

# Изоморфизм

## Мотивация для изоморфизма

Ещё раз вспомним аксиоматическое определение поля комплексных чисел.

**Опр: 1.** Поле комплексных чисел называется поле  $\mathbb{C}$ , обладающее следующими свойствами:

- 1)  $\mathbb{R} \subset \mathbb{C}$ ;
- 2)  $i \in \mathbb{C}: i^2 = -1$ , этот элемент называется мнимой единицей;
- 3) **Условие минимальности:** Если  $K$  - подполе:  $\mathbb{R} \subseteq K \subseteq \mathbb{C}, i \in K \Rightarrow K = \mathbb{C}$ ;

Пока остаются открытыми вопросы: существует ли поле комплексных чисел и если существует, то оно одно такое или их много? Начнем с вопроса единственности. Могут ли быть единственными математические структуры, которые определены аксиоматически своими свойствами?

Пусть у нас есть поле  $\mathbb{C}$ , удовлетворяющее свойствам из определения выше. Все элементы кроме тех, что в  $\mathbb{R}$  взаимнооднозначно заменим на элементы какого-то другого множества. Например:

$$\forall z \in \mathbb{C} \setminus \mathbb{R}, z \mapsto (z, z) \Rightarrow \mathbb{C} \mapsto \mathbb{C}'$$

Над удвоенными копиями элементов исходного множества определим операции так, чтобы они в точности соответствовали операциям над оригинальными элементами:

$$\forall (z, z), (w, w) \in \mathbb{C}', (z, z) + (w, w) = (z + w, z + w)$$

$$\forall (z, z), (w, w) \in \mathbb{C}', (z, z) \cdot (w, w) = (z \cdot w, z \cdot w)$$

Следовательно,  $\mathbb{C}$  - тоже поле комплексных чисел.

Таким образом, такое же возможно для любых математических объектов/структур, которые определяются своими свойствами (то есть, аксиоматически), они не могут быть единственными в буквальном смысле слова. Одновременно с этим понятно, что представленные две модели поля комплексных чисел по сути своей ничем друг от друга не отличаются: между ними можно установить взаимнооднозначное соответствие, с помощью которого всё что можно сказать в одной модели переносится на другую.

Похожее построение делалось для  $\mathbb{R}$  в математическом анализе: с помощью Дедекиндова сечения и с помощью бесконечных десятичных дробей. В обеих моделях можно определить операции над действительными числами, отношение больше/меньше (то есть, всё что говорим про числа из  $\mathbb{R}$ ).

В математике важно не то из чего сделана та или иная математическая структура, а то - какими свойствами она обладает. Если две структуры неотличимы по своим свойствам (в рамках данной теории), то их можно отождествить между собой. Поэтому нужно иметь правильный способ отождествления две математических структур, которые с точки зрения своих свойств данной теории ведут себя абсолютно одинаково. Для таких отождествлений придуман изоморфизм.

## Изоморфизм

**Опр: 2.** Изоморфизм групп/колец/полей это отображение  $\varphi: A \rightarrow B$ , где  $A, B$  - две группы/два кольца/два поля, которое обладает следующими свойствами:

- 1)  $\varphi$  - взаимнооднозначно (биективно);
- 2)  $\varphi$  согласовано с алгебраическими операциями для соответствующих структур:

(а) **Группы:**

$$\forall x, y \in A, \varphi(x \circ y) = \varphi(x) \cdot \varphi(y)$$

где  $\circ$  - операция, заданная на группе  $A$  и  $\cdot$  - операция, заданная на группе  $B$ ;

(б) **Кольца/поля:**

$$\forall x, y \in A, \varphi(x \circ y) = \varphi(x) \cdot \varphi(y)$$

$$\forall x, y \in A, \varphi(x + y) = \varphi(x) \oplus \varphi(y)$$

где  $\circ$  - операция произведения, заданная на кольце/поле  $A$  и  $\cdot$  - операция произведения, заданная на кольце/поле  $B$ , а  $+$  - операция сложения, заданная на кольце/поле  $A$  и  $\oplus$  - операция сложения, заданная на кольце/поле  $B$ ;

Обозначение:  $\varphi: A \xrightarrow{\sim} B$  или  $\varphi: A \xrightarrow{\sim} B$ .

