NGUYỄN THÀNH ANH

ENGLISH FOR MATHEMATICS

MANUSCRIPT OF LECTURE NOTES

HNUE, January 2013

Some useful websites:

1. `http://en.wikipedia.org`
2. `http://tratu.soha.vn`
3. `https://www.khanacademy.org`
4. `http://ocw.mit.edu/courses/mathematics`
5. `http://libgen.org`

CONTENTS

Unit 1. Sets and Functions

1. Reading

The concept of set and operations on sets

The concept of set plays an extraordinarily important role in modern mathematics because, in modern formal treatments, most mathematical objects (numbers, relations, functions, etc.) are defined in terms of sets. There are several theories of sets used in the discussion of the foundations of mathematics. Here we shall briefly discuss very basic set-theoretic concepts in the naive point of view. Unlike axiomatic set theories, which are defined using a formal logic, naive set theory is defined informally, in natural language.

Basic notations

In naive set theory, a ***set*** is described as a well-defined collection of objects. These objects are called the ***elements*** or ***members*** of the set. Objects can be anything: numbers, people, other sets, etc.

We shall denote sets by capital letters $A, B, \dots$ and their elements by lowercase letters $a, b, \dots$. The statement "the element a ***belongs to*** the set A" will be written symbolically as $a \in A$; the expression $a \notin A$ means that the element a does not belong to the set A. If all the elements of which the set A consists are also contained in the set B then A will be called a ***subset*** of B and we shall write $A \subset B$. We say that A is ***equal to*** B and write $A = B$ if $A \subset B$ and $B \subset A$, otherwise, we write $A \neq B$. The set A is said to be a ***proper subset*** of the set B, written $A \subsetneq B$, if $A \subset B$ and $A \neq B$.

Sometimes, in speaking about an arbitrary set (for example, about the set of roots of a given equation) we do not know in advance whether or not this set contains even one element. For this reason it is convenient to introduce the concept of the so-called ***empty set***, that is, the set which does not contain any elements. We shall denote this set by the symbol $\emptyset$. Every set contains $\emptyset$ as a subset.

How does one go about specifying a set? If the set has only a few elements, one can simply list the elements in the set, writing "A is the set consisting of elements a, b, c". In symbols, this statement becomes $A = \{a, b, c\}$, where the curly brackets are used to enclose the list of elements.

The usual way to specify a set, however, is to take some set A of objects and some property that elements of A may or may not possess, and to form the set consisting of all elements of A having that property. For instance, one might take the set of real numbers and form the subset B consisting of all even integers. In symbols, this statement becomes $B = \{x \mid x \text{ is an even integer}\}$. Here the braces stand for the words "the set of", and the vertical bar stands for the words "such that". The equation is read "B is the set of all x such that x is an even integer".

Union, intersection and difference

If A and B are arbitrary sets, then their ***union***, written $A \cup B$, is the set consisting of all elements which belong to at least one of the sets A and B. The ***intersection*** of two sets A and B, denoted by $A \cap B$, is the set which consists of all the elements belonging to both A and B. The ***difference*** of the sets A and B, written $A \backslash B$, is the set of those elements in A which are not contained in B. In general it is not assumed here that $B \subset A$. If $B \subset A$, $A \backslash B$ is also called the ***complement*** of B in A. In symbols, we write

$$A \cup B = \{x \mid x \in A \vee x \in B\},$$
$$A \cap B = \{x \mid x \in A \wedge x \in B\},$$
$$A \backslash B = \{x \mid x \in A \wedge x \notin B\}.$$

The logical signs "$\wedge$" and "$\vee$" are read "and" and "or" respectively.

In certain settings all sets under discussion are considered to be subsets of a given ***universal*** set U. In such cases, $U \backslash A$ is called the ***absolute complement*** or simply ***complement*** of A, and is denoted by A^c or $\overline{A}$. In symbols, $A^c = \{x \mid x \notin A\}$.

The following are useful properties of the operators mentioned above:

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C), \qquad \overline{B \cap C} = \overline{B} \cup \overline{C},$$
$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C), \qquad \overline{B \cup C} = \overline{B} \cap \overline{C},$$
$$\overline{\overline{A}} = A, \qquad A \backslash B = A \cap \overline{B}.$$

Cartesian product

Given sets A and B, we define their ***Cartesian product*** $A \times B$ to be the set of all ***ordered pairs*** (a, b) for which a is an element of A and b is an element of B. Formally,

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

We can extend this definition to a set $A \times B \times C$ of ***ordered triples***, and more generally to sets of ***ordered n-tuples*** for any positive integer n. It is even possible to define infinite Cartesian products, but to do this we need a more recondite definition of the product.

Functions

The concept of function

The concept of function is one you have seen many times already, so it is hardly necessary to remind you how central it is to all mathematics. In this subsection, we give the precise mathematical definition, and we explore some of the associated concepts.

A function is usually thought of as a rule that assigns to each element of a set A, an element of a set B. In calculus, a function is often given by a simple formula such as $f(x) = 3x^2 + 2$ or perhaps by a more complicated formula such as

$$f(x) = \sum_{k=1}^{\infty} x^k.$$

One often does not even mention the sets A and B explicitly, agreeing to take A to be the set of all real numbers for which the rule makes sense and B to be the set of all real numbers. As one goes further in mathematics, however, one needs to be more precise about what a function is. Mathematicians think of functions in the way we just described, but the definition they use is more exact. This definition relies on the notion of the cartesian product.

A ***function*** (or ***mapping***) f from X to Y is a subset G of the cartesian product $X \times Y$ subject to the following condition: every element of X is the first component of one and only one ordered pair in the subset. In other words, for every x in X there is exactly one element y such that the ordered pair (x, y) belongs to G. This formal definition is a precise rendition of the idea that to each x is associated an element y of Y, namely the uniquely specified element y with the property just mentioned.

A function f from X to Y is commonly denoted by $f : X \to Y$. The sets X is called ***domain*** of f, while Y is called ***codomain*** of f. The elements of X are called ***arguments*** of f. For each argument x, the corresponding unique y in the codomain is called the ***value*** of f at x or the image of x under f. It is written as $f(x)$. One says that f associates y with x or maps x to y. This is abbreviated by $y = f(x)$.

If A is any subset of the domain X, then the set $f(A) = \{f(x) \mid x \in A\}$ is called the ***image*** of A under f. Especially, $f(X)$ is called the ***range*** or the ***image*** of f. On the other hand, if B is subset of Y, the set $f^{-1}(B) = \{x \mid f(x) \in B\}$ is called the ***inverse image*** or ***preimage*** of B under f.

Injective and surjective functions

A function $f : X \to Y$ is called ***injective*** (or ***one-to-one***, or an ***injection***) if $f(a) \neq f(b)$ for any two different elements a and b of X. It is called ***surjective*** (or f is said to map X ***onto*** Y) if $f(X) = Y$. That is, it is surjective if for every element y in the codomain there is an x in X such that $f(x) = y$. Finally, f is called ***bijective*** if it is both injective and surjective.

If f is bijective, there exists a function from Y to X called the ***inverse*** of f. It is denoted by f^{-1}, read "f inverse", and defined by letting $f^{-1}(y)$ be that unique element x of X for which $f(x) = y$. Given $y \in Y$, the fact that f is surjective implies that there exists such an element $x \in X$; the fact that f is injective implies that there is only one such element x. It is easy to see that f^{-1} is also bijective.

Restrictions and extensions

Given function $f : X \to Y$. If A is any subset of X, the ***restriction*** of f to A is the function $f|_A$ from A to Y such that $f|_A(a) = f(a)$ for all a in A. The notation $f|_A$ is read "f restricted to A". If g is a restriction of f, then it is said that f is an ***extension*** of g.

Function composition

Given functions $f : X \to Y$ and $g : Y \to Z$. The ***composite*** (or ***composition***) of f and g is the function $g \circ f : X \to Z$ defined by $(g \circ f)(x) = g(f(x)), \forall x \in X$.

Note that $g \circ f$ is defined only when the codomain of f equals the domain of g.

Exercise 1.1. Fill in each blank with a suitable mathematical term. Some terms are given in the box below.

bijection / graph / periodic / superset / surjection / one-to-one

Example. A set A is .... of a set B if A is a subset of B, but B is not a subset of A.

$\rightsquigarrow$ A set A is **a proper subset** of a set B if A is a subset of B, but B is not a subset of A.

a) The .... of $\{1, 2, 3, 4\}$ and $\{1, 3, 5\}$ is the set $\{1, 3\}$.

b) The .... of $\{a, b\}$ in $\{a, b, c\}$ is the set $\{c\}$.

c) The empty set is a .... of every set.

d) If A is a subset of B, then B is called a .... of A.

e) A mapping $f : X \to Y$ is .... if, for any $y \in Y$, $f^{-1}(y)$ contains not more than one element.

f) A function f is .... if and only if $f^{-1}(y)$ is not empty for any y in its codomain.

g) A function $f: X \to Y$ is a .... if and only if for any $y \in Y$ there is a unique element $x \in X$ such that $f(x) = y$.

h) The .... of a function f is the set of all possible values of $f(x)$ as x varies throughout the domain.

i) If f is a function with domain A, then its .... is the set of ordered pairs $\{(x, f(x)) \mid x \in A\}$.

j) The sine and cosine functions are .... with the same period 2π.

2. Speaking and writing

Exercise 1.2. Read aloud the following notations/expressions/statements. Refer to appendices A-1, A-2 and A-3. Leaners are encouraged to write down the words they read.

Example. $A = \{x \in \mathbb{R} \mid x \leqslant 3\}$. It is read as "A is the set of all real numbers that are less than or equal to 3".

Example. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$. It is read as "The inverse image of the intersection of A and B (under f) equals the intersection of the inverse images of A and B" or "f inverse of A intersection B is equal to f inverse of A intersection f inverse of B".

a) $A = \{2, 4, 6, 8\}$.

b) $A = \{n \in \mathbb{N} \mid 10 \leqslant n \leqslant 100\}$.

c) $A \subset B \Rightarrow A \cup B = B$.

d) $\overline{\bigcap_{k=1}^{n} A_k} = \bigcup_{k=1}^{n} \overline{A_k}$.

e) $x \in A \cup B \Leftrightarrow (x \in A \vee x \in B)$.

f) $x \in A \backslash B \Leftrightarrow (x \in A \wedge x \notin B)$.

g) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

h) $f^{-1}(A \backslash B) = f^{-1}(A) \backslash f^{-1}(B)$.

i) $f(A \cup B) = f(A) \cup f(B)$.

j) $f(x) = 2^x \ln x$.

k) $f(x) = \frac{\sqrt[3]{x}.\sin x}{x^2 + \sqrt{x}}$.

l) $P(x) = \sum_{k=0}^{n} a_k x^k$.

Exercise 1.3. Translate the following sentences into Vietnamese.

Example. Ta nói hai tập hợp A và B tương đương (***equivalent***) với nhau hay có cùng lực lượng (***cardinality***) nếu có một song ánh từ A vào B.

$\rightsquigarrow$ We say that two sets A and B are ***equivalent*** (or have the same ***cardinality***) if there exists a bijection f from A into B.

a) Nếu A là tập con của B và B là tập con của C thì A là tập con của C. $\rightsquigarrow$.

....

....

b) Kí hiệu $\mathscr{P}(X)$ là tập hợp tất cả các tập con của tập hợp X. Nếu X có n phần tử thì $\mathscr{P}(X)$ có 2^n phần tử. $\rightsquigarrow$ ....

....

c) Ta nói hai tập hợp A và B ***rời nhau*** (***disjoint***) nếu chúng không có phần tử chung. $\rightsquigarrow$ ....

....

d) Để chứng minh tập hợp A là tập con của tập hợp B ta chứng tỏ mỗi phần tử của A đều là phần tử của B. $\rightsquigarrow$ ....

....

....

e) Nếu $f : X \to Y$ và $g : Y \to Z$ là những đơn ánh thì ánh xạ hợp thành $h = g \circ f$ cũng là một đơn ánh. $\rightsquigarrow$ ....

....

f) Ta nói tập hợp A là hữu hạn (***finite***) nếu A tương đương với tập hợp $\{1, 2, \ldots, n\}$ với số nguyên dương n nào đó. Nếu tập hợp A không hữu hạn thì được gọi là vô hạn (***infinite***). $\rightsquigarrow$ ....

....

