Calculus 1, 3rd lecture

Axioms for the real numbers. Complex numbers.

Axioms for the real numbers

$\mathbb{R}$ is a set whose elements are called real numbers. Two operations, called addition and multiplication are defined in $\mathbb{R}$ such that $\mathbb{R}$ is closed under these operations, that is, $\forall\, a, b \in \mathbb{R}\ \ (a + b \in \mathbb{R}$ and $a \cdot b \in \mathbb{R})$.

Addition:

1) $\forall\, a, b \in \mathbb{R}\ (a + b = b + a)$ (commutativity),
2) $\forall\, a, b, c \in \mathbb{R}\ \ ((a + b) + c) = a + (b + c))$ (associativity),
3) $\exists\, 0 \in \mathbb{R}\ \ (\forall\, a \in \mathbb{R}\ \ (a + 0 = 0 + a = 0))$ (existence of a zero element),
4) $\forall\, a \in \mathbb{R}\ (\exists\, b \in \mathbb{R}\ (a + b = 0))$ (existence of an additive inverse, notation: $b = -a$).

Multiplication:

5) $\forall\, a, b \in \mathbb{R}\ \ (a \cdot b = b \cdot a)$ (commutativity),
6) $\forall\, a, b, c \in \mathbb{R}\ \ ((a \cdot b) \cdot c = a \cdot (b \cdot c))$ (associativity),
7) $\exists\, 1 \in \mathbb{R}\ \ (\forall\, a \in \mathbb{R}\ (a \cdot 1 = 1 \cdot a = a))$ (existence of a unit element),
8) $\forall\, a \in \mathbb{R} \setminus \{0\}\ (\exists\, b \in \mathbb{R}\ \ (a \cdot b = 1))$ (existence of a multiplicative inverse, notation: $b = a^{-1}$).

For the two operations above:

9) $\forall\, a, b, c \in \mathbb{R}\ \ (a + b) \cdot c = a \cdot c + b \cdot c$ (the multiplication is distributive with respect to the addition).

Axioms (1)–(9) are the axioms for a **field**.

Ordering:

10) Exactly one of the following is true: $a < b,\ \ b < a,\ \ a = b$ (trichotomy),
11) $\forall\, a, b, c \in \mathbb{R}\ \ ((a < b) \wedge (b < c)) \implies (a < c)$ (transitivity),
12) $\forall\, a, b, c \in \mathbb{R}\ \ ((a < b) \wedge c > 0) \implies a \cdot c < b \cdot c$
13) $\forall\, a, b, c \in \mathbb{R}\ \ (a < b) \implies a + c < b + c$ (monotonicity)

Axioms (1)–(13) are the axioms for an **ordered field**.

Archimedian axiom:

14) $\forall\, a \in \mathbb{R}\ \ (\exists\, n \in \mathbb{N}\ \ (a < n))$.

Axioms 1) – 14) are true both for $\mathbb{R}$ and $\mathbb{Q}$.

Cantor axiom:

15) Let $a_1, b_1, a_2, b_2, \ldots \in \mathbb{R}$.

$(\forall\, n \in \mathbb{N}\ \ (a_n \le a_{n+1} \le b_{n+1} \le b_n)) \implies (\exists\, x \in \mathbb{R}\ \ (\forall\, n \in \mathbb{N}\ \ (x \in [a_n, b_n])))$

$\left(\text{so } \bigcap_{n=1}^{\infty} [a_n, b_n] \neq \emptyset\right)$.

It states that any nested sequence of closed intervals has a non-empty intersection.

Example: Let $a_1 = 1.4$ and $b_1 = 1.5$

$a_2 = 1.41$ $b_2 = 1.42$

$a_3 = 1.414$ $b_3 = 1.415$

$a_4 = 1.4142$ $b_4 = 1.4143$

... ...

$a_n = \left[10^n \cdot \sqrt{2}\right] \cdot 10^{-n}$ $b_n = \left(\left[10^n \cdot \sqrt{2}\right] + 1\right) \cdot 10^{-n}$

where [.] denotes the floor function.