**Опр: 3.** Группы/кольца/поля называются изоморфными, если между ними существует изоморфизм.

Обозначение:  $A \simeq B \Leftrightarrow A$  изоморфно  $B$ .

**Пример:** Рассмотрим  $(\mathbb{R}, +)$  - группа и  $(\mathbb{R}^+, \cdot)$ , где  $\mathbb{R}^+ = \{y \in \mathbb{R} \mid y > 0\}$  - тоже будет группой (все аксиомы группы будут выполнены). Это две разные группы как геометрически (одна группа это прямая, другая группа это луч на этой прямой), так и алгебраически (в одной группе операция  $+$ , в другой операция  $\cdot$ ). Тем не менее эти группы изоморфны:

$$(\mathbb{R}, +) \simeq (\mathbb{R}^+, \cdot)$$

Построим изоморфизм  $\varphi: (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, \cdot)$  и проверим свойства:

$$\varphi(x) = e^x \Rightarrow \forall x, y \in \mathbb{R}, \varphi(x + y) = e^{x+y} = e^x \cdot e^y = \varphi(x) \cdot \varphi(y)$$

Следовательно, согласованность с операциями выполняется. Биективность вытекает из свойств экспоненты (непрерывность и строгая монотонность  $\Rightarrow$  работает теорема об обратной функции), обратная функция - логарифм.

Смысл изоморфизма: изоморфные математические структуры одинаковы по своим свойствам. Следовательно, их можно отождествить в рамках данной теории.

Нам не важно что у нас есть несколько моделей поля действительных чисел и не важно с какой из них работать, это всё равно по сути один и тот же объект  $\Rightarrow$  всё что мы можем сказать в одной модели, мы можем дословно перенести на другую модель и наоборот. Для  $\mathbb{R}$  это так. Так ли это для  $\mathbb{C}$ ?

## Единственность поля комплексных чисел

С учетом изоморфизма, первое свойство в определении поля комплексных чисел будет корректнее записать немного другим образом.

**Опр: 4. (Правильная формулировка):** Поле комплексных чисел называется поле  $\mathbb{C}$ , обладающее следующими свойствами:

- 1)  $\mathbb{C}$  содержит подполе, изоморфное  $\mathbb{R}$ :  $\mathbb{R} \simeq \mathbb{R}' \subset \mathbb{C}$ ;
- 2)  $i \in \mathbb{C}$ :  $i^2 = -1$ , этот элемент называется мнимой единицей;
- 3) **Условие минимальности:** Если  $K$  - подполе:  $\mathbb{R} \subseteq K \subseteq \mathbb{C}$ ,  $i \in K \Rightarrow K = \mathbb{C}$ ;

**Теорема 1.** Поле комплексных чисел единственно с точностью до изоморфизма.

□ Пусть  $\mathbb{C}'$  - другое поле комплексных чисел такое, что:

- 1)  $\mathbb{C}' \supset \mathbb{R}' \simeq \mathbb{R}$ ;
- 2)  $i' \in \mathbb{C}'$ :  $(i')^2 = -1$ ;
- 3)  $\mathbb{R}' \subseteq K' \subseteq \mathbb{C}'$ ,  $i' \in K' \Rightarrow K' = \mathbb{C}'$ ;

Отождествим  $\mathbb{R}'$  с  $\mathbb{R}$  с помощью изоморфизма и, заменив  $\mathbb{R}'$  на  $\mathbb{R}$ , мы можем считать, что  $\mathbb{C}' \supset \mathbb{R}$ .  
Конструкция изоморфизма  $\varphi: \mathbb{C} \xrightarrow{\sim} \mathbb{C}'$ :

$$\forall z = x + iy \in \mathbb{C}, x = \operatorname{Re}(z) \in \mathbb{R}, y = \operatorname{Im}(z) \in \mathbb{R}, \varphi(z) = x + i' \cdot y$$