....

g) Ta nói tập hợp A là đếm được (***countable***) nếu nó tương đương với tập hợp các số nguyên $\mathbb{Z}$. $\rightsquigarrow$ ....

....

h) Tập hợp A là vô hạn khi và chỉ khi A tương đương với một tập con thực sự nào đó của nó. $\rightsquigarrow$ ....

....

Exercise 1.4. Prove the following assertions. Write down proofs and talk things out with your classmates or friends.

Example. $A \setminus (A \setminus B) = A \cap B$.

Proof. In order to show the two sets are equal, we will show that an element belongs to one if and only if it belongs to the other. We have

$$\begin{aligned} x \in A \setminus (A \setminus B) &\Leftrightarrow (x \in A) \wedge [x \notin (A \setminus B)] \\ &\Leftrightarrow (x \in A) \wedge [(x \notin A) \vee (x \in B)] \\ &\Leftrightarrow [(x \in A) \wedge (x \notin A)] \vee [(x \in A) \wedge (x \in B)] \\ &\Leftrightarrow (x \in A) \wedge (x \in B) \\ &\Leftrightarrow x \in A \cap B. \end{aligned}$$

Thus, $A\backslash(A\backslash B) = A\cap B$. The equality can be also proved as follows:

$$\begin{aligned} A\backslash(A\backslash B) &= A\backslash(A\cap \overline{B}) = A\cap \overline{A\cap \overline{B}} = A\cap (\overline{A}\cup \overline{\overline{B}}) \\ &= A\cap (\overline{A}\cup B) = (A\cap \overline{A})\cup (A\cap B) = \emptyset \cap (A\cap B) = A\cap B. \end{aligned}$$ □

Example. If functions $f: X\to Y$ and $g: Y\to Z$ are surjective, then the composite $g\circ f$ is also surjective.

Proof. Suppose both f and g are surjective. For any z in Z, since g is surjective, there exists an $y\in Y$ such that $g(y) = z$. Also, since f is surjective, there exists $x\in X$ such that $y = f(x)$. Thus, $z = g\circ f(x)$, and therefore $g\circ f$ is surjective. □

a) $A\cup (A\cap B) = A$.

b) $A\backslash(B\cap C) = (A\backslash B)\cup (A\backslash C)$.

c) $A\times (B\cup C) = (A\times B)\cup (A\times C)$.

d) $A\times (B\backslash C) = (A\times B)\backslash(A\times C)$.

e) If functions $f: X\to Y$ and $g: Y\to Z$ are injective, then the composite $g\circ f$ is also injective.

f) The function $f:\mathbb{R}\to\mathbb{R}$ defined by $f(x) = 2x+1$ is bijective.

g) Let $f: X\to Y$ be a function, $A\subset Y$. Then $f(f^{-1}(A))\subset A$ and equality holds if f is surjective.

h) Let $f: X\to Y$ be a function, $A, B\subset X$. Then $f(A\cap B)\subset f(A)\cap f(B)$ and equality holds if f is injective.

Unit 2. Real Numbers. Limit and Continuity

1. Reading

Construction of the real numbers

There are many ways to construct the real number system, for example, starting from natural numbers, then defining rational numbers algebraically, and finally defining real numbers as equivalence classes of their Cauchy sequences or as Dedekind cuts, which are certain subsets of rational numbers. Another way is simply to assume a set of axioms for the real numbers and work from these axioms. In the present subsection, we shall sketch this approach to the real numbers.

Firstly, let us introduce some needed notations.

Totally ordered set. Least upper and greatest lower bounds

A ***relation*** on a set X is a subset R of the cartesian product $X \times X$.

If R is a relation on X, we use the notation $x R y$ to mean the same thing as $(x, y) \in R$. We read it "x is in the relation R to y."

Recall that a function $f : X \to X$ is also a subset of $X \times X$. But it is a subset of a very special kind: namely, one such that each element of X appears as the first coordinate of an element of f exactly once. So any function f from X into itself is also a relation on X. The inverse is not always true.

A relation R on a set X is called an ***total order relation*** (or ***linear order***, or ***simple order***) if it has the following properties:

(1) For all x in $\mathbb{R}$, $x \leqslant x$; (reflexivity)
(2) For all x and y in $\mathbb{R}$, if $x \leqslant y$ and $y \leqslant x$, then $x = y$; (antisymmetry)
(3) For all x, y and z in $\mathbb{R}$, if $x \leqslant y$ and $y \leqslant z$, then $x \leqslant z$; (transitivity)
(4) For all x and y in $\mathbb{R}$, either $x \leqslant y$ or $y \leqslant x$. (totality)

If $\leqslant$ is a total order relation on the set X, then the couple $(X, \leqslant)$ is called a ***totally ordered set***.

Let $(X, \leqslant)$ be a totally ordered set. Let A be subset of X. We say that the element a is the ***largest element*** of A if $a \in A$ and if $x \leqslant a$ for every $x \in A$. Similarly, we say that a is the ***smallest element*** of A if $a \in A$ and $a \leqslant x$ for every $x \in A$. It is easy to see that a set has at most one largest element and at most one smallest element.

We say that the subset A of X is ***bounded above*** if there is an element b of X such that $x < b$ for every $x \in A$; the element b is called an ***upper bound*** for A. If the set of all upper bounds for A has a smallest element, that element is called the ***least upper bound***, or the ***supremum***, of A. It is denoted by $\sup A$; it may or may not belong to A. If it does, it is the largest element of A.

Similarly, A is ***bounded below*** if there is an element b of X such that $b \leqslant x$ for every $x \in A$; the element b is called ***lower bound*** for A. If the set of all lower bounds for A has a largest element, that element is called the ***greatest lower bound***,or the ***infimum***, of A. It is denoted by $\inf A$; it may or may not belong to A. If it does, it is the smallest element of A.

Binary operation

A ***binary operation*** on a set X is a function f mapping $X \times X$ into X.

When dealing with a binary operation f on a set X, we usually use a notation different from the standard functional notation. Instead of denoting the value of the function f at the point (x, y) by $f(x, y)$, we usually write the symbol for the function between the two coordinates of the point in question, writing the value of the function at (x, y) as xfy. Furthermore (just as was the case with relations), it is more common to use some symbol other than a letter to denote an operation. Symbols often used are the plus symbol $+$, the multiplication symbols $\cdot$ and $\circ$, and the asterisk $*$; however, there are many others.

Axioms of real numbers

A ***model for the real number system*** consists a set $\mathbb{R}$, two binary operations $+$ and $\cdot$ on $\mathbb{R}$ (called ***addition*** and ***multiplication***, respectively), and a total order relation $\leqslant$ on $\mathbb{R}$ satisfying the following properties:

1) $(\mathbb{R}, +, \cdot)$ forms a ***field***. In other words,
   - For all x, y and z in $\mathbb{R}$, $(x+y)+z = x+(y+z)$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$; (associativity of addition and multiplication)
   - For all x and y in $\mathbb{R}$, $x + y = y + x$ and $x \cdot y = y \cdot x$; (commutativity of addition and multiplication)
   - For all x, y and z in $\mathbb{R}$, $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$; (distributivity of multiplication over addition)
   - There exists an element of $\mathbb{R}$, called ***zero*** and denoted by 0, such that $x + 0 = x$, for all x in $\mathbb{R}$; (existence of additive identity)
   - There exists an element of $\mathbb{R}$ which is different from 0, called ***one*** and denoted by 1, such that $x \cdot 1 = x$, for all x in $\mathbb{R}$; (existence of multiplicative identity)
   - For every x in $\mathbb{R}$, there exists an element $-x$ in $\mathbb{R}$, called the ***negative*** (or ***opposite***) of x, such that $x + (-x) = 0$;
   - For every $x \neq 0$ in $\mathbb{R}$, there exists an element x^{-1} in $\mathbb{R}$, called the ***reciprocal*** of x, such that $x \cdot x^{-1} = 1$.
2) The field operations $+$ and $\cdot$ are compatible with the order $\leqslant$. In other words,
   - For all x, y and z in $\mathbb{R}$, if $x \leqslant y$, then $x + y \leqslant y + z$; (preservation of order under addition)
   - For all x, y and z in $\mathbb{R}$, if $x \leqslant y$ and $0 \leqslant z$, then $x \cdot z \leqslant y \cdot z$. (preservation of order under multiplication)
3) The order $\leqslant$ is ***complete*** in the following sense: every non-empty sub-

set of $\mathbb{R}$ bounded above has a least upper bound.

It can be proved that any two models for the real number system must be ***isomorphic***, i.e., there is a bijection between the two sets of the models preserving both the field operations and the order. For this reason, any model for the real number system defines "the" ***real number system***, in other words, the real number system is defined uniquely up to an isomorphism.

Some notations

Let $(\mathbb{R}, +, \cdot, \leqslant)$ be the real number system. Then each element x of $\mathbb{R}$ is called a ***real number***. We say a real number x to be ***positive*** if $x > 0$, and to be ***negative*** of $x < 0$. Here we write $a < b$ if $a \leqslant b$ and $a \neq b$. It can be proved that the number 1 is positive. Let us denote by $\mathbb{R}_+$ the set of all positive real numbers.

Natural numbers, integers and rational numbers

A subset A of the real numbers is said to be ***inductive*** if it contains the number 1, and if for every x in A, the number $x+1$ is also in A. Let $\mathscr{A}$ be the collection of all inductive subsets of $\mathbb{R}$. Then the set $\mathbb{Z}_+$ of ***positive integers*** is defined by the equation

$$Z_+ = \bigcap_{A \in \mathscr{A}} A.$$

The sets $\mathbb{N}$ of ***natural numbers***, $\mathbb{Z}$ of ***integers***, and $\mathbb{Q}$ of ***rational numbers*** are respectively defined by

$$\mathbb{N} = \{0\} \cup \mathbb{Z}_+,$$
$$\mathbb{Z} = \{x \mid x = 0 \text{ or } x \in \mathbb{Z}_+ \text{ or } -x \in \mathbb{Z}_+\},$$
$$\mathbb{Q} = \{x \cdot y^{-1} \mid x, y \in \mathbb{Z}, y \neq 0\}.$$

Exercise 2.1. Fill in each blank with a suitable mathematical term from the box.

bounded / continuous / convergent / decreasing / defined / dense / increasing / integer / irrational / maximum / minimum / monotone / monotonically / positive / sequence / series / strictly / uniformly

a) A real number that is not rational is called . . . .

b) The set of rational numbers is . . . . in $\mathbb{R}$, that is, for any a and b in $\mathbb{R}$, $a < b$, there exists a rational number c such that $a < c < b$.

c) Each function $u : \mathbb{N} \to \mathbb{R}$ from the set of natural numbers into the set of real numbers is called a . . . . of real numbers.

d) Any bounded sequence of real numbers has a .... subsequence.

e) If the sequence (u_n) is a monotonically .... and is .... from below, then (u_n) is convergent.

f) If a sequence is either increasing or decreasing it is called a .... sequence.

g) If the real-valued function f is .... on a closed interval $[a, b]$ and λ is some number between $f(a)$ and $f(b)$, then there is some number c in $[a, b]$ such that $f(c) = \lambda$.

h) If the real-valued function f is continuous on the closed interval $[a, b]$, then f is .... continuous on this interval.

i) If $f(x) < f(y)$ for all x, y in $[a, b]$, $x < y$, then we say that f is .... increasing on $[a, b]$.

j) ***Principle of mathematical induction***. If for each .... integer n there is a corresponding statement P_n, then all the statements P_n are true, provided the following two conditions are satisfied:

(1) P_1 is true.
(2) Whenever k is a positive .... such that P_k is true, then P_{k+1} is also true.

2. Speaking and writing

Exercise 2.2. State the definition for each of the following concepts. Use given hints.

Example. ***Continuity*** of a function at a point. $\rightsquigarrow$ A function $f : D \to \mathbb{R}$ is said to be ***continuous*** at a point $x_0 \in D$ if $\lim_{x \to x_0} f(x) = f(x_0)$, in other words, for every $\epsilon > 0$ there exists a $\delta > 0$ such that for all $x \in D$, if $|x - c| < \delta$ then $|f(x) - f(x_0)| < \epsilon$.

Example. ***Boundedness*** of a function. $\rightsquigarrow$ We say that a function $f : D \to \mathbb{R}$ is ***bounded*** if there exists a positive number M such that $|f(x)| \leqslant M$ for all $x \in D$.

a) ***Convergence*** of a sequence. $\rightsquigarrow$ We say that a sequence (u_n) ....
....
....

b) ***Cauchy sequence*** of a real numbers. $\rightsquigarrow$ ....
....