Then $a_1 < a_2 < a_3 < a_4 < \ldots < \sqrt{2} < \ldots < b_4 < b_3 < b_2 < b_1$, so $\bigcap_{n=1}^{\infty} [a_n, b_n] = \left\{\sqrt{2}\right\} \in \mathbb{R} \setminus \mathbb{Q}$.

Remark. Closeness is important, for example if $I_n = \left(0, \frac{1}{n}\right]$ then $\bigcap_{n=1}^{\infty} I_n = \emptyset$.

Consequences

Some elementary laws of algebra and inequalities follow from the axioms. For example:

1) For all $a \in \mathbb{R}$, exactly one of the following properties hold: $a > 0$, $a = 0$, $a < 0$.
$(a > 0 \iff -a < 0)$

2) $(a < b) \wedge (c < d) \Longrightarrow a + c < b + d$
Specifically: $(a > 0) \wedge (b > 0) \Longrightarrow a + b > 0$

3) $(0 \le a < b) \wedge (0 \le c < d) \Longrightarrow a\,c < b\,d$
Specifically: $(a > 0) \wedge (b > 0) \Longrightarrow a\,b > 0$

4) $(a < b) \wedge (c < 0) \Longrightarrow a\,c > b\,c$
Specifically: $a < b \Longrightarrow -a > -b$

5) (i) $0 < a < b \Longrightarrow \frac{1}{a} > \frac{1}{b}$ (ii) $a < b < 0 \Longrightarrow \frac{1}{a} > \frac{1}{b}$ (iii) $a < 0 < b \Longrightarrow \frac{1}{a} < \frac{1}{b}$

6) For all $a, b \in \mathbb{R}$, $|a + b| \le |a| + |b|$ and $||a| - |b|| \le |a - b|$.

7) If n is a positive integer and $0 < a < b$ then $a^n < b^n$.
8) $\forall x \in \mathbb{R} \ (x \cdot 0 = 0)$
9) $\forall x \in \mathbb{R} \ (x \cdot y = 0 \Longrightarrow x = 0 \text{ or } y = 0)$

Proof of 8):
$x \cdot 0 = x \cdot 0 + 0 = x \cdot 0 + (x \cdot 0 - x \cdot 0) = (x \cdot 0 + x \cdot 0) - x \cdot 0 = x \cdot (0 + 0) - x \cdot 0 = x \cdot 0 - x \cdot 0 = 0.$

Proof of 9):
$x \neq 0 \Longrightarrow y = 1 \cdot y = ((1/x) \cdot x) \cdot y = (1/x) \cdot (x \cdot y) = (1/x) \cdot 0 = 0.$

Bounded subsets of real numbers

Definition. $A \subset \mathbb{R}$ **is bounded above** if there exists a $K \in \mathbb{R}$ such that $a \leq K$ for all $a \in A$.
In this case K is an **upper bound** of A.

Definition. $A \subset \mathbb{R}$ is **bounded below** if there exists a $k \in \mathbb{R}$ such that $a \geq k$ for all $a \in A$.
In this case k is a **lower bound** of A.

Definition. $A \subset \mathbb{R}$ is **bounded** if it is has an upper bound and a lower bound.
It means that there exists a $K > 0$ such that $|a| < K$ for all $a \in A$.

Remark: A bounded set has infinitely many lower and upper bounds.

Examples: 1) $\mathbb{N}$ is bounded below
2) $(0, 1] = \{x \in \mathbb{R} : 0 < x \leq 1\}$ is bounded (for example, upper bounds are $1, 2, \pi, \ldots$, lower bounds are $0, -3, -100, \ldots$)
3) $\mathbb{Q}$ has no upper bound or lower bound

Definition. If a set A is bounded above, then the **supremum** of A is the **least upper bound** of A.
Notation: $\sup A$. If A is not bounded above, then $\sup A = \infty$.

Definition. If a set A is bounded below then the **infimum** of A is the **greatest lower bound** of A.
Notation: $\inf A$. If A is not bounded below, then $\inf A = -\infty$.

Examples: 1) $\inf \mathbb{N} = 1$, $\sup \mathbb{N} = \infty$; 2) $\inf(0, 1] = 0$, $\sup(0, 1] = 1$; 3) $\inf \mathbb{Q} = -\infty$, $\sup \mathbb{Q} = \infty$

Definition. The **minimum** of the set A is a if $a \in A$ and $a = \inf A$.
The **maximum** of the set A is b if $b \in A$ and $b = \sup A$.

