Introduction

Abdennour Kitouni, Anatoliy Malyarenko and Sergei Silvestrov

November 12, 2015

Abstract

Contents of the lecture.

- ☞ Basic definitions of set theory.
- ☞ Relations.
- ☞ Cardinal numbers.
- ☞ Partitions and equivalence relations.
- ☞ Roots of unity.

About definitions

Because it is impossible to define *every* concept, mathematicians realise that there must be some *undefined* or *primitive* concept with which to start.

One of such a primitive concepts is a **set**.

It is useful in practice to use short symbols to denote certain sets. For instance, we denote by $\mathbb{Z}$ the set of all integers, i.e. all numbers of the type 0, ± 1, ± 2, $\dots$.

Instead of saying that x is an element of a set X, we shall also frequently say that x **lies** in X, and write $x \in X$. For instance, we have $1 \in \mathbb{Z}$, and also $-4 \in \mathbb{Z}$.

Basic definitions of set theory

Definition 1. If X and Y are sets, and if every element of Y is an element of X, then we say that Y is a **subset** of X.

To denote the fact that Y is a subset of X, we write $Y \subset X$, and also say that Y is **contained** in X.

Example 1. The set of positive integers $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$ is a subset of $\mathbb{Z}$.

Definition 2. If Y is a subset of X, but $Y \neq X$, then we say that Y is a **proper** subset of X.

Example 2. $\mathbb{Z}$ is an improper subset of $\mathbb{Z}$, and $\mathbb{Z}^+$ is a proper subset of $\mathbb{Z}$.

Definition 3. If X and Y are sets, then the **intersection** of X and Y, denoted by $X \cap Y$, is the set of elements which lie in both X and Y.

Example 3. If X is the set of integers ≥ 1 and Y is the set of integers ≤ 1, then

$$X \cap Y = \{1\}$$

(the set consisting of the number 1).

Definition 4. The **union** of X and Y, denoted by $X \cup Y$, is the set of elements which lie in X or in Y.

Example 4. If X is the set of integers ≤ 0 and Y is the set of integers ≥ 0, then $X \cup Y = \mathbb{Z}$ is the set of all integers.

Definition 5. If a set has no elements, it is called the **empty** set and is denoted by $\varnothing$.

Example 5. The set of all integers x such that $x > 0$ and $x < 0$ is empty, because there is no such integer x.

Definition 6. If X and Y are sets, we call the set of all pairs (x, y) with $x \in X$ and $y \in Y$ the **Cartesian product** of X and Y and denote it by $X \times Y$.

Note that $X \times \varnothing = \varnothing \times X = \varnothing$.

Example 6. Let $\mathbb{R}$ be the set of all real numbers. Then $\mathbb{R} \times \mathbb{R}$ is a Cartesian plane.

Relations

Definition 7. A subset $\mathscr{R}$ of $X \times Y$ is called a **relation** *between* X and Y. If $X = Y$, then a subset $\mathscr{R}$ of $X \times X$ is called a **relation** *on* X. If $(x, y) \in \mathscr{R}$, we write $x \mathscr{R} y$.

Example 7. The *equality relation* on X is the subset $\mathscr{R} = \{\, (x,x) : x \in X \,\} \subset X \times X$. We have $x \mathscr{R} y$ if and only if $x = y$.

Example 8. The graph of the function $f(x) = x^2$ is the subset $\{\, (x, x^2) : x \in \mathbb{R} \,\} \subset \mathbb{R} \times \mathbb{R}$. Note that each $x \in \mathbb{R}$ appears as the first member of exactly *one* ordered pair (x, x^2).

Definition 8. A **function** (map) f mapping X into Y is a relation between X and Y with the property that each $x \in X$ appears as the first member of exactly **one** ordered pair $(x,y) \in f$. We write $f\colon X \mapsto Y$ end express $(x,y) \in f$ by $f(x) = y$. The **domain** of f is the set X and the **codomain** of f is the set Y. The **range** of f is

$$f[X] = \{\, f(x) \colon x \in X \,\}.$$

One-to-one and onto functions

Definition 9. A function $f\colon X \mapsto Y$ is **one-to-one** or **injective** if $f(x) = f(y)$ only when $x = y$.

Definition 10. A function $f\colon X \mapsto Y$ is **onto** or **surjective** if $f[X] = Y$.

Definition 11. A function $f\colon X \mapsto Y$ is **one-to-one correspondence** or **bijective** if it is both one to one and onto.

Cardinal numbers

Definition 12 (A naive definition of cardinality)**.** The **cardinality** or the **cardinal number** of a set X is the number of elements in X. It is denoted by $|X|$.

A question: do $\mathbb{Z}$ and $\mathbb{R}$ have the same cardinal number?

Definition 13. Two sets X and Y have the same cardinality if there exists a one-to-one correspondence or a bijection between X and Y.

