Q}[\sqrt{2}]$. We show $x \in \mathbb{Q}[\sqrt{8}] \Rightarrow x \in \mathbb{Q}[\sqrt{2}]$: $x \in \mathbb{Q}[\sqrt{8}] \Rightarrow x = a_0 + a_1\sqrt{8} = a_0 + 2a_1\sqrt{2}; a_0, 2a_1 \in \mathbb{Q} \Rightarrow x \in \mathbb{Q}[\sqrt{2}]$.
(ii) Second, we prove $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt{8}]$ by showing $x \in \mathbb{Q}[\sqrt{2}] \Rightarrow x \in \mathbb{Q}[\sqrt{8}]$: $x \in \mathbb{Q}[\sqrt{2}] \Rightarrow x = a_0 + a_1\sqrt{2} = a_0 + \frac{2}{2}a_1\sqrt{2} = a_0 + \frac{1}{2}a_1 2\sqrt{2} = a_0 + \frac{1}{2}a_1\sqrt{8}; a_0, \frac{1}{2}a_1 \in \mathbb{Q} \Rightarrow x \in \mathbb{Q}[\sqrt{8}]$. From (i) and (ii), $\mathbb{Q}[\sqrt{8}] = \mathbb{Q}[\sqrt{2}]$.
(b) We show that $\mathbb{Z}\left[\sqrt{8}\right] \subsetneq \mathbb{Z}\left[\sqrt{2}\right]$. We start by inspecting the inclusion (i) $\mathbb{Z}\left[\sqrt{8}\right] \subseteq \mathbb{Z}\left[\sqrt{2}\right]$. Equivalently, $x \in \mathbb{Z}\left[\sqrt{8}\right] \Rightarrow \mathbb{Z}\left[\sqrt{2}\right] : x = a_0 + a_1\sqrt{8} = a_0 + 2a_1\sqrt{2}, \quad a_0, 2a_1 \in \mathbb{Z} \Rightarrow x \in \mathbb{Z}\left[\sqrt{2}\right]$. Then we inspect the reverse inclusion (ii) $\mathbb{Z}\left[\sqrt{2}\right] \subseteq \mathbb{Z}\left[\sqrt{8}\right]$, equivalently, $x \in \mathbb{Z}\left[\sqrt{2}\right] \Rightarrow \mathbb{Z}\left[\sqrt{8}\right] : x = a_0 + a_1\sqrt{2} = a_0 + \frac{a_1}{2}\sqrt{8}, \quad a_0 \in \mathbb{Z}$ but $\frac{a_1}{2}$ does not have to belong to $\mathbb{Z}$. A counterexample might be $x = \sqrt{2} = \frac{1}{2}\sqrt{8}$ where $\frac{1}{2} \notin \mathbb{Z}$. We have $x \in \mathbb{Z}\left[\sqrt{2}\right]$ but $x \notin \mathbb{Z}\left[\sqrt{8}\right]$ and so $\mathbb{Z}\left[\sqrt{2}\right] \neq \mathbb{Z}\left[\sqrt{8}\right]$.
(c) We show that $\mathbb{Q}\left[1+\sqrt{3}\right] = \mathbb{Q}\left[1-\sqrt{3}\right]$. We firstly show (i) $\mathbb{Q}\left[1+\sqrt{3}\right] \subseteq \mathbb{Q}\left[1-\sqrt{3}\right]$. Equivalently, $x \in \mathbb{Q}\left[1+\sqrt{3}\right] \Rightarrow x \in \mathbb{Q}\left[1-\sqrt{3}\right] : x = a_0 + a_1(1+\sqrt{3}) = a_0 + a_1 + a_1\sqrt{3} = a_0 + a_1 - (-a_1)\sqrt{3} = a_0 - a_1(1-\sqrt{3}) + 2a_1 = (a_0 + 2a_1) - a_1(1-\sqrt{3}), \quad a_0 + 2a_1, -a_1 \in \mathbb{Q} \Rightarrow x \in \mathbb{Q}\left[1-\sqrt{3}\right]$. The second inclusion is (ii) $\mathbb{Q}\left[1-\sqrt{3}\right] \subseteq \mathbb{Q}\left[1+\sqrt{3}\right]$. Equivalently, $x \in \mathbb{Q}\left[1-\sqrt{3}\right] \Rightarrow x \in \mathbb{Q}\left[1+\sqrt{3}\right] : x = a_0 + a_1(1-\sqrt{3}) = a_0 + a_1 - a_1\sqrt{3} = a_0 + a_1 + (-a_1)\sqrt{3} = a_0 - a_1(1+\sqrt{3}) + 2a_1 = (a_0 + 2a_1) - a_1(1+\sqrt{3})$, here $a_0 + 2a_1, -a_1 \in \mathbb{Q} \Rightarrow x \in \mathbb{Q}\left[1+\sqrt{3}\right]$. From (i) and (ii), $\mathbb{Q}\left[1+\sqrt{3}\right] = \mathbb{Q}\left[1-\sqrt{3}\right]$.

