Note 4

Polynomials

4.1 Definition of polynomials

In this chapter we will investigate a certain type of expressions called polynomials. Polynomials will come up again later, when we discuss differential equations, examples of vector spaces, and eigenvalues of a matrix, but that is for later. For now, we start by defining what a polynomial is.

Definition 4.1

A *polynomial* $p(Z)$ in a variable Z is an expression of the form:

$$p(Z) = a_0 Z^0 + a_1 Z^1 + a_2 Z^2 + \cdots + a_n Z^n, \text{ with } n \in \mathbb{Z}_{\geq 0} \text{ a non-negative integer.}$$

Here the symbols $a_0, a_1, a_2, \ldots, a_n \in \mathbb{C}$ denote complex numbers, which are called the *coefficients* of $p(Z)$. The expressions $a_0 Z^0, a_1 Z^1, \ldots, a_n Z^n$ are called the *terms* of the polynomial $p(Z)$. The largest i for which $a_i \neq 0$ is called the *degree* of $p(Z)$ and is denoted by $\deg(p(Z))$. The corresponding coefficient is called the *leading coefficient*. Finally, the set of all polynomials in Z with complex coefficients is denoted by $\mathbb{C}[Z]$.

It is common not to write Z^0 and to write Z instead of Z^1. Then a polynomial is simply written as $p(Z) = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_n Z^n$. A polynomial of degree zero can then just be interpreted as a nonzero constant a_0, while a polynomial of degree one has the form $a_0 + a_1 Z$. The polynomial all of whose coefficients are zero is called the *zero* *polynomial* and denoted by 0. It is customary to define the degree of the zero polynomial to be $-\infty$, minus infinity.

By definition, the coefficients completely determine a polynomial. In other words: two polynomials $p_1(Z) = a_0 + a_1 Z \cdots + a_n Z^n$ of degree n and $p_2(Z) = b_0 + b_1 Z \cdots + b_m Z^m$ of degree m are equal if and only if $n = m$ and $a_i = b_i$ for all i. The order of the terms is not important. For example, the polynomials $Z^2 + 2Z + 3$, $Z^2 + 3 + 2Z$ and $3 + 2Z + Z^2$ are all the same. The notation $\mathbb{C}[Z]$ for the set of all polynomials with coefficients in $\mathbb{C}$ is standard, but the symbol used to indicate the variable, in our case Z, varies from book to book. We have chosen Z, since we have been using z for complex numbers. Other sets of polynomials can be obtained by replacing $\mathbb{C}$ by something else. For example, we will frequently use $\mathbb{R}[Z]$, which denotes the set of all polynomials with coefficients in $\mathbb{R}$. Note that $\mathbb{R}[Z] \subseteq \mathbb{C}[Z]$, since $\mathbb{R} \subseteq \mathbb{C}$.

|||| Example 4.2

Indicate which of the following expressions is an element of $\mathbb{C}[Z]$. If the expression is a polynomial, give its degree and leading coefficient.

1. $1 + Z^2$
2. $Z^{-1} + 1 + Z^3$
3. i
4. $\sin(Z) + Z^{12}$
5. $1 + 2Z + 5Z^{10} + 0Z^{11}$
6. $1 + Z + Z^{2.5}$
7. $(1 + Z)^2$

Answer:

1. $1 + Z^2$ is a polynomial in Z. If we want to write it in the form $a_0 + a_1 Z + a_2 Z^2 + \cdots + a_n Z^n$ as in Definition 4.1, we can write it as $1 + 0Z + 1Z^2$. Hence $n = 2$, $a_0 = a_2 = 1$ and $a_1 = 0$. Because $a_2 \neq 0$, the polynomial is of degree 2, while its leading coefficient is a_2, which is equal to 1.
2. $Z^{-1} + 1 + Z^3$ is not a polynomial in Z because of the term Z^{-1}. The exponents of Z of the terms in a polynomial may not be negative.

3. The complex number i can be interpreted as a polynomial in $\mathbb{C}[Z]$. One chooses $n = 0$ and $a_0 = i$ in Definition 4.1. The polynomial i has therefore degree 0 and leading coefficient i.

4. $\sin(Z) + Z^{12}$ is not a polynomial because of the term $\sin(Z)$.

5. $1 + 2Z + 5Z^{10} + 0Z^{11}$ is a polynomial in $\mathbb{C}[Z]$. The term of degree eleven can be left out though, since the coefficient of Z^{11} is 0. The highest power of Z with a coefficient different from zero is therefore 10. This means that $\deg(1 + 2Z + 5Z^{10} + 0Z^{11}) = 10$, while its leading coefficient is 5.

6. $1 + Z + Z^{2.5}$ is not a polynomial, because of the term $Z^{2.5}$. The exponents of Z must be natural numbers.

7. $(2 + Z)^2$ is a polynomial in $\mathbb{C}[Z]$, though it is not written in the form as in Definition 4.1. However, it can be rewritten in this form, since $(2 + Z)^2 = 4 + 4Z + Z^2 = 4 + 4Z + 1Z^2$. We have that $\deg((2 + Z)^2) = 2$. The leading coefficient of $(1 + Z)^2$ is 1.

Given a polynomial $p(Z) \in \mathbb{C}[Z]$, one can evaluate the polynomial in any complex number $z \in \mathbb{C}$. More precisely, if $p(Z) = a_0 + a_1 Z + \cdots + a_n Z^n \in \mathbb{C}[Z]$ and $z \in \mathbb{C}$, then we can define $p(z) = a_0 + a_1 \cdot z + \cdots + a_n \cdot z^n \in \mathbb{C}$. In this way, any polynomial $p(Z) \in \mathbb{C}[Z]$ gives rise to a function $p : \mathbb{C} \to \mathbb{C}$, defined by $z \mapsto p(z)$. A function $f : \mathbb{C} \to \mathbb{C}$ is called a *polynomial function*, if there exists a polynomial $p(Z) \in \mathbb{C}[Z]$ such that for all $z \in \mathbb{C}$ it holds that $f(z) = p(z)$. Similarly, a function $f : \mathbb{R} \to \mathbb{R}$ is called a polynomial function, if there exists a polynomial $p(Z) \in \mathbb{R}[Z]$ such that for all $x \in \mathbb{R}$ it holds that $f(x) = p(x)$.

Two polynomials $p_1(Z) = a_0 + a_1 Z \cdots + a_n Z^n$ and $p_2(Z) = b_0 + b_1 Z \cdots + b_m Z^m$ can be multiplied by adding all the terms $a_i b_j Z^{i+j}$, where $0 \leq i \leq n$ and $0 \leq j \leq m$. This simply means that in order to compute $p_1(Z) \cdot p_2(Z)$, one simply multiplies each term in $p_1(Z)$ with each term in $p_2(Z)$ and then adds up the resulting terms. Let us look at some examples.

|||| Example 4.3

Write the following polynomials in the form as in Definition 4.1.

1. $(Z + 5) \cdot (Z + 6)$.
2. $(3Z + 2) \cdot (3Z - 2)$.
3. $(Z - 1) \cdot (Z^2 + Z + 1)$.

Answer:

1. $(Z+5)\cdot(Z+6) = Z\cdot(Z+6)+5\cdot(Z+6) = Z^2+6Z+5Z+30 = Z^2+11Z+30.$
2. $(3Z+2)\cdot(3Z-2) = (3z)^2-6Z+6Z-2^2 = 9Z^2-4.$
3. In this example, the only difference from the previous two is that there will be more terms when multiplying, but otherwise there is no difference:
$$\begin{aligned}(Z-1)\cdot(Z^2+Z+1) &= Z\cdot(Z^2+Z+1)-(Z^2+Z+1)\\ &= Z^3+Z^2+Z-Z^2-Z-1\\ &= Z^3-1.\end{aligned}$$

Note that if a polynomial is a product of two other polynomials, say $p(Z) = p_1(Z)\cdot p_2(Z)$, then $\deg p(Z) = \deg p_1(Z) + \deg p_2(Z)$. In other words:

$$p(Z) = p_1(Z)\cdot p_2(Z) \quad\Rightarrow\quad \deg p(Z) = \deg p_1(Z) + \deg p_2(Z). \tag{4-1}$$

If $p(Z) \in \mathbb{C}[Z]$ is a polynomial, then the equation $p(z) = 0$ is called a *polynomial equation*. Solutions to a polynomial equation have a special name:

Definition 4.4

Let $p(Z) \in \mathbb{C}[Z]$ be a polynomial. A complex number $\lambda \in \mathbb{C}$ is called a *root* of $p(Z)$ precisely if $p(\lambda) = 0$.

