22 Lecture 22 – Fundamental Theorem of Algebra and Definition of Vector Space

22.1 Fundamental Theorem of Algebra

For more details see [3, Chapter 4].

Let $n \in \mathbb{N}$ and $a_0, a_1, \ldots, a_n$ be a complex numbers. We set

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0, \quad z \in \mathbb{C}.$$

The function f is called a **polynomial function**. The numbers $a_0, a_1, \ldots, a_n$ are coefficients of the polynomial f. If $a_n \neq 0$, then the number n is called the **degree** of f and is denoted by $\deg f := n$.

In this section, we are going to prove that the equation $f(z) = 0$ as at most n solutions. The next theorem is called the fundamental theorem of algebra and we formulate it without prof. The prof will be given at the course of complex analysis using Liouville's theorem.

Theorem 22.1 (Fundamental theorem of algebra)**.** *For every $n \in \mathbb{N}$ and $a_0, a_1, \ldots, a_n \in \mathbb{C}$, $a_n \neq 0$, the equation*

$$a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0 = 0$$

has at least one solution in $\mathbb{C}$.

Theorem 22.2. *Let f be a polynomial function of degree $n \in \mathbb{N}$. Then*

1) for any $w \in \mathbb{C}$ we have that $f(w) = 0$ iff there exists a polynomial g of degree $n-1$ such that

$$f(z) = (z - w) g(z), \quad z \in \mathbb{C};$$

2) there exist at most n distinct complex solutions of the polynomial equation $f(z) = 0$;

3) there exist $w_1, \ldots, w_n \in \mathbb{C}$ (not necessary distinct) such that

$$f(z) = a_n (z - w_1) \ldots (z - w_n), \quad z \in \mathbb{C},$$

where a_n denotes the coefficient about z^n.

Proof. To prove 1), we first recall that for each $a, b \in \mathbb{R}$

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2} b + \ldots + a b^{n-2} + b^{n-1}) = (a - b) \sum_{k=1}^{n} a^{n-k} b^{k-1}.$$

Let $f(w) = 0$. Then

$$\begin{aligned} f(z) = f(z) - f(w) &= a_n (z^n - w^n) + a_{n-1}(z^{n-1} - w^{n-1}) + \ldots + a_1 (z - w) \\ &= a_n (z - w) \sum_{k=1}^{n} z^{n-k} w^{k-1} + a_{n-1}(z - w) \sum_{k=1}^{n-1} z^{n-k-1} w^{k-1} + \ldots + a_1 (z - w) \\ &= (z - w) \left(a_n \sum_{k=1}^{n} z^{n-k} w^{k-1} + a_{n-1} \sum_{k=1}^{n-1} z^{n-k-1} w^{k-1} + \ldots + a_1 \right) = (z - w) g(z), \end{aligned}$$

where $g(z) = a_n \sum_{k=1}^{n} z^{n-k} w^{k-1} + a_{n-1} \sum_{k=1}^{n-1} z^{n-k-1} w^{k-1} + \ldots + a_1$, $z \in \mathbb{C}$, is a polynomial of degree $n-1$.

Now, we prove 3). Let w_1 be a complex number such that $f(w_1) = 0$, which exists according to Theorem 22.1. Applying the part 1) of Theorem 22.2, we have that there exists a polynomial g_1 such that $f(z) = (z - w_1)g_1(z)$, $z \in \mathbb{C}$. Next, using Theorem 22.1 again, we obtain that there exists w_2 such that $f(w_2) = 0$. By Theorem 22.2 1), there exists a polynomial g_2 such that $g_1(z) = (z - w_2)g_2(z)$, $z \in \mathbb{C}$. Consequently, $f(z) = (z - w_1)(z - w_2)g_2(z)$, $z \in \mathbb{C}$. Applying theorems 22.1 and 22.2 1) n times, we get that

$$f(z) = (z - w_1)\ldots(z - w_n)g_n, \quad z \in \mathbb{C}, \tag{47}$$

for some $w_1, w_2, \ldots, w_n \in \mathbb{C}$ and a polynomial g_n of degree 0 which is a constant function. Since the right hand side of (47) is a polynomial with the coefficient g_n about z_n, we can conclude that $g_n = a_n$.

The part 2) of the theorem easily follows from 3).

□

Exercise 22.1. For a complex number α show that the coefficients of the polynomial

$$p(z) = (z - \alpha)(z - \overline{\alpha})$$

are real numbers.

Exercise 22.2. Let $p(z)$ be a polynomial with real coefficients and let α be a complex number. Prove that $p(\alpha) = 0$ if and only if $p(\overline{\alpha}) = 0$.

Exercise 22.3. Prove that any polynomial $p(z)$ with real coefficients can be decomposed into a product of polynomials of the form $az^2 + bz + c$, where $a, b, c \in \mathbb{R}$.

22.2 Definition and some Examples of Vector Spaces

For more details see [3, Chapter 5].

