Vector Geometry

Oleg Viro

February 24, 2017

1 Complex numbers

1.1 Naive definition

As well-known, there is no real number x such that $x^2 = -1$. However the system of real numbers can be extended to a number system in which the equation $x^2 = -1$ has a solution. The simplest of them is the system of complex numbers.

Let i be a solution of the equation $x^2 = -1$, that is $i^2 = -1$. An arbitrary *complex number* can be obtained from real numbers and i by operations of addition, subtraction and multiplication.

The relation $i^2 = i \cdot i = -1$ applied together with the usual rules of elementary algebra allow to present any complex number in the form $x + yi$, where x and y are real numbers. We will call this form *standard.* For example,

$$\begin{aligned} i + i^2\sqrt{2} + 2i^3(1-i) &= i - \sqrt{2} + 2(-1)i(1-i) \\ &= i - \sqrt{2} - 2i - 2 = (-2-\sqrt{2}) + (-1)i. \end{aligned}$$

Two fundamental exercises: Let $z_1 = x_1 + y_1 i$ and $z_2 = x_2 + y_2 i$. Let us present their sum $z_1 + z_2$ and product $z_1 \cdot z_2$ in the standard form:

$$z_1 + z_2 = (x_1 + y_1 i) + (x_2 + y_2 i) = x_1 + y_1 i + x_2 + y_2 i = (x_1 + x_2) + (y_1 + y_2) i$$

$$z_1 \cdot z_2 = (x_1 + y_1 i) \cdot (x_2 + y_2 i) = x_1 x_2 + x_1, y_2 i + y_1 i x_2 + (y_1 i)(y_2 i)$$
$$= (x_1 x_2 - y_1 y_2) + (x_1 y_2 + y_1 x_2)i.$$

From the very beginning in a study of complex numbers, we may assume that each complex number is already presented in the standard form. More complicated formulas (like the formula $i + i^2\sqrt{2} + 2i^3(1-i)$ discussed above) are considered as prescriptions for calculations, that is for transforming them into the standard form.

The standard form $x + yi$ of a complex number z is encoded by an ordered pair (x, y) of real numbers. It happens to be unique. In order to eliminate an apparent mysterious flavor of i, we will lay down the foundations of the theory of complex numbers by speaking only about ordered pairs of real numbers representing complex numbers. This approach is realized below.

1.2 Complex numbers as a pairs of real numbers

A *complex number* is an ordered pair (x, y) of real numbers. [1] The set of all complex numbers is denoted by $\mathbb{C}$. A complex number (x, y) is associated to the point with Cartesian coordinates x and y on the plane.

Define addition and multiplication of $z_1 = (x_1, y_1)$ and $z_2 = (x_2, y_2)$ by formulas:[2]

$$z_1 + z_2 = (x_1, y_1) + (x_2, y_2) = (x_1 + x_2,\ y_1 + y_2)$$

and

$$z_1 \cdot z_2 = (x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 - y_1 y_2,\ x_1 y_2 + x_2 y_1).$$

A real number x is identified with the complex number $(x, 0)$.

Under this identification, the arithmetic operations with real numbers agree with the arithmetic operations with the corresponding complex numbers. Namely, the sum of complex numbers $(x_1, 0)$, $(x_2, 0)$ corresponding to real numbers x_1 and x_2 corresponds to the sum $x_1 + x_2$ of the real numbers:

[1] Notice: no i is involved!

[2] Motivated by the two fundamental exercises in section 1.1

$(x_1, 0) + (x_2, 0) = (x_1 + x_2,\ 0 + 0) = (x_1 + x_2,\ 0).$

Similarly, for multiplication:

$(x_1, 0) \cdot (x_2, 0) = (x_1 \cdot x_2 - 0 \cdot 0,\ x_1 \cdot 0 + 0 \cdot x_2) = (x_1 \cdot x_2, 0).$

Multiplication by a real number

Let $r \in \mathbb{R}$ and $z = (x, y) \in \mathbb{C}$. Then $r \cdot z = r \cdot (x, y) = (r \cdot x,\ r \cdot y)$. Indeed,

$r \cdot z = r \cdot (x, y) = (r, 0) \cdot (x, y) = (r \cdot x - 0 \cdot y,\ r \cdot y + 0 \cdot x) = (r \cdot x,\ r \cdot y).$

1.3 Properties of the operations

Commutativity of addition. $z_1 + z_2 = z_2 + z_1$ for any $z_1, z_2 \in \mathbb{C}$.

Proof. $z_1 + z_2 = (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) = (x_2 + x_1, y_2 + y_1) = (x_2, y_2) + (x_1, y_1) = z_2 + z_1$. □

Associativity of addition. $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$ for any $z_1, z_2, z_3 \in \mathbb{C}$.

Proof. $(z_1 + z_2) + z_3 = ((x_1, y_1) + (x_2, y_2)) + (x_3, y_3) = (x_1 + x_2,\ y_1 + y_2) + (x_3, y_3) = ((x_1 + x_2) + x_3,\ (y_1 + y_2) + y_3) = (x_1 + (x_2 + x_3),\ y_1 + (y_2 + y_3)) = (x_1, y_1) + ((x_2, y_2) + (x_3, y_3)) = z_1 + (z_2 + z_3)$ □

The zero. $z + 0 = z$ for any $z \in \mathbb{C}$.

Proof. $z + 0 = (x, y) + (0, 0) = (x + 0, y + 0) = (x, y) = z$. □

Additive inverse. For any $z = (x, y) \in \mathbb{C}$, denote by $-z$ the complex number $(-x, -y)$. Then $z + (-z) = (x, y) + (-x, -y) = (0, 0) = 0$.

Distributivity. $z_1(z_2 + z_3) = z_1 z_2 + z_1 z_3$ for any $z_1, z_2, z_3 \in \mathbb{C}$.

Proof. Let $z_1 = (x_1, y_1)$, $z_2 = (x_2, y_2)$ and $z_3 = (x_3, y_3)$. Then $z_1(z_2 + z_3) = (x_1, y_1)\,((x_2, y_2) + (x_3, y_3)) = (x_1, y_1) \cdot (x_2 + x_3,\ y_2 + y_3) = (x_1(x_2 + x_3),\ y_1(y_2 + y_3)) = (x_1 x_2 + x_1 x_3,\ y_1 y_2 + y_1 y_3) = (x_1, y_1)(x_2, y_2) + (x_1, y_1)(x_3, y_3) = z_1 z_2 + z_1 z_3$ □

Commutativity of multiplication. $z_1 z_2 = z_2 z_1$ for any $z_1, z_2 \in \mathbb{C}$.

Proof. $z_1z_2 = (x_1, y_1)(x_2, y_2) = (x_1x_2, y_1y_2) = (x_2x_1,\ y_2y_1) = (x_2, y_2)(x_1, y_1) = z_2z_1 =$ $\square$

Associativity of multiplication. $(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$ for any $z_1, z_2, z_3 \in \mathbb{C}$.

Proof. $(z_1 \cdot z_2) \cdot z_3 = ((x_1, y_1) \cdot (x_2, y_2)) \cdot (x_3, y_3) = ((x_1 \cdot x_2) \cdot x_3,\ (y_1 \cdot y_2) \cdot y_3) = (x_1 \cdot (x_2 \cdot x_3),\ y_1 \cdot (y_2 \cdot y_3)) = (x_1, y_1) \cdot ((x_2, y_2) \cdot (x_3, y_3)) = z_1 \cdot (z_2 \cdot z_3)$ $\square$

The unit. $z \cdot 1 = z$ for any $z \in \mathbb{C}$.

Proof. $z \cdot 1 = (x, y)(1, 0) = (x \cdot 1 - y \cdot 0,\ x \cdot 0 + y \cdot 1) = (x, y) = z.$ $\square$

We proved that the arithmetic operations of addition and multiplication of complex numbers introduced in Section 1.2 have the usual properties that we expect for operations with these names. So, we really may deal with them in the same way as we did with real numbers.

As usual, *subtraction* is defined as addition of the additive inverse:

$$z_1 - z_2 = z_1 + (-z_2).$$

Denote the complex number $(0, 1)$ by i.

The square of i. $i^2 = -1$.

Proof. $i^2 = i \cdot i = (0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1,\ 0 \cdot 1 + 1 \cdot 0) = (-1, 0) = -1.$ $\square$

Back to the traditional notation of complex numbers.

Now the presentation of any complex number z in the form $z = x + yi$ with $i^2 = -1$ makes sense:

$z = (x, y) = (x, 0) + (0, y) = (x, 0) + y(0, 1) = x + yi.$

This is more specific and meaningful notation than $z = (x, y)$, and we switch to it. Here x is called the *real part* of z and denoted by $\operatorname{Re} z$, while y is called the *imaginary part* of z and denoted by $\operatorname{Im} z$. Thus $z = \operatorname{Re} z + i \operatorname{Im} z$.

Notice, that both real and imaginary parts are *real* numbers.

