

# **ШАД. Хэндбук поступающего**

Автор: Даниил Скороходов

@neuralspeedster

22.09.2025

# Содержание

A. Алгебра .....	4
A.1. Подстановки .....	4
A.1.1. Умножение подстановок .....	4
A.1.2. Циклы и транспозиции .....	5
A.1.3. Чётность подстановки .....	6
A.2. Комплексные числа .....	7
A.2.1. Геометрическая интерпретация .....	7
A.2.2. Формы записи .....	9
A.2.3. Об умножении комплексных чисел .....	10
A.2.4. Извлечение корней .....	11
A.2.5. Корни из единицы .....	12
A.3. Системы линейных уравнений .....	13
A.4. Линейная зависимость и ранг .....	14
B. Математический анализ .....	15
C. Комбинаторика .....	16
C.1. Основные правила комбинаторики .....	16
C.1.1. Правила суммы и произведения .....	16
C.1.2. Принцип Дирихле .....	17
C.1.3. Примеры .....	18
C.2. Множества .....	19
C.2.1. Операции на множествах .....	19
C.2.2. Свойства бинарных операций над множествами .....	19
C.2.3. Картесийский произведение .....	19
C.2.4. Декартово произведение .....	20
C.2.5. Мощность множества .....	20
C.2.6. Круги Эйлера .....	21
C.2.7. Формула включений и исключений .....	21
C.3. Перестановки, сочетания и размещения .....	22
D. Теория вероятностей .....	23
D.1. Основные понятия .....	23
D.1.1. Операции над событиями .....	23
D.1.2. Аксиомы вероятности .....	24
D.1.3. Следствия из Аксиом .....	25
E. Алгоритмы и структуры данных && программирование .....	26

Е.1. Основные понятия .....	26
Е.2. Анализ сложности и эффективности структур данных .....	26
Е.2.1. О-символика .....	26
Е.3. Дополнительные сведения .....	27
Е.3.1. Метод двух указателей .....	27
Г. Анализ данных .....	28

## А. Алгебра

Здесь много базы!

### А.1. Подстановки

Пусть  $\Omega$  - конечное множество из  $n$  элементов. Удобно считать, что  $\Omega = \{1, 2, \dots, n\}$ .  
Зададим множество всех биективных преобразований  $\Omega \rightarrow \Omega$ :

$$S = S_n(\Omega) = \{\sigma : \Omega \rightarrow \Omega \mid \sigma - \text{биективно}\} \quad (1)$$

Элементы множества  $S$  называются *подстановками* (или *перестановками*) множества  $\Omega$ .

Развёрнутая запись подстановки  $\pi : i \rightarrow \pi(i) \forall i = 1, 2, \dots, n$  имеет вид:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix} \quad (2)$$

Подстановка  $e = e_\Omega = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$  называется *единичной подстановкой*.

#### А.1.1. Умножение подстановок

Пусть  $\pi, \sigma \in S$ . Тогда их произведение  $\pi\sigma$  находится из общего определения композиции преобразований:

$$(\pi\sigma)(i) = \pi(\sigma(i)) \quad (3)$$

Пусть, например,  $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$  и  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ . Тогда:

$$(\pi\sigma)(1) = \pi(\sigma(1)) = \pi(4) = 1 \quad (4)$$

$$(\pi\sigma)(2) = \pi(\sigma(2)) = \pi(3) = 4 \quad (5)$$

$$(\pi\sigma)(3) = \pi(\sigma(3)) = \pi(2) = 3 \quad (6)$$

$$(\pi\sigma)(4) = \pi(\sigma(4)) = \pi(1) = 2 \quad (7)$$

Таким образом,  $\pi\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ . Заметим, что вообще говоря,  $\pi\sigma \neq \sigma\pi$ . Имеем:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad (8)$$

Свойства произведения подстановок:

1. Ассоциативность:  $\forall \alpha, \beta, \gamma \in S_n : \alpha(\beta\gamma) = (\alpha\beta)\gamma$ .
2. Единичный элемент:  $\exists e \in S_n : \forall \alpha \in S_n \alpha e = e\alpha$ .
3. Обратная подстановка:  $\forall \alpha \in S_n \exists \alpha^{-1} \in S_n : \alpha\alpha^{-1} = \alpha^{-1}\alpha = e$ .

**Порядок группы подстановок** или же попросту мощность множества подстановок равна факториалу количества элементов  $\Omega$ . Действительно, для каждого из  $n$  элементов множества  $\Omega$  можно выбрать одно из  $n$  мест, затем для оставшихся  $n - 1$  элементов — одно из  $n - 1$  мест и так далее. В итоге получаем:

$$\text{Card } S_n = n(n - 1)(n - 2) \dots 1 = n! \quad (9)$$

### А.1.2. Циклы и транспозиции

**Циклом** длины  $m \leq n$  множества  $\Omega$  называется такая подстановка  $\sigma \in S_n$ , что  $\sigma(i) = (i + 1) \forall i = 1, 2, \dots, (m - 1)$  и  $\sigma(m) = 1$ , а все элементы  $\Omega$ , не указанные перечислением, остаются на своих местах. Т. е.  $\forall k \notin \{1, \dots, m\} : \sigma(k) = k$ .