. . . .

c) The ***limit*** of a function as x approachs x_0. $\rightsquigarrow$ A real number l . . . .
. . . .
. . . .

d) The ***limit*** of a function as x approachs ∞. $\rightsquigarrow$ We call a real number l .
. . . .
. . . .
. . . .

e) ***Uniform continuity*** of a function on a set D. $\rightsquigarrow$ A function . . . .
. . . .
. . . .

Exercise 2.3. Read aloud the following notations/expressions/statements. Refer to appendices A-1 – A-4. Leaners are encouraged to write down the words they read.

Example. $\forall \epsilon > 0 \exists \delta > 0 \forall x \in \mathrm{I} (0 < |x-a| < \delta \Rightarrow |f(x) - l| < \epsilon)$.

$\rightsquigarrow$ It is read as "For any positive number ϵ, there exists a positive number δ such that for every (real number) x in I, if the distance from x to a (or the absolute value of x minus a) is greater than zero and is less than δ, then the distance from f of x to l is less than ϵ".

a) $0.0012 = 12 \times 10^{-4}$.

b) $\pi \approx 3.14$.

c) $\frac{1}{4} + \frac{3}{2} = \frac{7}{4}$.

d) $\cos^2 x = \frac{1+\cos 2x}{2}$.

e) $\sqrt{a^2} = |a|$.

f) $\lim_{x \to 0^+} \ln x = -\infty$.

g) $\lim_{x \to -\infty} 2^x = 0$.

h) $\lim_{x \to 0} \frac{e^x - 1}{x} = 1$.

i) $(a^b)^c = a^{bc}$ $(a > 0)$.

j) $a^{\log_a b} = b$ $(0 < a \neq 1, b > 0)$.

k) $\log_a \prod_{k=1}^{n} b_k = \sum_{k=1}^{n} \log_a b_k$ $(0 < a \neq 1, b_k > 0)$.

l) $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.

m) $|ab + cd| \leqslant \sqrt{a^2+c^2}\sqrt{b^2+d^2}$.

n) $ab \leqslant \frac{a^p}{p} + \frac{b^q}{q}$ $(a, b > 0, p, q > 1, \frac{1}{p} + \frac{1}{q} = 1)$.

o) $\forall \epsilon > 0 \exists \mathrm{N} \in \mathbb{N} (n \geqslant \mathrm{N} \Rightarrow |u_n - a| < \epsilon)$.

p) $\forall \mathrm{M} > 0 \exists \mathrm{N} > 0 \forall x \in \mathbb{R}$ $(x < -\mathrm{N} \Rightarrow f(x) > \mathrm{M})$.

q) $\mathrm{M} = \sup \mathrm{A} \Leftrightarrow \begin{cases} a \leqslant \mathrm{M}, \forall a \in \mathrm{A} \\ \forall \epsilon > 0 \exists a_0 \in \mathrm{A} : \mathrm{M} - \epsilon < a_0. \end{cases}$

r) $m = \inf \mathrm{A} \Leftrightarrow \begin{cases} m \leqslant a, \forall a \in \mathrm{A} \\ \forall \epsilon > 0 \exists a_0 \in \mathrm{A} : a_0 < m + \epsilon. \end{cases}$

Exercise 2.4. Translate the following sentences/paragraphs into English.

a) Mỗi dãy số đơn điệu tăng và bị chặn trên đều hội tụ. $\rightsquigarrow$ ....
....
b) Một dãy số là hội tụ khi và chỉ khi nó là dãy Cauchy. $\rightsquigarrow$ ....
....
c) Hàm số f liên tục tại x_0 khi và chỉ khi với mọi dãy số $\{x_n\} \subset D$, nếu $x_n \to x_0$ thì $f(x_n) \to f(x_0)$. $\rightsquigarrow$ ....
....
....
d) Nếu hàm số f liên tục trên đoạn $[a,b]$ thì f bị chặn trên đoạn này, nghĩa là, tồn tại số dương M sao cho $|f(x)| \leqslant M$ với mọi $x \in [a,b]$. $\rightsquigarrow$ ....
....
....
e) Nếu f là hàm số liên tục và đơn điệu nghiêm ngặt trên đoạn $[a,b]$ thì f có hàm số ngược cũng là, một hàm liên tục và đơn điệu nghiêm ngặt. $\rightsquigarrow$
....
....
f) Giả sử (f_n) là một dãy hàm liên tục trên $[a,b]$ và hội tụ đều đến hàm f trên đoạn này thì f liên tục trên $[a,b]$. $\rightsquigarrow$ ....
....
....
g) Giả sử f là hàm số liên tục và đơn điệu nghiêm ngặt trên $[a,b]$. Nếu $f(a).f(b) < 0$ thì phương trình $f(x) = 0$ có nghiệm duy nhất trên $[a,b]$. $\rightsquigarrow$.
....
....

Exercise 2.5. Using the axioms of real numbers, prove the following properties for $\mathbb{R}$. Write down the proofs and talk things out with your classmates or friends.

Example. If $x + y = x$, then $y = 0$.

Proof. We have

$$\begin{aligned} x + y = x &\Rightarrow y + x = x && \text{(commutativity of addition)} \\ &\Rightarrow y + x + (-x) = x + (-x) && \text{("+" is an operation)} \\ &\Rightarrow y + 0 = 0 && \text{(property of } -x\text{)} \\ &\Rightarrow y = 0. && \text{(property of } 0\text{)} \end{aligned}$$

So the assertion is proved. □

a) If $x + y = x$, then $y = 0$.

b) $0 \cdot x = 0$.

c) $-0=0$.

d) $-(-x)=x$.

e) $x\cdot(-y)=-(x\cdot y)$.

f) $(-1)\cdot x=-x$.

g) $x\cdot(x-y)=x\cdot y-x\cdot z$.

h) $x\leqslant y\wedge z\leqslant w\Rightarrow x+z\leqslant y+w$.

i) $x>0\wedge y>0\Rightarrow xy>0$.

j) $x>0\Leftrightarrow -x<0$.

Exercise 2.6. For the following assignments, write down your solutions and talk things out with your classmates or friends.

Example. Prove that $\sum\limits_{i=1}^{n}(2i-1)=n^2$ for every positive integer n.

Solution. The statement is true for $n=1$ since $\sum\limits_{i=1}^{1}(2i-1)=1=1^2$.

Assume that the statement is true for some positive integer k, that is, $\sum\limits_{i=1}^{k}(2i-1)=k^2$. Then we have

$$\begin{aligned}\sum_{i=1}^{k+1}(2i-1)&=\sum_{i=1}^{k}(2i-1)+2(k+1)-1\\&=k^2+2k+1\qquad\text{(by the induction hypothesis)}\\&=(k+1)^2.\end{aligned}$$

This means the statement is true for $k+1$. By principle of mathematical induction, the statement is true for all positive integer n. □

a) Let A and B be nonempty bounded subsets of $\mathbb{R}$. Explain why if $\mathrm{A}\subset\mathrm{B}$, then $\sup\mathrm{A}\leqslant\sup\mathrm{B}$ and $\inf\mathrm{A}\geqslant\inf\mathrm{B}$.

b) Let $\mathrm{A}=\{\frac{n}{n+1}\mid n\in\mathbb{N}\}$. Find $\sup\mathrm{A}$ and $\inf\mathrm{A}$.

c) Prove by induction that for each positive integer n,

$$\sum_{i=1}^{n}(2i-1)^2=\frac{n(2n-1)(2n+1)}{3}.$$

d) Prove by contradiction that the square root of 3 is irrational.

e) Prove that a convergent sequence has a unique limit.

f) Prove that if f is a real-valued function which is continuous on a closed interval $[a,b]$, then f is bounded on $[a,b]$.

Unit 3. Calculus

1. Reading

Calculus is a branch of mathematics focused on limits, functions, derivatives, integrals, and infinite series. While geometry is the study of shape and algebra is the study of operations and their application to solving equations, calculus is the study of change. It has widespread applications in science, economics, and engineering and can solve many problems for which algebra alone is insufficient.

Calculus has two major branches, ***differential calculus*** and ***integral calculus***, which are related by the ***fundamental theorem of calculus***.

Differential calculus

Differential calculus is the study of the definition, properties, and applications of the derivative of a function.

The concept of derivative

Let f be a given real-valued function of a single real variable. It is often written as $y = f(x)$. Usually we call x the ***independent variable*** and y the ***dependent variable***. Sometimes, x is called the ***input***, while y is called the ***output***.

Geometrically, the ***derivative*** of f at a point equals the ***slope*** of the ***tangent line*** to the graph of the function at that point. It determines the best linear approximation to the function at that point.

If the function f is ***linear*** (that is, if the ***graph*** of the function is a straight line), then the function can be written as $y = mx+b$, b is the y-intercept, and

$$m = \frac{\text{rise}}{\text{run}} = \frac{\text{change in } y}{\text{change in } x} = \frac{\Delta y}{\Delta x}.$$

This gives an exact value for the slope of a straight line. If the graph of the function f is not a straight line, however, then the change in y divided by the change in x varies. Derivatives give an exact meaning to the notion of change in output with respect to change in input. To be concrete, fix a point a in the domain of f. $(a, f(a))$ is a point on the graph of the function. If h is a number close to zero, then $a+h$ is a number close to a. Therefore $(a+h, f(a+h))$ is close to $(a, f(a))$ (in case f is continuous). The slope between these two points is

$$m = \frac{f(a+h) - f(a)}{h}.$$

This expression is called a ***difference quotient***. A line through two points on a curve is called a ***secant line***, so m is the slope of the secant line between $(a, f(a))$ and $(a+h, f(a+h))$. The secant line is only an approximation to the behavior of the function at the point a because it does not account for what happens between a and $a+h$. It is not possible to discover the behavior at a by setting h to zero because this would require dividing by zero, which is impossible. The derivative of f at the point a is defined by taking the limit as h tends to zero:

$$f'(a) = \lim_{h\to 0} \frac{f(a+h) - f(a)}{h}.$$

By finding the derivative of f at every point in its domain, it is possible to produce a new function, denoted by f' and called the ***derivative function*** or just the ***derivative*** of the function f.

If the derivative of f exists at a point x, then f is said to be ***differentiable*** at x. The process of finding the derivative of f is called ***differentiation***.

Some definitions and theorems

Let f be a (real-valued) function with the domain $\mathrm{D} \subset \mathbb{R}$. We say the function f attains an ***absolute*** (or ***global***) ***maximum*** at c in D if $f(c) \geqslant f(x)$ for all x in D. The number $f(c)$ is called the (***absolute***) ***maximum value*** of f on D. Similarly, f attains an ***absolute minimum*** at c in D if $f(c) \leqslant f(x)$ for all x in D and the number is called the (***absolute***) ***minimum value*** of f on D. The maximum and minimum values of are called the ***extreme values*** of f.

A point x_0 of D is called a ***local*** (or ***relative***) ***maximum point*** of f if there is some $\delta > 0$ such that

$$f(x) \leqslant f(x_0) \text{ for all } x \in \mathrm{D} \cap (x_0 - \delta, x_0 + \delta).$$

The number $f(x_0)$ itself is called a ***local*** (or ***relative***) ***maximum*** of f.

Local minimum points and ***local minima*** are defined similarly. A local minimum or local maximum of f is called a ***local extremum*** of f.

Theorem (Fermat's theorem). *If a function f defined on (a,b) and has a local maximum (or minimum) at $x \in (a,b)$, and f is differentiable at x, then $f'(x) = 0$.*

Theorem (Rolle's theorem). *If a function f is continuous on $[a,b]$ and differentiable in (a,b), and $f(a) = f(b)$, then there exists a number x in (a,b) such that $f'(x) = 0$.*

Theorem (The mean value theorem). *If f is a continuous function on $[a,b]$ which is differentiable in (a,b), then there is a point c in (a,b) such that*

$$f(b)-f(a)=f'(c)(b-a).$$

Theorem. *Suppose a function f is differentiable in (a,b).*

(i) *If $f'(x)\geqslant 0$ for all $x\in(a,b)$, then f is* ***monotonically increasing*** *on (a,b).*
(ii) *If $f'(x)=0$ for all $x\in(a,b)$, then f is a* ***constant function****.*
(iii) *If $f'(x)\leqslant 0$ for all $x\in(a,b)$, then f is* ***monotonically decreasing*** *on (a,b).*

Integral calculus

Integral calculus is the study of the definitions, properties, and applications of two related concepts, the indefinite integral and the definite integral.