1.4 Conjugation

For $z = x + iy \in \mathbb{C}$, denote the complex number $x - yi$ by $\overline{z}$ and call it the *conjugate* to z. Notice that $\overline{\overline{z}} = z$. Indeed, $\overline{(\overline{x + yi})} = \overline{x - yi} = x - (-y)i = x + yi$. Complex numbers $x + yi$ and $x - yi$ are said to be *conjugate to each other*, we say about them as about a pair of conjugate complex numbers.

Passing from z to $\overline{z}$ is a map $\mathbb{C} \to \mathbb{C}$. It has several remarkable and useful properties. First of all, it respects the arithmetic operations.

1.A Theorem. *For any complex numbers z and w*

$$\overline{z + w} = \overline{z} + \overline{w} \qquad \textit{and} \qquad \overline{z \cdot w} = \overline{z} \cdot \overline{w}$$

Proof. Let $z = x + yi$ and $w = u + vi$. Then

$$\begin{aligned}\overline{z + w} = \overline{(x + yi) + (u + iv)} = \overline{(x + u) + (y + v)i}&\\ = (x + u) - (y + v)i = x - yi + u - vi = \overline{z} + \overline{w}&\end{aligned}$$

and

$$\begin{aligned}\overline{z \cdot w} = \overline{(x + yi)(u + vi)} = \overline{(xu - yv) + (xv + yu)i}&\\ = (xu - yv) - (xv + uy)i = (xu - (-y)(-v)) + (x(-v) + (-y)u)i&\\ = (x - yi)(u - vi) = \overline{z}\overline{w}.&\end{aligned}$$

□

1.B Theorem. $z + \overline{z} = 2 \operatorname{Re} z$ *and* $z - \overline{z} = 2i \operatorname{Im} z$ *for any complex number* z.

Proof. Let $z = x + yi$. Then $z + \overline{z} = x + yi + x - iy = 2x = 2 \operatorname{Re} z$ and $z - \overline{z} = x + yi - (x - yi) = 2yi = 2i \operatorname{Im} z$. □

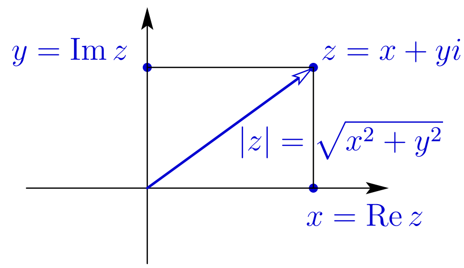
1.C Theorem. $z \cdot \overline{z} = (\operatorname{Re} z)^2 + (\operatorname{Im} z)^2$.

Proof. Let $z = x + yi$. Then $z \cdot \overline{z} = (x + yi)(x - yi) = x^2 - y^2 i^2 = x^2 + y^2 = (\operatorname{Re} z)^2 + (\operatorname{Im} z)^2$. □

1 Corollary. *For any complex number z the product $z \cdot \overline{z}$ is a non-negative real number. It equals zero if and only if $z = 0$.* □

1.5 The module of a complex number

For a complex number z, the real number $\sqrt{z \cdot \bar{z}}$ is called the ***module***, or the ***absolute value***, or the ***norm*** of z and is denoted by $|z|$. As it follows from Theorem 1.C, $|z| = \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2}$. By the Pythagoras theorem, $|z| = \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2}$ is the distance from the origin to the point corresponding to z.



If z is a real number, then $\operatorname{Im} z = 0$, $z = \operatorname{Re} z$ and $|z|$ coincides with the absolute value defined for z, as a real number, by the formula

$$|z| = \begin{cases} z, & \text{if } z \geq 0 \\ -z, & \text{if } z < 0. \end{cases}$$

Indeed, $|x + 0i| = \sqrt{x^2 + 0^2} = \sqrt{x^2} = |x|$ for any real x.

For an arbitrary complex number z, the module is related to the real and imaginary parts by inequalities $|z| \geq |\operatorname{Re} z|$ and $|z| \geq |\operatorname{Im} z|$.

Indeed, $|z| = \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2} \geq \sqrt{(\operatorname{Re} z)^2} = |\operatorname{Re} z|$. Similar proof works for $\operatorname{Im} z$. $\square$

1.D Theorem. *For any complex numbers z and w,*

$$|z \cdot w| = |z| \cdot |w|$$

Proof. By the definition of module, $|z \cdot w| = \sqrt{(z \cdot w) \cdot \overline{(z \cdot w)}} = \sqrt{z \cdot w \cdot \bar{z} \cdot \bar{w}} = \sqrt{z \cdot \bar{z} \cdot w \cdot \bar{w}}$. Since $z \cdot \bar{z}$ and $w \cdot \bar{w}$ are non-negative real numbers, $\sqrt{z \cdot \bar{z} \cdot w \cdot \bar{w}} = \sqrt{z \cdot \bar{z}}\sqrt{w \cdot \bar{w}}$. Hence $|z \cdot w| = \sqrt{z \cdot \bar{z}}\sqrt{w \cdot \bar{w}} = |z| \cdot |w|$. $\square$

1.E Theorem (Triangle Inequality). *For any complex numbers z and w,*

$$|z + w| \leq |z| + |w|.$$

Proof. $|z+w| = \sqrt{(z+w)\overline{(z+w)}} = \sqrt{(z+w)(\overline{z}+\overline{w})} = \sqrt{z\overline{z}+z\overline{w}+w\overline{z}+w\overline{w}}$. Observe, that $z\overline{z} = |z|^2$, $w\overline{w} = |w|^2$ and $w\overline{z} = \overline{z\overline{w}}$. Therefore,

$$|z+w| = \sqrt{|z|^2 + z\overline{w} + \overline{z\overline{w}} + |w|^2} = \sqrt{|z|^2 + 2\,\mathrm{Re}(z\overline{w}) + |w|^2}.$$

As it was proven above, $|\,\mathrm{Re}(z\overline{w})| \le |z\overline{w}| = |z||w|$. Therefore,

$$|z|^2 + 2\,\mathrm{Re}(z\overline{w}) + |w|^2 \le |z|^2 + 2|z||w| + |w|^2 = (|z|+|w|)^2.$$

Hence, $|z+w| = \sqrt{|z|^2 + 2\,\mathrm{Re}(z\overline{w}) + |w|^2} \le |z| + |w|$. $\square$

1.6 Division of complex numbers

Let $z = x + iy$ be a complex number. Assume that $z \ne 0$. Then the complex number

$$w = \frac{\overline{z}}{|z|^2} = \frac{x}{x^2+y^2} + i\frac{y}{x^2+y^2}$$

has the following remarkable property: $z \cdot w = 1$.

Indeed, $z \cdot w = \dfrac{z \cdot \overline{z}}{|z|^2} = \dfrac{z \cdot \overline{z}}{z \cdot \overline{z}} = 1$.

Recall a few general facts about multiplicative inverse and division. First, here is a definition for multiplicative inverse: B is called the *multiplicative inverse* for A if $AB = 1$. The multiplicative inverse to A is denoted by A^{-1} or $\dfrac{1}{A}$. Thus for a complex number z which is not 0 the multiplicative inverse exists and is given by the formula $z^{-1} = \dfrac{\overline{z}}{|z|^2}$.

Recall that division is the operation inverse to multiplication: $X = A/B$ if $X \cdot B = A$. It can be performed as multiplication of the divising by the multiplicative inverse to the divisor: $A/B = A \cdot B^{-1}$. Indeed, if $X = A/B$ then $X \cdot B = A$. By multiplying both sides of the latter equality by B^{-1} we get $X \cdot B \cdot B^{-1} = A \cdot B^{-1}$. The left hand side here is $X \cdot B \cdot B^{-1} = X \cdot 1 = X$. Thus we have $A/B = X = A \cdot B^{-1}$.

Since we have found the multiplicative inverse for each non-zero complex number, we can divide one complex number to any non-zero complex number.

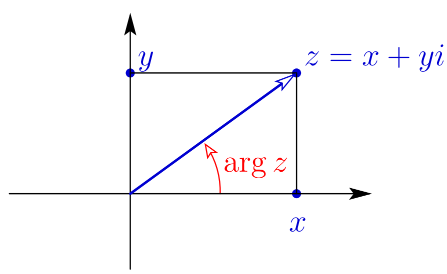
Let $z = x + yi$ and $w = u + vi \neq 0$. Then

$$\frac{z}{w} = \frac{x+yi}{u+iv} = z \cdot w^{-1} = z \cdot \frac{\overline{w}}{|w|^2} = \frac{(x+yi)(u-vi)}{u^2+v^2} = \frac{xu+yv}{u^2+v^2} + i\frac{yu-xv}{u^2+v^2}.$$

There is no need to remember this formula. Instead, remember that you can simplify a complex fraction by multiplying both numerator and denominator by the number conjugate to the denominator: $\dfrac{x+yi}{u+vi} = \dfrac{(x+yi)(u-vi)}{(u+vi)(u-vi)}$. This makes the denominator real: $\dfrac{(x+yi)(u-vi)}{(u+vi)(u-vi)} = \dfrac{(x+yi)(u-vi)}{u^2+v^2}$. Division of a complex number by a real number is nothing but separate division of its real and imaginary parts by this real number.