Биективность  $\Leftrightarrow$  существование и единственность алгебраической формы записи комплексного числа (существование  $\Leftrightarrow$  сюръективность, единственность  $\Leftrightarrow$  инъективность):

$$\forall z \in \mathbb{C}, \exists! (x, y) \in \mathbb{R}^2: z = x + iy$$

$$\forall z' \in \mathbb{C}', \exists! (x, y) \in \mathbb{R}^2: z' = x + i'y$$

$$z \in \mathbb{C} \leftrightarrow (x, y) \in \mathbb{R}^2 \leftrightarrow z' \in \mathbb{C}' \Rightarrow z \leftrightarrow \varphi(z) = z'$$

Согласованность с операциями следует из того, что операции над комплексными числами сводится к операциям над  $\operatorname{Re}$  и  $\operatorname{Im}$ , а они одинаковы у  $z$  и  $\varphi(z)$ :

$$z_1 = x_1 + iy_1, z_2 = x_2 + iy_2 \in \mathbb{C} \Rightarrow \varphi(z_1) = x_1 + i'y_1, \varphi(z_2) = x_2 + i'y_2 \in \mathbb{C}'$$

$$z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2) \Rightarrow \varphi(z_1) + \varphi(z_2) = (x_1 + x_2) + i'(y_1 + y_2) = \varphi(z_1 + z_2)$$

$$z_1 \cdot z_2 = (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1) \Rightarrow \varphi(z_1) \cdot \varphi(z_2) = (x_1x_2 - y_1y_2) + i'(x_1y_2 + x_2y_1) = \varphi(z_1 \cdot z_2)$$

■

Остается вопрос про существование поля комплексных чисел. Существует ли хотя бы одно поле, удовлетворяющее трём свойствам? Для этого необходимо построить модель поля комплексных чисел - явно задать это множество  $\mathbb{C}$  (предъявить некоторую конструкцию), задать на нём операции, проверить что это будет поле и проверить три свойства из определения.

## Существование поля комплексных чисел

**Модель комплексных чисел:** Определим  $\mathbb{C} = \mathbb{R}^2$  и зададим операции сложения и умножения.

### Операции:

$$(+): \forall (x, y), (x', y') \in \mathbb{R}^2, (x, y) + (x', y') = (x + x', y + y');$$

$$(\cdot): \forall (x, y), (x', y') \in \mathbb{R}^2, (x, y) \cdot (x', y') = (xx' - yy', xy' + x'y);$$

### Проверим аксиом поля:

1) **Коммутативность сложения:**  $\forall (x, y), (x', y') \in \mathbb{R}^2$ :

$$(x, y) + (x', y') = (x + x', y + y') = (x' + x, y' + y) = (x', y') + (x, y)$$

2) **Коммутативность умножения:**  $\forall (x, y), (x', y') \in \mathbb{R}^2$ :

$$(x, y) \cdot (x', y') = (xx' - yy', xy' + x'y) = (x'x - y'y, x'y + xy') = (x', y') \cdot (x, y)$$

3) **Ассоциативность сложения:**  $\forall (x, y), (x', y'), (x'', y'') \in \mathbb{R}^2$ :

$$\begin{aligned} [(x, y) + (x', y')] + (x'', y'') &= ([x + x'] + x'', [y + y'] + y'') = \\ &= (x + [x' + x''], y + [y' + y'']) = (x, y) + [(x', y') + (x'', y'')] \end{aligned}$$

4) **Ассоциативность умножения:**  $\forall (x, y), (x', y'), (x'', y'') \in \mathbb{R}^2$ :

$$\begin{aligned} [(x, y) \cdot (x', y')] \cdot (x'', y'') &= (xx' - yy', xy' + x'y) \cdot (x'', y'') = \\ &= (xx'x'' - yy'x'' - xy'y'' - yx'y'', xx'y'' - yy'y'' + xy'x'' + x'yx'') = \\ &= (x, y) \cdot [(x', y') \cdot (x'', y'')] = (x, y) \cdot (x'x'' - y'y'', x'y'' + x''y') = \\ &= (xx'x'' - xy'y'' - yx'y'' - yx''y', xx'y'' + xx''y' + yx'x'' - yy'y'') = [(x, y) \cdot (x', y')] \cdot (x'', y'') \end{aligned}$$