Example 9. The function $f\colon \mathbb{Z}^+ \mapsto \mathbb{Z}$ defined by

$$f(n) = \begin{cases} 0, & n = 1, \\ -k, & n = 2k, k \geq 1, \\ k, & n = 2k+1, k \geq 1 \end{cases}$$

is the one-to-one correspondence between $\mathbb{Z}^+$ and $\mathbb{Z}$. It follows that the sets $\mathbb{Z}$ and $\mathbb{Z}^+$ have the same cardinal number: $|\mathbb{Z}^+| = |\mathbb{Z}|$. This cardinal number is denoted by $\aleph_0$ (read “aleph-naught", aleph is the first letter of the Jewish alphabet).

Example 10 (The Diagonal Cantor Method, 1873)**.** We prove that $\aleph_0 < |\mathbb{R}|$. Because the function $f(x) = \tan(\pi x - \pi/2)$ establishes a one-to-one correspondence between the open interval $S =$

$(0,1)$ and $\mathbb{R}$, it suffices to show that $\aleph_0 < |S|$. If $\aleph_0 = |S|$, there is a one-to-one correspondence $f\colon \mathbb{Z}^+ \mapsto S$. Let $x_n = f(n)$, $n \in \mathbb{Z}^+$. Write each number $x \in S$ as an infinite decimal:

$$x_1 = 0.y_{1,1}y_{1,2}\dots y_{1,m}\dots$$

$$x_2 = 0.y_{2,1}y_{2,2}\dots y_{2,m}\dots$$

$$\dots\dots$$

$$x_n = 0.y_{n,1}y_{n,2}\dots y_{n,m}\dots$$

$$\dots\dots$$

and let

$$z_m = \begin{cases} 0, & y_{m,m} \neq 0, \\ 1, & y_{m,m} = 0. \end{cases}$$

The number $z = 0.z_1z_2\dots z_m\dots$ is **not** in $f[\mathbb{Z}^+]$.

Partitions

Definition 14. A family of subsets A_j of a set X is called **pairwise disjoint** if $A_j \cap A_k = \varnothing$ for all $j \neq k$.

Definition 15. A **partition** of a set X is a family of pairwise disjoint nonempty subsets, called **cells**, whose union is all of X.

Example 11 (The residue classes modulo n)**.** Split $\mathbb{Z}^+$ into the cell of even positive integers and the cell of odd positive integers.

Split $\mathbb{Z}^+$ into three cells: one consisting of the positive integers divisible by 3, another containing all positive integers leaving a remainder of 1 when divided by 3, and the last containing positive integers leaving a remainder of 2 when divided by 3.

Generally, for any $n \in \mathbb{Z}^+$ split $\mathbb{Z}^+$ into n cells according to whether the remainder is 0, 1, $\dots$, $n-1$ when a positive integer is dividing by n. These cells are called the **residue classes modulo** n in $\mathbb{Z}^+$.

Partitions and relations

If x, $y \in X$, define $x\mathscr{R}y$ if there is j with both $x \in A_j$ and $y \in A_j$. The relation $\mathscr{R}$ the three properties in the following definition.

Definition 16. A relation $x\mathscr{R}y$ on a set X is

- **reflexive** if $x\mathscr{R}x$ for all $x \in X$;
- **symmetric** if $x\mathscr{R}y$ implies $y\mathscr{R}x$ for all $x, y \in X$;
- **transitive** if $x\mathscr{R}y$ and $y\mathscr{R}z$ imply $x\mathscr{R}z$ for all $x, y, z \in X$.

Example 12. The *equality relation* on any nonempty set X is an equivalence relation

Example 13. The equivalence relation on $\mathbb{Z}^+$ corresponding to the partition of $\mathbb{Z}^+$ into residue classes modulo n (Example 11) is called the **congruence modulo** n, where $n \in \mathbb{Z}^+$, and is denoted by $\equiv_n$. Rather than write $a \equiv_n b$, we usually write $a \equiv b \pmod{n}$.

Theorem 1. *If $\mathscr{R}$ is an equivalence relation on a set X, then the equivalence classes*

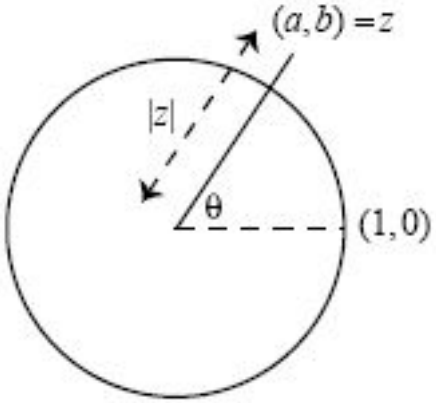
$$\bar{x} = \{ y \in X : y\mathscr{R}x \}$$

form a partition of X. Conversely, given a partition A_j of X, the relation "$x\mathscr{R}y$ if there is j with both $x \in A_j$ and $y \in A_j$" is the equivalence relation.