The ***indefinite integral*** is the antiderivative, the inverse operation to the derivative. F is an indefinite integral of f when f is a derivative of F. (This use of lower- and upper-case letters for a function and its indefinite integral is common in calculus.)

The ***definite integral***, also called ***Riemann integral***, inputs a function and outputs a number. Given a function f of a real variable x and an interval $[a,b]$ of the real line, the definite integral $\int_a^b f(x)dx$ is defined informally to be the area of the region in the xy-plane bounded by the graph of f, the x-axis, and the vertical lines $x=a$ and $x=b$, such that area above the x-axis adds to the total, and that below the x-axis subtracts from the total. Formally, the definite integral is defined as the limit of a Riemann sum of the function with respect to a tagged partition of the interval.

A ***tagged partition*** is a finite sequence

$$a=x_0\leqslant t_1\leqslant x_1\leqslant t_2\leqslant x_2\leqslant\cdots\leqslant x_{n-1}\leqslant t_n\leqslant x_n=b.$$

This partitions the interval $[a,b]$ into n sub-intervals $[x_{i-1},x_i]$ indexed by i, each of which is "tagged" with a distinguished point $t_i\in[x_{i-1},x_i]$. Let $\triangle_i=x_i-x_{i-1}$ be the width of sub-interval i. The ***mesh*** of such a tagged partition is the width of the largest sub-interval formed by the partition, $\max\limits_{1\leqslant i\leqslant n}\triangle_i$. A ***Riemann sum*** of the function f with respect to such a tagged partition is defined as

$$\sum_{i=1}^{n} f(t_i)\triangle_i;$$

thus each term of the sum is the area of a rectangle with height equal to the function value at the distinguished point of the given sub-interval, and width the same as the sub-interval width. The Riemann integral of a function f over the interval $[a,b]$ is equal to a number I if: For all $\epsilon > 0$ there exists $\delta > 0$ such that, for any tagged partition $[a,b]$ with mesh less than δ, we have

$$|\mathrm{I} - \sum_{i=1}^{n} f(t_i)\triangle| < \delta.$$

In this case, f is said to be ***integrable*** on the interval $[a,b]$.

Some theorems

Theorem. *If f is an integrable real-valued function on the closed interval $[a,b]$, then f is bounded on $[a,b]$.*

Theorem. *If a function f is continuous on $[a,b]$, then f is integrable on $[a,b]$.*

Theorem. *Let f be an integrable function on $[a,b]$ satisfying*

$$m \leqslant f(x) \leqslant \mathrm{M} \textit{ for all } x \textit{ in } [a,b].$$

Then

$$m(b-a) \leqslant \int_a^b f(x)dx \leqslant \mathrm{M}(b-a).$$

Theorem (The mean value theorem for integration). *Suppose f is a continuous function on $[a,b]$. Then there exists a number c in $[a,b]$ such that*

$$\int_a^b f(x)dx = f(c)(b-a).$$

Fundamental theorem of calculus

The fundamental theorem of calculus is a theorem that links the concept of the derivative of a function with the concept of the integral.

The first part of the theorem, sometimes called the ***first fundamental theorem of calculus***, shows that an indefinite integration can be reversed by a differentiation. This part of the theorem is also important because it guarantees the existence of antiderivatives for continuous functions. Specifically, it is stated as follows.

Theorem. *Let f be a continuous real-valued function defined on a closed interval $[a,b]$. Let F be the function defined by*

$$\mathrm{F}(x) = \int_a^x f(t)dt, \forall x \in [a,b].$$

Then F is differentiable on $[a,b]$, and $\mathrm{F}'(x) = f(x), \forall x \in [a,b]$.

The second part, sometimes called the ***second fundamental theorem of calculus***, allows one to compute the definite integral of a function by using any one of its infinitely many antiderivatives. This part of the theorem has invaluable practical applications, because it markedly simplifies the computation of definite integrals. Specifically, it says as follows:

Theorem. *Let f and F be real-valued functions defined on a closed interval [a, b] such that $F'(x) = f(x)$ for all $x \in [a,b]$. If f is Riemann integrable on $[a,b]$, then*

$$\int_a^b f(x)dx = F(b) - F(a).$$

Exercise 3.1. Fill in each blank with a suitable mathematical term. Some terms are given in the box below.

antiderivative / area / asymptotes / critical point / cubic / decreasing / domain / first / improper / increasing / inflection / primitive integral / second / tangent line

a) A polynomial of degree 3 $P(x) = ax^3 + bx^2 + cx + d$ $(a \neq 0)$ is called a .... function.

b) Let f be a function defined on D. A point c in D is called a .... of f if $f'(c) = 0$ or $f'(c)$ does not exist.

c) If a function f is differentiable on (a,b) and its derivative is nonnegative in (a,b), then f is .... on this interval.

d) The function $F(x) = \sin x$ is an .... of the function $f(x) = \cos x$.

e) The equation of the .... of the graph of a differentiable function f at a point $(a, f(a))$ is given by $y = f'(a)(x-a) + f(a)$.

f) Let f and g be continuous functions on a closed interval $[a,b]$. The .... of the region bounded by the curves $y = f(x)$, $y = g(x)$, and lines $x = a$, $x = b$ is computed by $S = \int_a^b |f(x) - g(x)|dx$.

g) Let f be nonnegative continuous function on $[a,b]$. The .... of the solid obtained by rotating about the x-axis the region under the curve $y = f(x)$ from a to b is $V = \pi \int_a^b f^2(x)dx$.

h) The .... integral of a function f on the interval $[0,+\infty)$ is defined by $\int_0^{+\infty} f(x)dx = \lim\limits_{A\to+\infty} \int_0^A f(x)dx$.

i) Steps to sketch the graph of a function $f(x)$:

- Find the .... of f.
- Find the .... derivative $f'(x)$.

- Find .... points of $f(x)$ - whenever $f'(x) = 0$ or undefined.
- Find the .... derivative $f''(x)$.
- Find .... points of $f(x)$ - whenever $f''(x) = 0$.
- Find (vertical, horizontal, oblique) .... (if any).
- Draw the sign table for $f'(x)$ and $f''(x)$ which contains all critical and inflection points (and vertical asymptotes, if there are any).
- State the intervals on which f(x) is increasing, ..., concave up and concave down.
- Computing values of f at critical and inflection points.
- Plot the critical and inflection points of the graph, and x and y intercepts.
- Sketch the graph.

2. Speaking and writing

Exercise 3.2. Read aloud the following notations/expressions/statements. Refer to appendices A-2 and A-4. Leaners are encouraged to write down the words they read.

a) $(x^\alpha)' = \alpha x^{\alpha-1}, x > 0.$

b) $(\log_a x)' = \dfrac{1}{x\ln a}.$

c) $e^x = \sum\limits_{n=0}^{\infty} \frac{x^n}{n!}.$

d) $S = \int_a^b |f(x) - g(x)|dx.$

e) $V = \pi\int_a^b f^2(x)dx.$

f) $\Delta u = \dfrac{\partial^2 u}{\partial x^2} + \dfrac{\partial^2 u}{\partial y^2}.$

g) $(\arcsin x)' = \frac{1}{\sqrt{1-x^2}}, \forall x \in (-1,1).$

h) $(f.g)^{(n)}(x) = \sum\limits_{k=0}^{n} \binom{n}{k} f^{(k)}(x).g^{(n-k)}(x).$

i) $\int_a^b uv'dx = uv\big|_a^b - \int_a^b u'v dx.$

j) $\displaystyle\int \frac{dx}{\sqrt{x^2+a^2}} = \ln(x + \sqrt{x^2+a^2}) + C.$

k) $\left(\int\limits_a^b f(x)g(x)dx\right)^2 \leqslant \int\limits_a^b f^2(x)dx \int\limits_a^b g^2(x)dx.$

l) $\displaystyle\int\limits_0^{+\infty} \frac{\sin x}{x}dx = \frac{\pi}{2}.$

Exercise 3.3. Translate the following sentences/paragraphs into Vietnamese.

a) Nếu hàm số f khả vi tại điểm x_0 thì nó liên tục tại điểm đó. ⇝ ....
....

b) Hàm số $f(x) = |x|$ không khả vi tại điểm $x = 0$ nhưng đạt giá trị nhỏ nhất tại điểm này. ⇝ ....
....

c) Ta nói một hàm số đơn điệu trên một khoảng nào đó nếu nó tăng hoặc giảm trên khoảng đó. ⇝ ....

....

d) Nếu hàm số f liên tục trên đoạn $[a,b]$ thì f đạt giá trị lớn nhất và giá trị nhỏ nhất trên đoạn này. $\rightsquigarrow$ ....

....

....

e) Giả sử f là hàm số liên tục trên đoạn $[a,b]$, khả vi trên khoảng (a,b). Để tìm giá trị lớn nhất và giá trị nhỏ nhất của f trên $[a,b]$:

1. Tìm các điểm tới hạn và giá trị của f tại các điểm này.
2. Tìm giá trị của f tại a và b.
3. Các giá trị lớn nhất và nhỏ nhất trong các giá trị ở cả hai bước trên tương ứng là giá trị lớn nhất và giá trị nhỏ nhất của f trên $[a,b]$.

$\rightsquigarrow$ ....

....

....

....

....

....

f) Lấy ví dụ chứng tỏ có những hàm số liên tục nhưng không khả vi. $\rightsquigarrow$.

....

g) Điều kiện cần để một hàm khả tích trên đoạn $[a,b]$ là nó bị chặn trên đoạn này. $\rightsquigarrow$ ....

....

h) Viết phương trình tiếp tuyến của đồ thị hàm số $y = x^2 + 2$ biết nó đi qua điểm $\mathrm{A}(1,3)$. $\rightsquigarrow$ ....

....

i) Chứng minh rằng đồ thị hai hàm số $y = f(x)$ và $y = g(x)$ cắt nhau tại hai điểm phân biệt. $\rightsquigarrow$ ....

....

j) Tính diện tích hình phẳng giới hạn bởi parabol $y = x^2$, tiếp tuyến của parabol này tại điểm $\mathrm{M}(1,1)$ và trục hoành. $\rightsquigarrow$ ....

....

....

k) Hãy tính thể tích của vật thể tròn xoay do quay quanh trục tung hình phẳng giới hạn bởi các đường $y = x^2$ và $y = 1$. $\rightsquigarrow$ ....

....

....

Exercise 3.4. For the following assignments, write down your solutions and then discuss with your classmates.

Example. Prove the first fundamental theorem of calculus.

Proof. Let f be a continuous function on $[a,b]$ and

$$\mathrm{F}(x)=\int_a^x f(t)dt, x\in[a,b].$$

Fix arbitrary x in $[a,b]$. For any nonzero number h such that $x+h\in[a,b]$ we have

$$\mathrm{F}(x+h)-\mathrm{F}(x)=\int_a^x f(t)dt-\int_a^{x+h} f(t)dt=\int_x^{x+h} f(t)dt. \qquad (3.1)$$

According to the mean value theorem for integration, there exists a number c between x and $x+h$ such that

$$\int_x^{x+h} f(t)dt=f(c)h.$$

Substituting this equality into (3.1) we obtain

$$\mathrm{F}(x+h)-\mathrm{F}(x)=f(c)h.$$

Dividing both sides by h gives

$$\frac{\mathrm{F}(x+h)-\mathrm{F}(x)}{h}=f(c). \qquad (3.2)$$

Since $c\to x$ as $h\to 0$ and f is continuous at x, we have

$$\lim_{h\to 0} f(c)=f(x).$$

Thus, we can take the limit as $h\to 0$ the both sides of the equality (3.2) to receive

$$\mathrm{F}'(x)=f(x),$$

which completes the proof. □

a) Prove the mean value theorem for integration.

b) Prove the second fundamental theorem of calculus.

c) Sketch the graph of the function $f(x)=x^3-3x$. Determine the equation of the tangent line to the graph at $x=2$.

d) Sketch the graph of the function $f(x)=\dfrac{2x-1}{x+1}$.