Exercise 14.2: The procedure is analogous to that in Exercise 14.1.

Exercise 14.3: (a) $\mathbb{Q}\left[\sqrt{3}\right] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$: First, we denote $\{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ as B. We want to prove that B is a ring. Let us have $x, y \in B, \quad x = a + b\sqrt{3}, y = c + d\sqrt{3}$. The difference of the two elements is $x - y = (a - c) + (b - d)\sqrt{3} \in B$. The multiplication of the two elements is $x \cdot y = ac + ad\sqrt{3} + bc\sqrt{3} + 3bd = (ac + 3bd) + (ad + bc)\sqrt{3} \in B$. We continue by proving that $\mathbb{Q}\left[\sqrt{3}\right] \subseteq B$. So $x \in \langle \mathbb{Q} \cup \{\sqrt{3}\}\rangle \subseteq B$. If $x \in \mathbb{Q}$, then $x = x + 0\sqrt{3} + \cdots + 0(\sqrt{3})^n \Rightarrow x \in B$. If $x \in \{\sqrt{3}\}$, then $x = 0 + 1\sqrt{3} + 0(\sqrt{3})^2 + \cdots + 0(\sqrt{3})^n \Rightarrow \sqrt{3} \in B$. So we have $x \in B, \sqrt{3} \in B$, which implies $x \in \mathbb{Q} \cup \{\sqrt{3}\} \subseteq B$. Thus $\langle \mathbb{Q} \cup \{\sqrt{3}\}\rangle \subseteq B$.
The procedure in (b), (c), (d) is analogous.

Exercise 14.4: The procedure is analogous to that in Exercise 14.1.

Exercise 14.5: The procedure is analogous to that in Exercise 14.1.

Exercise 14.6: (a) $\sqrt{5} + 1 = t \quad |^2;\ 6 + 2\sqrt{5} = t^2;\ 2\sqrt{5} = t^2 - 6 \quad |^2;\ t^4 - 12t^2 + 16 = 0;\ (\sqrt{5} + 1)^4 - 12(\sqrt{5} + 1)^2 + 16 = 0$. There are non-zero coefficient, and they are from $\mathbb{Z}$, so $\sqrt{5} + 1$ is an algebraic number. (b) $2 - 3i = t \quad |^2;\ -12i = t^2 + 5 \quad |^2;\ t^4 + 10t^2 + 169 = 0;\ (2 - 3i)^4 + 10(2 - 3i)^2 + 169 = 0$. It is an algebraic number. (c) $(\sqrt{3} + \sqrt{2})^4 - 10(\sqrt{3} + \sqrt{2})^2 + 1 = 0$. It is an algebraic number. (d) $(\sqrt{2 + \sqrt{2}})^4 - 4(\sqrt{2 + \sqrt{2}})^2 + 2 = 0$. It is an algebraic number. (e) $3(\sqrt{3} + \frac{1}{\sqrt{3}})^4 - 16 = 0$. It is an algebraic number over $\mathbb{Z}$. (f) $(\sqrt{5} + \sqrt[4]{5})^8 - 20(\sqrt{5} + \sqrt[4]{5})^6 + 140(\sqrt{5} + \sqrt[4]{5})^4 - 530(\sqrt{5} + \sqrt[4]{5})^2 + 400 = 0$. It is an algebraic number over $\mathbb{Z}$.