1.7 Argument (aka phase)

Let z be a complex number, $z \neq 0$. The angle subtended in counter-clockwise direction between the positive direction of the real axis and the segment connecting 0 to z is called the **argument** or the **phase** of z. It is denoted by $\arg z$. The word phase is used mostly in Physics and in engineering applications.



Traditionally argument is measured in radians (not degrees).

A few examples: $\arg i = \frac{\pi}{2}$, $\arg 1 = 0$, $\arg(-1) = \pi$, $\arg(-i) = \frac{3\pi}{2} = -\frac{\pi}{2}$. Since the argument is defined only up to adding $2\pi n$, the argument of the same complex numbers take also the following values: $\arg i = -\frac{3\pi}{2}$, $\arg 1 = 2\pi = -4\pi$, etc. Further, $\arg(\frac{1}{2} + \frac{\sqrt{3}}{2}i) = \frac{\pi}{3}$, $\arg(1+i) = \frac{\pi}{4}$, $\arg(1-i) = -\frac{\pi}{4} = \frac{7\pi}{4}$.

Since argument is a measurement of an angle, it is defined up to adding $2\pi n$, where n is an arbitrary integer. There are three ways to look at a numerical measurement of an angle:

- the result is a unique real number which belongs to an interval of length 2π chosen once forever (say, $[0, 2\pi)$ or $(-\pi, \pi]$);
- the result is a real number defined up to adding of a multiple of 2π (the same angle amounts $\frac{3\pi}{2}$ and $-\frac{\pi}{2}$ and $-\frac{9\pi}{2}$);
- the result is an infinite set of numbers, which can be obtained from a measurement in the first sense by adding $2n\pi$ for all integers n.

Each approach has its advantages and disadvantages. The first one eliminates the ambiguity, but at the cost of two drawbacks: a need to choose an interval of length 2π when no choice is natural, and an unavoidable discontinuity of measurement. In order to understand the nature of the discontinuity, assume that all measurements are restricted to the interval $(-\pi, \pi]$ and consider an angle increasing continuously. Its measurement increases continuously until it reaches π, and then it jumps down by -2π. The second approach means that the result of measurement is not a true function of the angle, because it is not univalued. The third approach involves infinite sets which seem to be cumbersome and inappropriate.

For our needs, the second approach seems to be most appropriate. The ambiguity is similar to other ambiguities. For example, every rational number can be presented by infinitely many fractions and each of these fractions represents the number adequately, a choice of a fraction is a matter of convenience.

Arguments of complex numbers will appear in formulas. However the formulas respect the ambiguity. For example, since the basic trigonometric functions are 2π-periodic, the values which they take on an argument are not affected by adding of 2π to the argument. For example, $\cos(\varphi + 2\pi) = \cos\varphi$. Therefore, expressions $\cos(\arg z)$, $\sin(\arg z)$, $\sin(3\arg z)$ and $\tan(\arg z)$ have well-defined numerical values for any complex number z.

There are several formulas which express the argument as a function of real and imaginary parts, but each of them is applicable only to z from some domain. For instance, if $\operatorname{Re} z \geq 0$, then $\arg z = \arcsin \frac{\operatorname{Im} z}{|z|}$. This is so due to the fact that the range of arcsin is $[-\frac{\pi}{2}, \frac{\pi}{2}]$.

Similarly,

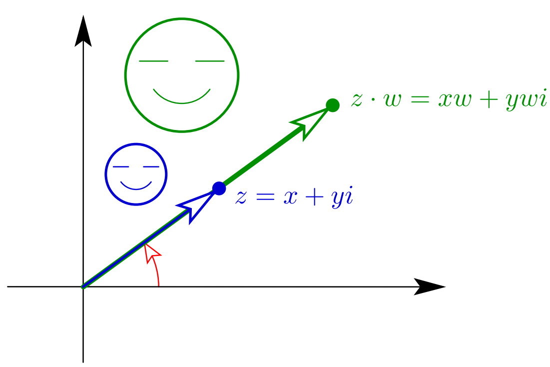
- if $\operatorname{Im} z \geq 0$, then $\arg z = \arccos \frac{\operatorname{Re} z}{|z|}$;
- if $\operatorname{Re} z > 0$, then $\arg z = \arctan \frac{\operatorname{Im} z}{\operatorname{Re} z}$;
- if $\operatorname{Re} z < 0$, then $\arg z = \pi + \arctan \frac{\operatorname{Im} z}{\operatorname{Re} z}$;
- if $\operatorname{Re} z \leq 0$, then $\arg z = \pi + \arcsin \frac{-\operatorname{Im} z}{|z|}$.

1.8 Geometry of multiplication by a complex number

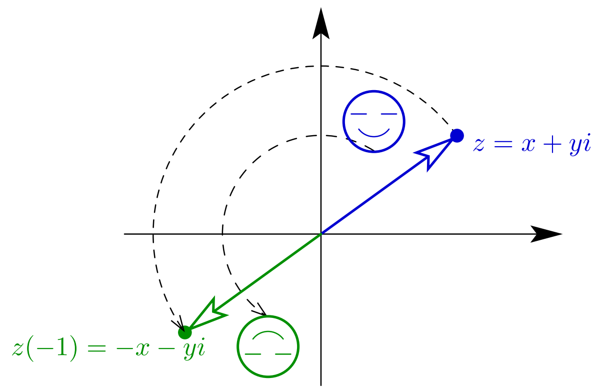
Let w be a complex number. In this section we study the map $\mathbb{C} \to \mathbb{C}$ defined by the formula $z \mapsto z \cdot w$.

Multiplication by null. First, let us consider the most special case. If $w = 0$, then this is a constant map which maps each complex number to 0, because $z \cdot 0 = 0$.

Multiplication by a positive real number. Second, let w be a positive real number. Then the points $z = x + yi$ and $zw = xw + ywi$ are on the same ray starting at 0, therefore the map does not change the argument. The module is multiplied by w. Indeed, $|zw| = |w||z| = w|z|$. Thus, the map is a *dilation* with factor w.

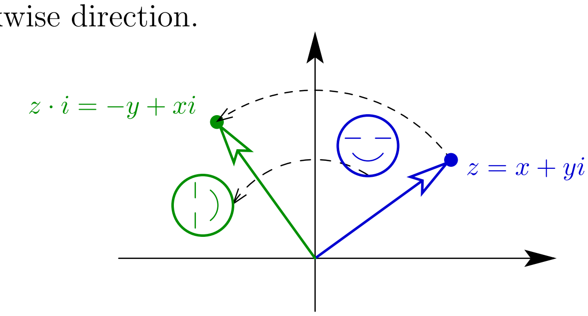


Multiplication by -1. Third, let $w = -1$. Then each $z = x + yi$ is mapped to its additive inverse $-z = -x - yi$. Geometrically, this map can be described as the symmetry about the origin, or as the rotation about the origin by π.



Multiplication by a negative real number. Fourth, let w be a negative real number. Then $w = -|w|$, and the map can be presented as the composition of two maps discussed above: $z \mapsto -z \mapsto (-z)|w| = zw$. So, this a symmetry about the origin followed by dilation with factor $|w|$.

Multiplication by i. Fifth, let $w = i$. Then $z = x + yi$ is mapped to $z \cdot w = z \cdot i = (x + yi)i = -y + xi$. The real axis is mapped to the imaginary axis. Indeed, $x + 0i \mapsto xi$. The imaginary axis is mapped to the real one, but the positive direction goes to the negative one. Indeed, $iy \mapsto i^2 y = -y$. Overall, the map seems to rotate the whole plane about the origin by $\frac{\pi}{2}$ in the counter-clockwise direction.



We will come back with a proof later.

Multiplication by a complex number of module 1. Now let us consider a more general w: assume that $|w| = 1$.

1.F Theorem. *Let w be a complex number with $|w| = 1$. Then the map $\mathbb{C} \to \mathbb{C} : z \mapsto z \cdot w$ preserve distances between points: for any z_1, z_2 the distance between $z_1 \cdot w$ and $z_2 \cdot w$ equals the distance between z_1 and z_2.*

Proof. By the Pythagoras Theorem, the distance between $z_1 = x_1 + y_1 i$ and $z_2 = x_2 + y_2 i$ is

$$\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} = |z_2 - z_1|$$

Similarly, the distance between $z_1 \cdot w$ and $z_2 \cdot w$ is

$$|z_2 \cdot w - z_1 \cdot w| = |(z_2 - z_1) \cdot w| = |z_2 - z_1| \cdot |w| = |z_2 - z_1|.$$

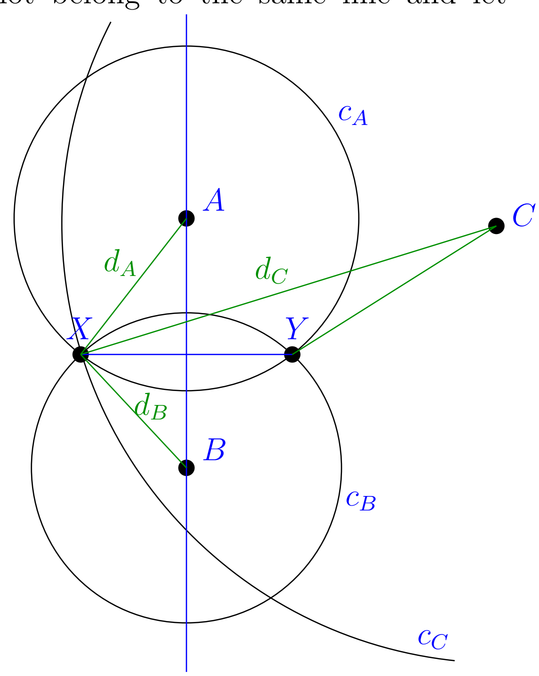
□

A map which preserves distances is called an *isometry*. An isometry is a mathematical counter-part to a motion of a rigid body.