Note that by definition, a complex number is a root of a polynomial $p(Z)$ if and only if it is a solution to the polynomial equation $p(z) = 0$.

4.2 Polynomials in $\mathbb{R}[Z]$ of degree two

To see why complex numbers were introduced in the first place, we will explain in this section how to find the roots of a polynomial $p(Z) \in \mathbb{R}[Z]$ of degree two. Note that we are assuming that $p(Z) \in \mathbb{R}[Z]$ so that the polynomial $p(Z)$ has real coefficients. Such a polynomial $p(Z)$ can therefore be written in the form

$$p(Z) = aZ^2 + bZ + c,$$

where $a, b, c \in \mathbb{R}$ and $a \neq 0$. To find its roots, we need to solve the polynomial equation $az^2 + bz + c = 0$. Now the following holds:

$$\begin{aligned} az^2 + bz + c = 0 &\Leftrightarrow 4a^2z^2 + 4abz + 4ac = 0 \\ &\Leftrightarrow (2az)^2 + 2(2az)b + b^2 = b^2 - 4ac \\ &\Leftrightarrow (2az + b)^2 = b^2 - 4ac. \end{aligned} \tag{4-2}$$

The expression $b^2 - 4ac$ is called the discriminant of the polynomial $aZ^2 + bZ + c$. We will denote it by D. From Equation (4-2) it follows that in order to compute the roots of the polynomial $aZ^2 + bZ + c$, we need to take the square root of its discriminant D. If $D \geq 0$, one can use the usual square root, but now we will define the square root of any real number:

Definition 4.5

Let D be a real number. Then we define

$$\sqrt{D} = \begin{cases} \sqrt{D} & \text{if } D \geq 0, \\ i\sqrt{|D|} & \text{if } D < 0. \end{cases}$$

If $D \geq 0$, then $\sqrt{D}$ is exactly what we are used to and it holds that $\sqrt{D}^2 = D$. If $D < 0$, it holds that $\sqrt{D}^2 = (i\sqrt{|D|})^2 = i^2\sqrt{|D|}^2 = (-1)|D| = D$. Therefore, for all real numbers D it holds that $\sqrt{D}^2 = D$. This is exactly the property that we would like the square root symbol to have. Moreover, all solutions to the equation $z^2 = D$ can now be given: they are $z = \sqrt{D}$ and $z = -\sqrt{D}$. Later, in Theorem 4.13, we will even be able to describe all the solutions to equations of the form $z^n = w$ for any $n \in \mathbb{N}$ and $w \in \mathbb{C}$. We now return to the computation of the roots of the polynomial $p(z) = az^2 + bz + c$. Using the extended square root and Equation (4-2) we find that

$$\begin{aligned} az^2 + bz + c = 0 &\Leftrightarrow (2az + b)^2 = b^2 - 4ac \\ &\Leftrightarrow (2az + b) = \sqrt{b^2 - 4ac} \quad \vee \quad (2az + b) = -\sqrt{b^2 - 4ac} \\ &\Leftrightarrow z = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \vee \quad z = \frac{-b - \sqrt{b^2 - 4ac}}{2a}. \end{aligned} \tag{4-3}$$

We get the usual formula to solve an equation of degree two, but the square root of the discriminant is now also defined if the discriminant is negative. In fact we now have shown the following theorem.

Theorem 4.6

The polynomial $p(Z) = aZ^2 + bZ + c \in \mathbb{R}[Z]$ with $a \neq 0$, has precisely the following roots in $\mathbb{C}$:

$$\frac{-b+\sqrt{D}}{2a} \text{ and } \frac{-b-\sqrt{D}}{2a}, \text{ where } D = b^2 - 4ac.$$

To be more precise, the polynomial has

1. two real roots $z = \dfrac{-b \pm \sqrt{D}}{2a}$ if $D > 0$,
2. one real root $z = \dfrac{-b}{2a}$ if $D = 0$,
3. two non-real roots $z = \dfrac{-b \pm i\sqrt{|D|}}{2a}$ if $D < 0$.

The description of the roots in Theorem 4.6 is very algorithmic in nature. In fact, let us write some pseudo-code for an algorithm:

Algorithm 1 for computing the roots of $p(Z) \in \mathbb{R}[Z]$ of degree two.

Input: $p(Z) \in \mathbb{R}[Z]$, with $\deg(p(Z)) = 2$

$a \leftarrow$ coefficient of Z^2 in $p(Z)$
$b \leftarrow$ coefficient of Z^1 in $p(Z)$
$c \leftarrow$ coefficient of Z^0 in $p(Z)$
$D \leftarrow b^2 - 4ac$
if $D \geq 0$ **then**
    return $\dfrac{-b+\sqrt{D}}{2a}$ and $\dfrac{-b-\sqrt{D}}{2a}$
else
    return $\dfrac{-b+i\sqrt{|D|}}{2a}$ and $\dfrac{-b-i\sqrt{|D|}}{2a}$

In Figure 4.1, we have drawn the graphs of some second degree polynomials. Real roots of a second degree polynomial correspond to intersection points of the x-axis and its graph. If there are no intersection points, the polynomial does not have real roots, but complex roots. If $D = b^2 - 4ac = 0$, the polynomial equation $az^2 + bz + c = 0$ has one solution and we say in this case that the polynomial has a *double root*, or a root of multiplicity two. If $D \neq 0$, one says that the roots have multiplicity one. We see that any polynomial of degree two has two roots if the roots are counted with their multiplicities.

We will return to roots and multiplicities in more detail in Section 4.6. If we consider the graph of a polynomial function $f : \mathbb{R} \to \mathbb{R}$ coming from a degree two polynomial in $\mathbb{R}[Z]$, then this graph intersects the horizontal axis twice if $D > 0$, once if $D = 0$ and not at all if $D < 0$. See Figure 4.1 for an illustration.

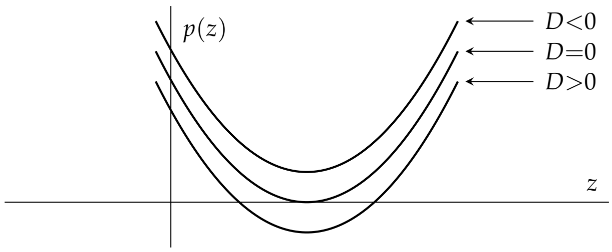


Figure 4.1: A degree two polynomial $p(Z) \in \mathbb{R}[Z]$ has two real roots if $D > 0$, a double root if $D = 0$, and two complex, two non-real roots if $D < 0$.

|||| Example 4.7

Compute all complex roots of the polynomial $2Z^2 - 4Z + 10 = 0$.

Answer: The discriminant of the polynomial $2Z^2 - 4Z + 10$ equals

$$D = (-4)^2 - 4 \cdot 2 \cdot 10 = -64.$$

According to Definition 4.5 we then find that

$$\sqrt{D} = \sqrt{-64} = i\sqrt{64} = 8i.$$

Therefore the polynomial equation $2z^2 - 4z + 10 = 0$ has two non-real roots, namely

$$z = \frac{-(-4) + 8i}{2 \cdot 2} = 1 + 2i \quad \vee \quad z = \frac{-(-4) - 8i}{2 \cdot 2} = 1 - 2i.$$

Although Theorem 4.6 guarantees that $1 + 2i$ and $1 - 2i$ are the roots of the polynomial $2Z^2 - 4Z + 10$, let us check that $1 + 2i$ is a root by hand:

$$\begin{aligned} 2 \cdot (1 + 2i)^2 - 4 \cdot (1 + 2i) + 10 &= 2 \cdot (1^2 + 4i + (2i)^2) - 4 \cdot (1 + 2i) + 10 \\ &= 2 \cdot (1 - 4 + 4i) - 4 \cdot (1 + 2i) + 10 \\ &= 2 \cdot (-3 + 4i) - 4 \cdot (1 + 2i) + 10 \\ &= (-6 + 8i) - (4 + 8i) + 10 \\ &= 0. \end{aligned}$$

Hence indeed, just as the theory predicts, $1 + 2i$ is a root of $2Z^2 - 4Z + 10$.