Exercise 14.7: It is a set $\{a_0 + a_1\sqrt[4]{2} + \cdots + a_r(\sqrt[4]{2})^2 \mid a_0, a_1, \ldots, a_r \in \mathbb{Q}; 0, 1, 2, \ldots, n \in \mathbb{N}\}$.

Exercise 14.8: The rings $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ are not isomorphic.

15 Polynomial function of one variable

Exercise 15.1: $f(x) = (72i\sqrt{3} - 48i\sqrt{2})x^3 + (-16i\sqrt{3} + 36i\sqrt{2})x$.

Exercise 15.2: (a) Let the polynomial function f be as follows: $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3$. By substituting respective numbers into the polynomial function we get four equations

$$\begin{aligned} f(0) &= a_0 = 5, \\ f(-1) &= 5 - a_1 + a_2 - a_3 = 6, \\ f(1) &= 5 + a_1 + a_2 + a_3 = 4, \\ f(2) &= 5 + 2a_1 + 4a_2 + 8a_3 = 9. \end{aligned}$$

The solution may be easily found and it is $f(x) = 5 - 2x + x^3$.

(b) Let us have the polynomial function g, $g(x) = a_0 + a_1 x$. Note that a_0 and a_1 are now in the form of complex numbers, i.e. $a + bi$.

$$\begin{aligned} g(0) &= a_0 = 1 - i, \\ g(1+i) &= 1 - i + a_1(1+i) = 1 - i + a_1 + a_1 i = 1 + i, \\ g(1-i) &= 1 - i + a_1(1-i) = 1 - i + a_1 - a_1 i = 3 - i. \end{aligned}$$

From the last two rows we get $2a_1 i = -2 + 2i$, so a_1 equals $1 + i$. The solution is $g(x) = 1 - i + (1+i)x$.

Exercise 15.3: By comparing the function values of each of the six functions in the points 0, 1 and 2 we find out that f_1 is equal to f_2, f_4 is equal to f_6.

Exercise 15.4:
(a) In $\mathbb{R}[x]$: $f(x) + g(x) = 6 + 4x + 7x^2 + 7x^3 + 3x^4$,
$f(x) \cdot g(x) = 8 + 10x + 27x^2 + 35x^3 + 27x^4 + 32x^5 + 25x^6 + 6x^7$.
(b) In $\mathbb{Z}_7[x]$: $f(x) + g(x) = 6 + 4x + 3x^4$,
$f(x) \cdot g(x) = 1 + 3x + 6x^2 + 6x^4 + 4x^5 + 4x^6 + 6x^7$.
(c) In $\mathbb{Z}_6[x]$: $f(x) + g(x) = 4x + x^2 + x^3 + 3x^4$,
$f(x) \cdot g(x) = 2 + 4x + 3x^2 + 5x^3 + 3x^4 + 2x^5 + x^6$.

Exercise 15.5: Let $\mathbb{F} = \mathbb{Z}_2 = \{0, 1\}$. We show that the sets
$\mathbb{Z}_2^{\mathbb{Z}_2} = \{f : \mathbb{Z}_2 \to \mathbb{Z}_2; f - \text{function}\}$ and
$\mathbb{Z}_2\langle x \rangle$ of polynomial functions over $\mathbb{Z}_2$ are the same:
$\mathbb{Z}_2^{\mathbb{Z}_2}$: $f_0 = \{[0,0],[1,0]\}$, so $f_0(x) = 0 + 0x + 0x^2 + \cdots + 0x^n = 0$,
$f_1 = \{[0,1],[1,0]\}$, so $f_1(x) = 1 + 0x + 0x^2 + \cdots + 0x^n = 1$,
$f_2 = \{[0,0],[1,1]\}$, so $f_2(x) = 0 + 1x + 0x^2 + \cdots + 0x^n = x$,
$f_3 = \{[0,1],[1,1]\}$, so $f_3(x) = 1 + 1x + 0x^2 + \cdots + 0x^n = 1 + x$.
Clearly, $\mathbb{Z}_2\langle x \rangle \subseteq \mathbb{Z}_2^{\mathbb{Z}_2}$ and we showed the equality (instead of $\subseteq$) by expressing each $f \in \mathbb{Z}_2^{\mathbb{Z}_2}$ as a polynomial function, i.e. an element of $\mathbb{Z}_2\langle x \rangle$.
An alternative way of showing that $\subseteq$ is $=$ would be the cardinality argument: evidently $|\mathbb{Z}_2^{\mathbb{Z}_2}| = 4$ an so it suffices to find four different elements of $\mathbb{Z}_2\langle x \rangle$: those are e.g. $0, 1, x, 1 + x$.