In general, in order to understand a map, one needs to understand how each point is mapped. However, if the map is an isometry, then a knowledge on mapping of a few points suffices for recovery of the whole map.

1.G Theorem. *An isometry $f : \mathbb{C} \to \mathbb{C}$ is uniquely determined by its values on any three points, which do not lie on the same straight line.*

Proof. Let points $A, B, C \in \mathbb{C}$ do not belong to the same line and let $f : \mathbb{C} \to \mathbb{C}$ be an isometry. Our task is to recover $f(X)$ for any $X \in \mathbb{C}$ if we know $f(A)$, $f(B)$ and $f(C)$.
Denote by d_A, d_B and d_C the distances from X to A, B and C, respectively. The point X belongs to the circles c_A, c_B and c_C centered at A, B and C and of radii d_A, d_B and d_C, respectively.
These circles have only one common point. Indeed, two circles with different centers may intersect either in two points, or in one point (and then the circles kiss each other at this point), or have no common point at all. Our circles have common point X, so the latter situation is not realized for any two of them.



If two of the circles are tangent to each other at X, then X is the only common point for these two circles and then a fortiori the only common point for all three circles (and we are done). If two circles have two common points, and the third circle passes through both of these points, then the points A, B and C belong to the locus of points which are at the same distance of these two points. As well known, this locus is a line (the mid-perpendicular line). But by assumption, A, B and C do not belong to the same line. Hence the intersection of the three circles consists of X.

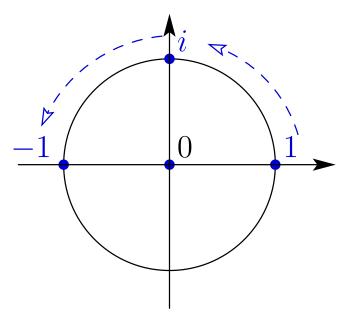
An isometry f maps a circle centered at a point P with radius R to a circle of the same radius centered at $f(P)$. Indeed, the circle is the locus of points which are at the distance R from P and the images of such points under an *isometry* have to be at distance R from $f(P)$, i.e., they have to belong to the circle centered at $f(P)$ of radius R.

Hence $f(X)$ belongs to the circles centered at $f(A)$, $f(B)$ and $f(C)$ of radii d_A, d_B and d_C, respectively. An isometry f maps triangle ABC to a congruent triangle. Since A, B and C are not collinear, the points $f(A)$, $f(B)$ and $f(C)$ are not collinear either. Therefore, there is only one possible position for $f(X)$, and we know how to find it: this is the only common point of the circles centered at $f(A)$, $f(B)$ and $f(C)$ and having the radii d_A, d_B and d_C, respectively. □

Theorem 1.G ensures that if two isometries $\mathbb{C} \to \mathbb{C}$ coincides with each other on a triple of non-collinear points, then these isometries coincide.

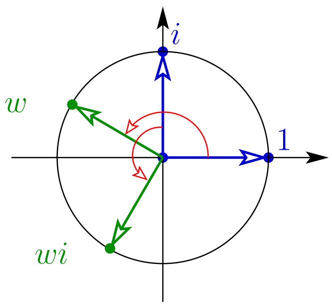
Now let us come back to the map $\mathbb{C} \to \mathbb{C} : z \mapsto z \cdot i$. Clearly,

- $0 \mapsto 0 \cdot i = 0$,
- $1 \mapsto 1 \cdot i = i$,
- $i \mapsto i \cdot i = -1$.



On the other hand, consider the counter-clockwise rotation of the plane $\mathbb{C}$ about 0 by the right angle. It maps 0, 1 and i exactly in the same way. It is an isometry. Hence, these two maps coincide.

1.H Theorem. *Let w be a complex number with $|w| = 1$. Then the map $\mathbb{C} \to \mathbb{C} : z \mapsto z \cdot w$ is the rotation about the origin by angle $\arg w$ in counter-clockwise direction.*



Proof. Consider the images of 0, 1 and i under this map:

- $0 \cdot w = 0$,
- $1 \cdot w = w$,
- $i \cdot w = w \cdot i$

The latter is the image of w under the multiplication by i. As we proved above, it is obtained from w by the rotation about the origin by the right angle in counter-clockwise direction. Its argument is obtained from $\arg w$ by adding $\frac{\pi}{2}$.

Compare this to the action of the rotation about the origin by angle $\arg w$ in counter-clockwise direction. For $z \neq 0$, the rotation does not change the distance to the origin, and adds $\arg w$ to the argument. Both maps map $0 \mapsto 0$. The image of 1 is w for both maps. The third point, i, has argument $\frac{\pi}{2}$, its image under the rotation by $\arg w$ has argument $\frac{\pi}{2} + \arg w$. $\square$

Finally, consider the case of the most general w. Assume that $w \neq 0$, $\operatorname{Im} w \neq 0$, and $|w| \neq 1$. Then $w = |w| \cdot \frac{w}{|w|}$. Then the map $\mathbb{C} \to \mathbb{C} : z \mapsto z \cdot w$ can be presented as a composition of two maps considered above: a dilation $z \mapsto z \cdot |w|$ followed by rotation $z \mapsto \frac{w}{|w|}$.

1.I Theorem. *Let z and w be complex numbers, $z \neq 0 \neq w$. Then*

$$\arg(z \cdot w) = \arg z + \arg w.$$

Proof. If $|w| = 1$, then by Theorem 1.H the map $\mathbb{C} \to \mathbb{C} : z \mapsto z \cdot w$ is a counter-clockwise rotation by $\arg w$. Hence, $\arg(z \cdot w) = \arg z + \arg w$.

In general case, $z \cdot w = z \cdot \left(\frac{w}{|w|} \cdot |w|\right) = \left(z \cdot \frac{w}{|w|}\right) |w|$. Multiplication by real positive number $|w|$ does not change the argument. Therefore

$$\arg(z \cdot w) = \arg\left(\left(z \cdot \frac{w}{|w|}\right) |w|\right) = \arg\left(z \cdot \frac{w}{|w|}\right).$$

Since $|\frac{w}{|w|}| = \frac{|w|}{|w|} = 1$, we can apply the result discussed above, so

$$\arg\left(z \cdot \frac{w}{|w|}\right) = \arg z + \arg \frac{w}{|w|}.$$

Further,

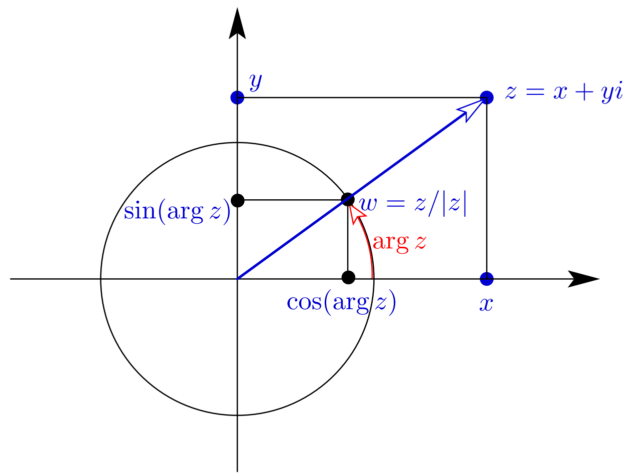
$$\arg \frac{w}{|w|} = \arg\left(w \cdot \frac{1}{|w|}\right) = \arg w,$$

since $\dfrac{1}{|w|}$ is a positive real number. Combining these equalities, we obtain the desired result. $\square$

1.9 Trigonometric form of a complex number

1.J Theorem. *The argument and the module of a complex number z characterize z completely. Namely, if $|z| = 0$ then $z = 0$, if $|z| \neq 0$, then*

$$z = |z|(\cos(\arg z) + i \sin(\arg z)). \tag{1}$$



Proof. For z with $|z| = 1$ formula (1) follows immediately from the definition of cos and sin. Recall that $\cos\varphi$ and $\sin\varphi$ are defined as coordinates of the point on the unit circle centered at 0 such that the counter-clockwise angle subtended between the x-axis and the direction to this point is φ. The point z with $|z| = 1$ lies on the unit circle, the angle φ is $\arg z$, and $z = \cos\varphi + i\sin\varphi$.