Examples: 1) The minimum of $\mathbb{N}$ is 1 and it has no maximum.
2) The maximum of $(0, 1]$ is 1 and it has no minimum.
3) $\mathbb{Q}$ has no minimum and no maximum.

Least-upper-bound property

Theorem (Least-upper-bound property, Dedekind):
If a non-empty subset of $\mathbb{R}$ is bounded above then it has a least upper bound in $\mathbb{R}$.

Consequence. If a non-empty subset of $\mathbb{R}$ is bounded below then it has a greatest lower bound in $\mathbb{R}$.

Remarks. 1) In the above system of axioms, the axioms of Cantor and Archimedes can be replaced by this statement.

2) The set of rational numbers does not have the least-upper-bound property under the usual order.
For example, $\{x \in \mathbb{Q} : x^2 \leq 2\} = \mathbb{Q} \cap \left(-\sqrt{2}, \sqrt{2}\right)$ has an upper bound in $\mathbb{Q}$ but does not have a least upper bound in $\mathbb{Q}$ since $\sqrt{2}$ is irrational.

Complex numbers

Definition

The complex field $\mathbb{C}$ is the set of ordered pairs of real numbers: $\mathbb{C} = \mathbb{R}^2 = \{(a, b) : a, b \in \mathbb{R}\}$ with addition and multiplication defined by

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b)(c, d) = (a c - b d, a d + b c).$$

The field axioms

Commutativity and associativity of addition and multiplication as well as distributivity (see 1), 2), 5), 6), 9)) follow easily from the same properties of reals numbers.
3) the additive identity or zero element is $(0, 0)$
4) the additive inverse of (a, b) is $(-a, -b)$
7) the multiplicative identity or unit element is $(1, 0)$
8) the multiplicative inverse of $(a, b) \neq (0, 0)$ can be found in the following way:

$$(a, b)(x, y) = (1, 0) \iff \begin{matrix} a x - b y = 1 \\ b x + a y = 0 \end{matrix} \iff x = \frac{a}{a^2 + b^2}, \; y = \frac{-b}{a^2 + b^2}$$

Thus the complex numbers form a field.

Some consequences

We associate the complex number of the form $(a, 0)$ with the corresponding real number a.
Then $(a_1, 0) + (a_2, 0) = (a_1 + a_2, 0)$ corresponds to $a_1 + a_2$ and
$(a_1, 0)(a_2, 0) = (a_1 a_2, 0)$ corresponds to $a_1 a_2$.

Since $(0, 1)(0, 1) = (-1, 0) = -1$, then we can say that $(0, 1)$ is a square root of -1 and it will be denoted by i. That is, $i^2 = -1$, where i is called the **imaginary unit**.
Remark: $i^2 = (-i)^2 = -1$.

The algebraic form of complex numbers

We can rewrite any complex number in the following way:

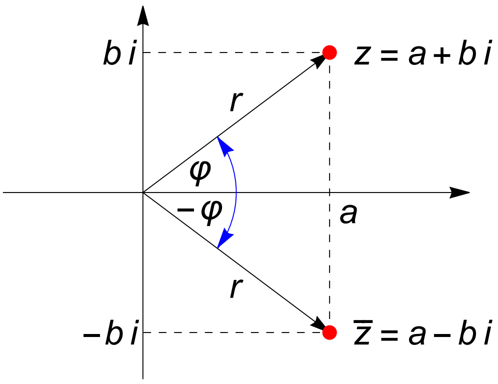
$$(a, b) = (a, 0) + (0, b) = a + b i$$

where $a, b \in \mathbb{R}$ and $i^2 = -1$.

$\Longrightarrow$ Addition: $(a + b i) + (c + d i) = (a + b) + (c + d) i$
Multiplication: $(a + b i)(c + d i) = a c + b d i^2 + a d i + b c i = (a c - b d) + (a d + b c) i$

The complex plane

To each complex number $z = a + b\,i$ we associate the point (a, b) in the Cartesian plane.
Real numbers are thus associated with points on the x-axis, called the **real axis** and
the purely imaginary numbers $b\,i$ correspond to points on the y-axis, called the **imaginary axis**.