Let $\mathbb{F}$ denote the set of real numbers $\mathbb{R}$ or complex numbers $\mathbb{C}$. We will call $\mathbb{F}$ a **field**. We also consider a set V, whose elements are called **vectors** and will be denoted by $\mathbf{v}, \mathbf{u}, \mathbf{w} \ldots$ etc. We define on V two operations:

- **vector addition** $+ : V \times V \to V$, that maps two elements $\mathbf{u}, \mathbf{v}$ of V to $\mathbf{u} + \mathbf{v} \in V$;
- **scalar multiplication** $\cdot : \mathbb{F} \times V \to V$, that maps $a \in \mathbb{F}$ and $\mathbf{u} \in V$ to $a \cdot \mathbf{u} = a\mathbf{u} \in V$.

Definition 22.1. A **vector space** over $\mathbb{F}$ is a set V together with operations of vector addition and scalar multiplication which satisfy the following properties:

1) **commutativity**: $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ for all $\mathbf{u}, \mathbf{v} \in V$;
2) **associativity**: $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$ and $(ab)\mathbf{v} = a(b\mathbf{v})$ for all $a, b \in \mathbb{F}$ and $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$;
3) **additive identity**: there exists a vector $\mathbf{0} \in V$ such that $\mathbf{0} + \mathbf{v} = \mathbf{v}$ for all $\mathbf{v} \in V$;
4) **additive inverse**: for every $\mathbf{v} \in V$ there exists a vector $\mathbf{w} \in V$ (denoted by $-\mathbf{v}$) such that $\mathbf{v} + \mathbf{w} = \mathbf{0}$;
5) **multiplicative identity**: $1 \cdot \mathbf{v} = \mathbf{v}$ for all $\mathbf{v} \in V$;

6) **distributivity**: $a(\mathbf{u}+\mathbf{v}) = a\mathbf{u} + a\mathbf{v}$ and $(a+b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$ for all $a, b \in \mathbb{F}$, $\mathbf{u}, \mathbf{v} \in V$.

A vector space over $\mathbb{R}$ will be called a **real vector space** and a vector space over $\mathbb{C}$ is similarly called a **complex vector space**.

Example 22.1. The set $V = \mathbb{F}$ with the usual operations of addition and multiplication is trivially a vector space over $\mathbb{F}$.

Example 22.2. The set

$$\mathbb{F}^n = \{\mathbf{x} = (x_1, x_2, \dots, x_n) : \ x_k \in \mathbb{F}, \ k = 1, \dots, n\}$$

with operations

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$$

and

$$a\mathbf{x} = (ax_1, ax_2, \dots, ax_n),$$

for all $a \in \mathbb{F}$, $\mathbf{x} = (x_1, x_2, \dots, x_n)$, $\mathbf{y} = (y_1, y_2, \dots, y_n) \in \mathbb{F}^n$, is a vector space. It is easily to see that the additive identity is $\mathbf{0} = (0, 0, \dots, 0)$ and the additive inverse of $\mathbf{x} = (x_1, x_2, \dots, x_n)$ is $-\mathbf{x} = (-x_1, -x_2, \dots, -x_n)$.

Example 22.3. Similarly, the set

$$\mathbb{F}^\infty = \{\mathbf{x} = (x_1, x_2, \dots) : \ x_k \in \mathbb{F}, \ k \in \mathbb{N}\}$$

with operations

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, \dots)$$

and

$$a\mathbf{x} = (ax_1, ax_2, \dots),$$

for all $a \in \mathbb{F}$, $\mathbf{x} = (x_1, x_2, \dots)$, $\mathbf{y} = (y_1, y_2, \dots) \in \mathbb{F}^\infty$, is also a vector space, where $\mathbf{0} = (0, 0, \dots)$ is additive identity and $-\mathbf{x} = (-x_1, -x_2, \dots)$ is the additive inverse of $\mathbf{x} = (x_1, x_2, \dots)$.

Example 22.4. The set of all polynomials of degree at most n

$$\mathbb{F}^n[z] = \{\mathbf{p}(z) = a_n z^n + \dots + a_1 z + a_0, \ z \in \mathbb{F} : \ a_k \in \mathbb{F}, \ k = 1, \dots, n\}$$

with the addition

$$(\mathbf{p} + \mathbf{q})(z) = (a_n + b_n) z^n + \dots + (a_1 + b_1) z + a_0 + b_0, \quad z \in \mathbb{F},$$

and scalar multiplication

$$(a\mathbf{p})(z) = a a_n z^n + \dots + a a_1 z + a a_0, \quad z \in \mathbb{F},$$

for all $a \in \mathbb{F}$ and $\mathbf{p}(z) = a_n z^n + \dots + a_1 z + a_0$, $\mathbf{q}(z) = b_n z^n + \dots + b_1 z + b_0$, $z \in \mathbb{F}$, from $\mathbb{F}^n[z]$ is also a vector space.

Exercise 22.4. The vector space $\mathbb{F}[z]$ of all polynomials of any degree can be defined similarly as $\mathbb{F}^n[z]$ and is also a vector space.