Assume that $z \neq 0$ and $|z| \neq 1$. Since $z \neq 0$, we can consider $w = \frac{z}{|z|}$. Obviously, $|w| = |\frac{z}{|z|}| = |z \cdot \frac{1}{|z|}| = |z|\frac{1}{|z|} = 1$. By applying the formula to w, we get

$$w = \cos(\arg w) + i\sin(\arg w).$$

Notice that $\arg w = \arg z$, since $w = \frac{1}{|z|}z$ and therefore z and w lie on the same ray which starts at 0. Hence, we can rewrite the formula $w = \cos(\arg w) + i\sin(\arg w)$ as

$$\frac{z}{|z|} = \cos(\arg z) + i\sin(\arg z).$$

Multiplying both sides of this formula by $|z|$, we obtain the required result.

If $z = 0$, then $\arg z$ is not defined, and formula (1) does not make sense. However in this case $z = |z|$, and thus $|z|$ characterizes z alone. $\square$

A presentation of a complex number z as $r(\cos\varphi + i\sin\varphi)$ with real $r > 0$ and φ is called a *trigonometric form* of z. As follows from Theorem 1.J, here

$r = |z|$ and $\varphi = \arg z$. Any complex number $z \neq 0$ can be presented in trigonometric form.

Since $\arg z$ is defined by z only up to addition of $2\pi n$ with $n \in \mathbb{Z}$, the trigonometric form also is not defined by z, it depends on the choice of representative for $\arg z$.

The trigonometric form is multiplication friendly in the following sense: given trigonometric forms of complex numbers z and w, one can easily find a trigonometric form of their product $z \cdot w$. Indeed, by Theorem 1.F, $|z \cdot w| = |z| \cdot |w|$, as for the argument, and, by Theorem 1.I, $\arg(z \cdot w) = \arg z + \arg w$. Therefore

$$z \cdot w = |z| \cdot |w|(\cos(\arg z + \arg w) + i \sin(\arg z + \arg w)). \tag{2}$$

1.10 Trigonometric addition formulas

In this section we consider applications to trigonometry.

1.K Theorem. *For any real numbers φ and ψ,*

$$\cos(\varphi + \psi) = \cos\varphi \cdot \cos\psi - \sin\varphi \cdot \sin\psi \tag{3}$$
$$\sin(\varphi + \psi) = \sin\varphi \cdot \cos\psi + \cos\varphi \cdot \sin\psi \tag{4}$$

Proof. Let $z = \cos\varphi + i \sin\varphi$ and $w = \cos\psi + i \sin\psi$. Then by (2),

$$zw = \cos(\varphi + \psi) + i \sin(\varphi + psi).$$

On the other hand,

$$\begin{aligned} zw &= (\cos\varphi + i \sin\varphi)(\cos\psi + i \sin\psi) \\ &= (\cos\varphi \cdot \cos\psi - \sin\varphi \cdot \sin\psi) + i(\sin\varphi \cdot \cos\psi + \cos\varphi \cdot \sin\psi) \end{aligned}$$

Comparison of these two formulas gives the desired result. □

Corollaries.

$$\cos(\varphi-\psi)=\cos\varphi\cdot\cos\psi+\sin\varphi\cdot\sin\psi \tag{5}$$
$$\sin(\varphi-\psi)=\sin\varphi\cdot\cos\psi-\cos\varphi\cdot\sin\psi \tag{6}$$
$$\cos 2\varphi=\cos^2\varphi-\sin^2\varphi \tag{7}$$
$$\sin 2\varphi=2\sin\varphi\cos\varphi \tag{8}$$
$$\tan(\varphi+\psi)=\frac{\tan\varphi+\tan\psi}{1-\tan\varphi\tan\psi} \tag{9}$$

2 Vector spaces

2.1 Coordinate vector space $\mathbb{R}^n$

Let n be a natural number. Denote by $\mathbb{R}^n$ the set of n-element sequences of real numbers. In formula it can be written as follows: $\mathbb{R}^n=\{(x_1,\dots,x_n)\mid x_i\in\mathbb{R} \text{ for } i=1,\dots n\}$.

For example, $\mathbb{R}^2$ is the set of ordered pairs of real numbers. Here are some of its elements: $(1,2)$, $(-1.3,52)$, $(0,\sqrt{7})$, $(0,0)$, $(\pi,-\log 22)$. We met this set in the definition of complex numbers. Recall that complex numbers were formally defined as ordered pairs of real numbers. Thus, as a set, the set $\mathbb{C}$ of all complex numbers coincides with $\mathbb{R}^2$.

Elements of $\mathbb{R}^n$ are called real n-*tuples* of real numbers. The jth element x_j of an n-tuple $(x_1,\dots,x_n)$ is called the jth coordinate of this n-tuple. The whole set $\mathbb{R}^n$ of real n-tuples is called the real *coordinate space* of dimension n.

When talking about n-tuples of real numbers, we often do not mention the n real numbers forming it, but denote an n-tuple by a single letter. Say, $(x_1,\dots,x_n)$ is denoted by x. We write $x=(x_1,\dots,x_n)$, $x\in\mathbb{R}^n$.

The operation of addition of complex numbers (which were considered as pairs of real numbers) are generalized to $\mathbb{R}^n$ with any n. Namely, for $x=(x_1,\dots,x_n)$ and $y=(y_1,\dots,y_n)$ we define

$$x+y=(x_1+y_1,\dots,x_n+y_n).$$

This addition of n-tuples can be considered as a map of the set of pairs of n-tuples to the set of n-tuples, that is a map $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$.

The operation of multiplication of complex numbers does not admit a single reasonable generalization in any n. However multiplication of a complex number by a real number is very simple. (Recall that $r \cdot (x, y) = (rx, ry)$ for $r \in \mathbb{R}$ and $(x, y) \in \mathbb{C}$.) It admits the following straightforward generalization:

$$r \cdot (x_1, \dots, x_n) = (rx_1, \dots, rx_n) \text{ for } r \in \mathbb{R}, (x_1, \dots, x_n) \in \mathbb{R}^n.$$

If $x_1, \dots, x_n$ is denoted by x, then the n-vector $(rx_1, \dots, rx_n)$ is denoted by rx. It is called the product of n-vector $x = (x_1, \dots, x_n)$ by r. We may consider this multiplication as a map $\mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$.

Thus, we have in $\mathbb{R}^n$ two operations: addition

$$\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n : ((x_1, \dots, x_n), (y_1, \dots, y_n)) \mapsto (x_1 + y_1, \dots, x_n + y_n)$$

and multiplication by real numbers

$$\mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n : (r, (x_1, \dots, x_n)) \mapsto (rx_1, \dots rx_n).$$

These two operations have the same properties which we already meet when we studied complex numbers. Namely,

Associativity of addition: $(x + y) + z = x + (y + z)$ for any $x, y, z \in \mathbb{R}^n$;

Commutativity of addition: $x + y = y + x$ for any $x, y \in \mathbb{R}^n$;

Zero: There is an element $(0, \dots, 0)$ of $\mathbb{R}^n$ made of zeros and denoted by 0 such that $x + 0 = x$ for any $x \in \mathbb{R}^n$;

Additive inversion: for each n-vector $x = (x_1, \dots, x_n) \in \mathbb{R}^n$, there is an n-vector $(-x_1, \dots, -x_n)$, which is denoted by $-x$, such that $x+(-x) = 0$;

Associativity of multiplication. $(r_1 r_2)x = r_1(r_2 x)$ for any $r_1, r_2 \in \mathbb{R}$ and $x \in \mathbb{R}^n$;

Distributivity. $r(x + y) = rx + ry$ for any $r \in \mathbb{R}$ and $x, y \in \mathbb{R}^n$;

Distributivity. $(r_1 + r_2)x = r_1 x + r_2 x$ for any $r_1, r_2 \in \mathbb{R}$ and $x \in \mathbb{R}^n$;

Multiplication by one. $1 \cdot x = x$ for any $x \in \mathbb{R}^n$.

Similar mathematical structure appear quite often. For example, for a fixed set X one can consider the set of all real valued functions $X \to \mathbb{R}$. For any two functions $f, g : X \to \mathbb{R}$ we can define a function $f + g$ by formula $(f+g)(x) = f(x)+g(x)$ for any $x \in X$; for any real number r and a function $f : X \to \mathbb{R}$ define a function rf by formula $(rf)(x) = r(f(x))$. One can easily check that these operation have the same properties as formulated above.

This construction alone gives a huge collection of examples, as we can take different sets X. Furthermore, one can take instead of arbitrary functions more special functions. Say, if $X = \mathbb{R}$, take only continuous functions, or only polynomial functions, or only linear functions. All these sets are closed with respect to addition of functions and multiplication by a number: the sum of two functions of each of these types is a function of the same type, the same for product of a function by a number. Moreover, there are sets with addition and multiplication by numbers which come from absolutely other sources. This motivated introduction of a general axiomatic notion of vector space introduced below.

2.2 Vector space, the general notion

Let V be a set, equipped with two operations discussed below.

The first of them is called *addition*. This is a map $V \times V \to V$. It assigns to a pair (u, v) of elements of V an element of V, which is denoted by $u + v$, like the usual sum of numbers.

