POLYNOMIALS

One week

Contents

Module **2**

Motivation **2**

Learning outcomes **2**

1 Polynomials and operations **3**
1.1 Summary . . . 3
1.2 Exercises . . . 3
Exercise 1.1 . . . 3
Exercise 1.2 . . . 3

2 Euclidean division of polynomials **4**
2.1 Summary . . . 4
2.2 Exercises . . . 4
Exercise 2.3 . . . 4
Exercise 2.4 . . . 4

3 Roots and factorization **4**
3.1 Summary . . . 4
3.2 Exercises . . . 5
Exercise 3.5 . . . 5
Exercise 3.6 . . . 5
Exercise 3.7 . . . 5
Exercise 3.8 . . . 6
Exercise 3.9 . . . 6
★ Exercise 3.10 . . . 6

Module

This chapter is part of the APEF module: Analysis, Polynomials, Differential Equations, Functions. It is in the B3.

The **prerequisites** are:

- Module [MATH-S1-1-OBM] (seminar).
- Expanding a product of polynomials.
- Solving a 2nd degree equation.

Motivation

This chapter is partly an extension of the "Number theory" chapter (S1). It will deal with the arithmetic of polynomials, which includes studying the roots and factorizing a polynomial.

A polynomial with coefficients in a given set $\mathbb{K}$ is an expression resulting of adding and multiplying the variables and the coefficients. Formally, when there is only one variable, a polynomial $P = a_0 + a_1X + \cdots + a_NX^N$ can be represented[1] by the sequence (a_n) of its coefficients. This sequence has a finite support, that is, its terms are zeros above a certain rank.

You have handled polynomials with real coefficients before. Their purpose was to define real functions of a real variable. They will mainly be used in that purpose this semester. However, they can be used to define other objects. For example, the polynomial $P = X^2 - 3X + +2$ can also define the differential operator $f \longmapsto f'' - 3f' + 2f$. You will see at the next chapter the connection between the roots of P and the solution set of the differential equation $f'' - 3f' + 2f = 0$.

On the sets of polynomials with one variable and real or complex coefficients –denoted by $\mathbb{R}[X]$ and $\mathbb{C}[X]$– we naturally define an addition and a multiplication. These operations satisfy the same properties than those on the set of integers. It is hence possible to extend the concepts defined for the integers: divisibility relation, euclidean division, GCD, Bézout theorem, etc. Irreducible polynomials are equivalent to prime numbers: they cannot be split as a product of two smaller degree polynomials. And any polynomial can be factorized in a unique way as the product of a constant number and irreducible unitary polynomials[2].

Yet, the polynomials do not behave exactly like integers: they are more complex objects, they have other operations such as differentiation and composition. Still, they are generated by basic operations and remain quite easy to handle. That's why they are good candidates for interpolation problems (approximations with easy to handle objects). Later, you will use Taylor formula, Lagrange's interpolation, Weierstrass theorem or Fourier series using trigonometric polynomials[3].

Learning outcomes

At the end of this chapter, you are expected to be able to combine the operations of factorizing a polynomial and of finding its roots and their orders of multiplicity.

In that purpose, you will have to be able to:

- Find the degree of a polynomial, of a sum or a product of polynomials.
- State the euclidean division theorem for polynomials.

[1] It is the representation that you would use in a programming framework, for example with a list.

[2] A polynomial is unitary if its highest degree coefficient is 1. The multiplication of polynomials by constant numbers does not change the divisibility relation and we restrict to unitary polynomials to ensure the uniqueness of the factorization.

[3] These methods even make it possible to define sequences of polynomials converging to the function we want to model and enabling one to control of the speed of convergence.

- Execute a euclidean division of polynomials.
- Connect the notions of finding a polynomial's root and of factorizing this polynomial.
- Connect the multiplicity of a root with the values if the successive derivatives.
- Find the order of multiplicity of a polynomial's root.
- Factorize a polynomial as a product of irreducible polynomials (irreducible in $\mathbb{C}[X]$ or in $\mathbb{R}[X]$).

1 Polynomials and operations

1.1 Summary

Formally, a polynomial with one variable and coefficients in $\mathbb{R}$ or $\mathbb{C}$ can be represented with the sequence (a_n) of its coefficients, whose terms are zeros above a certain rank.

This definition enables one to define the degree of the polynomial, as well as the classical operations of addition, intern multiplication and external multiplication. It also enables one to define the derivative polynomial. The coefficients of a polynomial can be related with the successive derivatives of the polynomial at a given point (see Taylor formulas).