Exercise 15.6: $\mathbb{Z}_2[x] = a_0 + a_1 x + a_2 x^2 + a_3 x^3$; $\quad a_0, a_1, a_2, a_3 \in \mathbb{Z}_2$

degree 0	$f(x) = a_0, \quad a_0 \in \mathbb{Z}_2$
	$f_1(x) = 0, \quad f_2(x) = 1,$
degree 1	$f(x) = a_0 + a_1 x, \quad a_0, a_1 \in \mathbb{Z}_2$
	$f_3(x) = x, \quad f_4(x) = 1 + x,$
degree 2	$f(x) = a_0 + a_1 x + a_2 x^2, \quad a_0, a_1, a_2 \in \mathbb{Z}_2$
	$f_5(x) = x^2, \quad f_6(x) = x + x^2, \quad f_7(x) = 1 + x^2, \quad f_8(x) = 1 + x + x^2,$
degree 3	$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3, \quad a_0, a_1, a_2, a_3 \in \mathbb{Z}_2$

$f_9(x) = x^3$, $f_{10}(x) = x^2 + x^3$, $f_{11}(x) = x + x^3$,
$f_{12}(x) = 1 + x^3$, $f_{13}(x) = x + x^2 + x^3$, $f_{14}(x) = 1 + x^2 + x^3$,
$f_{15}(x) = 1 + x + x^3$, $f_{16}(x) = 1 + x + x^2 + x^3$.

You can notice that the number of polynomials in the ring $\mathbb{Z}_2[x]$ of degree at most zero is 2, at most one is 4 (those of degree zero plus of degree one), at most two is 8, at most three is 16 and so forth, so the numbers are 2, 4, 8, 16, 32, 64, 128, ... There exist in general exactly 2^{k+1} ($k \in \mathbb{N}^+$) polynomials of degree at most k in the ring $\mathbb{Z}_2[x]$.

16 Divisibility of polynomials

Exercise 16.1:
(a) $q(x) = x + 9$, $r(x) = 66x^2 + 66$, (b) $q(x) = x - 8$, $r(x) = 1$, (c) $q(x) = x^3 - 2x^2 + 7x - 5$, $r(x) = 0$, (d) $q(x) = x^3 + (6-i)x - 2 - 10i$, $r(x) = (-6+i)x - 36i - 6$, (e) $q(x) = \frac{5}{7}x^2 + \frac{4}{7}x - \frac{10}{49}$, $r(x) = x^3 + \frac{181}{49}x^2 + \frac{12}{49}x + \frac{69}{49}$.

Exercise 16.2:
(a) $q(x) = 2x^2 + 2x + 2$, $r(x) = 1$, (b) $q(x) = 2x^2 + 4x$, $r(x) = x^2 + 3x + 2$, (c) $q(x) = x^2 + 3x + 3$, $r(x) = 4x^2$, (d) $q(x) = 2x + 2$, $r(x) = 0$.

Exercise 16.3: (a) $a = -1$, $b = -6$, (b) $a = -50$, $b = -10$.

Exercise 16.4: (a) $[a, b, c] = \{[-4, -1, -1], [-14, 5, 1], [-2, 1, -3], [0, 3, 3]\}$, (b) $[a, b, c] = \{[-2, -2, -1], [2, 2, 1]\}$.

Exercise 16.5: (a) $gcd(f(x), g(x)) \sim x^2 + 1$, (b) $gcd(f(x), g(x)) \sim 2$, (c) $gcd(f(x), g(x)) \sim x + 1$, (d) $gcd(f(x), g(x)) \sim x^2 + 3x + 2$, (e) $gcd(f(x), g(x)) \sim x^2 - 2x + 2$.

Exercise 16.6: (a) $gcd(f(x), g(x)) \sim -1$, (b) $gcd(f(x), g(x)) \sim -2x + 3$.