Let the addition have the following four properties:

1. **Associativity.** $(u + v) + w = u + (v + w)$ for any $u, v, w \in V$;
2. **Commutativity.** $u + v = v + u$ for any $u, v \in V$;
3. **Zero.** There exists an element of V denoted by 0 such that $u + 0 = u$ for any $u \in V$;

4. **Additive inversion.** for each $u \in V$ there exists an element of V which is denoted by $-u$ such that $u + (-u) = 0$.

The second operation is a map $\mathbb{R} \times V \to V$. It assigns to a pair (r, u) which is formed by a number $r \in \mathbb{R}$ and an element u of V an element of V denoted by ru and called the *product* of r by u. Let, together with the addition, the multiplication have the following properties:

5. **Associativity of multiplication.** $(r_1 r_2)u = r_1(r_2 u)$ for any $r_1, r_2 \in \mathbb{R}$ and $u \in V$;
6. **Distributivity.** $r(u + v) = ru + rv$ for any $r \in \mathbb{R}$ and $u, v \in V$;
7. **Distributivity.** $(r_1 + r_2)u = r_1 u + r_2 u$ for any $r_1, r_2 \in \mathbb{R}$ and $u \in V$;
8. **Multiplication by one.** $1 \cdot u = u$ for any $u \in V$.

The eight properties listed above are called the *axioms of vector space*. If they hold true, V is called a *vector space* (over $\mathbb{R}$), its elements are called *vectors*. In a vector space, the addition of vectors and multiplication of vector by a number are called *linear operations* . The set $\mathbb{R}^n$ discussed above is a vector space.

2.3 The simplest consequences of axioms

The third axiom claims that in a vector space V there exists a special element 0 such that $0 + u = u$ for any $u \in V$. The axioms do not claim explicitly that such element is unique. However, it follows from the axioms.

2.A. Uniqueness of zero. *In any vector space V, the vector $0 \in V$ such that $0 + u = u$ for any $u \in V$ is unique.*

Proof. Assume that there are two elements, 0_1 and 0_2, which share this property, that is $0_1 + u = u$ and $0_2 + u = u$ for any $u \in V$. Then $0_1 + 0_2 = 0_2$ and $0_2 + 0_1 = 0_1$. By commutativity of addition, $0_1 + 0_2 = 0_2 + 0_1$. Hence $0_2 = 0_1 + 0_2 = 0_2 + 0_1 = 0_1$. $\square$

2.B. Uniqueness of additive inverse. *For any vector $u \in V$, the vector which is additive inverse to $u \in V$ is unique.*

Proof. Assume that there are two element, v_1 and v_2, which are both additive inverse to u, that is $u + v_1 = 0$ and $u + v_2 = 0$. Then consider the vector $v_1 + u + v_2$. On one hand, $v_1 + u + v_2 = v_1 + (u + v_2) = v_1 + 0 = v_1$. On the other hand, $v_1 + u + v_2 = (v_1 + u) + v_2 = (u + v_1) + v_2 = 0 + v_2 = v_2$. Hence $v_1 = v_2$. $\square$

2.C. Multiplication by number zero. $0 \cdot u = 0$ *for any vector $u \in V$.*

Proof. First, observe that since $0+0 = 0$, we have $0 \cdot u = (0+0)u = 0 \cdot u + 0 \cdot u$. Now let us add to both sides of the equality $0 \cdot u = 0 \cdot u + 0 \cdot u$ the vector additive inverse to $0 \cdot u$. This turns the equality into $0 \cdot u + 0 = 0$. By the definition of 0, the left hand side of the latter equality is $0 \cdot u$. $\square$

2.D. Multiple of the zero vector. $r \cdot 0$ *is the zero vector for any $r \in \mathbb{R}$.*

Proof. $r0 = r(0 + 0) = r0 + r0$. Let us add to both sides of the equality $r \cdot 0 = r \cdot 0 + r \cdot 0$ the vector additive inverse to $r \cdot 0$. This gives the equality $0 = r \cdot 0$. $\square$

2.E. Multiplication by negative one. *Let V be a vector space and $u \in V$. Then $(-1)u$ is the additive inverse to u.*

Proof. We have to prove that $u + (-1)u = 0$. Indeed, $u + (-1)u = 1u + (-1)u = (1 + (-1))u = 0u = u$. $\square$

2.F. Subtraction. *For any vectors $u, v \in V$ there exists a unique solution of equation $x + u = v$.*

Proof. The vector $v + (-u)$ is a solution for the equation $x + u = v$. Indeed, $(v + (-u)) + u = v + ((-u) + u) = v + 0 = v$. Assume that x_1 and x_2 are two solutions. Then $x_1 + u = x_2 + u$. By adding $-u$ to both sides of this equality, we get $x_1 = x_2$. $\square$

In the usual arithmetic, the subtraction $a - b$ is defined as the solution of equation $x + b = a$, and the solution can be identified as in Proposition 2.F as $a + (-b)$. Here similarly we define difference $v - u$ of vectors as the solution of equation $x + u = v$ and observe that $v - u = v + (-u)$.

2.4 Subspaces

Let V be a vector space. A subset $W \subset V$ is called a ***vector subspace*** of V if for any vectors $u, v \in W$ their sum $u + v$ also belongs to W and for any $u \in W$ and any real number r the product ru belongs to W.

This property is described by saying that W is ***closed*** with respect to the linear operations of V, meaning that the operations do not lead out of the subset.

It is useful to re-phrase this as follows. For any set $W \subset V$ consider the restriction of the addition $V \times V \to V$ to $W \times W \subset V \times V$. This is a map $W \times W \to V$. The fact that W is closed with respect to the addition means that the image of this map is contained in W. Thus the addition in V determines a map $W \times W \to W$, provided that W is a vector subspace of V. Similarly, the multiplication by numbers $\mathbb{R} \times V \to V$ in V determines a map $\mathbb{R} \times W \to W$.

2.G. A vector subspace is a vector space. *Let V be a vector space and $W \subset V$ be its subspace. Then W with the maps $W \times W \to W$ and $\mathbb{R} \times W \to W$, which are determined by the linear operations in V, is a vector space on its own.*

Proof. We have to prove that the axioms of vector space hold true. Associativity and commutativity of addition, associativity of multiplication, distributivities hold true because they are literally special cases of the same properties of the ambient space. Further, for each vector $u \in W$, the additive inverse vector $-u$ can be obtained from u by multiplying it by -1 (indeed, $u + (-1)u = 1u + (-1)u = (1 + (-1))u = 0u = u$). Hence, $-u \in W$, as this is a product of u by a number -1. Then, $0 \in W$, because 0 is the sum of any $u \in W$ with $-u$, which as we have just seen also belongs to W. $\square$

In any vector space, there is the smallest vector subspace. It consists of a single element 0. This subspace is denoted also by 0. In any vector space V, there is also the largest subspace, the space V itself.

Exercises

1. Prove that the intersection of any family of vector subspaces of a vector space V is also a vector subspace of V.

2. Find an example of two vector subspaces $\mathbb{R}^2$, such that their union is not a vector subspace of V.

3 Linear maps

3.1 Definition

Let V and W be vector spaces. A map $f : V \to W$ is said to be *linear* if it satisfy the following two requirements:

Additivity $f(u+v) = f(u) + f(v)$ for any $u, v \in V$;

Homogenuity $f(ru) = rf(u)$ for any $u \in V$ and $r \in \mathbb{R}$.

These two requirements mean that a linear map respects the linear operations in V and W. A linear map also respect the zero. There is no need to require this separately, because it follows from additivity. Namely, the following holds true:

3.A. A linear map maps zero to zero. *Any linear map $f : V \to W$ maps $0 \mapsto 0$.*

Proof. Indeed, $f(0) = f(0+0) = f(0) + f(0)$. Add $-f(0)$ to both sides of the equality $f(0) = f(0) + f(0)$. This turns the equality into $0 = f(0)$. □

3.B. A linear map maps inverse to inverse. *For any linear map $f : V \to W$ and any $u \in V$, $f(-u) = -f(u)$.*

Proof. By Proposition 2.E, $-u = (-1)u$. Hence $f(-u) = f((-1)u) = (-1)f(u) = -f(u)$. □

3.2 The simplest examples of linear maps

1. The zero map. For any vector spaces V and W, consider the map which sends any vector $u \in V$ to $0 \in W$. The requirements from the definition of linear map is satisfied. Indeed, $f(u+v) = 0$ and $f(u) + f(v) = 0 + 0 = 0$, $f(ru) = 0$ and $rf(u) = r \cdot 0 = 0$. $\square$.

2. The identity map. For any vector space V, the identity map $\mathrm{id} : V \to V$ (that is the map which sends each $u \in V$ to itself) is a linear map. The verification is straightforward.

3. Dilation and contraction maps. Let $c \in \mathbb{R}$ and V be any vector space. The map $f : V \to V : u \to c \cdot u$ is a linear map. Indeed, $f(u+v) = c(u+v) = cu + cv = cf(u) + cf(v)$ and $f(ru) = c \cdot (ru) = r \cdot (cu) = r \cdot f(u)$ $\square$.

4. Inclusion map. Let W be a subspace of a vector space V. Then the inclusion map $W \to V$ is linear. Indeed, the inclusion map maps each vector $u \in W$ to the same vector, but considered as an element of V and the linear operations in W are the same as in V. $\square$

3.3 Two important subspaces determined by a linear map

Let $f : V \to W$ be a linear map. In this section we introduce a subspace of V and a subspace of W, which are determined by f and to a great extend characterize it. We start with a subspace of W.