Unit 4. Elementary Number Theory

1. Reading

Elementary number theory is a branch of ***number theory*** that investigates properties of the integers by elementary methods. These methods include the use of divisibility properties, various forms of the axiom of induction and combinatorial arguments

Divisibility

Let a and b be integers, $a \neq 0$. If there exists an integer c such that $ac = b$, then we say that a ***divides*** b and write $a|b$. In this case, we also say that a is a ***divisor*** of b, or a is a ***factor*** of b, or b is ***divisible*** by a, or b is a ***multiple*** of a. If a does not divide b, we write $a \nmid b$.

The basic properties of ***division*** are listed below.

Theorem. *For integers a, b and c the following holds:*

(1) If $a \neq 0$, then $a|a$ and $a|0$.
(2) $1|a$.
(3) If $a|b$ and $a|c$, then $a|(br + cs)$, for any integers r, s.
(4) If $a|b$ and $b|c$, then $a|c$.
(5) If $a > 0, b > 0$, $a|b$ and $b|c$, then $a = b$.
(6) If $a > 0, b > 0$, and $a|b$ then $a \leqslant b$.

Prime number

A ***prime number*** (or a ***prime***) is an integer greater than 1 that has no positive divisors other than 1 and itself. An integer greater than 1 that is not a prime number is called a ***composite*** number.

The crucial importance of prime numbers to number theory and mathematics in general stems from the ***fundamental theorem of arithmetic***, which states as follows.

Theorem. *Every integer n greater than 1 factors into a product of primes:*

$$n = p_1 p_2 \cdots p_s.$$

Further, writing the primes in increasing order $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_s$ makes the factorization unique.

Some of the primes in the product may be equal. For instance, $60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5$. So the fundamental theorem is sometimes stated as: every integer greater than 1 can be factored uniquely as a product of powers of primes:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where $p_1 < p_2 < \cdots < p_k$ are primes, $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers. This equality is called the ***canonical decomposition*** of the integer n.

By means of the canonical decomposition of a positive integer one can compute the values of the number-theoretic functions $\tau(n)$, $S(n)$ and $\phi(n)$, which denote, respectively, the number of divisors of n, the sum of the divisors of n and the amount of positive integers $m \leqslant n$ that are ***coprime*** (or ***relatively prime***) with n (i.e., $\gcd(m, n) = 1$):

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1),$$

$$S(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 + 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 + 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k + 1},$$

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

An essential feature of these formulas is their dependence on the arithmetical structure of n.

The prime numbers play the role of "construction blocks" from which one can construct all other natural numbers. Therefore, questions on the disposition of the prime numbers in the sequence of natural numbers evoked the interest of scholars. The first proof that the set of prime numbers is infinite is due to Euclid. Only in the middle of the 19th century did P. L. Chebyshev take the following step in the study of the function $\pi(x)$, the number of prime numbers not exceeding n. He succeeded in proving by elementary means inequalities that imply

$$0.92120 \frac{x}{\ln x} < \pi(x) < 1.10555 \frac{x}{\ln x}$$

for all sufficiently large x. Actually, $\pi(x) \sim \dfrac{x}{\ln x}$ as $x \to \infty$, but this was not established until the end of the 19th century by means of complex analysis. For a long time it was considered impossible to obtain the result by elementary means. However, in 1949, A. Selberg obtained an elementary proof of this theorem.

Greatest common divisor and least common multiple

If a and b are integers and d is a positive integer such that $d|a$ and $d|b$, then d is called a ***common divisor*** of a and b. If both a and b are zero then they have infinitely many common divisors. However, if one of them is nonzero, the number of common divisors of a and b is finite. Hence, there must be a largest common divisor which is called the ***greatest common divisor*** of a and b, and is denoted by $\gcd(a, b)$.

By convention, it is accepted that $\gcd(0,0)=0$. The greatest common divisor of three or more integers may be defined similarly as for two integers.

The ***least common multiple*** of two integers a and b, usually denoted by $\operatorname{lcm}(a,b)$, is the smallest positive integer that is divisible by both a and b. If either a or b is 0, $\operatorname{lcm}(a,b)$ is defined to be zero. Similarly, ones can define the least common multiple of three or more integers.

Congruence

For a positive integer n, two integers a and b are said to be ***congruent modulo*** n, written as $a \equiv b \pmod n$, if their difference $a-b$ is a multiple of n. The number n is called the ***modulus*** of the congruence. The congruence $a \equiv b \pmod n$ expresses that a and b have identical ***remainders*** when divided by n.

Congruence modulo a fixed n is an equivalence relation. Indeed, for integers a, b and c, the following hold:

(1) $a \equiv a \pmod n$; (reflectivity)

(2) If $a \equiv b \pmod n$, then $b \equiv a \pmod n$; (symmetry)

(3) If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$. (transitivity)

Therefore, the relation congruence divides the set of all integers into non-intersecting equivalence classes which are called ***residue classes*** modulo n. Every integer is congruent modulo n with just one of the numbers $0,\dots,n-1$; the numbers $0,\dots,n-1$ belong to different classes, so that there are exactly n residue classes, while the numbers $0,\dots,n-1$ form a set of representatives of these classes.

Congruence modulo a fixed n is compatible with both addition and multiplication on the integers. Specifically, it follows from

$$a \equiv b \pmod n \text{ and } c \equiv d \pmod n$$

that

$$a \pm c \equiv b \pm d \pmod n \text{ and } ac \equiv bd \pmod n.$$

The operations of addition, subtraction and multiplication of congruences induce similar operations on the residue classes. Thus, if a and b are arbitrary elements from the residue classes A and B, respectively, then $a+b$ always belongs to one and the same residue class, called the sum $\mathrm{A}+\mathrm{B}$ of the classes A and B. The difference $\mathrm{A}-\mathrm{B}$ and the product $\mathrm{A}\cdot\mathrm{B}$ of the two residue classes A and B are defined in the same way. The residue classes modulo n form an ***Abelian group*** of order n with respect to addition.

An important application

For a long time, number theory in general, and the study of prime numbers in particular, was seen as the canonical example of pure mathematics, with no applications outside of the self-interest of studying the topic. In particular, number theorists such as British mathematician G. H. Hardy prided themselves on doing work that had absolutely no military significance. However, this vision was shattered in the 1970s, when it was publicly announced that prime numbers could be used as the basis for the creation of ***public key cryptography*** algorithms.

Exercise 4.1. Fill in each blank with a suitable mathematical term from the box.

congruent / incongruent / divisible / divisor / remainder / prime / composite / coprime / relative / relatively / infinite / infinitely

a) An integer n is said to be ***even*** if it is .... by 2 and is ***odd*** otherwise.

b) Number 1 is neither .... nor ....

c) If the difference $a-b$ is not divisible by n, then a and b are said to be .... modulo n.

d) Two integers a and b are congruent modulo n if a and b leave the same .... when divided by n.

e) The set of all prime numbers is ....

f) Two integers are called ***relatively prime***, or .... if their greatest common divisor equals 1.

g) If $ac \equiv bc \pmod{m}$, and c and m are .... prime, then $a \equiv b \pmod{m}$.

2. Speaking and writing

Exercise 4.2. Translate the following sentences/paragraphs into English.

a) Giả sử p là một số nguyên tố, a và b là các số nguyên. Nếu $p|ab$ thì $p|a$ hoặc $p|b$. $\rightsquigarrow$ ....

b) Mọi số nguyên dương chẵn trừ số 2 đều là số nguyên tố. $\rightsquigarrow$ ....

c) Mỗi số nguyên lớn hơn 1 đều là tích của những số nguyên tố. $\rightsquigarrow$ ....

d) Cho hai số nguyên a và b. Đặt $S = \{ra+sb \mid r,s \in \mathbb{Z}$ và $ra+sb>0\}$. Số nguyên dương d là ước số chung lớn nhất của hai số nguyên a và b khi và

chỉ khi d là phần tử bé nhất của S. $\rightsquigarrow$ ....
....
....

e) Hai số nguyên a và b là nguyên tố cùng nhau khi và chỉ khi tồn tại các số nguyên r và s sao cho $ra + sb = 1$. $\rightsquigarrow$ ....
....

f) Với các số nguyên a, b và c, nếu a và b là nguyên tố cùng nhau và $a|c$, $b|c$ thì $ab|c$. $\rightsquigarrow$ ....
....

g) Giả sử a và b là hai số nguyên, m là số nguyên dương. Nếu a và m là nguyên tố cùng nhau thì phương trình đồng dư tuyến tính (***linear congruence equation***) $ax \equiv b \pmod{m}$ có nghiệm duy nhất. $\rightsquigarrow$ ....
....
....

Exercise 4.3. Solve the following problems. Write down solutions and talk things out with your classmates or friends.

a) Show that, for any integers a, b and c, if a divides c and $a + b = c$ then a divides b.

b) For every positive integer n, show that 2 divides $n^2 - n$ and 6 divides $n^3 - n$.

c) Using induction, we show that 6 divides $7^n - 1$, for any positive integer n.

d) Prove by induction that $n^3 - n^2 + 2$ is divisible by 3 for every positive integer n.

e) Show that if $a \equiv b \pmod{m}$ and $d|m$, where $d > 0$, then $a \equiv b \pmod{d}$.

f) Suppose that $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$. Prove that if $\gcd(m, n) = 1$, then $a \equiv b \pmod{mn}$.

Unit 5. Algebra

Unit 6. Euclidean Geometry

1. Reading

Euclidean Geometry is the geometry of space described by the system of axioms first stated systematically by Euclid in his textbook, the **Elements**. Euclid's method consists in assuming a small set of intuitively appealing axioms, and deducing many other propositions (theorems) from these. However, Euclid's axioms are ***incomplete***, meaning that they are insufficient to produce the results one would like to be true in Euclidean geometry. Consequently, other axiomatic systems were devised in an attempt to fill in the gaps. The first sufficiently precise axiomatization of Euclidean geometry was given by D. Hilbert.

Hilbert's system of axioms

The ***primary*** (***undefined***) ***notions*** of Hilbert's system of axioms are ***points***, ***straight lines***, ***planes***, and relations between them consisting ***incidence*** (expressed by the words "belongs to", "lie on", "contains" or "passes through", etc), ***order*** (expressed by the word "between") and ***congruence***" (expressed by the word "congruent to" and denoted by the symbol "≡").

Note that, in the following, a ***line segment***, a ***ray***, a ***angle***, a ***triangle***, and a ***half-plane*** bounded by a straight line may be defined in terms of points and straight lines, using the relations incidence and order.

Hilbert's system contains 20 axioms, which are subdivided into five groups.

Group I: Axioms of incidence

I.1. For any two points there exists a straight line passing through them.

I.2. There exists only one straight line passing through any two distinct points.

I.3. At least two points lie on any straight line. There exist at least three points not lying on the same straight line.

I.4. There exists a plane passing through any three points not lying on the same straight line. At least one point lies on any given plane.

I.5. There exists only one plane passing through any three points not lying on the same straight line.

I.6. If two points A and B of a straight line a lie in a plane (α), then all points of a lie in (α).

I.7. If two planes have one point in common, then they have at least one more point in common.

I.8. There exist at least four points not lying in the same plane.

Group II: Axioms of order

II.1. If a point B lies between a point A and a point A, then A, B and C are distinct points on the same straight line and B also lies between C and A.

II.2. For any two points A and B on the straight line a there exists at least one point C such that the point B lies between A and C.

II.3. Of any three points on a line there exists no more than one that lies between the other two.

II.4. Let A, B, C be three points not lying in the same straight line and let a be a straight line lying in the plane (ABC) and not passing through any of the points A, B, C. Then, if the straight line a passes through a point of the segment AB, it will also pass through either a point of the segment BC or a point of the segment AC.

Group III: Axioms of congruence

III.1. Given a segment AB and a ray OX, there exists a point C on OX such that the segment AB is congruent to the segment OC, i.e. $AB \equiv OC$.

III.2. If $AB \equiv A'B'$ and $AB \equiv A''B''$, then $A'B' \equiv A''B''$.

III.3. On a line a, let AB and BC be two segments which, except for B, have no points in common. Furthermore, on the same or another line a', let $A'B'$ and $B'C'$ be two segments which, except for B', have no points in common. In that case if $AB \equiv A'B'$ and $BC \equiv B'C'$, then $AC \equiv A'C'$.

III.4. Let there be given an angle $\angle AOB$, a ray $O'A'$ and a half-plane π bounded by the straight line $O'A'$. Then π contains one and only one ray $O'B'$ such that $\angle AOB \equiv \angle A'O'B'$. Moreover, every angle is congruent to itself.