5) **Дистрибутивность умножения относительно сложения:**  $\forall (x, y), (x', y'), (x'', y'') \in \mathbb{R}^2$ :

$$\begin{aligned} (x, y) \cdot [(x', y') + (x'', y'')] &= (x, y) \cdot (x' + x'', y' + y'') = (xx' + xx'' - yy' - yy'', xy' + xy'' + yx' + yx'') = \\ &= (xx' - yy', xy' + x'y) + (xx'' - yy'', xy'' + x''y) = \\ &= (xx' + xx'' - yy' - yy'', xy' + xy'' + x'y + x''y) = (x, y) \cdot [(x', y') + (x'', y'')] \end{aligned}$$

6) **Существование нулевого элемента:**  $\forall (x, y) \in \mathbb{R}^2$ :

$$\exists (0, 0) \in \mathbb{R}^2: (x, y) + (0, 0) = (x, y)$$

7) **Существование единичного элемента:**  $\forall (x, y) \in \mathbb{R}^2$ :

$$\exists (1, 0) \in \mathbb{R}^2: (x, y) \cdot (1, 0) = (x \cdot 1 - y \cdot 0, x \cdot 0 + y \cdot 1) = (x, y)$$

8) **Существование противоположного элемента:**  $\forall (x, y) \in \mathbb{R}^2$ :

$$\exists (-x, -y) \in \mathbb{R}^2: (x, y) + (-x, -y) = (x - x, y - y) = (0, 0)$$

9) **Существование обратного элемента:**  $\forall (x, y) \in \mathbb{R}^2, (x, y) \neq (0, 0)$ :

$$\exists (x, y)^{-1} = \left( \frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right) \in \mathbb{R}^2: (x, y) \cdot (x, y)^{-1} = \left( \frac{x \cdot x - y \cdot (-y)}{x^2 + y^2}, \frac{x \cdot (-y) + x \cdot y}{x^2 + y^2} \right) = (1, 0)$$

Таким образом, мы проверили, что  $\mathbb{C} = \mathbb{R}^2$  с введенными операциями является полем.

### Проверим свойства поля комплексных чисел:

1) Рассмотрим подмножество  $\mathbb{R} \times \{0\} = \{(x, 0) \mid x \in \mathbb{R}\} \subset \mathbb{R}^2$ . Проверим, что оно будет **подполем**:

(a) **Замкнутость относительно сложения:**  $\forall (x, 0), (x', 0) \in \mathbb{R} \times \{0\}$ :

$$(x, 0) + (x', 0) = (x + x', 0)$$

(b) **Замкнутость относительно умножения:**  $\forall (x, 0), (x', 0) \in \mathbb{R} \times \{0\}$ :

$$(x, 0) \cdot (x', 0) = (x \cdot x' - 0 \cdot 0, x \cdot 0 + x' \cdot 0) = (xx', 0)$$

(c) **Непустота подмножества:**

$$(0, 0) \in \mathbb{R} \times \{0\}$$

(d) **Существование противоположного элемента:**  $\forall (x, 0) \in \mathbb{R} \times \{0\}$ :

$$\exists (-x, 0) \in \mathbb{R} \times \{0\}: (x, 0) + (-x, 0) = (0, 0)$$

(e) **Число элементов в подмножестве больше 1:**

$$(0, 0), (1, 0) \in \mathbb{R} \times \{0\}, \forall x \in \mathbb{R}, (x, 0) \in \mathbb{R} \times \{0\}$$

(f) **Существование обратного элемента:**  $\forall (x, 0) \in \mathbb{R} \times \{0\}$ :

$$\exists (x, 0)^{-1} = \left( \frac{1}{x}, 0 \right): (x, 0) \cdot (x, 0)^{-1} = (1, 0)$$