Exercise 16.7: $a = -3$, $b = 2$.

17 Decomposition of polynomials

Exercise 17.1: Let us compute a discriminant of $x^2 + 4 = 0$.
The discriminant $D = -16$ is negative, the polynomial is irreducible in $\mathbb{R}[x]$.

Exercise 17.2: (a) $(x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$. Hint: Find the complex roots of the polynomial (there are obviously 4 such roots), and multiply two and two in decomposition, in order to get rid of complex parts of the roots. (b) $(x^2 + \sqrt{3}x + 1)(x^2 - \sqrt{3}x + 1)$. Hint: Decompose the polynomial as in the previous case, or utilize the fact that the cubic element is missing, i.e. the decomposition in such case looks like $(x^2 + ax + b)(x^2 - ax + c)$.

Exercise 17.3:

$gcd(f(x), g(x)) = x^2 + 2x + 4, \quad lcm(f(x), g(x)) = (x-2)(x^2+2x+4)(x-1)(x+1)$.

Exercise 17.4:
$gcd(f(x), g(x)) = x + i, \quad lcm(f(x), g(x)) = (x+1)(x+i)^2(x-i)^2$.

18 Roots of polynomial functions

Exercise 18.1: (a) $q(x) = 2x^4 + 5x^3 - 8x^2 - 8x + 23, \quad r(x) = 8$,
(b) $q(x) = 2x^4 - 3x^3 - 4x^2 + 12x - 5, \quad r(x) = 0$.

Exercise 18.2: $k = 3$

	3	−16	25	−6	−4	−8
2		6	−20	10	8	8
	3	−10	5	4	4	0
2		6	−8	−6	−4	
	3	−4	−3	−2	0	
2		6	4	2		
	3	2	1	0		
2		6	16			
	3	8	17	$\neq 0$		

Exercise 18.3:
(a) $f(-2) = (-2)^7 + 2(-2)^6 + (-2)^4 - 5(-2)^3 + 3(-2)^2 + 1 = 69$
(b)

	1	2	0	1	−5	3	0	1
−2		−2	0	0	−2	14	−34	68
	1	0	0	1	−7	17	−34	69

Exercise 18.4:

(a) $(x+3) \mid (x^3+2x^2+ax+24)$, i.e. -3 is a root

$$\begin{aligned}(-3)^3+2(-3)^2+a(-3)+24&=0\\ 15-3a&=0\\ a&=5\end{aligned}$$

(b)

	1	2	a	24
-3		-3	3	$-9-3a$
	1	-1	$3+a$	$-3a+15$
				$\Rightarrow a=5$

Exercise 18.5:

	1	$2-2i$	0	$1+i$	$-(1+i)$	0	$2i$
$-1+i$		$-1+i$	$2i$	$-2-2i$	2	$2i$	$-2-2i$
	1	$1-i$	$2i$	$-1-i$	$1-i$	$2i$	-2

$q(x)=x^5+(1-i)x^4+2ix^3-(1+i)x^2+(1-i)x+2i, \quad r(x)=-2.$

Exercise 18.6: $a=11, b=-32$. Hint: Find the roots of the polynomial x^2-4x+3, and substitute them one by one to the given polynomial.

Exercise 18.7: $[a,b,c]=\{[3,-6,-28]\}$. Hint: Proceed by Horner's scheme and then solve the system of three linear equations in three variables a,b,c.

19 Polynomials with complex, real and integer coefficients

Exercise 19.1: The roots of the given polynomial function are $1+i$, $1-i$, $-1-\sqrt{3}$, $-1+\sqrt{3}$. Hint: Begin with the utilization of the Theorem 19.3.

Exercise 19.2: $f(x)=x^5-2x4-x^3+8x^2-10x+4$. Hint: Have in mind the Theorem 19.3.

Exercise 19.3: (a) Rational roots are $-2,-\frac{1}{2},1$. (b) Rational roots are $1,2,3$. (c) Rational root is a 2-root $-\frac{1}{2}$.

Exercise 19.4: $16x^4-8x+3=16(x-\frac{1}{2})^2(x+\frac{1}{2}+\frac{\sqrt{2}i}{2})(x+\frac{1}{2}-\frac{\sqrt{2}i}{2})$.