4.3 Polynomials with real coefficients

In the previous section, we studied degree two polynomials with real coefficients. Many of the polynomials we will encounter later on will have real coefficients. In this section we will therefore collect some facts about such polynomials. Complex conjugation as introduced in Definition 3.8, will play an important role. Complex conjugation has several nice properties. We list some of these in the following lemma.

Lemma 4.8

Let $z, z_1, z_2 \in \mathbb{C}$ be complex numbers. Then it holds that

1. $\overline{\overline{z}} = z$,
2. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$,
3. $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$,
4. $\overline{1/z} = 1/\overline{z} \quad$ provided $z \neq 0$,
5. $\overline{z^n} = (\overline{z})^n$, where $n \in \mathbb{Z}$.

Proof. We will prove the second and third item of the lemma. Proving the remaining items is left to the reader. For a sum of two complex numbers $z_1 = a + bi$ and $z_2 = c + di$ on rectangular form it holds that

$$\overline{z_1 + z_2} = \overline{(a+c) + (b+d)i} = (a+c) - (b+d)i = (a - bi) + (c - di) = \overline{z_1} + \overline{z_2}.$$

For a product of two complex numbers $z_1 = a + bi$ and $z_2 = c + di$ on rectangular form we have $z_1 \cdot z_2 = (ac - bd) + (ad + bc)i$. Therefore

$$\overline{z_1 \cdot z_2} = (ac - bd) - (ad + bc)i.$$

On the other hand,

$$\begin{aligned} \overline{z_1} \cdot \overline{z_2} &= (a - bi) \cdot (c - di) \\ &= ac - adi - bci + (-b) \cdot (-d) i^2 \\ &= ac - (ad + bc)i + bd \cdot (-1) \\ &= ac - bd - (ad + bc)i. \end{aligned}$$

This shows that $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$. □

|||| Example 4.9

Express the following complex numbers on rectangular form.

1. $\overline{-3+6i}$
2. $\overline{\pi}$
3. $\overline{-97i}$

Answer:

1. From the definition of the complex conjugate we find $\overline{-3+6i} = -3-6i$.
2. $\overline{\pi} = \overline{\pi + 0i} = \pi - 0i = \pi$. This illustrates the more general fact that $\overline{z} = z$, if z is a real number.
3. $\overline{-97i} = -(-97i) = 97i$. It turns out that more generally $\overline{z} = -z$ for all purely imaginary numbers.

Complex conjugation also interacts well with the complex exponential function.

|||| Lemma 4.10

Let $z \in \mathbb{C}$ be a complex number and $\alpha \in \mathbb{R}$ a real number. It holds that

1. $\overline{e^z} = e^{\overline{z}}$,
2. $\overline{e^{i\alpha}} = e^{-i\alpha}$,
3. $\overline{z} = |z|e^{-i\arg(z)}$.

Proof. We prove the first two parts of the lemma. The third part of the lemma is illustrated in Figure 4.2. Suppose that $z = a + bi$ is the rectangular form of z. From the definition of the complex exponential function we find that

$$\overline{e^z} = \overline{e^a \cos(b) + e^a \sin(b) i} = e^a \cos(b) - e^a \sin(b) i$$

$$= e^a \cos(-b) + e^a \sin(-b) i = e^{a-bi} = e^{\overline{z}}.$$

If $z = i\alpha$ (with $\alpha \in \mathbb{R}$) we get the special case

$$\overline{e^{i\alpha}} = e^{\overline{i\alpha}} = e^{-i\alpha}.$$

□

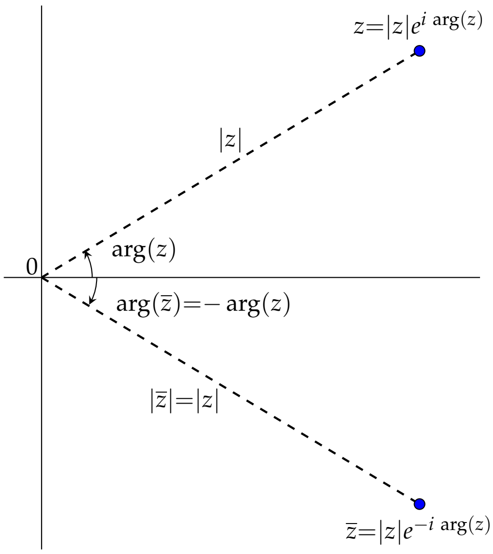


Figure 4.2: Polar form of a complex number z and its complex conjugate $\overline{z}$.

|||| Example 4.11

Write the complex number $\overline{5e^{i\pi/3}}$ in polar form.

Answer:

$\overline{5e^{i\pi/3}} = \overline{5}\,\overline{e^{i\pi/3}} = 5e^{-i\pi/3}$. This illustrates the third part of the previous lemma, which says that $\overline{z} = |z|e^{-i\arg(z)}$.

Now let us return to our discussion of polynomials with real coefficients. The reason we have introduced complex conjugation is the following property:

Lemma 4.12

Let $p(Z) \in \mathbb{R}[Z]$ be a polynomial with real coefficients and let $\lambda \in \mathbb{C}$ be a root of $p(Z)$. Then the complex number $\overline{\lambda} \in \mathbb{C}$ is also a root of $p(Z)$.

Proof. Let us write $p(Z) = a_n Z^n + \cdots + a_1 Z + a_0$. Since $p(Z)$ has real coefficients, it holds that $a_n, \ldots, a_0 \in \mathbb{R}$. It is given that $\lambda \in \mathbb{C}$ is a root of $p(Z)$ and therefore it holds that

$$0 = a_n \lambda^n + \cdots + a_1 \lambda + a_0.$$

We will now show that $\overline{\lambda}$ is a root of $p(Z)$ as well, by taking the complex conjugate in this equation. We find that

$$0 = \overline{a_n \lambda^n + \cdots + a_1 \lambda + a_0}.$$

Using this and the properties given in Lemma 4.8, we get:

$$\begin{aligned}
0 &= \overline{a_n \lambda^n + a_{n-1} \lambda^{n-1} \cdots + a_1 \lambda + a_0} \\
&= \overline{a_n \lambda^n} + \overline{a_{n-1} \lambda^{n-1}} + \cdots + \overline{a_1 \lambda} + \overline{a_0} \\
&= \overline{a_n}\,\overline{\lambda^n} + \overline{a_{n-1}}\,\overline{\lambda^{n-1}} + \cdots + \overline{a_1}\,\overline{\lambda} + \overline{a_0} \\
&= \overline{a_n}(\overline{\lambda})^n + \overline{a_{n-1}}(\overline{\lambda})^{n-1} + \cdots + \overline{a_1}\,\overline{\lambda} + \overline{a_0} \\
&= a_n(\overline{\lambda})^n + a_{n-1}(\overline{\lambda})^{n-1} + \cdots + a_1\overline{\lambda} + a_0 \\
&= p(\overline{\lambda})
\end{aligned}$$

In the fifth equality we have used that the coefficients of the polynomial $p(Z)$ are real numbers, so that $\overline{a_j} = a_j$ for all j between 0 and n. We have now shown that $p(\overline{\lambda}) = 0$ and hence can conclude that $\overline{\lambda}$ is a root of the polynomial $p(Z)$ as well. □

Lemma 4.12 has the following consequence: non-real roots of a polynomial with real coefficients come in pairs. Take for example the polynomial $2Z^2 - 4Z + 10$. We have seen in Example 4.7 that one of its roots is $1 + 2i$. Lemma 4.12 implies that the complex number $1 - 2i$ then is a root of $2Z^2 - 4Z + 10$ as well. We have seen in Example 4.7 that this indeed is the case.