Complex numbers

We define a complex number $z = a + bi$ to be the point (a, b) in the plane; a is called the **real part** of z and b is called its **imaginary part**. The **modulus** $|z|$ of $z = a + bi$ is the distance from z to the origin:

$$|z| = \sqrt{a^2 + b^2}.$$



Theorem 2 (Polar decomposition)**.** *Every complex number z has a factorisation*

$$z = r(\cos\theta + i\sin\theta),$$

where $r = |z| \geq 0$ and $0 \leq \theta < 2\pi$.

It follows that every complex number z of modulus 1 is a point on the unit circle U, and so it has coordinates $(\cos\theta, \sin\theta)$. The real number θ lies in the interval $[0, 2\pi) = \mathbb{R}_{2\pi}$.

If $z = a + bi = r(\cos\theta + i\sin\theta)$, then (r, θ) are the **polar coordinates** of z; this is the reason why Theorem 2 is called the polar decomposition of z.

Theorem 3 (Addition theorem)**.** *If $z_1 = \cos\theta_1 + i\sin\theta_1$ and $z_2 = \cos\theta_2 + i\sin\theta_2$, then*

$$z_1 z_2 = \cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2).$$

Of course if $\theta_1 + \theta_2 > 2\pi$ then the angle in $\mathbb{R}_{2\pi}$ associated with $z_1 z_2$ is $\theta_1 + \theta_2 - 2\pi$. This gives us an **addition modulo 2π** on $\mathbb{R}_{2\pi}$, which is denoted by $+_{2\pi}$.

According to the addition theorem, complex number multiplication on U and addition modulo 2π on $\mathbb{R}_{2\pi}$ have the same algebraic properties. There exist a one-to-one correspondence $z \leftrightarrow \theta$ such that if $z_1 \leftrightarrow \theta_1$ and $z_2 \leftrightarrow \theta_2$, then $z_1 z_2 \leftrightarrow \theta_1 +_{2\pi} \theta_2$. Such a correspondence is called an **isomorphism**.

In 1707, A. De Moivre (1667–1754) proved the following elegant result.

Theorem 4 (De Moivre)**.** *For every real number x and every positive integer n,*

$$\cos(nx) + i\sin(nx) = (\cos x + i\sin x)^n.$$

Theorem 5 (Euler's theorem)**.** *For all real numbers x,*

$$e^{ix} = \cos x + i\sin x.$$

It is said that Euler was especially pleased with the equation

$$e^{\pi i} = -1;$$

indeed, this formula is inscribed on his tombstone.

As a consequence of Euler's theorem, the polar decomposition can be rewritten in exponential form: Every complex number z has a factorisation

$$z = re^{i\theta}$$

where $r \geq 0$ and $0 \leq \theta < 2\pi$. The addition theorem and De Moivre's theorem can be restated in complex exponential form. The first becomes

$$e^{ix}e^{iy} = e^{i(x+y)};$$

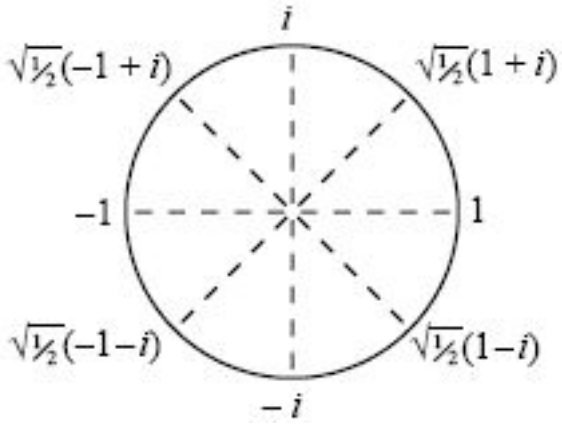
the second becomes

$$(e^{ix})^n = e^{inx}.$$

Roots of unity

Definition 17. If $n \geq 1$ is an integer, then an n**th root of unity** is a complex number ζ with $\zeta^n = 1$.

The geometric interpretation of complex multiplication is particularly interesting when z and w lie on the unit circle, so that $|z| = 1 = |w|$. Given a positive integer n, let $\theta = 2\pi/n$ and let $\zeta = e^{i\theta}$. The polar coordinates of ζ are $(1,\theta)$, the polar coordinates of ζ^2 are $(1,2\theta)$, the polar coordinates of ζ^3 are $(1,3\theta)$, ..., the polar coordinates of ζ^{n-1} are $(1,(n-1)\theta)$, and the polar coordinates of $\zeta^n = 1$ are $(1,n\theta) = (1,0)$. Thus, the nth roots of unity are equally spaced around the unit circle. The following figure shows the 8th roots of unity.



Theorem 6. *Every nth root of unity is equal to*

$$e^{2\pi ik/n} = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)$$

for some $k = 0, 1, 2, \ldots, n-1$.

Let U_n be the set of all nth roots of unity. Let $\mathbb{Z}_n = \{0,1,2,\ldots,n-1\}$. We see that $\mathbb{Z}_n \subset \mathbb{R}_n$ and addition modulo n is closed in $\mathbb{Z}_n$. The correspondence $e^{2\pi ik/n} \leftrightarrow k$ is an isomorphism between U_n and $\mathbb{Z}_n$ (prove!)