1.2 Exercises

Exercise 1.1

1. Let $P(X) = -2X^3 + 3X - 4$, $Q(X) = 3X^2 + 6X - 2$ and $R(X) = 1 + 2X^3$.

   Compute $P(X) + Q(X)$, $P(X) + R(X)$ and $Q(X) + R(X)$. Deduce a formula for the degree of a sum of 2 polynomials.

2. Find the degree (and the highest degree monomial) of $A(X) = X^2(X^3 - 4)(2X + 1)^2$. Same question for $B(X) = (5X^2 + X - 3)^2 - X^3 + 2$.

Exercise 1.2

Consider the polynomial $P(X) = 3X^3 - 2X^2 - 7X + 6 = \sum_{k=0}^{3} a_k X^k$.

1. What are the values of a_0, a_1, a_2 and a_3?
2. Compute the successive derivatives of P at $x = 0$.
3. Find the relation between $P(0)$ and the coefficients of P.
4. Similarly, find the relations between $P'(0)$, $P''(0)$, $P^{(3)}(0)$ and the coefficients of P.
5. Propose a general formula between the derivatives of P at $x = 0$ and the coefficients of P. Deduce a new expression of P.
6. ($\star$) Let $Y = X - 1$.

   (a) Explain why $P(X)$ can be expressed as: $Q(Y) = \sum_{k=0}^{3} b_k Y^k$

   where, for all $k \in [\![0, 3]\!]$, $b_k = \dfrac{Q^{(k)}(0)}{k!}$.

   (b) Deduce that

$$P(X) = \sum_{k=0}^{3} \frac{P^{(k)}(1)}{k!}(X - 1)^k$$

2 Euclidean division of polynomials

2.1 Summary

The euclidean division of polynomials is similar to the one of integers, but the condition for the remainder is slightly different: it is a condition about its degree. This condition ensures the convergence of Euclid algorithm, because the sequence of the remainders' degree is positive and strictly decreasing, as long as the remainder is non-zero. Here also, the algorithm results in the GCD of two polynomials.

The euclidean division is done with an algorithm: at each step, the degree of the remainder is decremented until it satisfies the condition (then we cannot execute the next step). Running several euclidean division until getting the GCD of two polynomials may be long when done manually, but it raises no problem with a computer.

For the GCD's definition, we add the condition that its highest degree coefficient is equal to 1: this means it is a unitary polynomial and this condition ensures the uniqueness of the GCD. Indeed, the divisibility relation between polynomials is not altered when one of them is multiplied by a non-zero constant number and any common divisor remains a common divisor when multiplied by such a constant. More generally, the condition for a divisor to be a unitary polynomial is often used, it ensures the uniqueness of the operation's result ***modulo a constant value***.

At last, note that there exist other divisions of polynomials[4]. For example, the division by increasing power order is similar to the euclidean division, but in the reverse direction; at each step, the remainder's degree is incremented.

2.2 Exercises

Exercise 2.3

1. Do the euclidean division of $2X^4 - X^2 + X - 5$ by $X^2 + X - 2$.
2. Do the euclidean division of $X^3 + X + 1$ by $2X + 1$.

Exercise 2.4

1. Do the euclidean division of $X^4 + 2X^3 + X$ by $X^2 + 1$.
2. Deduce a primitive over $\mathbb{R}$ of the function $\left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \dfrac{x^4 + 2x^3 + x}{x^2 + 1} \end{array} \right.$

3 Roots and factorization

3.1 Summary

The roots of a polynomials P are the values of the variable for which $P(x)$ is equal to 0. Studying the roots enables one to solve numerous problems involving polynomial models. Furthermore, the relation between roots and factorization, which is explored in exercise 3-5, suggests an iterative process to factorize a polynomial, provided that an efficient method to find the roots exists.

Similarly to the multiplicity of prime factors for an integer number, the multiplicity of a root a of a polynomial P is the power of $(X - a)$ in the factorization of P. It is possible to characterize the multiplicity with the successive derivatives of P: ***grosso modo***, the multiplicity of a root is decremented from 1 at each derivation. A root of multiplicity at least 2 is hence also a root of P'. For example, it is possible to outline the part of P containing all the factors of multiplicity at least 2: just calculate the GCD of P and P'[5].