4.4 Binomials

In this section we look at polynomials of the form $Z^n - w$ for some natural number $n \in \mathbb{N}$ and a complex number $w \in \mathbb{C}$ different from 0. The number n is the degree of the polynomial $Z^n - w$. Because a polynomial of the form $Z^n - w$ only has two terms, namely Z^n and $-w$, it is often called a *binomial*. The corresponding equation $z^n = w$ is called a *binomial equation*. We will give an exact expression for all roots of a binomial $Z^n - w \in \mathbb{C}[Z]$. This means that we have to compute all $z \in \mathbb{C}$ satisfying the equation $z^n = w$. It turns out that the polar form of the complex number w is of great help.

Theorem 4.13

Let $w \in \mathbb{C}\setminus\{0\}$. The equation $z^n = w$ has exactly n different solutions, namely:

$$z = \sqrt[n]{|w|}e^{i\left(\frac{\arg(w)}{n}+p\frac{2\pi}{n}\right)},\ p \in \{0,\ldots,n-1\}.$$

Here $\sqrt[n]{|w|}$ denotes the unique positive real number satisfying $\left(\sqrt[n]{|w|}\right)^n = |w|$.

Proof. The main idea of this proof is to try to find all solutions z to the equation $z^n = w$ in polar form. Therefore we write $z = |z|e^{iu}$ and we will try to determine the possible values of $|z|$ and u such that $z^n = |w|e^{i\alpha}$. In the first place we have $z^n = (|z|e^{iu})^n = |z|^n e^{inu}$ and this expression should be equal to $|w|e^{i\alpha}$. This holds if and only if $|w| = |z|^n$ and $e^{inu} = e^{i\alpha}$, or in other words, if and only if $|w| = |z|^n$ and $e^{i(nu-\alpha)} = 1$. The equation $|w| = |z|^n$ has exactly one solution for $|z| \in \mathbb{R}_{>0}$, namely $|z| = \sqrt[n]{|w|}$, while according to Lemma 3.26, the equation $e^{i(nu-\alpha)} = 1$ is satisfied if and only if $nu - \alpha = \arg(1)$. The possible arguments of 1 are precisely the integral multiples of 2π, that is to say, $\arg(1) = p2\pi$ for some integer $p \in \mathbb{Z}$.

All solutions to $z^n = w$ are therefore of the form $z = \sqrt[n]{|w|}e^{i\left(\frac{\alpha}{n}+p\frac{2\pi}{n}\right)}$, where $p \in \mathbb{Z}$. In principle, we find a solution for any choice of $p \in \mathbb{Z}$, but when p runs through the set $\{0,\ldots,n-1\}$ we already get all different possibilities for z. $\square$

When drawn in the complex plane, the solutions to the equation $z^n = w$ form the vertices of a regular n-gon with center in 0. Let us illustrate this in an example.

|||| Example 4.14

In this example we will find all roots of the polynomial $Z^4 + 8 - i8\sqrt{3}$ and write them in rectangular form.

Answer: We can use Theorem 4.13, with $n = 4$ and $w = -(8 - i8\sqrt{3})$. First, we need to write the complex number $-(8 - i8\sqrt{3} = -8 + i8\sqrt{3})$ in polar form. We have

$$|-8 + i8\sqrt{3}| = \sqrt{(-8)^2 + (8\sqrt{3})^2} = 16$$

and

$$\arg(-8 + i8\sqrt{3}) = \arctan(8\sqrt{3}/(-8)) + \pi = 2\pi/3.$$

Therefore we find that $-8 + i8\sqrt{3} = 16e^{i2\pi/3}$, which is the desired polar form. According to Theorem 4.13 all solutions to $z^4 = -8 + i8\sqrt{3}$ are given by:

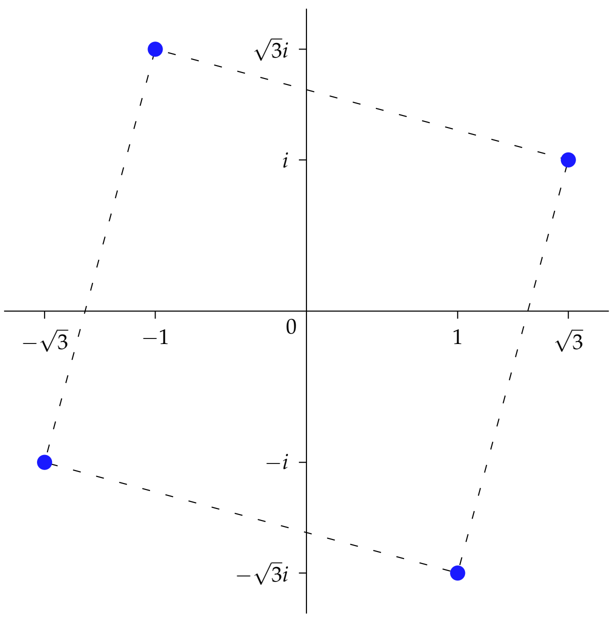
$$z = \sqrt[4]{16}e^{i\left(\frac{2\pi}{3\cdot 4} + p\frac{2\pi}{4}\right)}, \text{where } p \text{ can be chosen freely from the set } \{0, 1, 2, 3\}, \text{ so}$$

$$z = 2e^{i\frac{\pi}{6}} \quad \vee \quad z = 2e^{i\frac{2\pi}{3}} \quad \vee \quad z = 2e^{i\frac{7\pi}{6}} \quad \vee \quad z = 2e^{i\frac{5\pi}{3}}.$$

Now we still need to write these roots in rectangular form. Using the formula $e^{it} = \cos(t) + i\sin(t)$ we get:

$$z = \sqrt{3} + i \quad \vee \quad z = -1 + i\sqrt{3} \quad \vee \quad z = -\sqrt{3} - i \quad \vee \quad z = 1 - i\sqrt{3}.$$

As remarked after Theorem 4.13, these solutions form the vertices of a regular 4-gon (that is to say, a square) with center in zero. This is indeed the case as shown in the following figure.



4.4.1 Polynomials in $\mathbb{C}[Z]$ of degree two

In Section 4.2, we have seen how to find the roots of a degree two polynomials in $\mathbb{R}[Z]$. Now that we know how to find the roots of binomial polynomials, we can find the roots of a degree two polynomials in $\mathbb{C}[Z]$ without much additional effort. The main observation is that for any polynomial $aZ^2 + bZ + c \in \mathbb{C}[Z]$ such that $a \neq 0$, Equation (4-3) is still valid. Hence $az^2 + bz + c = 0 \Leftrightarrow (2az + b)^2 = b^2 - 4ac$. We know from Theorem 4.13 that the equation $t^2 = b^2 - 4ac$ has exactly two solutions, say s and $se^{i\pi} = -s$. Then $az^2 + bz + c = 0 \Leftrightarrow 2az + b = s \vee 2az + b = -s$. Solving for z, we then obtain the following result:

|||| Theorem 4.15

Let $p(Z) = aZ^2 + bZ + c \in \mathbb{C}[Z]$ be a polynomial of degree two. Further, let $s \in \mathbb{C}$ be a solution to the binomial equation $s^2 = b^2 - 4ac$. Then $p(Z)$ has precisely the following roots:

$$\frac{-b+s}{2a} \text{ and } \frac{-b-s}{2a}.$$

|||| Example 4.16

As an example, let us find the roots of the polynomial $Z^2 + 2Z + 1 - i$.