*Примечание:* элементы цикла приведены условно как  $\{1, \dots, m\}$ .

**Транспозицией** называется цикл длины 2. Записывается как  $\tau = (i \ j)$ , где  $i$  и  $j$  — элементы, которые меняются местами.

Исходя из общего определения цикла, очевидно, что транспозиция оставляет неподвижными все элементы, кроме двух указанных.

**Th. 1 (О разложении перестановок).** Любая подстановка  $\pi \in S_n \setminus \{e\}$  может быть представлена в виде произведения циклов.

*Доказательство:* Пусть  $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$ . Разобьём множество  $\Omega$  на непересекающиеся циклы. Для этого будем рассматривать последовательности элементов, которые переходят друг в друга под действием подстановки  $\pi$ .

**Следствие 1.** Любая подстановка может быть разложена в произведение транспозиций.

*Доказательство:* Разложим подстановку  $\pi = \pi_1 \pi_2 \dots \pi_k$ , где  $\pi_1, \pi_2, \dots, \pi_k$  — циклы. Каждый цикл  $\pi_j$  можно представить в виде произведения транспозиций, например, так:  $(1 \ 2 \ \dots \ m) = (1 \ l)(1 \ l-1) \dots (1 \ 3)(1 \ 2)$ . ■

**Индуктивное определение степени подстановки.** Пусть  $\pi \in S_n$ . Тогда:

$$\pi^s = \begin{cases} \pi(\pi^{s-1}), & \text{если } s > 0 \\ e, & \text{если } s = 0 \\ \pi^{-1}((\pi^{-1})^{-s-1}), & \text{если } s < 0 \end{cases} \quad (10)$$

Вернёмся к примеру  $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$  и  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ . Здесь  $\pi$  — цикл длины 4, а  $\sigma$  раскладывается в произведение двух транспозиций:  $\sigma = (1 \ 4)(2 \ 3)$ .

$$\sigma^2 = (1 \ 3)(2 \ 4), \sigma^4 = (\sigma^2)^2 = e, \pi^2 = e$$

### А.1.3. Чётность подстановки

Пусть подстановка  $\pi \in S_n$  раскладывается на множители  $\pi = \tau_1 \tau_2 \dots \tau_k$ , где  $\tau_j$  — транспозиции.

*Знаком*(или *чётностью*) подстановки называется число

$$\varepsilon_\pi = (-1)^k \quad (11)$$

**Th. 2:** Чётность подстановки не зависит от выбора разложения на транспозиции.

**Th. 2.1 (О знаке произведения):**

$$\varepsilon_{\alpha\beta} = \varepsilon_\alpha \varepsilon_\beta \quad (12)$$

**Th. 3:** Количество чётных подстановок равно количеству нечётных и равно  $\frac{n!}{2}$ .

## А.2. Комплексные числа

Комплексным числом называется пара действительных чисел  $(a, b)$ .

$$\mathbb{C} = \{(a, b) \mid a, b \in \mathbb{R}\} \quad (13)$$

Если  $z = (a, b)$ , то

$$a = \Re(z) \quad (14)$$

$$b = \Im(z) \quad (15)$$

$a$  называется действительной частью комплексного числа  $z$ ,  $b$  — мнимой частью.

Для комплексных чисел операции сложения и умножения определяются так:

1.  $(a, b) + (c, d) = (a + c, b + d)$
2.  $(a, b)(c, d) = (ac - bd, ad + bc)$

Заметим, что  $(a, 0) = a \ \forall a \in \mathbb{R}$ . Так что  $\mathbb{R} \subset \mathbb{C}$ .

**Мнимая единица.**  $(0, 1)^2 = (0, 1)(0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0) = -1$ .

Число  $(0, 1)$  принято обозначать  $i$  и называть мнимой единицей. Итак,

$$i^2 = -1 \quad (16)$$

Стандартное обозначение для комплексного числа  $z = (a, b)$ :

$$z = a + bi \quad (17)$$

Для произвольных комплексных чисел нельзя корректно ввести бинарное отношение порядка( $<$ ).

### А.2.1. Геометрическая интерпретация

Комплексному числу можно сопоставить точку в двумерном пространстве с декартовыми координатами  $(a, b)$ . По оси абсцисс откладывается действительная часть, по оси ординат — мнимая.