[4]Similarly, there are non euclidean divisions of integers. For example, the division of the CamL language results in a remainder with the minimum absolute value: $-\frac{b}{2} < r \leqslant \frac{b}{2}$. The resulting Euclid algorithm is slightly altered and its convergence a little bit faster.

[5]That is the reason why the factorization algorithms, such as Berlekamp or Cantor-Zassenhaus algorithms, focus on the roots of multiplicity 1: they suppose that the first step has been done to search before the roots of greater multiplicity.

There are methods to extracts the roots of degree 2 polynomials (also for the degrees 3 and 4, with heavy substitutions and complex numbers) but there are no general methods for greater degrees. Searching for the roots of polynomials is a challenge for many algorithmic researches. The real roots may be numerically approximated by numerical sequences using functional analysis properties (for example, research by dichotomy), but these methods do not work for complex roots. Hence, problems involving only simple operations (additions and multiplications) can be very complex to solve.

Similar to integers factorization, polynomials factorization enables divide and rule' strategies and parallelization. We will see later the interest of polynomials in linear algebra (reduction of square matrices) and how their factorization can simplify some calculations which at first glance seem to be extremely complex.

3.2 Exercises

Exercise 3.5

1. Let $P \in \mathbb{K}[X]$ where $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$, and $a \in \mathbb{K}$. What is the remainder of the euclidean division of P by $X - a$?

2. Deduce the following property:

$$(X - a) \mid P \iff P(a) = 0$$

3. Let $P \in \mathbb{R}[X]$ and $(a, b) \in \mathbb{R}^2$ such that $a \neq b$. Show that

$$(X - a)(X - b) \mid P \iff P(a) = P(b) = 0$$

Exercise 3.6

Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$, $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ and $\alpha \in \mathbb{N}^*$.

1. (a) What is the sense (in terms of divisibility) of "a is a root of order of multiplicity at least α of P" and of "a is a root of order of multiplicity exactly α of P"?

   (b) Practical case: consider $P(X) = (X^2 - X)(X - 1)^2(-1 - X) \in \mathbb{R}[X]$. Find the roots of P and their exact orders of multiplicity.

2. (a) What is the connection between the order of multiplicity of the root a and the successive derivatives of P at a?

   (b) We accept without proof that the polynomial P above can also be written $P(X) = -X^5 + 2X^4 - 2X^2 + X$. Using the successive derivatives of P, confirm the answers that you got at question 1.(b).

3. (a) What is the sense of "P is irreducible in $\mathbb{K}[X]$"? Which polynomials are irreducible in $\mathbb{R}[X]$ and in $\mathbb{C}[X]$?

   (b) Let $P(X) = (X^3 + X)(X^2 - 2X)$. Express P as a product of irreducible polynomials in $\mathbb{R}[X]$, then irreducible in $\mathbb{C}[X]$.

Exercise 3.7

1. Consider the polynomial $P(X) = X^4 + 2X^3 - X - 2$.

   (a) Show that 1 and -2 are roots of P. What can you deduce in terms of divisibility?

   (b) Using a euclidean division, factorize P as a product of irreducible polynomials in $\mathbb{R}[X]$.

2. **(Homework)** Consider the polynomial $Q(X) = X^4 - 2X^3 - 3X^2 + 8X - 4$.

   (a) Show that 2 and -2 are roots of Q. What can you deduce in terms of divisibility?

(b) Using a euclidean division, factorize Q as a product of irreducible polynomials in $\mathbb{R}[X]$.

3. Consider the polynomial $R(X) = X^4 - 3X^3 - 3X^2 + 11X - 6$.

   (a) Show that 1 is a root of R. Find its multiplicity. What can you deduce in terms of divisibility?

   (b) Using a euclidean division, factorize R as a product of irreducible polynomials in $\mathbb{R}[X]$.

Exercise 3.8

Let $n \geqslant 2$.

1. Show that $P(X) = (X+1)^{2n} - 1$ is a multiple of $X^2 + 2X$.
2. Show that $(X-1)^2$ divides $nX^{n+1} - (n+1)X^n + 1$.
3. Show that 1 is a root of the polynomial $nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$. Find its multiplicity.

Exercise 3.9

Find the remainder of the euclidean division of $P(X) = (X-2)^{2n} + (X-1)^n - 2$ by

1. $(X-2)(X-1)$.
2. $(X-1)^2$.

★ **Exercise 3.10**

Find the unitary polynomials in $\mathbb{R}[X]$ of degree 3, multiples of $X-1$, with equal remainders after the divisions by $X-2$, $X-3$ and $X-4$.