Answer: The discriminant of the polynomial $Z^2 + 2Z + 1 - i$ is equal to $2^2 - 4 \cdot 1 \cdot (1 - i) = 4i$. Therefore, we first need to solve the binomial equation $s^2 = 4i$. We have $|4i| = 4$ and $\mathrm{Arg}(4i) = \pi/2$. Using Theorem 4.13, we see that the equation $s^2 = 4i$ has solutions

$$2 \cdot e^{\pi/4\, i} = 2 \cdot (\cos(\pi/4) + i \sin(\pi/4)) = 2 \cdot (\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i) = \sqrt{2} + \sqrt{2}\, i$$

and

$$2 \cdot e^{(\pi/4+\pi)\, i} = 2 \cdot (\cos(5\pi/4) + i \sin(5\pi/4)) = 2 \cdot (-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i) = -\sqrt{2} - \sqrt{2}\, i.$$

Hence using Theorem 4.15, we obtain that the roots of the polynomial $Z^2 + Z + 1 - i$ are given by

$$\frac{-2+\sqrt{2}+i\sqrt{2}}{2} = -1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i \quad \text{and} \quad \frac{-2-\sqrt{2}-i\sqrt{2}}{2} = -1 - \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i.$$

4.5 The division algorithm

In the previous section, we have seen how to find the roots of some specific polynomials. To study the behaviour of roots for more general polynomials, we begin with the following observation:

Lemma 4.17

Let $p(Z) \in \mathbb{C}[Z]$ be a polynomial and suppose that $p(Z) = p_1(Z) \cdot p_2(Z)$ for certain polynomials $p_1(Z), p_2(Z) \in \mathbb{C}[Z]$. Further, let $\lambda \in \mathbb{C}$. Then λ is a root of $p(Z)$ if and only if λ is a root of $p_1(Z)$ or of $p_2(Z)$.

Before proving this lemma, let us relate the statement of the lemma to propositional logic from Note 1 to clarify what really is stated. A statement like

"λ is a root of $p(Z)$ if and only if λ is a root of $p_1(Z)$ or of $p_2(Z)$"

in a mathematical text, is just a way to express a statement from propositional logic into more common language. Reformulating everything in propositional logic, we simply get the statement

$$\lambda \text{ is a root of } p(Z) \quad \Leftrightarrow \quad \lambda \text{ is a root of } p_1(Z) \vee \lambda \text{ is a root of } p_2(Z).$$

We can even go further and remove all words:

$$p(\lambda) = 0 \quad \Leftrightarrow \quad p_1(\lambda) = 0 \vee p_2(\lambda) = 0.$$

It is a good habit to make sure that you understand what a mathematical statement, when formulated in common language, really means. Here it is for example perfectly possible that λ is a root of both $p_1(Z)$ and $p_2(Z)$, even though in language "or" often is used in the meaning of "either one or the other, but not both". In mathematical texts, "or" typically has the same meaning as "$\vee$". With this in mind, let us continue to the proof of the lemma:

Proof. The number λ is a root of $p(Z)$ if and only if $p(\lambda) = 0$. Since $p(Z) = p_1(Z)p_2(Z)$ this is equivalent to saying that $p_1(\lambda)p_2(\lambda) = 0$ and therefore with the statement that $p_1(\lambda) = 0 \vee p_2(\lambda) = 0$. This statement is logically equivalent to saying that λ is a root of $p_1(Z)$ or of $p_2(Z)$. $\square$

If one wants to find all roots of a polynomial, the above lemma suggests that it is always a good idea to try to write the polynomial as a product of polynomials of lower degree. If $p(Z) = p_1(Z) \cdot p_2(Z)$ as in the previous lemma, one says that $p_1(Z)$ and $p_2(Z)$ are *factors* of the polynomial $p(Z)$. It is therefore useful to have an algorithm that allows one to decide whether or not a given polynomial $p_1(Z) \in \mathbb{C}[Z]$ is a factor of a given second polynomial $p(Z) \in \mathbb{C}[Z]$. Equation (4-1) is already of some help, since it implies that $p(Z) = p_1(Z) \cdot p_2(Z)$ can only be true if $\deg p(Z) = \deg p_1(Z) + \deg p_2(Z)$. In particular, $p_1(Z)$ cannot be a factor of $p(Z)$ if $\deg p_1(Z) > \deg p(Z)$. However, this still leaves the case $\deg p_1(Z) \le \deg p(Z)$ open. Before giving the algorithm that solves the problem completely, let us first consider a few examples.

|||| Example 4.18

1. Decide if the polynomial $Z + 3$ is a factor of the polynomial $2Z^2 + 3Z - 9$.
2. Decide if the polynomial $Z + 4$ is a factor of the polynomial $3Z^3 + 2Z + 1$.
3. Decide if the polynomial $2Z^2 + Z + 3$ is a factor of the polynomial $6Z^4 + 3Z^3 + 19Z^2 + 5Z + 15$.

Answer:

1. We will try to find a polynomial $q(Z) \in \mathbb{C}[Z]$ such that $(Z+3) \cdot q(Z) = 2Z^2 + 3Z - 9$. If $q(Z)$ exists, it should have degree 1 using Equation (4-1). Hence if $q(Z)$ exists, it should be of the form $q(Z) = b_1 Z + b_0$ for certain numbers $b_1, b_0 \in \mathbb{C}$. We first try to find b_1. Without simplifying the product $(Z+3) \cdot (b_1 Z + b_0)$ we can already see that the highest power of Z in the product is 2 and that the coefficient of Z^2 in the product is b_1. This means that $(Z+3) \cdot (b_1 Z + b_0) = b_1 Z^2 +$ terms of degree less than 2. On the other hand we want that $(Z+3) \cdot (b_1 Z + b_0) = 2Z^2 + 3Z - 9$. We see that b_1 has to be 2. Now that we know that $b_1 = 2$, we will determine b_0. On the one hand we want that $(Z+3) \cdot (2Z + b_0) = 2Z^2 + 3Z - 9$, but on the other hand we can write $(Z+3) \cdot (2Z + b_0) = (Z+3) \cdot 2Z + (Z+3) \cdot b_0$. Therefore, we can conclude that

$$(Z+3) \cdot b_0 = 2Z^2 + 3Z - 9 - (Z+3) \cdot 2Z = -3Z - 9. \tag{4-4}$$

The important observation here is that previously we have chosen b_1 in such a way that the Z^2 term in Equation (4-4) is gone. By looking at the coefficients of Z, we conclude that $b_0 = -3$. We have shown the implication $(Z+3) \cdot q(Z) = 2Z^2 + 3Z - 9 \Rightarrow q(Z) = 2Z - 3$. A direct check verifies that indeed $2Z^2 + 3Z - 9 = (Z+3) \cdot (2Z - 3)$. We can conclude that indeed $Z + 3$ is a factor of $2Z^2 + 3Z - 9$. Since -3 is the root of $Z + 3$, Lemma 4.17 then implies that -3 is also a root of the polynomial $2Z^2 + 3Z - 9$. Indeed, we have $2 \cdot (-3)^2 + 3 \cdot (-3) - 9 = 0$.

There is a more convenient way to write down the calculations we just carried out. The first step was to calculate b_1 and to subtract $b_1 \cdot (Z + 3)$ from $2Z^2 + 3Z - 9$:

$$\begin{array}{r|r|l} Z+3 & 2Z^2+3Z-9 & 2Z \\ & 2Z^2+6Z & \\ \cline{2-2} & -3Z-9 & \end{array}$$

The first line contains the polynomials we start with $Z + 3$ and $2Z^2 + 3Z - 9$ as well as all terms of $q(Z)$ we have calculated in the first step. The second line consists of the multiple of $Z + 3$ which we subtracted from $2Z^2 + 3Z - 9$ in Equation (4-4). The third line gives, after some simplifications, the expression $2Z^2 + 3Z - 9 - 2Z \cdot (Z + 3)$. We also got this in the righthand side of Equation (4-4). The next step was to determine the b_0. We again get that $b_0 = -3$ and update the above scheme as follows:

$$\begin{array}{r|r|l} Z+3 & 2Z^2+3Z-9 & 2Z-3 \\ & 2Z^2+6Z & \\ \cline{2-2} & -3Z-9 & \\ & -3Z-9 & \\ \cline{2-2} & 0 & \end{array}$$

This just means that $2Z^2 + 3Z - 9 - (Z + 3) \cdot (2Z - 3) = 0$. This zero on the righthand side comes from the last line in the above scheme. The conclusion is therefore that $Z + 3$ is a factor of the polynomial $2Z^2 + 3Z - 9$. More than that we can even write the factorization down, since we showed that $2Z^2 + 3Z - 9 = (Z + 3) \cdot (2Z - 3)$.