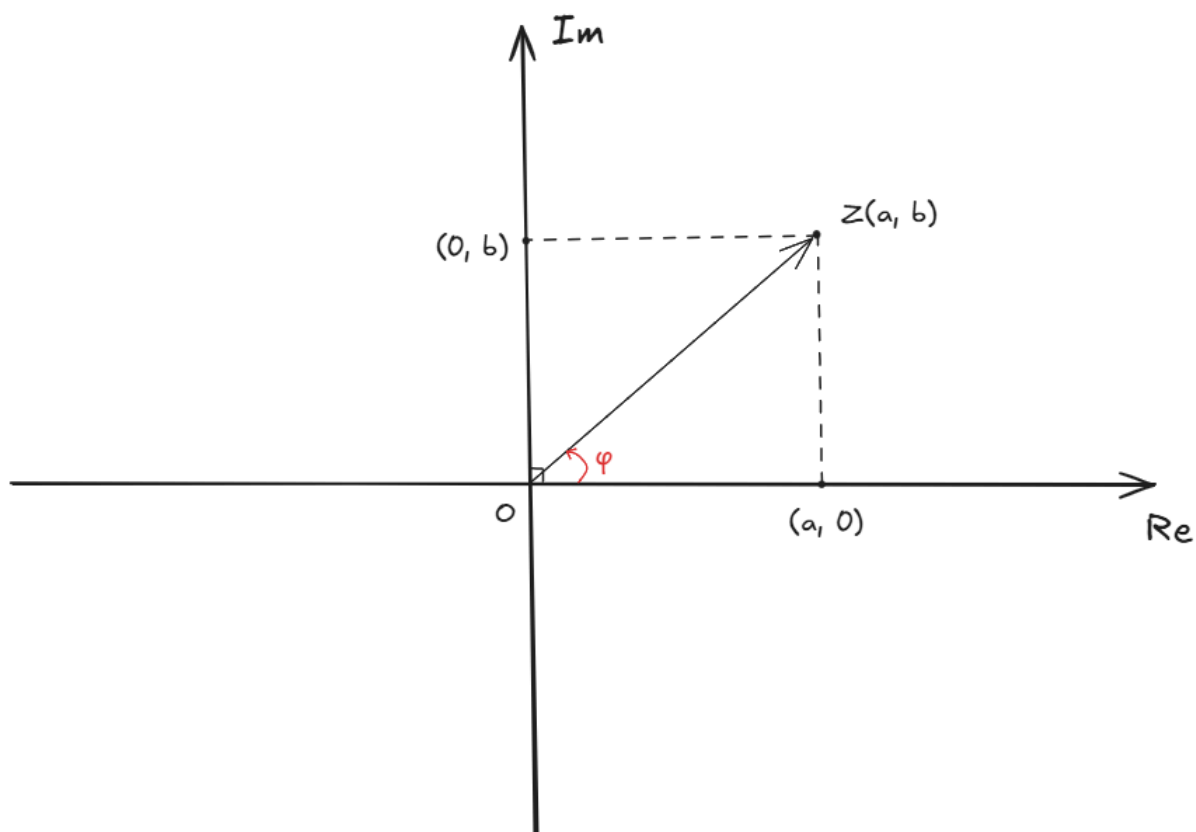


Рис. 1 - комплексная плоскость

**Операция сопряжения.** Число  $\bar{z} = a - bi$  называется *сопряжённым* числу  $z = a + bi$ . Операция сопряжения соответствует симметрии  $S_{\Re}$  относительно действительной оси.

Заметим, что  $\Im(z\bar{z}) = 0 \Leftrightarrow z\bar{z} \in \mathbb{R}$

**Модуль комплексного числа.** Величина  $|z| = \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$  называется *модулем*  $z$ .

**Аргумент комплексного числа.** Величина  $\arg(z) = \varphi$ , где  $\varphi \in (-\pi; \pi]$  — ориентированный угол между радиус-вектором  $z$  и положительным направлением оси абсцисс называется *аргументом комплексного числа*. Аргумент числа  $(0, 0)$  не определён.

**Неравенство треугольника в комплексных числах.**  $\forall z_1, z_2 \in \mathbb{C}$  :

$$|z_1 + z_2| \leq |z_1| + |z_2| \quad (18)$$

(Доказывается алгебраическими преобразованиями или использованием неравенства Коши-Буняковского-Шварца)



**Переход в полярные координаты.** Пусть  $z = x + yi$  Сделаем замену:

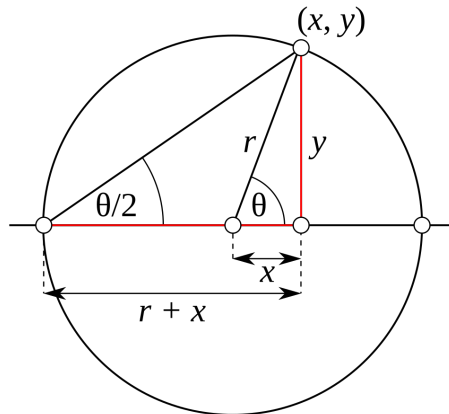
$$\begin{cases} r = |z| = \sqrt{x^2 + y^2} \\ \theta = \arg(z) \end{cases} \quad (19)$$

Главными называются значения аргумента из полуинтервала  $(-\pi; \pi]$ .