The image of a linear map

The image of a map $f : V \to W$ is the set

$$\{w \in W \mid w = f(v) \text{ for some } v \in V\}.$$

It is denoted in two ways: first, there is a general notation $f(V)$ which used in any part of mathematics and applicable to any map f; second, the image of linear map f is denoted by $\operatorname{Im} f$.

By the definition of surjectivity, a map $f : V \to W$ is surjective if and only if $f(V) = W$.

3.C. *If V and W are vector spaces and $f : V \to W$ is a linear map, then* $\operatorname{Im} f$ *is a vector subspace of* W

Proof. Exercise. Prove this. $\square$

The kernel of a linear map

For a linear map $f : V \to W$, the set $\{u \in V \mid f(u) = 0\}$ is called the ***kernel of*** f and denoted by $\operatorname{Ker} f$. The kernel of f can be defined in words as the pre-image of 0, or in a formula, $\operatorname{Ker} f = f^{-1}(0)$.

3.D Proposition. *For any linear map $f : V \to W$, the set* $\operatorname{Ker} f$ *is a vector subspace of V.*

Proof. Indeed, if $u, v \in \operatorname{Ker} f$, then $f(u) = 0$ and $f(v) = 0$, hence $f(u+v) = f(u) + f(v) = 0 + 0 = 0$, and $u + v \in \operatorname{Ker} f$; if $u \in \operatorname{Ker} f$ and $r \in \mathbb{R}$, then $f(ru) = rf(u) = r0 = 0$ and hence $ru \in \operatorname{Ker} f$. $\square$

Clearly, the map $f : V \to W$ is zero, if and only if $\operatorname{Ker} f = V$.

3.E Theorem. *A linear map $f : V \to W$ is injective if and only if* $\operatorname{Ker} f = 0$.

Proof. By the definition of injectivity, f is injective, iff the preimage of each $v \in W$ consists of at most one element. As a vector subspace, $\operatorname{Ker} f$ must contain 0. Thus, if f is injective, then $\operatorname{Ker} f = 0$.

Let us prove the converse. Assume that $\operatorname{Ker} f = 0$. Let $u, v \in V$ and $f(u) = f(v)$. Then $f(u + (-v)) = f(u) + f(-v) = f(u) + (-f(v)) = f(v) + (-f(v)) = 0$. Hence $u - v \in \operatorname{Ker} f$. Hence $u - v = 0$ and $u = v$. $\square$

3.4 Linear maps from a coordinate space

In this section we will study linear maps from a coordinate space $\mathbb{R}^n$ to an arbitrary vector space W. To begin with, we present a formula which describes such a map. The formula looks quite special. However after that we will see that any linear map $\mathbb{R}^n \to W$ is described by a formula of this type.

3.F. *Let W be a vector space and let $u = (u_1, \dots, u_n)$ be any n-tuples of vectors of W. Then the map*

$$L_u : \mathbb{R}^n \to W : (x_1, \dots, x_n) \mapsto x_1 u_1 + \dots + x_n u_n.$$

is linear.

Proof. We have to verify additivity and homogenuity of this map. Let $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ and $y = (y_1, \dots, y_n) \in \mathbb{R}^n$. Additivity:

$$\begin{aligned} L_u(x+y) = (x_1+y_1)u_1 + \dots + (x_n+y_n)u_n \\ = x_1u_1 + y_1u_1 + \dots x_nu_n + y_nu_n \\ = x_1u_1 + \dots + x_nu_n + y_1u_1 + \dots + y_nu_n \\ = L_u(x) + L_u(y) \end{aligned}$$

Homogenuity:

$$L_u(rx) = rx_1u_1 + \dots + rx_nu_n = r(x_1u_1 + \dots + x_nu_n) = rL_u(x)$$

$\square$

Let us denote by $e_i \in \mathbb{R}^n$ the n-tuple of real numbers, whose ith coordinate is 1 and all other coordinates are 0. So, $e_1 = (1, 0, \dots, 0)$, $e_2 = (0, 1, 0, \dots, 0)$, $\dots e_n = (0, \dots, 0, 1)$.

It is easy to check that any $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ can be presented as $x_1e_1 + \dots x_ne_n$. Indeed, in the sum $x_1e_1 + \dots x_ne_n$ the ith summand has all coordinates 0, besides the ith one, which is $x_i \cdot 1 = x_i$. Hence the sum has exactly the same coordinates as x.

3.G Proposition. *Any linear map $L : \mathbb{R}^n \to W$ is L_u for $u = (u_1, \dots, u_n)$, where $u_1 = L(e_1)$, $\dots$, $u_n = L(e_i)$.*

Proof. Indeed, for $x = (x_1, \dots, x_n)$

$$
\begin{aligned}
L(x) = L(x_1e_1 + \cdots + x_ne_n) \\
&= L(x_1e_1) + \cdots + L(x_ne_n) \\
&= x_1L(e_1) + \cdots + x_nL(e_n) \\
&= x_1u_1 + \cdots + x_nu_n = L_u(x).
\end{aligned}
$$

□

Thus, linear maps from a coordinate vector space $\mathbb{R}^n$ to an arbitrary vector space W are encoded by n-tuples of vectors $u_1, \dots, u_n$ of V.

4 Dimensions

4.1 Linear dependence

A vector $b \in V$ is said to be linearly dependent on vectors $a_1, \dots, a_n \in V$ if it can be obtained by applying a sequence of linear operations to $a_1, \dots, a_n$. Of course, any such vector can be presented as $x_1a_1 + \cdots + x_na_n$ for some real numbers $x_1, \dots, x_n$. Hence, a vector b linearly depends on $a_1, \dots, a_n$, if it belongs to the image of the linear map $\mathbb{R}^n \to V$ defined by $a_1, \dots, a_n$.

A vector $x_1a_1 + \cdots + x_na_n$ is called a *linear combination* of $a_1, \dots, a_n$.

The set of all linear combinations of vectors $a_1, \dots, a_n$ is called *linear hull* or *linear span* of $a_1, \dots, a_n$ and denoted by $\mathrm{Lin}(a_1, \dots, a_n)$. It coincides with the image of the linear map $L_a : \mathbb{R}^n \to V$ defined by $a = (a_1, \dots, a_n)$. Hence, this is a vector subspace of V.

A collection $a_1, \dots, a_n$ is said to *generate* V if $V = \mathrm{Lin}(a_1, \dots, a_n)$.

4.2 Linear independence

Vectors $a_1, \dots, a_n$ are said to be *linearly independent* if none of them depends on the others.

A linear combination, in which not all the coefficients are zero, is called *non-trivial*. Therefore, $L_{a_1,\dots,a_n} : \mathbb{R}^n \to V$ is not injective if and only if there exists a non-trivial linear combination of $a_1,\dots,\ a_n$ which equals zero.

4.A Proposition. *Vectors $a_1, \dots, a_n$ are linearly independent if and only if there is no non-trivial linear combination of $a_1,\dots,\ a_n$ which is equal to zero.*

Proof. Assume that vectors $a_1,\dots,\ a_n$ are **not** linearly independent. Then one of them is a linear combination of the others. Without loss of generality, we may assume that this is the last vector a_n, so $a_n = x_1a_1 \dots x_{n-1}a_{n-1}$. Then $x_1a_1 + \dots + x_{n-1}a_{n-1} + (-1)a_n = 0$. In the linear combination $x_1a_1 + \dots + x_{n-1}a_{n-1} + (-1)a_n$ at least the last coefficient is not zero (because it is -1.) Hence we have a non-trivial linear combination which is zero.

Conversely, let there exist a linear combination $x_1a_1 + \dots + x_na_n$ equal zero, in which at least one coefficient is not zero. Without loss of generality we may assume that $x_n \neq 0$. Then a_n is linearly dependent on $a_1,\ \dots,\ a_{n-1}$. Indeed, in the equality $x_1a_1 + \dots + x_na_n = 0$ move the last term of the left hand side to the right hand side and divide both sides by $-x_n$. It gives

$$-\frac{x_1}{x_n}a_1 + \dots - \frac{x_{n-1}}{x_n} = a_n.$$

□

4.B Theorem. *Vectors $a_1, \dots, a_n \in V$ are linearly independent if and only if the map $L_a : \mathbb{R}^n \to V$ with $a = (a_1, \dots, a_n)$ is injective.*

Proof. By Proposition 3.E, $L_a : \mathbb{R}^n \to V$ is injective if and only if $\operatorname{Ker} L_a = 0$. By the definition of L_a, the kernel of L_a consists of $(x_1, \dots, x_n)$ such that $x_1a_1 + \dots x_na_n = 0$.

Thus, $L_a : \mathbb{R}^n \to V$ is not injective if and only if there exist real numbers $x_1, \dots, x_n$, which are not all equal zero, such that the linear combination $x_1a_1 + \dots x_na_n$ equals zero. □

4.3 Basis of a vector space

A vector space V is said to be *infinite-dimensional* if it does not admit a finite generating set. Below we will work mainly with *finite-dimensional* vector spaces.