2. This time, let us investigate if the polynomial $Z + 4$ is a factor of the polynomial $3Z^3 + 2Z + 1$. We try to find a polynomial $q(Z)$ such that $(Z + 4) \cdot q(Z) = 3Z^3 + 2Z + 1$. We see that $q(Z)$ should have degree 2, that is to say $q(Z) = b_2Z^2 + b_1Z + b_0$, and we want to determine its three coefficients. By looking at the highest power of Z we see that $b_2 = 3$. This time we directly use the schematic procedure we described in the first part of this example. First we get:

$$\begin{array}{r|r|l} Z+4 & 3Z^3 \qquad\quad +2Z+1 & 3Z^2 \\ & 3Z^3+12Z^2 \qquad\qquad & \\ \cline{2-2} & -12Z^2+2Z+1 & \end{array}$$

Now we can see that the coefficient of Z in $q(Z)$ should be -12 and we find:

$$\begin{array}{r|r|l} Z+4 & 3Z^3 \qquad\quad +\ 2Z+1 & 3Z^2-12Z \\ & 3Z^3+12Z^2 \qquad\qquad & \\ \cline{2-2} & -12Z^2+\ 2Z+1 & \\ & -12Z^2-48Z \quad & \\ \cline{2-2} & 50Z+1 & \end{array}$$

We can now read of that the constant term b_0 of $q(Z)$ should be 50 and we get:

$$\begin{array}{r|rrrr|l}
Z+4 & 3Z^3 & & +\ 2Z+ & 1 & 3Z^2-12Z+50 \\
 & 3Z^3+12Z^2 & & & & \\ \hline
 & & -\ 12Z^2+ & 2Z+ & 1 & \\
 & & -\ 12Z^2- & 48Z & & \\ \hline
 & & & 50Z+ & 1 & \\
 & & & 50Z+ & 200 & \\ \hline
 & & & & -\ 199 &
\end{array}$$

This time we do not get a zero in the last line. What the above scheme actually shows is that $3Z^3 + 2Z + 1 - (Z + 4) \cdot (3Z^2 - 12Z + 50) = -199$. This means that $Z + 4$ cannot be a factor of $3Z^3 + 2Z + 1$, since then $Z + 4$ would also be a factor of $3Z^3 + 2Z + 1 - (Z + 4) \cdot (3Z^2 - 12Z + 50) = -199$. This would be impossible, since $\deg(Z + 4) = 1 > 0 = \deg(-199)$. Note that -4 is not a root of the polynomial $3Z^3 + 2Z + 1$, since $3 \cdot (-4)^3 + 2 \cdot (-4) + 1 = -199$.

3. We state the schematic procedure only this time:

$$\begin{array}{r|r|l}
2Z^2+Z+3 & 6Z^4+3Z^3+19Z^2+5Z+15 & 3Z^2+5 \\
 & 6Z^4+3Z^3+\ \ 9Z^2\qquad\qquad\ \ & \\ \hline
 & 10Z^2+5Z+15 & \\
 & 10Z^2+5Z+15 & \\ \hline
 & 0 &
\end{array}$$

The conclusion is that $6Z^4 + 3Z^3 + 19Z^2 + 5Z + 15 - (2Z^2 + Z + 3) \cdot (3Z^2 + 5) = 0$ and therefore that $6Z^4 + 3Z^3 + 19Z^2 + 5Z + 15 = (2Z^2 + Z + 3) \cdot (3Z^2 + 5)$. Hence $2Z^2 + Z + 3$ is a factor of the polynomial $6Z^4 + 3Z^3 + 19Z^2 + 5Z + 15$.

The algorithm described in the above examples is called *polynomial division* or the *division algorithm* or sometimes also *long division*. Let us describe it in full generality.

Given as input are two polynomials $p(Z), d(Z) \in \mathbb{C}[Z]$, where $d(Z)$ is not the zero polynomial. What we want, is to compute two polynomials $q(Z)$ and $r(Z)$ in $\mathbb{C}[Z]$ such that:

1. $p(Z) = d(Z)q(Z) + r(Z)$.
2. $r(Z) = 0 \quad \vee \quad deg(r(z)) < \deg(d(z))$.

The produced polynomial $q(Z)$ is called the *quotient* of $p(Z)$ modulo $d(Z)$, while the polynomial $r(Z)$ is called the *remainder* of $p(Z)$ modulo $d(Z)$. The polynomial $d(Z)$ is a factor of $p(Z)$ if and only if this remainder is the zero polynomial. Hence the division algorithm can also be used to determine if any given polynomial divides $p(Z)$.

To find the quotient and remainder, we start the following schematic procedure:

$$\begin{array}{c|c|c} \underline{d(Z)} & p(Z) & \underline{0} \end{array}$$

If we are lucky, we have $\deg p(Z) < \deg d(Z)$. In this case, we can already stop the division algorithm and return the values $q(Z) = 0$ and $r(Z) = p(Z)$. Otherwise, we would start the long division and find a simple multiple of $d(Z)$ that has the same degree and leading coefficient as $p(Z)$. Now let us denote the degree of $d(Z)$ by m, the leading coefficient of $d(Z)$ by d_m, and the leading coefficient of $p(Z)$ by b. Then the polynomial $bd_m^{-1}Z^{\deg p(Z)-m} \cdot d(Z)$ has exactly the same degree and leading coefficient as $p(Z)$. Hence we update the schematic procedure as follows:

$$\begin{array}{c|l|l} \underline{d(Z)} & p(Z) & \underline{bd_m{}^{-1}Z^{\deg p(Z)-m}} \\ & bd_m{}^{-1}Z^{\deg p(Z)-m} \cdot d(Z) & \\ \cline{2-2} & p(Z) - bd_m{}^{-1}Z^{\deg p(Z)-m} \cdot d(Z) & \end{array}$$

Note that the degree of the polynomial $p(Z) - bd_m{}^{-1}Z^{\deg p(Z)-m} \cdot d(Z)$ is strictly less than $\deg p(Z)$, since the leading coefficients of $p(Z)$ and $bd_m{}^{-1}Z^{\deg p(Z)-m} \cdot d(Z)$ are the same and therefore cancel each other when the difference of the two polynomials is taken. If it so happens that the degree of the resulting polynomial $p(Z) - bd_m{}^{-1}Z^{\deg p(Z)-m} \cdot d(Z)$ is strictly less than that of $d(Z)$, we are done and can return as answer the polynomials $p(Z) - bd_m{}^{-1}Z^{\deg p(Z)-m} \cdot d(Z)$ for $r(Z)$ and $bd_m{}^{-1}Z^{\deg p(Z)-m} \cdot d(Z)$ for $q(Z)$, otherwise we continue to the next line.

Now suppose that we have carried out the procedure a couple of times and have arrived at the following:

$$\begin{array}{c|c|c} \underline{d(Z)} & p(Z) & \underline{q^*(Z)} \\ & \ddots & \\ \cline{2-2} & r^*(Z) & \end{array}$$

If $\deg r^*(Z) < \deg d(Z)$, then we are already done and can return $q^*(Z)$ and $r^*(Z)$ as the quotient and remainder we are looking for. Otherwise, we perform one more step in the long division and find a simple multiple of $d(Z)$ that has the same degree and leading coefficient as $r^*(Z)$. Very similarly as in the first step of the long division, now denoting by b the leading coefficient of $r^*(Z)$, we find that the polynomial $bd_m^{-1}Z^{\deg r^*(Z)-m} \cdot d(Z)$ has exactly the same degree and leading coefficient as $r^*(Z)$. Hence we update the schematic procedure as follows:

$$
\begin{array}{r|l|l}
\underline{d(Z)} & p(Z) & \underline{q^*(Z) + b{d_m}^{-1}Z^{\deg r^*(Z)-m}} \\
 & \ddots & \\
\hline
 & r^*(Z) & \\
 & b{d_m}^{-1}Z^{\deg r^*(Z)-m} \cdot d(Z) & \\
\hline
 & r^*(Z) - b{d_m}^{-1}Z^{\deg r^*(Z)-m} \cdot d(Z) &
\end{array}
$$

Since at each step of the iteration, the degree of the polynomial at the bottom of the scheme decreases, we will after finitely many steps arrive at the situation:

$$
\begin{array}{r|c|l}
\underline{d(Z)} & p(Z) & \underline{q(Z)} \\
 & \underline{\cdots} & \\
 & \ddots & \\
 & \overline{r(Z)} &
\end{array}
$$

Here $r(Z)$ is either the zero polynomial or $\deg r(Z) < \deg d(Z)$. The quotient and remainder are then the polynomials $q(Z)$ and $r(Z)$ found in the scheme. Let us for good measure also formulate this algorithm in pseudo-code. To indicate that the algorithm should keep running as long as $\deg r^*(Z) \geq \deg d(Z)$, we use what is known as a while loop in the pseudo-code.