**Явное выражение для главного значения аргумента.**

$$\text{Arg}(z) = 2 \arctg\left(\frac{y}{x + \sqrt{x^2 + y^2}}\right) \quad (20)$$

*Доказательство:* Пусть комплексное число  $(x, y)$  имеет аргумент  $\theta$ . Вписанный угол, опирающийся на дугу меры  $\theta$ , равен половине центрального угла  $\theta$ . Тогда из прямоугольного треугольника (см. рисунок).



$$\text{tg}\left(\frac{\theta}{2}\right) = \frac{y}{x + r} \quad (21)$$

Это и эквивалентно  $\theta = 2 \arctg\left(\frac{y}{x+r}\right)$ . ■

### А.2.2. Формы записи

1. Алгебраическая:

$$z = x + yi \quad (22)$$

2. Тригонометрическая:

$$z = r(\cos \varphi + i \sin \varphi) \quad (23)$$

3. Показательная:

$$z = re^{i\varphi} \quad (24)$$

Показательная форма есть просто следствие формулы Эйлера:

$$e^{i\varphi} = \cos \varphi + i \sin \varphi \quad (25)$$

Доказательство самой формулы Эйлера вытекает из следующих трёх разложений.  
 $\forall z \in \mathbb{C}$

$$\sin z = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \dots = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n+1}}{(2n+1)!} \quad (26)$$

$$\cos z = 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \dots = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n}}{(2n)!} \quad (27)$$

$$e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \dots = \sum_{n=0}^{\infty} \frac{z^n}{n!} \quad (28)$$

Подставим в разложение экспоненты  $z = i\varphi$ , где  $\varphi \in \mathbb{R}$  и учтем следующие тождества:  $i^2 = -1$ ,  $i^3 = -i$ ,  $i^4 = 1$ ,  $i^5 = i$ . Вообще говоря,  $i^n = i^{n-4}$ . Отсюда и следует требуемое. ■

### А.2.3. Об умножении комплексных чисел

Алгебраическое умножение комплексных чисел не столь удобно, особенно при возведении в степень.

Пусть даны два комплексных числа  $z_1 = r_1(\cos \varphi_1 + i \sin \varphi_1)$  и  $z_2 = r_2(\cos \varphi_2 + i \sin \varphi_2)$ . Тогда их произведение можно записать в виде:

$$\begin{aligned} z_1 z_2 &= r_1 r_2 (\cos \varphi_1 + i \sin \varphi_1)(\cos \varphi_2 + i \sin \varphi_2) = \\ &= r_1 r_2 (\cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2 + i(\sin \varphi_1 \cos \varphi_2 + \cos \varphi_1 \sin \varphi_2)) = \\ &= r_1 r_2 (\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)) \end{aligned} \quad (29)$$

Итак,

$$\begin{cases} |z_1 z_2| = |z_1| |z_2| \\ \arg(z_1 z_2) = \arg(z_1) + \arg(z_2) \end{cases} \quad (30)$$

Исходя из этого, можно быстро возводить комплексные числа в произвольную натуральную степень.

**Формула Муавра.**  $\forall z = r(\cos \varphi + i \sin \varphi) \in \mathbb{C}, n \in \mathbb{N}$ :

$$z^n = r^n (\cos(n\varphi) + i \sin(n\varphi)) \quad (31)$$

**Доказательство:** докажем по индукции.

1. База:  $n = 1$ . Тогда  $z^1 = z = r(\cos \varphi + i \sin \varphi)$ . Это уже получено. Для уверенности можем проверить случай  $n = 2$ . Легко видеть, что это следствие (30) для  $z = z_1 = z_2$ .
2. Предположение индукции. Пусть верно для  $n \in \mathbb{N}$ :  $z^n = r^n(\cos(n\varphi) + i \sin(n\varphi))$
3. Шаг индукции. Докажем для  $n + 1$ . Тогда

$$\begin{aligned} z^{n+1} &= z^n z = r^n r (\cos(n\varphi + \varphi) + i \sin(n\varphi + \varphi)) = \\ &= r^{n+1} (\cos((n+1)\varphi) + i \sin((n+1)\varphi)) \end{aligned} \quad (32)$$

■

Здесь мы снова использовали (30). Таким образом, формула верна для  $n + 1 \Rightarrow$  она верна  $\forall n \in \mathbb{N}$ .