Изоморфизм:  $\psi: \mathbb{R} \xrightarrow{\sim} \mathbb{R} \times \{0\}, \psi(x) = (x, 0) \Rightarrow$  видим, что пары складываются и перемножаются как действительные числа, а биективность очевидна  $\Rightarrow$  мы имеем подполе, изоморфное полю действительных чисел;

2) **Мнимая единица** принадлежит этому полю:

$$i \in \mathbb{R}^2, i = (0, 1) \Rightarrow i^2 = (0, 1) \cdot (0, 1) = (-1, 0) = -(1, 0)$$

3) **Минимальность:** пусть  $K$  - подполе такое, что:

$$\mathbb{R} \times \{0\} \subseteq K \subseteq \mathbb{R}^2 \Rightarrow \forall x \in \mathbb{R}, (x, 0) \in K, i \in K \Rightarrow (0, 1) \in K \Rightarrow$$

$$\Rightarrow \forall x, y \in \mathbb{R}, (x, 0) + (0, 1) \cdot (y, 0) \in K \Rightarrow$$

$$\Rightarrow (x, 0) + (0, 1) \cdot (y, 0) = (x, 0) + (0 \cdot y - 1 \cdot 0, y \cdot 1 + 0 \cdot 0) = (x, 0) + (0, y) = (x, y) \in K \Rightarrow K = \mathbb{R}^2$$

**Заключение:** множество пар  $\mathbb{R}^2$  с введёнными выше операциями является моделью поля  $\mathbb{C}$  и теорема существования поля комплексных чисел - доказана.

**Упр. 1.** Построить другую модель поля комплексных чисел. Рассмотреть подмножество:

$$\text{Mat}_2(\mathbb{R}) \supset \mathbb{C}' = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid x, y \in \mathbb{R} \right\}$$

На множестве матриц операции вводить не нужно (они уже есть). Доказать, что  $\mathbb{C}'$  - подполе (относительно операций  $+$  и  $\cdot$  матриц), которое тоже будет являться моделью поля комплексных чисел.

## Геометрическая интерпретация поля комплексных чисел

Вспомним, что  $\mathbb{R}$  мы умеем интерпретировать на геометрическом языке: изображаем действительные числа точками или векторами на действительной прямой. Как изображать  $\mathbb{C}$ ? Комплексные числа можно задавать парами чисел из  $\mathbb{R}$ : вещественная и мнимая части  $\Rightarrow$  комплексные числа удобно изображать как точки или векторы (которые тоже задаются парой координат) на координатной плоскости.

**Опр: 5.** Геометрически, комплексные числа это точки или векторы на координатной плоскости, которая называется комплексной плоскостью.

**Опр: 6.** Горизонтальная ось комплексной плоскости называется действительной осью.

Обозначение:  $\text{Re}$ .

**Опр: 7.** Вертикальная ось комплексной плоскости называется мнимой осью.

Обозначение:  $\text{Im}$ .

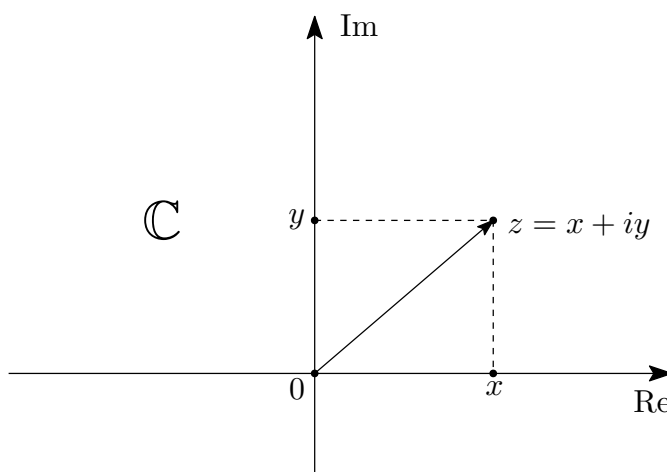


Рис. 1: Комплексная плоскость.