20 Derivatives of polynomials

Exercise 20.1: For $a = 9$ the third root is -1, and for $a = -\frac{13}{27}$ it is $\frac{13}{3}$.
Exercise 20.2: $g(x) = 1 - (x+3)^3 + (x+3)^4$.
Exercise 20.3: $h(x) = x^4 - 4x^3 + 6x^2 + 2x + 8$.

21 Polynomials in several indeterminates

Exercise 21.1: (a) 13, (b) -2, (c) 30.
Exercise 21.2: (a) $x^3-8x^2+21x-17$, (b) x^3-x^2-2x-1, (c) x^3-4x^2+5x-3, (d) $x^3 - 2x^2 + 5x - 1$.
Exercise 21.3: (a) $[x, y] = \{[-1, 2]\}$, (b) $[x, y] = \{[2, 3], [-3, -2]\}$, (c) $[x, y, z] = \{[-3, -1, 1]\}$, (d) $[x, y, z] = \{[-1, 1, 2]\}$.

22 Solving binomial equations

Exercise 22.1: (a) $x_0 = 1, x_1 = \frac{1}{2} + \frac{\sqrt{3}}{2}i, x_2 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i, x_3 = -1, x_4 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i, x_5 = \frac{1}{2} - \frac{\sqrt{3}}{2}i$, (b) $x_0 = \frac{1}{2}, x_1 = \frac{1}{2}i, x_2 = -\frac{1}{2}, x_3 = -\frac{1}{2}i$, (c) $x_0 = \sqrt{5}, x_1 = \frac{\sqrt{10}}{2} + \frac{\sqrt{10}}{2}i, x_2 = \sqrt{5}i, x_3 = -\frac{\sqrt{10}}{2} + \frac{\sqrt{10}}{2}i, x_4 = -\sqrt{5}, x_5 = -\frac{\sqrt{10}}{2} - \frac{\sqrt{10}}{2}i, x_6 = -\sqrt{5}i, x_7 = \frac{\sqrt{10}}{2} - \frac{\sqrt{10}}{2}i$, (d) $x_0 = \frac{\sqrt{3}}{2} + \frac{1}{2}i, x_1 = -\frac{\sqrt{3}}{2} + \frac{1}{2}i, x_2 = -i$.
Exercise 22.2: (a) $f(x) = (x^2 - x + 1)(x^2 + x + 1)(x + 1)(x - 1)$,
(b) $f(x) = (x^2+\sqrt{2+\sqrt{2}}x+1)(x^2-\sqrt{2+\sqrt{2}}x+1)(x^2+\sqrt{2-\sqrt{2}}x+1)(x^2-\sqrt{2-\sqrt{2}}x+1)$, (c) $f(x) = (x^2 + \sqrt[4]{8}x + \sqrt{2})(x^2 - \sqrt[4]{8}x + \sqrt{2})$.

23 Quadratic and cubic equations over $\mathbb{C}$

Exercise 23.1: (a) $x_1 = 3 - i, x_2 = -1 + 2i$, (b) $x_1 = 1 - i, x_2 = \frac{4}{5} - \frac{2}{5}i$, (c) $x_1 = 3 - 2i, x_2 = 3 - 2i$.
Exercise 23.2:
(a) $x^4 - 3x^2 + 4 = (x - \frac{\sqrt{7}}{2} - \frac{1}{2}i)(x + \frac{\sqrt{7}}{2} + \frac{1}{2}i)(x - \frac{\sqrt{7}}{2} + \frac{1}{2}i)(x + \frac{\sqrt{7}}{2} - \frac{1}{2}i)$,
(b) $x^4 - 3x^2 + 4 = (x^2 - \sqrt{7}x + 2)(x^2 + \sqrt{7}x + 2)$.
Exercise 23.3: $x^4 + 6x^3 + 9x^2 + 100 = (x^2 - 2x + 5)(x^2 + 8x + 20)$
Exercise 23.4: The polynomial may be firstly decomposed as a product of two quadratics, moreover the cubic term is missing so try to solve $(x^2 + ax + b)(x^2 - ax + c) = x^4 + 2x^2 - 24x + 72$. From there we have that $bc = 72$ and $a(b - c) = 24$. So we want to factor 72 as a product of two numbers whose difference divides 24. Surveying the options, we find out $b = 12, c = 6$, so

$a = 4$. From the factorization $(x^2 + 4x + 12)(x^2 - 4x + 6)$ we may quickly find all the roots of the polynomial and those are $x_1 = -2 + 2\sqrt{2}i, x_2 = -2 - 2\sqrt{2}i, x_3 = 2 + \sqrt{2}i, x_4 = 2 - \sqrt{2}i$.