A basis of a vector space V is a finite sequence $a_1, \dots a_n$ of its vectors, which generate V and are linearly independent.

4.C Theorem. *Let V be a vector space. An n-tuple $a = (a_1, \dots, a_n)$ of vectors of V is a basis of V if and only if the linear map $L_a : \mathbb{R}^n \to V$ is a bijection.*

Proof. We know from Section 4.1 that L_a is surjective if and only if $a_1, \dots, a_n$ generate V. By Theorem 4.B L_a is injective if and only if vectors $a_1, \dots, a_n$ are linearly independent. □

Theorem 4.C means that a basis of vector space allows to identify a vector space with the coordinate vector space $\mathbb{R}^n$. Linear operations in a vector space with a chosen basis are identified with linear operations in $\mathbb{R}^n$.

The basis is not unique, so there is no standard, canonical identification. Our goal in this section is to prove that the number of elements in a basis of a vector space depends only on the vector space, but not on the choice of basis. In particular, it would imply that from the point of view of linear algebra $\mathbb{R}^n$ with different n differ from each other, there is no bijective linear map between $\mathbb{R}^p$ and $\mathbb{R}^q$ if $p \neq q$.

4.D Theorem. *Let $a_1, \dots, a_p$ be linearly independent vectors in a vector space generated by q vectors. Then $p \leq q$.*

Proof. Let $b_1, \dots, b_q$ be generators of this vector space. Since $a_1 \in \mathrm{Lin}(b_1, \dots, b_q)$, it can be presented as

$$a_1 = x_1 b_1 + \dots + x_q b_q.$$

Vector a_1 is not zero, since it belongs to a system of linearly independent vectors. Therefore at least one of the coefficients $x_1, \dots, x_q$ is not zero. Without loss of generality, we may assume that $x_1 \neq 0$. Then the equality $a_1 = x_1 b_1 + \dots + x_q b_q$ can be transformed into an expression for b_1:

$$b_1 = \frac{1}{x_1} a_1 + \frac{-x_2}{x_1} b_2 + \dots + \frac{-x_q}{x_1} b_q.$$

Thus $b_1 \in \mathrm{Lin}(a_1, b_2, \dots, b_q)$. Therefore

$$\mathrm{Lin}(b_1, \dots, b_q) = \mathrm{Lin}(a_1, b_1, \dots, b_q) = \mathrm{Lin}(a_1, b_2, \dots, b_q).$$

Thus, we have replaced one of the generators (namely, b_1) by one of the vectors from the system of linearly independent vectors (namely, a_1). Then we repeat this process and replace in the same way one of the vector b_2 by a_2. In this step, we have to take efforts for keeping b_1 in the system of vectors. It is possible, since in the expression of b_2 as a linear combination of b_1, a_2, $\dots$, a_p at least one of the coefficients at $a_2,\dots,a_p$ is not zero, because otherwise b_2 would be dependent on b_1 alone, which would contradict to linear independence of $b_1, \dots, b_q$.

If $q > p$, then after repeating this process for p times we would replace all $a_1,\dots,a_p$ with $b_1,\dots,b_p$. Then $b_{p+1},\dots,b_q$ would be in $\mathrm{Lin}(b_1, \dots, b_p)$, which would contradict to linear independence of $b_1,\dots,b_q$. Hence $q \le p$. $\square$

Corollary. *Any two bases of a finite-dimensional vector space contain the same number of elements.*

The number of elements in a basis of a vector space V is called the *dimension* of V and denoted by $\dim V$.

4.4 How to build a basis

4.E Proposition. *Let $a_1, \dots, a_n$ be linearly independent vectors in V and $b \in V \setminus \mathrm{Lin}(a_1, \dots, a_n)$. Then vectors $b, a_1, \dots, a_n$ are linearly independent.*

Proof. If $b, a_1, \dots, a_n$ are linearly dependent, then there exists a non-trivial linear combination of them $xb + y_1a_1 + \dots + y_na_n$, which is equal to zero. Then $x \neq 0$, since otherwise this would be non-trivial zero linear combination of $a_1, \dots, a_n$ which is impossible, since $a_1, \dots, a_n$ are linearly independent. But then

$$b = \frac{(-1)}{x}(y_1a_1 + \dots + y_na_n) \in \mathrm{Lin}(a_1, \dots, a_n),$$

which contradicts to the assumption that $b \in V \setminus \mathrm{Lin}(a_1, \dots, a_n)$. $\square$

4.F Proposition. *Let V be a vector space. If a vector $b \in V$ linearly depends on $a_1, \dots, a_n \in V$, then* $\mathrm{Lin}(b, a_1, \dots, a_n) = \mathrm{Lin}(a_1, \dots, a_n)$.

Proof. Obviously, $\mathrm{Lin}(a_1, \dots, a_n) \subset \mathrm{Lin}(b, a_1, \dots, a_n)$. Let us prove the opposite inclusion. Take any element of $\mathrm{Lin}(b, a_1, \dots, a_n)$. It can be presented as a linear combination $xb+y_1a_1+\dots+y_na_n$ for some real $x, y_1, \dots, y_n$. Then $b = z_1a_1 + \dots + z_na_n$ for some $z_1, \dots, z_n \in \mathbb{R}$, since b linearly depends on $a_1, \dots, a_n$. By substituting this expression into $xb+y_1a_1+\dots+y_na_n$, we get $xb+y_1a_1+\dots+y_na_n = (xz_1+y_1)a_1+\dots(xz_n+y_n)a_n \in \mathrm{Lin}(a_1, \dots, a_n)$. $\square$

Theorem 4.D claims that the number of elements in any set of linearly independent vectors in a vector space is not greater than the number of vectors in a set of vectors generating this space. By Proposition 4.E, a system of linearly independent vectors that does not generate the vector space, can always be expanded to a larger system of linear independent vectors. If the vector space is finite-dimensional, then in this way we will construct a basis in a finite number of steps.

On the other hand, if vectors in a generating system are not linearly independent, then some of vectors can be removed from this system keeping the system generating. It can be done until we get a basis.

4.5 Coordinates

By Theorem 4.C, any basis $a = (a_1, \dots, a_n)$ of a vector space V provides a linear bijection $L_a : \mathbb{R}^n \to V$. This bijection is called a *coordinate system* in V determined by the basis a.

For each vector $u \in V$, the preimage $L_a^{-1}(u)$ is an n-tuple $x = (x_1, \dots, x_n)$ of real numbers such that $L_a(x) = u$. Numbers $x_1, \dots x_n$ a called the *coordinates* of vector u in basis a or in the corresponding coordinate system.

Recall that $L_a(x) = x_1a_1 + \dots + x_na_n$. Thus $x_1, \dots, x_n$ are coordinates of vector u in basis $a = (a_1, \dots, a_n)$ if

$$u = x_1a_1 + \dots + x_na_n$$

A coordinate system returns us from V to the coordinate space $\mathbb{R}^n$. Since the bijection L_a is linear, linear operations in V can be performed in the following way: first pull back all the vectors involved from V to $\mathbb{R}^n$, then perform the calculation in $\mathbb{R}^n$, then move the result to V again via L_a.

Appendix. Linear operations on linear maps

Addition of linear maps

Let V and W be vector spaces and let $f : V \to W$ and $g : V \to W$ be maps. Define $f + g : V \to W$ by formula $(f + g)(u) = f(u) + g(u)$.

4.G Proposition. *If f and g are linear maps, then the map $f + g$ is linear.*

Proof.

$$\begin{aligned}(f + g)(u + v) &= f(u + v) + g(u + v)\\ &= f(u) + f(v) + g(u) + g(v)\\ &= f(u) + g(u) + f(v) + g(v)\\ &= (f + g)(u) + (f + g)(v)\end{aligned}$$

$$\begin{aligned}(f + g)(ru) &= f(ru) + g(ru)\\ &= rf(u) + rg(u) = r(f(u) + g(u))\\ &= r((f + g)(u)).\end{aligned}$$

$\square$

Multiplication of a linear map by a number

Let V and W be vector spaces, $f : V \to W$ be a map and $c \in \mathbb{R}$. Define $cf : V \to W$ by formula $(cf)(u) = r(f(u))$.

4.H Proposition. *If f is a linear map, then the map cf is linear.*

Proof.

$$(cf)(u + v) = c(f(u + v)) = c(f(u) + f(v)) = cf(u) + cf(v)$$

$$(cf)(ru) = c(f(ru)) = c(rf(u)) = c \cdot r \cdot f(u) = r \cdot (c \cdot f(u))$$

$\square$

Vector spaces of linear maps

For vector spaces V and W, denote by $\mathcal{L}(V, W)$ the set of all linear maps $V \to W$. Above we have defined operations of addition and multiplication by a number in $\mathcal{L}(V, W)$.

Exercise. Verify that $\mathcal{L}(V, W)$ with these operations is a vector space (that is $\mathcal{L}(V, W)$ satisfy all the axioms of vector space).

Thus, any linear map $V \to W$ between two vector spaces is a vector of the appropriate vector space (made of all linear maps $V \to W$).