Definitions

If $z = a + b\,i$ then

- the **real part** of z is $\mathrm{Re}(z) = a \in \mathbb{R}$
- the **imaginary part** of z is $\mathrm{Im}(z) = b \in \mathbb{R}$
- the **conjugate** of z is $\bar{z} = a - b\,i$
- the **absolute value** or **modulus** of z is $r = |z| = \sqrt{a^2 + b^2} \geq 0$ (the length of the vector z)
- the **argument** of z, defined for $z \neq 0$, is the angle which the vector originating from 0 to z makes with the positive x-axis. Thus $\arg(z) = \varphi$ (modulo 2π) for which

$$\cos\varphi = \frac{\mathrm{Re}(z)}{|z|} = \frac{a}{r} \quad \text{and} \quad \sin\varphi = \frac{\mathrm{Im}(z)}{|z|} = \frac{b}{r}$$

Some identities

- $z\,\bar{z} = (a + b\,i)(a - b\,i) = a^2 - b^2 i^2 = a^2 + b^2 = |z|^2$
- $\overline{z_1 \pm z_2} = \overline{z_1} \pm \overline{z_1}$, $\quad \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_1}$, $\quad \overline{\left(\frac{z_1}{z_2}\right)} = \frac{\overline{z_1}}{\overline{z_2}}$, $\quad \bar{\bar{z}} = z$
- $\mathrm{Re}(z) = \dfrac{z + \bar{z}}{2}$, $\quad \mathrm{Im}(z) = \dfrac{z - \bar{z}}{2\,i}$

The trigonometric form (or polar form) of complex numbers

Let $z = a + b\,i \neq 0$, $r = |z|$ and $\varphi = \arg(z)$. Then $a = r\cos\varphi$ and $b = r\sin\varphi$ and

$$z = r(\cos\varphi + i\sin\varphi)$$

where r and φ are called the polar coordinates of z.

Multiplication and division

Let $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$ and $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$. Then

- $z_1 z_2 = r_1 r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2))$
- $\frac{z_1}{z_2} = \frac{r_1}{r_2}(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2))$ (if $r_2 \neq 0$)

Reciprocal, conjugation, *n*th power

Let $z = r(\cos\varphi + i\sin\varphi)$. Then

- $\frac{1}{z} = \frac{1}{r}(\cos(-\varphi) + i\sin(-\varphi))$ (if $r \neq 0$)
- $\bar{z} = r(\cos(-\varphi) + i\sin(-\varphi))$
- $z^n = r^n(\cos(n\varphi) + i\sin(n\varphi))$ $(n \in \mathbb{N}^+)$ If $r \neq 0$ then it holds for $n \in \mathbb{Z}$.

The *n*th root

If $z \neq 0$ and $n \in \mathbb{N}^+$ then $w \in \mathbb{C}$ is an nth root of z if $w^n = z$. Then

$$w = \sqrt[n]{r(\cos\varphi + i\sin\varphi)} = \sqrt[n]{r}\left(\cos\frac{\varphi + k \cdot 2\pi}{n} + i\sin\frac{\varphi + k \cdot 2\pi}{n}\right) \text{ where } k = 0, 1, \ldots, n-1.$$

Some identities

$$|z_1 z_2| = |z_1| \cdot |z_2|, \quad \left|\frac{1}{z}\right| = \frac{1}{|z|}, \quad \left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}, \quad |z^n| = |z|^n, \quad |\bar{z}| = |z|$$

Fundamental theorem of algebra

Every degree n polynomial with complex coefficients has exactly n complex roots, if counted with multiplicity.

Exercise

1. Using the field and ordering axioms prove that $\forall a \in \mathbb{R}$ $a^2 \geq 0$.
2. Show that no ordering can make the field of complex numbers into an ordered field.

Solution: See exercises 1.1.8 and 1.1.9 here:

http://etananyag.ttk.elte.hu/FiLeS/downloads/4b_FeherKosToth_MathAnExII.pdf