Сложение/вычитание комплексных чисел  $\Leftrightarrow$  сложение/вычитание соответствующих векторов в комплексной плоскости по правилу параллелограмма.

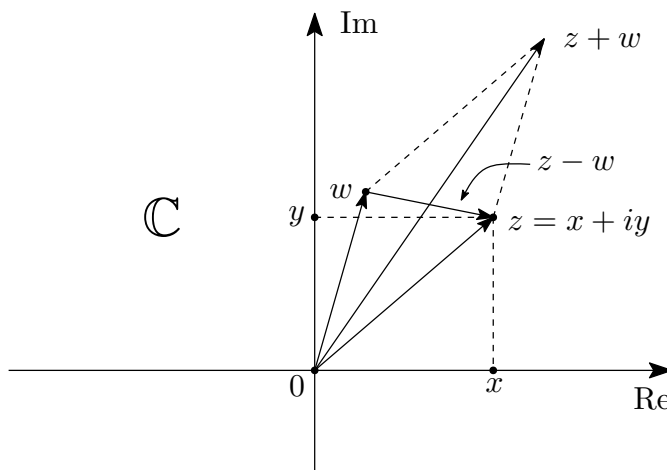


Рис. 2: Векторное сложение/вычитание.

Таким образом, операция прибавления комплексного числа (ко всем остальным комплексным числам) это тоже самое что и параллельный перенос на комплексной плоскости, с точки зрения геометрии.

**Опр: 8.** Модулем комплексного числа  $z = x + iy$  называется число  $|z| = \sqrt{x^2 + y^2}$ .

С геометрической точки зрения, модуль это расстояние от точки, соответствующей числу  $z$  до начала координат или, что тоже самое, длина вектора, задающего комплексное число  $z$ .

**Опр: 9.** Сопряженным комплексным числом числа  $z = x + iy$  называется число  $\bar{z} = x - iy$ .

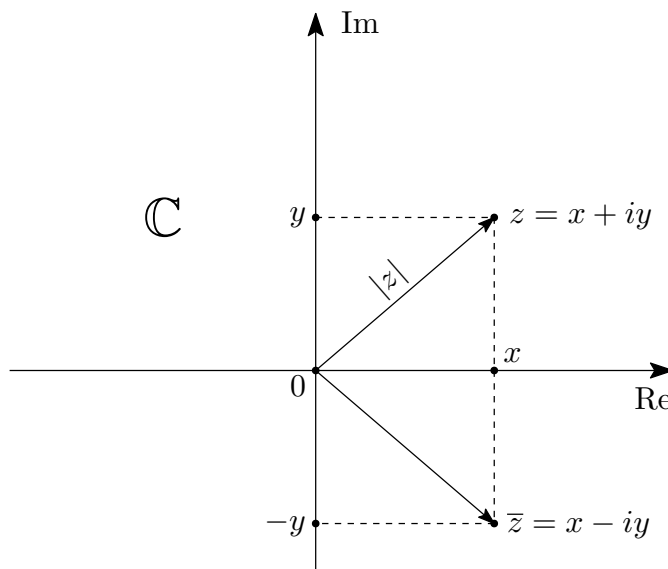


Рис. 3: Модуль числа  $z$  и его сопряженное комплексное число.

**Утв. 1.** (Свойства сопряженных чисел)

- 1)  $\overline{z + w} = \bar{z} + \bar{w}$ ;
- 2)  $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$ ;
- 3)  $\bar{\bar{z}} = z \Leftrightarrow z = \operatorname{Re}(z) \in \mathbb{R}$ ;
- 4)  $z \cdot \bar{z} = |z|^2$ ;
- 5)  $\bar{\bar{\bar{z}}} = \bar{z}$ ;
- 6)  $z + \bar{z} = 2 \operatorname{Re}(z)$ ;
- 7)  $z = -\bar{z} \Leftrightarrow z = i \operatorname{Im}(z) \in i\mathbb{C}$ ;