Exercise 23.5: (a) $x_1 = 1, x_2 = 4 + 2\sqrt{3}i, x_3 = 4 - 2\sqrt{3}i$, (b) $x_1 = 2\sqrt{3} - 1, x_2 = -1 - 2\sqrt{3}, x_3 = 2$, (c) $x_1 = -2, x_2 = 1 + 2i.x_3 = 1 - 2i$.

24 Reciprocal equations

Exercise 24.1:
(a) Proceed by substitution $z = x^2$ and then solve as a quadratic equation.
(b) It is a positively reciprocal equation of even degree. In the first step, multiply the equation by $\frac{1}{x^2}$ and then follow by substitution to find the roots. $x_1 = \frac{1}{2} + \frac{\sqrt{3}}{2}i, x_2 = \frac{1}{2} - \frac{\sqrt{3}}{2}i, x_3 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i, x_4 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$.

Exercise 24.2: (a) Proceed by de Moivre's Theorem to get all five roots. They form the regular pentagon inscribed in circle with radius of one.
(b) It is a negatively reciprocal equation of odd degree, i.e. the first known root is one. Then proceed, for instance, by Horner's scheme to divide the polynomial by $x - 1$, and you get the positively reciprocal equation of even degree. $x_1 = 1, x_2 = \frac{-1+\sqrt{5}}{4} + \sqrt{\frac{5+\sqrt{5}}{8}}i, x_3 = \frac{-1+\sqrt{5}}{4} - \sqrt{\frac{5+\sqrt{5}}{8}}i, x_4 = -\frac{1+\sqrt{5}}{4} + \sqrt{\frac{5-\sqrt{5}}{8}}i, x_5 = -\frac{1+\sqrt{5}}{4} - \sqrt{\frac{5-\sqrt{5}}{8}}i$.

Exercise 24.3: (a) $x_1 = \frac{3}{2} + \frac{\sqrt{5}}{2}, x_2 = \frac{3}{2} - \frac{\sqrt{5}}{2}, x_3 = \frac{1}{2} + \frac{\sqrt{3}}{2}i, x_4 = \frac{1}{2} - \frac{\sqrt{3}}{2}i$, (b) $x_1 = \frac{-1+\sqrt{2}}{2} + \frac{\sqrt{1+2\sqrt{2}}}{2}i, x_2 = \frac{-1+\sqrt{2}}{2} - \frac{\sqrt{1+2\sqrt{2}}}{2}i, x_3 = \frac{-1-\sqrt{2}}{2} + \frac{\sqrt{-1+2\sqrt{2}}}{2}i, x_4 = \frac{-1-\sqrt{2}}{2} - \frac{\sqrt{-1+2\sqrt{2}}}{2}i$, (c) $x_1 = i, x_2 = -i, x_3 = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, x_4 = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i, x_5 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, x_6 = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$, (d) $x_1 = \frac{1}{2}, x_2 = \frac{1}{2}, x_3 = \frac{-1+\sqrt{5}}{4} + \sqrt{\frac{5+\sqrt{5}}{8}}i, x_4 = \frac{-1+\sqrt{5}}{4} - \sqrt{\frac{5+\sqrt{5}}{8}}i, x_5 = -\frac{1+\sqrt{5}}{4} + \sqrt{\frac{5-\sqrt{5}}{8}}i, x_6 = -\frac{1+\sqrt{5}}{4} - \sqrt{\frac{5-\sqrt{5}}{8}}i$.