**Дополнительно.** Легко видеть, что умножение  $z_1 = r_1(\cos \varphi_1 + i \sin \varphi_1)$  на  $z_2 = r_2(\cos \varphi_2 + i \sin \varphi_2)$  задаёт композицию поворота  $R_O^{\varphi_2}$  и гомотетии  $H_O^{r_2}$  точки  $z_1$  на плоскости  $\mathbb{C}$ . Полученное преобразование  $\mathbb{R}^2 \rightarrow \mathbb{R}^2$  называется *поворотной гомотетией*:  $H_O^{r_2, \varphi_2} = H_O^{r_2} \circ R_O^{\varphi_2}$ .

#### А.2.4. Извлечение корней

**Алгебраическим корнем степени  $n > 1$  числа  $z \in \mathbb{C}$**  называется множество  $\Omega = \{w \mid w^n = z \mid w \in \mathbb{C}, n \in \mathbb{N}\}$  и обозначается  $\sqrt[n]{z}$ .

$$\forall z \in \mathbb{C} : \text{Card}(\sqrt[n]{z}) = n.$$

Выведем формулу для корней из комплексного числа  $z = r(\cos \varphi + i \sin \varphi)$ .

Пусть  $\sqrt[n]{z} = \{w_k \mid w_k^n = z \mid k = 0, 1, \dots, n-1\}$ .

1. Очевидно, что  $|w_k| = \sqrt[n]{r}$ , где  $\sqrt[n]{r}$  — арифметический квадратный корень из действительного числа  $r$ . И правда, по формуле Муавра  $|z| = |w_k|^n$ .
2. Пусть  $\varphi_k = \arg(w_k)$ . Тогда по формуле Муавра:  $n\varphi_k = \varphi + 2\pi k$ . Для всех  $k \in \{k_0 + i \mid i = 0, 1, \dots, (n-1)\}$  будут получаться все  $n$  корней. Поэтому для удобства полагают  $k_0 = 0$ . ■

Итак, доказана формула корней числа  $z = r(\cos \varphi + i \sin \varphi) \forall k \in \{0, 1, \dots, n-1\}$ :

$$w_k = \sqrt[n]{r} \left( \cos \left( \frac{\varphi}{n} + 2\pi \frac{k}{n} \right) + i \sin \left( \frac{\varphi}{n} + 2\pi \frac{k}{n} \right) \right) \quad (33)$$

Все корни из числа  $z$  лежат на вершинах правильного  $n$ -угольника, вписанного в окружность с центром в начале координат и радиусом  $\sqrt[n]{r}$ .

Это легко видеть, исходя из того, что у всех корней одинаковый модуль, и каждый следующий получается из предыдущего поворотом на один и тот же угол  $\frac{2\pi}{n}$ .