III.5. If, for two triangles ABC and $A'B'C'$, one has $AB \equiv A'B'$, $AC \equiv A'C'$, $\angle BAC \equiv \angle B'A'C'$, then $\angle ABC \equiv \angle A'B'C'$.

Group IV: Axiom of parallels (Euclid's axiom)

IV. Let there be given a straight line a and a point A not on that straight line. Then there is at most one line in the plane that contains a and A that passes through A and does not intersect a.

Group V: Axiom of continuity

V.1. (**Archimedes' axiom**) Let AB and CD be two arbitrary segments. Then the straight line AB contains a finite set of points $A_1, A_2, \ldots, A_n$ such that the point A_1 lies between A and A_2, the point A_2 lies between A_1 and A_3, etc., and such that the segments $AA_1, A_1A_2, \ldots, A_{n-1}A_n$ are congruent to the segment CD, and B lies between A and A_n.

V.2. (**Cantor's axiom**) Let there be given, on any straight line (α), an infinite sequence of segments A_1AB_1, A_2B_2, ..., which satisfies two conditions:
a) each segment in the sequence forms a part of the segment which precedes it;
b) for each preassigned segment CD it is possible to find a natural number n such that $A_nB_n < CD$.
Then (α) contains a point M belonging to all the segments of this sequence.

All other axioms of Euclidean geometry are defined by the basic concepts of Hilbert's system of axioms, while all the statements regarding the properties of geometrical figures and not included in Hilbert's system must be logically deducible from the axioms, or from statements which are deducible from these axioms.

Hilbert's system of axioms is ***complete***; it is ***consistent*** if the arithmetic of real numbers is consistent. If, in Hilbert's system, the axiom about parallels is replaced by its negation, the new system of axioms thus obtained is also consistent (the system of axioms of ***Lobachevskii geometry***), which means that the axiom about parallels is ***independent*** of the other axioms in Hilbert's system. It is also possible to demonstrate that some other axioms of this system are independent of the others.

Hilbert's system of axioms is the first fairly rigorous foundation of Euclidean geometry.

Some definitions and theorems

Right angle

Two angles $\angle AOB$ and $\angle COB$ that have the common ***vertex*** O and the common ***side*** OB, while the other sides of these angles OA and OC lie on a straight line and intersect at the unique point O, are called ***supplementary*** (or ***adjacent***) ***angles***. An angle which is congruent to its supplementary angle is called a ***right angle***. If a point O lies between two points A and B, then the angle $\angle AOB$ is called a ***straight angle***.

Two intersecting straight lines a and b are called ***perpendicular*** to each other, written $a \perp b$, if all four angles formed by them at the intersection point are right angles.

Lengths of segments and sizes of angles

Hilbert's axioms do not explicitly mention measurement of distances or angles; they are constructed from the axioms. Indeed, we have the following theorems.

Theorem. *For any fixed given segment* OE *(O does not concide with* E*), there exists a unique function that associates each segment* AB *with a nonnegative real number, denoted by* $|\mathrm{AB}|$ *and called the **length** of the segment* AB *measured relative to the gauge unit* OE*, satisfying the following properties:*

(i) $|\mathrm{OE}| = 1$*;*
(ii) if $\mathrm{AB} \equiv \mathrm{CD}$*, then* $|\mathrm{AB}| = |\mathrm{CD}|$*;*
(iii) if a point B *lies between two points* A *and* C*, then* $|\mathrm{AC}| = |\mathrm{AB}| + |\mathrm{BC}|$.

Theorem. *Each angle* $\angle\mathrm{AOB}$ *is associated with some real number that is denoted by* $\measuredangle\mathrm{AOB}$ *and called the **size** or **measurement** of the angle* $\angle\mathrm{AOB}$ *so that the following conditions are fulfilled:*

(i) $0 \leqslant \measuredangle\mathrm{AOB} \leqslant \pi$*;*
(ii) if $\angle\mathrm{AOB}$ *is a straight angle, then* $\measuredangle\mathrm{AOB} = \pi$*;*
(iii) if $\angle\mathrm{AOB} \equiv \angle\mathrm{CID}$*, then* $\measuredangle\mathrm{AOB} = \measuredangle\mathrm{CID}$*;*
(iv) if a ray OC *lies inside an angle* $\angle\mathrm{AOB}$*, then* $\measuredangle\mathrm{AOB} = \measuredangle\mathrm{AOC} + \measuredangle\mathrm{COB}$.

Exercise 6.1. Fill in each blank with a suitable mathematical term. Use the pictures (Figure 0.1) as hints.

a) A .... of a triangle is a segment connecting a vertex and the ***midpoint*** (or ***center***) of the opposite side.

b) The three ***altitudes*** of a triangle intersect in a single point, called the .... of the triangle.

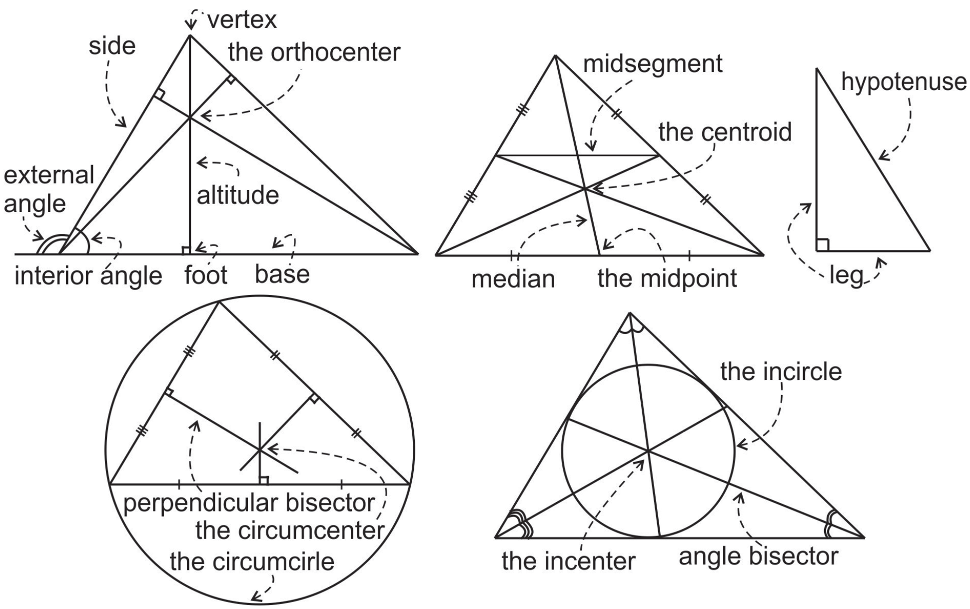
c) An angle that is .... to an internal angle of a triangle is called an ***external angle*** of this triangle.

d) In a right-angular triangle the side opposite to the right angle is called the .... Other two sides are called ....

e) The .... cuts every median in the ratio $2:1$.

f) In a triangle ABC, the .... is the intersection of the .... bisectors; it is the center of ...., the circle passing through the three vertices.

g) The .... of a triangle is the circle which lies inside the triangle and touches all three its sides. Its radius is called the ***inradius***.



Hình 0.1

2. Speaking and writing

Exercise 6.2. Complete the following sentences.

a) Two triangles are .... if their corresponding sides are equal in length and their corresponding angles are equal in size.

b) A triangle ABC is called ***isosceles*** if .... If AB ≡ AC, then the side BC is called the ***base*** of the isosceles triangle ABC, while the congruent sides AB and AC are called the ***lateral sides*** of this isosceles triangle.

c) An angle is said to be ***acute*** if ....

d) An angle is said to be ***obtuse*** if ....

e) A triangle .... is called an ***acute triangle*** or ***acute-angular triangle***.

f) A triangle .... is called an ***obtuse triangle*** or ***obtuse-anglular triangle***.

Exercise 6.3. Translate the following sentences/paragraphs into English.

a) Đường trung bình của tam giác là đoạn thẳng nối hai trung điểm của

hai cạnh; nó song song với cạnh còn lại của tam giác và có độ dài bằng một nửa cạnh này. ....
....
....

b) Giả sử a là đường thẳng nằm trên mặt phẳng (α). Khi đó qua mỗi điểm A trên (α), có duy nhất một đường thẳng b qua A, nằm trên (α) và vuông góc với a. ....
....
....

c) Ta nói đường thẳng a vuông góc với mặt phẳng (α) nếu a vuông góc với mọi đường thẳng nằm trên (α). ....
....
....

d) Điều kiện cần và đủ để đường thẳng a vuông góc với mặt phẳng (α) là đường thẳng a vuông góc với hai đường thẳng cắt nhau nằm trên (α). ...
....
....

e) Giả sử đường thẳng không nằm trên mặt phẳng (α). Khi đó a song song với (α) khi và chỉ khi a song song với một đường thẳng nào đó trên (α). ..
....
....

f) Tổng ba góc của một tam giác bằng $180°$. ....
....

g) Ta nói một tam giác là ***đều*** (***equilateral***) nếu ba cạnh của nó có độ dài bằng nhau. Tam giác đều đều có 3 góc đều bằng $60°$. ....
....
....

h) Trong tam giác cân đường cao ứng với cạnh đáy cũng là trung tuyến của tam giác đó. ....
....
....

i) Trong một tam giác, tổng độ dài hai cạnh lớn hơn độ dài cạnh còn lại.
....

j) Đường tròn là tập các điểm trong mặt phẳng cách một điểm cho trước một khoảng không đổi. ....
....

Unit 7. Linear Algebra

1. Reading

Linear algebra is the branch of mathematics concerning vector spaces, often finite or countably infinite dimensional, as well as linear mappings between such spaces. Such an investigation is initially motivated by a system of ***linear equations*** in several unknowns. Such equations are naturally represented using the formalism of matrices and vectors.

Vector space

The main structures of linear algebra are vector spaces. A ***vector space*** over a field F is a set V together with two binary operations. Elements of V are called ***vectors*** and elements of F are called ***scalars***. The first operation, called ***vector addition***, takes any two vectors v and w and outputs a third vector $v+w$. The second operation, called ***scalar multiplication***, takes any scalar α and any vector v and outputs a new vector vector αv. These operations satisfy the following axioms. In the list below, u, v and w are arbitrary vectors in V; α and β are scalars in F.

(1) $(u+v)+w = u+(v+w)$; (Associativity of addition)

(2) $u+v = v+u$; (Commutativity of addition)

(3) There exists an element $0 \in V$, called the ***zero vector***, such that $v+0 = v$ for all $v \in V$; (Identity element of addition)

(4) For every $v \in V$, there exists an element $-v \in V$, called the ***additive inverse*** of v, such that $v+(-v) = 0$; (Inverse elements of addition)

(5) $\alpha(u+v) = \alpha u + \alpha v$;
(Distributivity of scalar multiplication with respect to vector addition)

(6) $(\alpha+\beta)u = \alpha u + \beta u$;
(Distributivity of scalar multiplication with respect to field addition)

(7) $\alpha(\beta u) = (\alpha\beta)u$;
(Compatibility of scalar multiplication with field multiplication)

(8) $1v = v$, where 1 denotes the ***multiplicative identity*** in F.
(Identity element of scalar multiplication)

Subspaces, span, and basis

Again in analogue with theories of other algebraic objects, linear algebra is interested in subsets of vector spaces that are vector spaces themselves.

Let W be a nonempty subset of a vector space V over a field F. If W is also a vector space over F using the same addition and scalar multiplication operations, then W is said to be a ***linear subspaces*** of V.

A necessary and sufficient condition for a nonempty subset W of a vector space V over a field F to be a linear subspace of V is that W is ***closed*** under addition and scalar multiplication, i.e, $u+v \in W$ and $\alpha u \in W$ whenever $u, v \in W$ and $\alpha \in F$.

One of most common ways of forming a subspace is to take span of a given vectors. Let V be a vector space V over a field F. Let $S = \{v_1, v_2, \dots, v_n\}$ be a set of vectors V. Then any vector v of V of the form

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n \alpha_n,$$

where $\alpha_1, \alpha_2, \dots, \alpha_n$ are scalars, is called a ***linear combination*** of the vectors $v_1, v_2, \dots, v_n$. The set of all linear combinations of vectors $v_1, v_2, \dots, v_n$ forms a subspace of V, called the subspace ***spaned*** (or ***generated***) by S and denoted by $\mathrm{Span}(S)$ or $< S >$. Symbolically,

$$\mathrm{Span}(S) = \{\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n \alpha_n \mid \alpha_i \in F, i = 1, \dots, n\}.$$

Clearly, $\mathrm{Span}(S)$ is the smallest subspace of V which contains S.