25 Numerical methods for solving algebraic equations

Exercise 25.1:

```
>> NSolve[x^2 + 7 x - 3 == 0, x]
{{x -> -7.40512}, {x -> 0.405125}}
```

Exercise 25.2:

```
>> NSolve[x^5 + 7 x + 1 == 0, x]
{{x -> -1.11308 - 1.15173 I}, {x -> -1.11308 + 1.15173 I},
{x -> -0.142849}, {x -> 1.1845 - 1.15139 I},
{x -> 1.1845 + 1.15139 I}}
```

Exercise 25.3:

```
>> NSolve[x^4 + 3 x - 1 == 0, x]
{{x -> -1.53961}, {x -> 0.329409}, {x -> 0.605102 - 1.26713 I},
{x -> 0.605102 + 1.26713 I}}
```

Exercise 25.4:

```
>> NSolve[x^5 - 2 x + 3 == 0, x]
{{x -> -1.42361}, {x -> -0.246729 - 1.32082 I},
{x -> -0.246729 + 1.32082 I}, {x -> 0.958532 - 0.498428 I},
{x -> 0.958532 + 0.498428 I}}
```

Bibliography

[1] S.C. Althoen and R. McLaughlin, *Gauss-Jordan reduction: A brief history*, MAA Monthly **94** (1987), 130–142.

[2] G. Birkhoff and S. Mac Lane, *A survey of modern algebra*, Macmillan Publishing Co., New York, 1941. Slovak translation: *Prehľad modernej algebry*, Alfa, Bratislava, 1979.

[3] J.L. Chabert et. al., *A History of Algorithms: From the Pebble to the Microchip*, Springer-Verlag, 1999.

[4] M. Haviar, *ALGEBRA III: Lineárna algebra*, Lecture notes (in Slovak), Pedagogics faculty, M. Bel University, Banská Bystrica, 2001.

[5] M. Haviar and P. Klenovčan, *ALGEBRA I: Algebraické štruktúry*, Lecture notes (in Slovak), Pedagogics faculty, M. Bel University, Banská Bystrica, 1998.

[6] T. Katriňák et al., *Algebra a teoretická aritmetika 1* (in Slovak), Alfa, Bratislava, 1985.

[7] P. Klenovčan, *ALGEBRA II: Polynomická algebra*, Lecture notes (in Slovak), Pedagogics faculty, M. Bel University, Banská Bystrica, 2001.

[8] P. Klenovčan, A. Haviar and M. Haviar, *Úvod do štúdia matematiky*, Lecture notes (in Slovak), Pedagogics faculty, M. Bel University, Banská Bystrica, 1996.

[9] M. Kolibiar et al., *ALGEBRA a príbuzné disciplíny* (in Slovak), Alfa, Bratislava, 1991.

[10] M. Komorníková and K. Mikula, *Mathematica* (manual, in Slovak), STU, Bratislava, 1998.

[11] S. Mac Lane and G. Birkhoff, *Algebra*, The Mac Millan Co, New York, 1967. Slovak translation: *Algebra*, Alfa, Bratislava, 1973.

[12] M. Ronan, *Symmetry and the Monster: One of the Greatest Quests of Mathematics*, Oxford University Press, Oxford, 2006.

[13] P. Zlatoš, *LINEÁRNA ALGEBRA A GEOMETRIA, Cesta z troch rozmerov s presahmi do príbuzných odborov*, Marenčin PT, Bratislava, 2011.

[14] Wikipedia: The Free Encyclopedia. (Used for historical remarks only.) Available at `en.wikipedia.org/wiki/`.

[15] Wolfram Research, Inc., *Mathematica, Version 12.0*, `https://www.wolfram.com/mathematica`, Champaign, IL, 2020.

Index

Názov	**Basic Algebra for future teachers**
Autori	prof. RNDr. Miroslav Haviar, CSc. doc. RNDr. Pavel Klenovčan, CSc.
Počet strán Druhé vydanie	390
Tlačová úprava	doc. Mgr. Ján Karabáš, PhD. Sadzba používajúca LaTeX a KOMA-Script
Návrh obálky	Mgr. art. Zuzana Ceglédyová
Vydavateľ	Belianum, Vydavateľstvo Univerzity Mateja Bela v Banskej Bystrici, Fakulta prírodných vied, 2020
Tlač	Equilibria, s.r.o., Košice
ISBN 978-80-557-1746-3	
EAN 9788055717463	