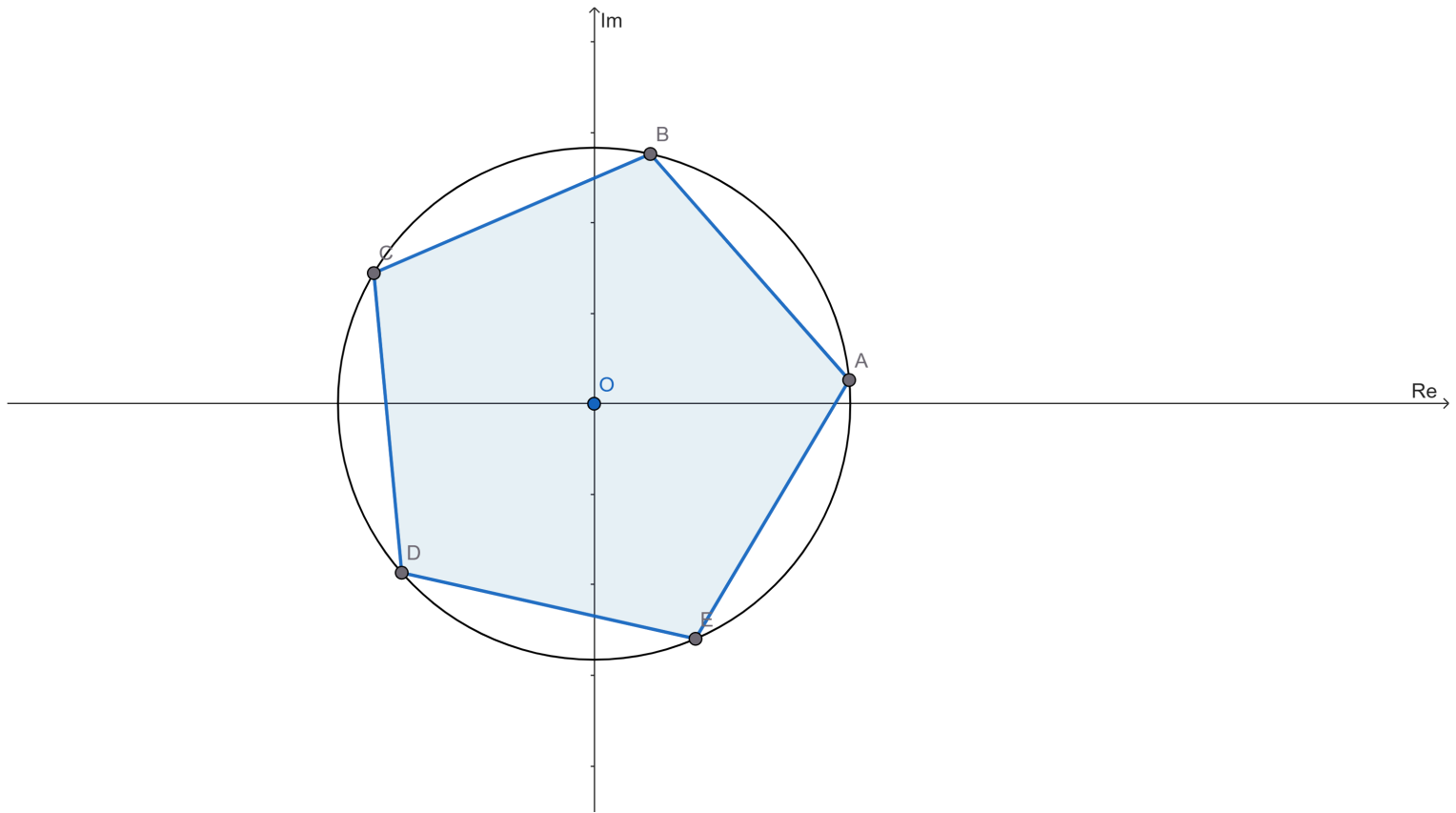


Рис. 2 — корни 5 степени из  $z = 4 + 4i$

#### А.2.5. Корни из единицы

Положим  $z = 1$ . Тогда корни степени  $n$  выражаются так:

$$\sqrt[n]{1} = \varepsilon_k = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right) \quad (34)$$

$$\forall k \in \{0, 1, \dots, n-1\}.$$

Все корни есть вершины правильного  $n$ -угольника, вписанного в окружность единичного радиуса. Её уравнение  $z\bar{z} = 1$ .

### **А.3. Системы линейных уравнений**

#### **А.4. Линейная зависимость и ранг**

## **В. Математический анализ**

## С. Комбинаторика

В этом разделе рассматриваются основные понятия и тождества комбинаторики, а так же основы теории множеств и теории графов.

### С.1. Основные правила комбинаторики

#### С.1.1. Правила суммы и произведения

**Правило суммы.** Если элемент множества  $A$  можно выбрать  $m$  способами, а элемент множества  $B$   $n$  способами, то выбор «либо  $A$ , либо  $B$ » может быть сделан  $m + n$  способами, при условии, что множества  $A$  и  $B$  не пересекаются.

*Доказательство:* Количество способов выбрать «либо  $A$ , либо  $B$ » равно мощности множества  $A \cup B$ . По условию  $A \cap B = \emptyset$ , поэтому надо доказать лемму:

$$A \cap B = \emptyset \Rightarrow |A \cup B| = |A| + |B| \quad (35)$$

*Доказательство леммы:* пусть  $A = \{a_1, \dots, a_m\}$  и  $B = \{b_1, \dots, b_n\}$  Тогда

$$A \cup B = \{a_1, \dots, a_m, b_1, \dots, b_n\} \quad (36)$$

Здесь существенно использовано то, что  $A \cap B = \emptyset$ , так как тогда  $\forall a \in A, \forall b \in B : a \neq b$ . Следовательно,  $|A \cup B| = m + n$ . ■

По лемме,  $|A \cup B| = |A| + |B|$ , что и требовалось доказать. ■

**Правило произведения.** Если объект  $A$  можно выбрать  $m$  способами и для каждого выбора  $A$  объект  $B$  можно выбрать  $n$  способами, то количество способов выбрать упорядоченные пары  $(A, B)$  равно  $m \cdot n$ .

*Доказательство:* Переформулируем доказываемое утверждение так: пусть  $|A| = m$ ,  $|B| = n$ . Тогда надо доказать, что мощность декартова произведения множеств равна произведению мощностей сомножителей:

$$|A \times B| = m \cdot n \quad (37)$$

. Перед доказательством сформулируем важную лемму, которая доказана в разделе, связанном с теорией множеств. Лемма о дистрибутивности декартова произведения относительно объединения множеств:

$$A \times (B \cup C) = (A \times B) \cup (A \times C) \quad (38)$$

. Докажем исходное утверждение индукцией по мощности второго сомножителя:

1. База индукции.



1.1.  $n = 0 : A \times B = A \times \emptyset = \emptyset$ . Но  $|\emptyset| = 0 = m \cdot n$ .