Algorithm 2 for performing long division in $\mathbb{C}[Z]$

Input: $p(Z) \in \mathbb{C}[Z], d(Z) \in \mathbb{C}[Z] \setminus \{0\}$.

$m \leftarrow \deg d(Z)$
$d_m \leftarrow$ leading coefficient of $d(Z)$
$q^*(Z) \leftarrow 0$ and $r^*(Z) \leftarrow p(Z)$
while $\deg r^*(Z) \geq m$ **do**
    $b \leftarrow$ leading coefficient of $r^*(Z)$
    $q^*(Z) \leftarrow q^*(Z) + bd_m^{-1}Z^{\deg r(Z)-m}$
    $r^*(Z) \leftarrow r^*(Z) - bd_m^{-1}Z^{\deg r^*(Z)-m} \cdot d(Z)$
return $q^*(Z), r^*(Z)$

4.6 Roots, multiplicities and factorizations

A surprising and beautiful theorem is that any polynomial $p(Z) \in \mathbb{C}[Z]$ of degree at least 1 has a root in $\mathbb{C}$. This result is often called the *fundamental theorem of algebra*. For future reference, let us state the theorem.

Theorem 4.19 Fundamental theorem of algebra

Let $p(Z) \in \mathbb{C}[Z]$ be a polynomial of degree at least one. Then $p(Z)$ has a root $\lambda \in \mathbb{C}$.

We will not prove this theorem, since the proof is quite involved. We have seen that the theorem is true for degree two polynomials in Theorem 4.15. Note that not every polynomial needs to have a real root. For example, the polynomial $Z^2 + 1$ does not have a real root, but has a pair of (non-real) complex roots, namely i and $-i$.

Given a polynomial, it can be difficult or downright impossible to find a useful exact expression for its roots, but often a numerical approximation of the roots is sufficient. One can make a precise statement on the number of roots a polynomial can have though. We will see that if a polynomial has degree n, then it has n roots if we count the roots in a particular way. Now that we have the division algorithm as a tool, we start our investigation of roots of a polynomial.

Lemma 4.20

Let $p(Z) \in \mathbb{C}[Z]$ be a polynomial of degree $n \geq 1$ and let $\lambda \in \mathbb{C}$ be a complex number. The number λ is a root of $p(Z)$ if and only if $Z - \lambda$ is a factor of $p(Z)$.

Proof. If $Z - \lambda$ is a factor of $p(Z)$, then there exists a polynomial $q(Z) \in \mathbb{C}[Z]$ such that $p(Z) = (Z - \lambda) \cdot q(Z)$. Therefore it then holds that $p(\lambda) = 0 \cdot q(\lambda) = 0$. This shows that λ is a root of $p(Z)$ if $Z - \lambda$ is a factor of $p(Z)$

Now suppose that λ is a root of $p(Z)$. Using the division algorithm we can find polynomials $q(Z)$ and $r(Z)$ such that

$$p(Z) = (Z - \lambda) \cdot q(z) + r(Z), \tag{4-5}$$

where $r(Z)$ is the zero polynomial, or $\deg(r(Z)) < \deg(Z - \lambda) = 1$. Since $r(Z) = 0$ or $\deg(r(Z)) < 1$, we see that $r(Z)$ actually is a constant $r \in \mathbb{C}$. By setting $Z = \lambda$ in Equation (4-5), we get that $p(\lambda) = r + 0 = r$. Therefore we actually have shown that $p(Z) = (Z - \lambda) \cdot q(Z) + p(\lambda)$. If λ is a root of $p(Z)$ (that is to say $p(\lambda) = 0$), we therefore get that $Z - \lambda$ is a factor of $p(Z)$. □

Using this lemma we can define the multiplicity of a root.

Definition 4.21

Let λ be a root of a polynomial $p(Z)$. The multiplicity of the root is defined to be the largest natural number $m \in \mathbb{N}$ such that $(Z - \lambda)^m$ is a factor of $p(Z)$. One says that λ is a root of $p(Z)$ of *multiplicity* m.

Note that Lemma 4.20 implies that any root of a polynomial has multiplicity at least 1. A root of multiplicity two is sometimes called a double root.

Example 4.22

Decide if -3 is a root of the following polynomials. If yes, determine its multiplicity.

- $p_1(Z) = 2Z^2 + 3Z - 9$.
- $p_2(Z) = Z^2 + 3Z + 1$.
- $p_3(Z) = Z^3 + 3Z^2 - 9Z - 27$.
- $p_4(Z) = (2Z^2 + 3Z - 9) \cdot (Z^3 + 3Z^2 - 9Z - 27) = 2Z^5 + 9Z^4 - 18Z^3 - 108Z^2 + 243$.

Answer:

1. We have $p_1(-3) = 18 - 9 - 9 = 0$. Therefore is -3 a root of the polynomial $2Z^2 + 3Z - 9$. We have seen in Example 4.18 that $2Z^2 + 3Z - 9 = (Z + 3) \cdot (2Z - 3)$. This means that the multiplicity of the root -3 equals 1. We can also see that the factor $2Z - 3$ gives rise to another root of $p_1(Z)$, namely the root $3/2$. This root also has multiplicity 1.
2. We have $p_2(-3) = 1$. Therefore -3 is not a root of $p_2(Z)$.
3. This time we have $p_3(-3) = 0$, so -3 is a root of $p_3(Z)$. Using the division algorithm, we find:

$$\begin{array}{r|l|l} Z+3 & Z^3 + 3Z^2 - 9Z - 27 & Z^2 - 9 \\ & Z^3 + 3Z^2 & \\ \hline & -9Z - 27 & \\ & -9Z - 27 & \\ \hline & 0 & \end{array}$$

   Therefore it holds that $Z^3 + 3Z^2 - 9Z - 27 = (Z + 3) \cdot (Z^2 - 9)$. The number -3 is also a root of the polynomial $Z^2 - 9$, so the multiplicity of the root -3 is at least 2. Actually, it holds that $Z^2 - 9 = (Z + 3) \cdot (Z - 3)$, so $Z^3 + 3Z^2 - 9Z - 27 = (Z + 3) \cdot (Z^2 - 9) = (Z + 3)^2 \cdot (Z - 3)$. This means that the root -3 of $p_3(Z)$ has multiplicity 2. We also showed that 3 is a root of $p_3(Z)$ and that this root has multiplicity 1.

4. We have $p_4(Z) = p_1(Z)p_3(Z)$. From the first and the third part of this example, we get that $p_4(Z) = (Z+3)^3 \cdot (2Z-3) \cdot (Z-3)$. This means that the root -3 has multiplicity 3. We also see that the numbers $3/2$ and 3 are roots of $p_4(Z)$, both with multiplicity 1. The graph of real polynomial function that $p_4(Z)$ gives rise to, is given in Figure 4.3.