In general, there may be many ways to express a vector of $\mathrm{Span}(S)$ as a linear combination of vectors $v_1, v_2, \dots, v_n$. The question that whether the expressions is unique leads to the following definitions.

A finite set $\{v_1, v_2, \dots, v_n\}$ of vectors of V is said to be ***linearly dependent*** if there exist scalars $\alpha_1, \alpha_2, \dots, \alpha_n$, not all zero, such that

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0.$$

The set $\{v_1, v_2, \dots, v_n\}$ is said to be ***linearly independent*** it is not linearly dependent, that is, the equality

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0 \text{ implies } \alpha_1 = \alpha_2 = \cdots = \alpha_n = 0.$$

By convention, we agree that the empty set is always linearly independent.

We can define linear dependence or independence for infinite sets of vectors. Let S be a infinite set of a vector space V. We say S is ***linearly independent*** if every finite subset of S is linearly independent, otherwise the set is said to be ***linearly dependent***, i.e., an infinite set of vectors of V is linearly dependent iff a least one finite subset of it is linearly dependent.

What should we mean by the span of S in the case of S being an infinite set of V? The difficulty is this: It is not always possible to assign a vector as the value of an infinite linear combination $\alpha_1 v_1 + \alpha_2 v_2 + \cdots$ in a consistent way. In algebra, it is customary to speak only of linear combination of finitely many vectors. Therefore, the span of an infinite set S must be interpreted as the set of those vector v which are linear combinations of *finitely many* elements of S:

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k, v_k \in S, \alpha_k \in F.$$

The number k is allowed to be arbitrary large, depending on the vector v.

Let S be a (infinite or not) subset of a vector space V. If S is linearly independent and $\mathrm{Span}(S) = V$, then any vector of V can be written uniquely as a linear combination of vectors in S. In this case, the set S is called a ***basis*** for the vector space V.

It can be proved that, if a vector space V is spaned by a finite set, then any two bases for V contain the same number of vectors. This number is called the ***dimension*** of V, denoted by $\dim(V)$.

Any set of vectors that spans V contains a basis, and any linearly independent set of vectors in V can be extended to a basis. It turns out that if we accept the axiom of choice, every vector space has a basis; nevertheless, this basis may be unnatural, and indeed, may not even be constructable. For instance, there exists a basis for the real numbers considered as a vector space over the rationals, but no explicit basis has been constructed.

Linear transformations

Similarly as in the theory of other algebraic structures, linear algebra studies mappings between vector spaces that preserve the vector-space structure. Given two vector spaces V and W over a field F, a ***linear transformation*** (also called ***linear map***, ***linear mapping*** or ***linear operator***) is a map $T : V \to W$ that is compatible with addition and scalar multiplication:

$$T(u + v) = T(u) + T(v), \quad T(\alpha u) = \alpha T(u)$$

for any vectors $u, v \in V$ and a scalar $\alpha \in F$.

When a bijective linear mapping exists between two vector spaces, we say that the two spaces are ***isomorphic***. Because an ***isomorphism*** preserves linear structure, two isomorphic vector spaces are "essentially the same" from the linear algebra point of view. If a mapping is not an isomorphism, linear algebra is interested in finding its ***range*** (or ***image***) and the set of elements that get mapped to zero, called the ***kernel*** of the mapping.

Matrices of linear transformations

Let V be a vector space of dimension n. An ***ordered basis*** for V is an ordered n-tuples $(v_1, v_2, \ldots, v_n)$ of vectors for which the set $\{v_1, v_2, \ldots, v_n\}$ is a basis of a vector space V.

Let $\mathscr{B} = (v_1, v_2, \ldots, v_n)$ be an ordered basis for V. Then for each $v \in V$ there is a unique ordered n-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of scalars for which

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n.$$

The n-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is called the ***coordinate*** of the vector v with respect to the ordered basis $\mathscr{B}$.

Now we can define the ***coordinate map*** $\Phi_{\mathscr{B}} : V \to F^n$ by

$$\Phi_{\mathscr{B}}(v) = [v]_{\mathscr{B}} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

The column vector $[v]_{\mathscr{B}}$ is called the ***coordinate vector*** (or ***coordinate matrix***) of v with respect to the ordered basis $\mathscr{B}$. Each vector v of V determines and is determined by its coordinate vector.

Let $\mathscr{B} = (v_1, v_2, \ldots, v_n)$ and $\mathscr{E} = (w_1, w_2, \ldots, w_n)$ be bases for vector spaces V and W, respectively. Let T be a linear transformation from V to W. Suppose that

$$T(v_j) = a_{1j} w_1 + a_{2j} w_2 + \cdots + a_{mj} w_m, j = 1, \ldots, n.$$

Then the $m \times n$ matrix

$$A = (a_{ij})_{i=1,\ldots,m; j=1,\ldots,n} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

is called the ***matrix*** of f with respect to the ordered bases $\mathscr{B}$ and $\mathscr{E}$. Different choices of the ordered bases leads to different matrices. For any v in V it holds that

$$[T(v)]_{\mathscr{B}} = A[v]_{\mathscr{E}}.$$

Thus, each linear transformation from V into W is determined by its matrix.

Exercise 7.1. Fill in each blank with a suitable mathematical term from the box.

invertible / isomorphic / isomorphism / square / eigenvalue / eigenvector / invariant / characteristic /

a) The matrix of a linear operator T from a finite-dimensional vector space V into itself is a .... matrix.

b) Let $T : V \to V$ be a linear operator on a vector space. A subspace W of V is called .... under T if $T(W) \subset W$.

c) Let $T : V \to V$ be a linear operator on a vector space. If there are a scalar λ and a nonzero vector v such that $T(v) = \lambda v$, then λ is called an .... of T. The vector v is called an .... of T.

d) A square matrix A is .... iff $\det A \neq 0$.

e) Let A be a square matrix. Then the .... polynomial of A is defined by $P(\lambda) = \det(\lambda I - A)$, where I be the ***identical matrix*** with the same size of A.

f) A linear operator T from a finite-dimensional vector space V into itself is a .... if and only if its ***determinant*** is nonzero.

2. Speaking and writing

Exercise 7.2. Complete the following sentences/paragraphs.

a) Any subset of a linearly independent set a vector space V is ....
....

b) Two vectors are .... iff one is a scalar multiple of the other.

Exercise 7.3. Translate the following sentences/paragraphs into English.

a) Giao của một họ những không gian vectơ con của một không gian vectơ V cũng là một không gian vectơ con của V. ....
....
....

b) Giả sử V là một không gian vector hữu hạn chiều. Nếu L là một tập con độc lập tuyến tính của V thì ta có thể bổ sung thêm những vector vào tập L để được một cơ sở của V. ⇝ ....
....
....

c) Nếu W là một không gian con của không gian vector hữu hạn chiều V thì W cũng hữu hạn chiều và $\dim \mathrm{W} \leqslant \dim \mathrm{V}$. Hơn nữa, $\dim \mathrm{W} = \dim \mathrm{V}$ khi và chỉ khi $\mathrm{W} = \mathrm{V}$. $\rightsquigarrow$ ....

....

....

d) Mỗi không gian vector n chiều trên trường F đều đồng cấu với không gian F^n. $\rightsquigarrow$ ....

....

e) Giả sử A và B là hai ma trận. Ta chỉ có thể thực hiện phép cộng $\mathrm{A}+\mathrm{B}$ khi hai ma trận A và B có cùng số dòng và cùng số cột. $\rightsquigarrow$ ....

....

....

f) Đa thức đặc trưng của toán tử tuyến tính T trên một không gian hữu hạn chiều V không phụ thuộc vào việc chọn cơ sở của V. $\rightsquigarrow$ ....

....

....

g) Các giá trị riêng của toán tử tuyến tính T là nghiệm của đa thức đặc trưng của nó. $\rightsquigarrow$ ....

....

h) Giả sử T một toán tử tuyến tính từ không gian vectơ hữu hạn chiều V vào chính nó. Các khẳng định sau là tương đương

i) T là khả ngược;

ii) T là đơn ánh;

ii) T là toàn ánh.

$\rightsquigarrow$ ....

....

....

....

i) Giả sử V là một không gian vector trên trường số phức $\mathbb{C}$ và T là một toán tử tuyến tính trên V. Khi đó T có ít nhất một giá trị riêng. $\rightsquigarrow$ ....

....

....

Unit 8. Analytical Geometry

Unit 9. Combination and Probability

Unit 10. Functions of a Complex Variable.

Unit 11. Metric Spaces

Unit 12. Review

APPENDICES

A. Reading mathematical symbols

A-1. Logic and sets

Symbol	How to read
$P \wedge Q$	P and Q; the conjunction of P and Q
$P \vee Q$	P or Q; the disjunction of P and Q
$P \Rightarrow Q$	P implies Q; if P then Q; Q is implied by P
$P \Leftrightarrow Q$	P if and only if Q; P is equivalent to Q; P and Q are equivalent
$\neg P$	not P
$a \in A$	*a* is an element/a member of (the set capital) A; *a* belongs to A; *x* is in A
$a \notin A$	*a* is not an element of A; *a* does not belong to A; *a* not belonging to A
$\emptyset$	(the) empty set
$A = \{a, b, c\}$	A is the set consisting elements *a, b, c*
$A = \{x \mid \cdots\}$	A is the set of all *x* such that $\cdots$
$A \subset B$	A is contained in B; A is a subset of B
$A \supset B$	A contains B; A is a superset of B
$A \cup B$	the union of A and B; A union B
$A \cap B$	the intersection of A and B, A intersect B; A intersected with B
$A \backslash B$	A minus B; the difference between A and B
$A^c, \overline{A}$	the complement of A; capital A c; capital A bar
$A \times B$	A times B; A cross B; the cartesian product of A and B
(a, b)	ordered pair *a b*
$\bigcup_{k=1}^{n} A_k$	the union of A_k for k from 1 to n

Symbol	How to read
$\bigcap_{\alpha \in I} A_\alpha$	the intersection of A_α for α belonging to I
$\prod_{k=1}^{n} A_k$	the cartesian product of A_k for k from 1 to n
$\forall x \in A$	for all (for every) x in A (such that) ...
$\exists x \in A$	there exists (there is) x in A (such that) ...
$\exists! x \in A$	there exists (there is) a unique x in A (such that) ...
$\nexists x \in A$	there is no x in A (such that) ...