Example 22.5. The set of (real-valued) continuous functions on an interval $[a, b]$ with the usual addition of functions and multiplication by a constant is a real vector space.

Exercise 22.5. The set of complex numbers $\mathbb{C} = \{x + iy : \; x, y \in \mathbb{R}\}$ can be considered as a real vector space with the usual addition of complex numbers and the multiplication by the real number.

Example 22.6. The set $V = \{\mathbf{0}\}$, where $\mathbf{0}$ is any element, with addition $\mathbf{0} + \mathbf{0} := \mathbf{0}$ and scalar multiplication $a \cdot \mathbf{0} := \mathbf{0}$ is a vector space. (Here $\mathbf{0}$ also plays a role of the additive identity).

Exercise 22.6. Show that the sets from the previous examples are vector spaces under corresponding addition and scalar multiplication.

Exercise 22.7. For each of the following sets, either show that the set is a vector space over $\mathbb{F}$ or explain why it is not a vector space.

a) The set $\mathbb{R}$ of real numbers under the usual operations of addition and multiplication, $\mathbb{F} = \mathbb{R}$.

b) The set $\mathbb{R}$ of real numbers under the usual operations of addition and multiplication, $\mathbb{F} = \mathbb{C}$.

c) The set $\{f \in \mathrm{C}[0, 1] : f(0) = 2\}$ under the usual operations of addition and multiplication of functions, $\mathbb{F} = \mathbb{R}$.

d) The set $\{f \in \mathrm{C}[0, 1] : f(0) = f(1) = 0\}$ under the usual operations of addition and multiplication of functions, $\mathbb{F} = \mathbb{R}$.

e) The set $\{(x, y, z) \in \mathbb{R}^3 : x - 2y + z = 0\}$ under the usual operations of addition and multiplication on $\mathbb{R}^3$, $\mathbb{F} = \mathbb{R}$.

f) The set $\{(x, y, z) \in \mathbb{C}^3 : 2x + z + i = 0\}$ under the usual operations of addition and multiplication on $\mathbb{C}^3$, $\mathbb{F} = \mathbb{C}$.

22.3 Elementary Properties of Vector Spaces

In this section, we prove some important and simple properties of vector spaces. Let V denote a vector space over $\mathbb{F}$.

Proposition 22.1. *Any vector space has a unique additive identity.*

Proof. Let us assume that there exist two additive identities $\mathbf{0}$ and $\mathbf{0}'$. Then

$$\mathbf{0} = \mathbf{0} + \mathbf{0}' = \mathbf{0}',$$

where the first identity holds since $\mathbf{0}'$ is an identity and the second equality holds since $\mathbf{0}$ is an identity. □

Proposition 22.2. *Every* $\mathbf{v} \in V$ *has a unique inverse.*

Proof. We assume that $\mathbf{w}$ and $\mathbf{w}'$ are additive inverses of $\mathbf{v}$ so that $\mathbf{v} + \mathbf{w} = \mathbf{0}$ and $\mathbf{v} + \mathbf{w}' = \mathbf{0}$. Then

$$\mathbf{w} = \mathbf{w} + \mathbf{0} = \mathbf{w} + (\mathbf{v} + \mathbf{w}') = (\mathbf{w} + \mathbf{v}) + \mathbf{w}' = \mathbf{0} + \mathbf{w}' = \mathbf{w}'.$$

□

Since the additive inverse of $\mathbf{v}$ is unique, we will denote it by $-\mathbf{v}$. We also define $\mathbf{w}-\mathbf{v} := \mathbf{w}+(-\mathbf{v})$.

Proposition 22.3. *For every* $\mathbf{v} \in V$ $0 \cdot \mathbf{v} = \mathbf{0}$.

Proof. For $\mathbf{v} \in V$ we have that

$$0 \cdot \mathbf{v} = (0+0) \cdot \mathbf{v} = 0 \cdot \mathbf{v} + 0 \cdot \mathbf{v}.$$

Adding the additive inverse of $0\mathbf{v}$ to both sides, we obtain

$$\mathbf{0} = 0\mathbf{v} - 0\mathbf{v} = (0\mathbf{v} + 0\mathbf{v}) - 0\mathbf{v} = 0\mathbf{v}.$$

□

Proposition 22.4. *For every* $a \in \mathbb{F}$ $a \cdot \mathbf{0} = \mathbf{0}$.

Exercise 22.8. Prove Proposition 22.4.

Proposition 22.5. *For every* $\mathbf{v} \in V$ $(-1) \cdot \mathbf{v} = -\mathbf{v}$.

We recall that the vector $-\mathbf{v}$ denotes the additive inverse of $\mathbf{v}$.

Proof. For $\mathbf{v} \in V$, we have

$$\mathbf{v} + (-1) \cdot \mathbf{v} = 1 \cdot \mathbf{v} + (-1) \cdot \mathbf{v} = (1 + (-1))\mathbf{v} = 0 \cdot \mathbf{v} = \mathbf{0},$$

by Proposition 22.3. □