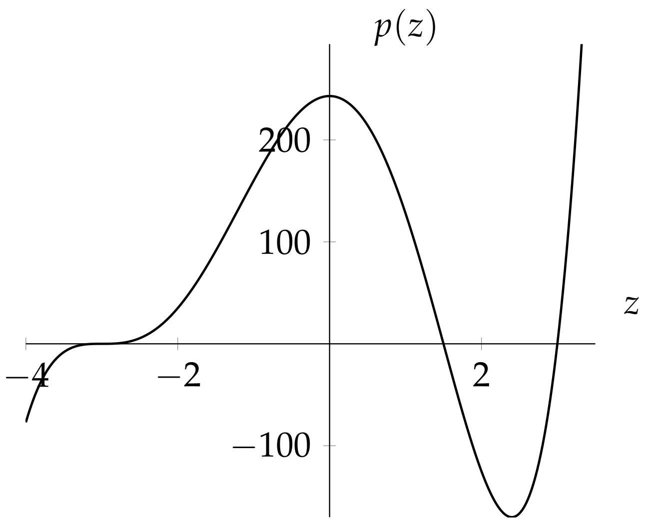


Figure 4.3: The graph of the polynomial function $p : \mathbb{R} \to \mathbb{R}$, where $p(z) = 2z^5 + 9z^4 - 18z^3 - 108z^2 + 243$.

The above example illustrates that there is a one to one correspondence between factors of degree one of a polynomial and the roots of a polynomial. The fundamental theorem of algebra (Theorem 4.19) says that each polynomial of degree at least 1 has a root. This has the following consequence:

|||| Theorem 4.23

Let $p(Z) = a_n Z^n + a_{n-1} Z^{n-1} + \cdots + a_1 Z + a_0$ be a polynomial of degree $n > 0$. Then there exist $\lambda_1, ..., \lambda_n \in \mathbb{C}$ such that

$$p(Z) = a_n \cdot (Z - \lambda_1) \cdots (Z - \lambda_n).$$

Proof. According to the fundamental theorem of algebra there exists a root $\lambda_1 \in \mathbb{C}$ of the polynomial $p(Z)$. Using Lemma 4.20, we can write $p(Z) = (Z - \lambda_1) q_1(Z)$ for a certain polynomial $q_1(Z)$. Note that $\deg(q_1(Z)) = \deg(p(Z)) - 1$. If $q_1(Z)$ is a constant, we are done. Otherwise, we can apply the fundamental theory of algebra to the polynomial $q_1(Z)$ and find a root $\lambda_2 \in \mathbb{C}$ of $q_1(Z)$. Again using Lemma 4.20, we can write $q_1(Z) = (Z - \lambda_2) \cdot q_2(Z)$. This implies that $p(Z) = (Z - \lambda_1) \cdot (Z - \lambda_2) \cdot q_2(Z)$. Continuing in this way, we can write $p(Z)$ as a product of polynomials of degree one of the form $Z - \lambda$ times a constant c. Since the leading coefficient of $p(Z)$ is a_n, this constant c is equal to a_n. □

|||| Example 4.24

As an example we take the polynomial $p_4(Z) = 2Z^5 + 9Z^4 - 18Z^3 - 108Z^2 + 243$ from Example 4.22. We wish to write this polynomial as in Theorem 4.23. We have already seen that $p_4(Z) = (Z+3)^3 \cdot (2Z-3) \cdot (Z-3)$. By pulling out the 2 from the factor $2Z - 3$ we get:

$$p_4(Z) = 2 \cdot (Z+3)^3 \cdot (Z-3/2) \cdot (Z-3) = 2 \cdot (Z+3) \cdot (Z+3) \cdot (Z+3) \cdot (Z-3/2) \cdot (Z-3).$$

In the notation of Theorem 4.23 we find that $\lambda_1 = -3$, $\lambda_2 = -3$, $\lambda_3 = -3$, $\lambda_4 = 3/2$, and $\lambda_5 = 3$. This illustrates once more that the multiplicities of the roots -3, $3/2$, and 3 are 3, 1, and 1. Note that the sum of all multiplicities is equal to 5, which is the degree of $p_4(Z)$.

In fact it always holds that the sum of all multiplicities of the roots of a polynomial is equal to its degree. In words one can therefore reformulate Theorem 4.23 as follows: a polynomial of degree $n \geq 1$ has exactly n roots, if the roots are counted with their multiplicities. For polynomials in $\mathbb{R}[Z]$, Theorem 4.23 has the following consequence

|||| Corollary 4.25

Any polynomial $p(Z) \in \mathbb{R}[Z]$ of degree at least one, can be written as the product of degree one and degree two polynomials from $\mathbb{R}[Z]$.

Proof. According to Theorem 4.23 any nonzero polynomial $p(Z)$ can be written as the product of the leading coefficient of $p(Z)$ and degree one factors of the form $Z - \lambda$. The $\lambda \in \mathbb{C}$ is a root of the polynomial $p(Z)$. Applying this to a polynomial $p(Z)$ with real coefficients, we see that the leading term is a real number as well, but the roots λ do not have to be real numbers. However, any real root λ gives rise to a factor of degree one with real coefficients, namely $Z - \lambda$.

Now let $\lambda \in \mathbb{C} \setminus \mathbb{R}$ be a root of $p(Z)$. Let us write $\lambda = a + bi$ in rectangular form. Since $\lambda \notin \mathbb{R}$, we know that $b \neq 0$. Lemma 4.12 implies that then the number $\overline{\lambda} = a - bi$ is also a root of $p(Z)$. Moreover, $\lambda \neq \overline{\lambda}$, since $b \neq 0$. Hence $Z - \lambda$ and $Z - \overline{\lambda}$ are two distinct factors of $p(Z)$ if we would work in $\mathbb{C}[Z]$. Now the idea is to multiply the factors $Z - \lambda$ and $Z - \overline{\lambda}$ together, since it turns out that $(Z - \lambda) \cdot (Z - \overline{\lambda})$ has real coefficients. Indeed, we have

$$\begin{aligned}(Z - \lambda) \cdot (Z - \overline{\lambda}) &= Z^2 - (\lambda + \overline{\lambda})Z + \lambda\overline{\lambda} \\ &= Z^2 - (a + bi + a - bi)Z + (a + bi) \cdot (a - bi) \\ &= Z^2 - 2aZ + (a^2 + b^2),\end{aligned}$$

which indeed is a polynomial of degree two in $\mathbb{R}[Z]$ since its coefficients are real numbers. In this way we can transform the factorization of $p(Z)$ in $\mathbb{C}[Z]$ from Theorem 4.23 into a factorization of $p(Z)$ in $\mathbb{R}[Z]$ in first and second degree factors with real coefficients. □

|||| Example 4.26

Write the following polynomials as a product of degree one and degree two polynomials with real coefficients.

1. $p_1(Z) = Z^3 - Z^2 + Z - 1$
2. $p_2(Z) = Z^4 + 4$

Answer:

1. The number 1 is a root of $p_1(Z)$, since $p(1) = 0$. Using the division algorithm, one can show that $p_1(Z) = (Z - 1) \cdot (Z^2 + 1)$. The polynomial $Z^2 + 1$ does not have any real root and therefore cannot be factorized further over the real numbers (over the complex numbers one could: $Z^2 + 1 = (Z + i) \cdot (Z - i)$). The desired factorization is therefore:
$$Z^3 - Z^2 + Z - 1 = (Z - 1) \cdot (Z^2 + 1).$$
2. Using the theory of Section 4.4 we can find all roots of the polynomial $Z^4 + 4$. In this way one can find the roots $1 + i, 1 - i, -1 + i$ and $-1 - i$. Therefore we have that
$$Z^4 + 4 = (Z - (1 + i)) \cdot (Z - (1 - i)) \cdot (Z - (-1 + i)) \cdot (Z - (-1 - i)).$$
As in the proof of Corollary 4.25 we can multiply pairs of complex conjugated factors together to get rid of the complex coefficients. Then we find that
$$(Z - (1 + i)) \cdot (Z - (1 - i)) = Z^2 - 2Z + 2$$

and

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

The desired factorization of Z^4+4 is therefore

$$Z^4+4 = (Z^2-2Z+2)\cdot(Z^2+2Z+2).$$