A-2. Arithmetic

Integers

0	zero
1	one
2	two
3	three
4	four
5	five
6	six
7	seven
8	eight
9	nine

10	ten
11	eleven
12	twelve
13	thirteen
14	fourteen
15	fifteen
16	sixteen
17	seventeen
18	eighteen
19	nineteen

20	twenty
21	twenty-one
22	twenty-two
30	thirty
40	forty
50	fifty
60	sixty
70	seventy
80	eighty
90	ninety

100	one hundred
800	eight hundred (not hundreds)
245	two hundred and forty-five
−902	minus nine hundred and two
1 000	one thousand
51 000	fifty-one thousand
315 401	three hundred and fifteen thousand four hundred and one
2 000 000	two million
999 999 000	nine hundred and ninety-nine million nine hundred and ninety-nine thousand
3 000 000 000	three billion; three thousand million
5 000 000 000 000	five trillion; five thousand billion

Ordinal numbers

0th	zeroth/noughth	10th	tenth	20th	twentieth
1st	first	11th	eleventh	21st	twenty-first
2nd	second	12th	twelfth	22sd	twenty-second
3rd	third	13th	thirteenth	23rd	twenty-three
4th	fourth	14th	fourteenth	24th	twenty-fourth
5th	fifth	15th	fifteenth	30th	thirtieth
6th	sixth	16th	sixteenth	40th	fortieth
7th	seventh	17th	seventeenth	50th	fiftieth
8th	eighth	18th	eighteenth	80th	eightieth
9th	ninth	19th	nineteenth	90th	ninetieth

Fractions (Rational numbers)

$\frac{1}{2}$	one half; one over two	$\frac{7}{2}$	seven halves; seven over two
$\frac{1}{3}$	one third; one over three	$\frac{2}{3}$	two thirds; two over three
$\frac{1}{4}$	one quarter; one fourth	$\frac{3}{4}$	three quarters/three fourths
$\frac{1}{5}$	one fifth; one over five	$\frac{2}{5}$	two fifths; two over five
$\frac{1}{10}$	one tenth; one over ten	$\frac{9}{10}$	nine tenths; nine over ten
$\frac{1}{17}$	one seventeenth	$\frac{2}{27}$	two twenty-sevenths
$\frac{1}{21}$	one twenty-first	$\frac{5}{21}$	five twenty-firsts
$\frac{1}{32}$	one thirty-second	$\frac{3}{32}$	three thirty-seconds
$\frac{1}{43}$	one forty-third	$\frac{10}{43}$	ten forty-thirds; ten over forty-three
$\frac{1}{54}$	one fifty-fourth	$\frac{5}{54}$	five fifty-fourths; five over fifty-four
$1\frac{1}{2}$	one and a half	$5\frac{3}{4}$	five and three quarters
$3\frac{1}{3}$	three and one third	$7\frac{2}{5}$	seven and two fifths

Real and complex numbers

0.03	nought point zero three; nought point oh oh three; three thousandths

-0.401	minus nought point four zero one
109.25	one hundred and nine point two five
-2.3×10^{-10}	minus two point three times ten to the (power of) minus ten
1.02×10^{6}	one point zero two times ten to the (power of) 6
i	i
$1-3i$	one minus three i
$x+yi$	x plus y i
$\overline{3-i}$	the (complex) conjugate of three minus i
$+$	the addition sign
$-$	the subtraction sign
$\cdot$ or $\times$	the multiplication sign
$\div$	the division sign
$=$	the equality sign
$a=b$	a equals b; a is equal to b
$a\neq b$	a is not equal to b; a does not equal b; a is different from b
$a\approx b$	a is approximately equal to b
$a+b$	a plus b
$a-b$	a minus b
$a\pm b$	a plus or minus b
$a.b$	ab; a times b; a multiplied by b
$\frac{a}{b}$; a/b	a over b; a divided by b
$-a$	minus a; negative a; the negative of a; the opposite of a
$\pm a$	plus or minus a
$a<b$	a (is) less than b
$a>b$	a (is) greater than b
$a\leqslant b$	a (is) less than or equal to b; b (is) not less than a
$a\geqslant b$	a (is) greater than or equal to b; a (is) not less than b

$a < b < c$	a is less than b is less than c; b is greater than a and is less than c
$a \leqslant b < c$	a is less than or equal to b is less than c; b is not less than a and is less than c
$a \ll b$	a is much less than b
$a \gg b$	a is much greater than b
a^b	a to the b; a (raised) to the power of b; a to the b-th power; a raised by the exponent of b
x^2	x squared
x^3	x cubed
a^{-b}	a to the (power of) minus b
x^{-1}; $\frac{1}{x}$	x to the minus one; (the) reciprocal of x; x inverse
$\sqrt{x}$	(the) square root of x
$\sqrt[3]{x}$	(the) cubic root of x
$\sqrt[4]{x}$	(the) fourth root of x
$\sqrt[n]{x}$	(the) n-th root of x
$n!$	n factorial
$(a+b)c$	a plus b all times (multiplied by) c; a plus b in parentheses times (multiplied by) c
$(a+b)^2$	a plus b all squared, a plus b in parentheses squared
$\left(\frac{a}{b}\right)^2$	a over b all squared
$\frac{a-b}{c}$	a minus b all over (divided by) c
$(blabla)\cdot(blbl)$	$blabla$; the whole times $blbl$
$\dfrac{blabla}{blbl}$	$blabla$; the whole divided by $blbl$
$\lvert x\rvert$	absolute value of x (if x is a real number)
$\lvert z\rvert$	modulus of z (if z is a complex number)
$\mathrm{Re}(z)$	the real part of z
$\mathrm{Im}(z)$	the imaginary part of z
5%	5 percent
30°	30 degrees

x_k	x k; x subscript k; x sub k; x suffix k
x^k	x super (superscript) k (if k is an index; not exponent!)
x_{kj}	x k j; x subscript k j; x sub k j
x_k^j	x k j ; x subscript k superscript j
${}_k a$	a pre-subscript k
${}^k a$	a pre-superscript k
$\overline{a}$	a bar; a overbar;
$\widehat{a}$	a hat
$\tilde{a}$	a tilde
$1,\ldots,n$ or $\overline{1,n}$	1 (up) to n
$x_1;\ldots;x_n$	x 1 up to x n
$\sum\limits_{k=1}^{n} a_k$	sum k equals 1 to n of a (sub) k; sum for k (running) from 1 to n of a (sub) k
$\sum\limits_{k=1}^{\infty} a_n$	the sum from 1 to infinite of a_n
$\prod_{k=1}^{n} a_k$	product for k (running) from 1 to n of a (sub) k

A-3. Functions

Symbol	How to read
$f : \mathrm{X} \to \mathrm{Y}$	(a function) f from X to Y
$x \mapsto y$	x maps to y; x is sent/mapped to y
$f(x)$	f x; f of x; the function f of x
$f(x, y)$	f of x (comma) y
$f(2x;3y)$	f of two x (comma) three y
$f(x_1, x_2, \ldots, x_n)$	f of x 1 x 2 up to x n
f^{-1}	the inverse (function) of f; f inverse
$f(\mathrm{A})$	the image of A (under f); f of A;
$f^{-1}(\mathrm{A})$	the inverse image of A (under f); f inverse of A

Symbol	How to read
$g \circ f$	g circle f; g composed with f; the composite/composition of f and g
a^x	a to the x
$e^x, \exp(x)$	exponential of x; e to the x
$\log_a x$	logarithm to the base (or with base, or in base) a of x
$\log x, \lg x$	log of x; common (or decadic, or decimal) logarithm of x
$\ln x$	natural logarithm of x; Napierian logarithm of x
$\sin x$	sine x
$\cos x$	cosine x
$\tan x$	tan x
$\arcsin x$	arc sine x
$\sinh x$	hyperbolic sine x

A-4. Limits, derivatives and integrals

Symbol	How to read
(a, b)	the open interval from a to b
$[a, b]$	the closed interval from a to b
$(a, b]$	the (half-open) interval from a to b excluding a; including b
$\infty, \pm\infty$	infinity, plus/minus infinity
$u_n \to a$	u n tends to/converges to/approaches a
$x \to a$	x tends to/goes to/approaches a
$\lim\limits_{x \to a} f(x)$	(the) limit of f (of) x as x tends to/goes to/approaches a
$f(x) \to l$ as $x \to a$	$f(x)$ approaches (or converges to/ is convergent to) l as x tends to/goes to/approaches a
$\lim\limits_{x \to a^+} f(x)$	the limit of f of x as x approaches a from above (or from the right)

Symbol	How to read
$\lim\limits_{x\to a^-} f(x)$	the limit of f of x as x approachs a from below (or from the left)
$f = o(g)$	f is litle oh of g
$f = \mathrm{O}(g)$	f is big oh of g
f'	f prime; f dashed; (the first) derivative of f
f''	f double prime; f double dashed; the second derivative of f
$f^{(3)}$	the third derivative of f
$f^{(n)}$	the n-th derivative of f
$\frac{df}{dx}$	d f by d x; the derivative of f by x
$\frac{d^2f}{dx^2}$	d squared f by d x squared; the second derivative of f by x
$\frac{\partial f}{\partial x}$	partial d f by d x; the partial derivative of f by x (with respect to x)
$\partial_x f$	partial d x f; derivative of f with respect to x
$\frac{\partial^2 f}{\partial x^2}$	partial d squared f by d x squared; the second partial derivative of f by x (with respect to x)
$\frac{\partial^2 f}{\partial x \partial y}$	???
∇f	nabla f; the gradient of f
Δf	delta f
$\mathrm{div} f$	divergence of f
$\int f(x)dx$	indefinite integral of f; antiderivative of f
$\int_a^b f(x)dx$	the integral from a to b of f (of) x d x
$\iint_{\mathrm{D}} f(x,y)dxdy$	the double integral over (the domain) D of f of x y d x d y
$\iiint_{\mathrm{D}}$	the triple integral over (the domain) D
$\int_{\mathrm{L}} f(x)ds$	the line/path/curve integral of f along the path/curve L
$\oint_{\mathrm{C}} f ds$	the contour integral of f over/around the contour/closed curve C

A-5. Number theory

$k\|n$	n is divisible by k; k divides n
$[x]$	the integer part of x
$\mathbb{Z}_n$	the set of integers modulo n

A-6. Linear algebra

$\|\|x\|\|$	the norm of x
A^{T}	A transpose; the transpose of A
A^{-1}	A inverse; the inverse of A
$\det \mathrm{A}$	the determinant of A

A-7. Geometrics

(a, b)	the point a b
AB	segment AB; line AB; length of segment AB
$\vec{a}$, $\overrightarrow{\mathrm{AB}}$	vector a; vector A B
$\angle\alpha$	angle alpha
$\angle\mathrm{ABC}$, $\widehat{\mathrm{ABC}}$	angle A B C
$a \equiv b$	a is identical with b
$a \not\equiv b$	a is not identical with b
$a \perp b$	a is perpendicular to b; a and b are perpendicular to each other
$a \parallel b$	(the line) a is parallel to (the line) b; (two) (lines) a and b are parallel to each other
$a \sim b$	a is similar to b; a and b are similar to each other
$a \cong b$	a is congruent to b; a and b are congruent to each other
$\langle a, b\rangle$	scalar product of (vectors) a and b
$[a, b]$	vector product of (vectors) a and b
$\triangle\mathrm{ABC}$	triangle A B C; triangle with vertices A B C

A-8. Greek letters (used in mathematics)

Lowercase letters

Letter	Name	Pronounce
α	alpha	ˈælfə
β	beta	ˈbeitə/ˈbitə
γ	gamma	ˈgæmə
δ	delta	ˈdɛltə
ϵ, ε	epsilon	ˈɛpsəˌlon/ɛpˈsailən
ζ	zeta	ˈzeitə/ˈzitə
η	eta	ˈeitə/ˈitə
θ, ϑ	theta	ˈθeitə/ˈθitə
ι	iota	aiˈoʊtə
κ	kappa	ˈkæpə
λ	lambda	ˈlæmdə
μ	mu	mjuː
ν	nu	njuː
ξ	xi	zai/sai Greek: ksi
π, ϖ	pi	pai
ρ, ϱ	rho	roʊ
σ, ς	sigma	ˈsigmə
τ	tau	taʊ
ϕ, φ	phi	fai
χ	chi	kai
ψ	psi	sai/psai
υ	upsilon	ˈʌpsəˌlon/ʌpˈsailən
ω	omega	oʊˈmigə/oʊˈmeigə

Capital letters

Letter	Name
Λ	Lambda
Υ	Upsilon
Γ	Gamma
Ξ	Xi
Φ	Phi
Δ	Delta
Π	Pi
Ψ	Psi
Θ	Theta
Σ	Sigma
Ω	Omega

BIBLIOGRAPHY

[1] *Từ điển toán học Anh - Việt*, Nhà xuất bản Khoa học & Kĩ thuật, 1976.

[2] Trần Vui, Lương Hà, *English for mathematics*, Nhà xuất bản giáo dục Việt Nam, 2009.

[3] D. Hilbert, *Foundations of geometry*, 1980 (1899), translated by E. J. Townsend, reprint edition, the open court publishing company, 1950.

[4] A. N. Kolmogorov and S. V. Fomin, *Introductory real analysis*, (Translated by R. A. Silverman) Dover, New York, 1975.

[5] J. R. Munkres, *Topology*, 2nd ed., Prentice Hall, 1999.

[6] Encyclopedia of Math., Springer, `http://www.encyclopediaofmath.org`.

[7] R. A. Sharipov, *Foundations of geometry for university students and high school students*, Ufa, 1998.

[8] M. Spivak, *Calculus*, 3rd ed., Publish or Perish publishing, 1994.

[9] J. Stewart, *Calculus: Early transcendentals*, 6th ed., Thomson Brooks / Cole, 2008.

[10] J. J. Tattersall, *Elementary number theory in nine chapters*, 2nd ed., Cambridge university press, 2005.

[11] J. Trzeciak, *Writing mathematical papers in English*, Gdańsk Teachers' Press, 1993.

[12] Wikipedia, `http://en.wikipedia.org`.