□

- 1) Пусть  $z = x + iy$ ,  $w = u + iv \Rightarrow \bar{z} = x - iy$ ,  $\bar{w} = u - iv$ , тогда:

$$z + w = (x + u) + i(y + v) \Rightarrow \overline{z + w} = (x + u) - i(y + v) = x - iy + u - iv = \bar{z} + \bar{w}$$

- 2) Пусть  $z = x + iy$ ,  $w = u + iv$ , тогда:

$$z \cdot w = (x \cdot u - y \cdot v) + i(x \cdot v + y \cdot u) \Rightarrow \overline{z \cdot w} = (x \cdot u - y \cdot v) - i(x \cdot v + y \cdot u)$$

$$\bar{z} \cdot \bar{w} = (x \cdot u - (-y) \cdot (-v)) + i(x \cdot (-v) + u \cdot (-y)) = (x \cdot u - y \cdot v) - i(x \cdot v + u \cdot y)$$



3) Пусть  $z = x + iy$ , тогда:

$$\bar{z} = x - iy = z = x + iy \Leftrightarrow y = 0 \Leftrightarrow z = x + i \cdot 0 = x = \operatorname{Re}(z) \in \mathbb{R}$$

4) Пусть  $z = x + iy \Rightarrow \bar{z} = x - iy$ , тогда:

$$z \cdot \bar{z} = (x + iy) \cdot (x - iy) = x^2 - i^2 \cdot y^2 = x^2 + y^2 = |z|^2$$

5) Пусть  $z = x + iy \Rightarrow \bar{z} = x - iy$ , тогда:

$$\bar{\bar{z}} = \overline{x - iy} = x + iy = z$$

6) Пусть  $z = x + iy \Rightarrow \bar{z} = x - iy$ , тогда:

$$z + \bar{z} = x + iy + x - iy = 2x = 2 \operatorname{Re}(z)$$

7) Пусть  $z = x + iy \Rightarrow \bar{z} = x - iy$ , тогда:

$$z = x + iy = -\bar{z} = -x + iy \Rightarrow x = -x \Rightarrow x = 0 \Rightarrow z = iy = \operatorname{Im}(z) \in \mathbb{C}$$

■

**Rm: 1.** Свойства 1) и 2) означают, что операция сопряжения:  $z \mapsto \bar{z}$  является изоморфизмом поля комплексных чисел само с собой:  $\mathbb{C} \xrightarrow{\sim} \mathbb{C}$  (биективность - очевидна по определению сопряжения, согласованность с операциями следует из 1) и 2)).

**Rm: 2.** Операция сопряжения является автоморфизмом поля  $\mathbb{C}$  в себя.

**Утв. 2.** (Деление комплексных чисел в алгебраической форме)

$$\forall z, w \in \mathbb{C}, z \neq 0, \frac{w}{z} = w \cdot z^{-1} = \frac{w \cdot \bar{z}}{|z|^2}$$

□

$$\forall z \in \mathbb{C}, z \cdot \bar{z} = |z|^2, z \neq 0 \Rightarrow |z| > 0 \Rightarrow z \cdot \frac{\bar{z}}{|z|^2} = 1 \Rightarrow z^{-1} = \frac{\bar{z}}{|z|^2} \Rightarrow$$

$$\Rightarrow \forall z, w \in \mathbb{C}, z \neq 0, w \cdot z^{-1} = \frac{w \cdot \bar{z}}{|z|^2}$$

■

**Rm: 3.** По-другому, можно было показать так:

$$\forall z, w \in \mathbb{C}, z \neq 0, \frac{w}{z} = \frac{w \cdot \bar{z}}{z \cdot \bar{z}} = \frac{w \cdot \bar{z}}{|z|^2}$$

то есть, если мы хотим поделить одно комплексное число на другое, то надо и числитель, и знаменатель этой дроби умножить на число, сопряженное к знаменателю, тогда в знаменателе появится положительное действительное число, на которое можно отдельно поделить, а в числителе будет произведение, которое мы можем выяснить в алгебраической форме.