1.2.  $n = 1 : A \times B = A \times \{b_1\} = \{(a_1, b_1), \dots, (a_m, b_1)\}$ . Легко видеть, что  $|\{(a_1, b_1), \dots, (a_m, b_1)\}| = m = m \cdot 1$ .

2. Предположение индукции. Пусть верно для некоторого  $n \in \mathbb{N}$ , что  $\forall A, B : |A \times B| = m \cdot n$ .

3. Шаг. Докажем для  $n + 1$  на основе предположения индукции. Пусть множество  $B_{n+1} = B_n \cup \{b_{n+1}\}$  и  $|B_n| = n$ .

$$A \times B_{n+1} = A \times (B_n \cup \{b_{n+1}\}) = A \times B_n \cup A \times \{b_{n+1}\} \quad (39)$$

Тогда

$$|A \times B_{n+1}| = |A \times B_n| + |A \times \{b_{n+1}\}| = m \cdot n + m \cdot 1 = m \cdot (n + 1) \quad (40)$$

Шаг индукции верен, поэтому утверждение доказано. ■

### Обобщённые правила суммы и произведения:

1. Обобщённое правило суммы. Пусть даны попарно непересекающиеся множества  $A_1, A_2, \dots, A_n$ . Число способов сделать выбор « $A_1$  или  $A_2$  ...или  $A_n$ » равно  $\sum_{i=1}^n |A_i|$ . Доказывается по индукции.
2. Обобщённое правило произведения. Пусть даны множества  $A_1, A_2, \dots, A_n$ . Число способов выбрать упорядоченный кортеж  $(a_1, \dots, a_n) \mid a_i \in A_i$  из  $n$  элементов равно  $\prod_{i=1}^n |A_i|$ . Доказывается по индукции.

**Пример использования обобщённого правила произведения.** Докажем, что порядок группы перестановок  $S_n = S(\Omega)$  равен  $n!$ , где  $n = |\Omega|$ . Для первой позиции образа мы можем выбрать любой из  $n$  прообразов. Далее для второй позиции уже  $(n - 1)$  прообраз и т. д. На последнюю позицию можно выбрать единственный элемент множества  $\Omega$ . Имеем:  $P_n = n \cdot (n - 1) \cdot \dots \cdot 1$  ■.

### С.1.2. Принцип Дирихле

Обозначим  $\lceil x \rceil = \min\{a \mid a \geq x, a \in \mathbb{Z}\}$

Принцип Дирихле. Если  $n$  объектов разместить в  $m$  ящиках и  $n > m$ , то существует хотя бы один ящик, в котором находится не менее  $\lceil \frac{n}{m} \rceil$  объектов.

*Доказательство.* Обозначим  $k = \lceil \frac{n}{m} \rceil$  и предположим противное: во всех ящиках лежит меньше  $k$  объектов. Тогда для любого ящика, в нем находится не более  $k - 1$  объектов. Общее число объектов тогда не превосходит  $m \cdot (k - 1)$ , т. е. имеет место

неравенство  $n \leq m \cdot (k - 1)$ . Но по свойству округления вверх:  $k - 1 = \lceil \frac{n}{m} \rceil - 1 < \frac{n}{m}$ .  
Имеем:

$$\begin{cases} n \leq m \cdot (k - 1) \\ n > m \cdot (k - 1) \end{cases} \quad (41)$$

Получили противоречие, значит противное неверно и исходное утверждение доказано. ■

### С.1.3. Примеры

## С.2. Множества

«Элемент  $a$  принадлежит множеству  $A$ » обозначают  $a \in A$ . Отрицание этого утверждения обозначается  $a \notin A$ .

Множество  $B$  называется подмножеством  $A$ , если  $\forall x \in B : x \in A$ . Обозначают  $B \subset A$ .

Множества  $A$  и  $B$  называются равными, если  $A \subset B \wedge B \subset A$ . Обозначают  $A = B$ .

Пустым множеством называется множество, не содержащее ни одного элемента. Оно является подмножеством любого множества. Обозначается  $\emptyset$ .  $\forall A : \emptyset \subset A$

### С.2.1. Операции на множествах

Основные бинарные операции над множествами определены так:

1. Объединение.  $A \cup B = \{x \mid x \in A \vee x \in B\}$
2. Пересечение.  $A \cap B = \{x \mid x \in A \wedge x \in B\}$
3. Разность.  $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$
4. Симметрическая разность.  $A \triangle B = (A \setminus B) \cup (B \setminus A)$

### С.2.2. Свойства бинарных операций над множествами

1. Коммутативность объединения и пересечения:

- $A \cup B = B \cup A$
- $A \cap B = B \cap A$ .

2. Ассоциативность объединения и пересечения:

- $(A \cup B) \cup C = A \cup (B \cup C)$
- $(A \cap B) \cap C = A \cap (B \cap C)$ .

3. Дистрибутивность объединения и пересечения:

- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ .

### С.2.3. Кортеж

Кортежем называется упорядоченная  $n$ -ка элементов. Обозначается как

$$(a_1, a_2, \dots, a_n) \text{ или } \langle a_1, a_2, \dots, a_n \rangle \quad (42)$$

.

Более строго, можно индуктивно сопоставить кортежи множествам:

- $\emptyset \leftrightarrow \langle \rangle$
- $\{a_1\} \leftrightarrow \langle a_1 \rangle$
- $\{a_1, \{a_1, a_2\}\} \leftrightarrow \langle a_1, a_2 \rangle$

Тогда:

- $\{a_1, a_2, \dots, a_n\} \leftrightarrow \langle a_1, a_2, \dots, a_n \rangle \stackrel{\text{def}}{=} \langle \langle a_1, a_2, \dots, a_{n-1} \rangle, a_n \rangle$

Альтернативно, можно дать такое определение:

$$\langle a_1, a_2, \dots, a_n \rangle = f : [n] \rightarrow \{a_1, a_2, \dots, a_n\} \quad (43)$$

### С.2.4. Декартово произведение

Декартовым произведением двух множеств  $A$  и  $B$  называется множество всех упорядоченных пар элементов из  $A$  и  $B$ .

$$A \times B = \{(a, b) \mid a \in A, b \in B\} \quad (44)$$

Свойства декартова произведения:

1. Некоммутативность. Вообще говоря,  $A \times B \neq B \times A$ , если  $A \neq B$
2. Ассоциативность.  $A \times (B \times C) = (A \times B) \times C$
3. Дистрибутивность относительно объединения и пересечения (по левому и по правому множителю):

- $A \times (B \cup C) = A \times B \cup A \times C$
- $A \times (B \cap C) = A \times B \cap A \times C$
- $(B \cup C) \times A = B \times A \cup C \times A$
- $(B \cap C) \times A = B \times A \cap C \times A$

### С.2.5. Мощность множества

Мощностью конечного множества  $A = \{a_1, a_2, \dots, a_n\}$  называется количество элементов в нём:  $|A| = n$ .

**Утверждение 1.**  $A \cap B = \emptyset \Rightarrow |A \cup B| = |A| + |B|$

(Уже доказано, см. 35)

**Утверждение 2.**  $|A \times B| = |A| \cdot |B|$

(Уже доказано, см. 37)

### С.2.6. Круги Эйлера

Отношения между множествами можно визуально представить с помощью кругов Эйлера.

### С.2.7. Формула включений и исключений

Пусть  $A_1, A_2, \dots, A_n$  - конечные множества. Тогда

$$\begin{aligned} \left| \bigcup_{i=1}^n A_i \right| &= \sum_i |A_i| - \sum_{i < j} |A_i \cap A_j| + \\ &+ \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n| \end{aligned} \tag{45}$$

### С.3. Перестановки, сочетания и размещения

Существуют две схемы выбора  $m$  элементов из множества мощности  $n$ :  $0 < m \leq n$ : с повторениями и без повторений.

В первой схеме выбранный элемент не возвращается в множество, а во второй схеме на каждом шаге элемент должен быть возвращён в множество.

**Перестановка.** Определение перестановки было дано в разделе 1.1.

Число всех перестановок длины  $n$  равно:

$$P_n = n! \quad (46)$$

**Размещением из  $n$  элементов по  $m$**  называют любое упорядоченное подмножество данного множества, содержащего  $n$  элементов.

Из определения вытекает, что размещения это комбинации, состоящие из  $m$  элементов, которые отличаются друг от друга либо составом, либо порядком расположения элементов.

Число всех размещений из  $n$  по  $m$ :

$$A_n^m = \frac{n!}{(n-m)!} \quad (47)$$

## Д. Теория вероятностей

### Д.1. Основные понятия

**Случайное событие** — событие, про которое нельзя точно сказать, произойдёт оно или нет. Обозначают буквами латинского алфавита:  $A, B, C \dots$

**Достоверным** называется событие, которое происходит всегда. Обозначается  $\Omega$ .

**Невозможным** называется событие, которое не может произойти. Обозначается  $\emptyset$ .

**Вероятность случайного события** это численная мера объективной возможности наступления данного события. Обозначение:  $P(A)$  — вероятность события  $A$ .

#### Д.1.1. Операции над событиями

$\bar{A}$  — событие, противоположное  $A$ . Заключается в том, что событие  $A$  не произошло.

$A \cap B$  — произведение событий. Это событие, которое заключается в совместном происхождении событий  $A, B$ .

Если  $A \cap B = \emptyset$ , то события  $A, B$  называются несовместными.

Вместо  $A \cap B$  иногда пишут  $AB$ .

$A \cup B$  — объединение или сумма событий. Заключается в том, что хотя бы одно из  $\{A, B\}$  верно.

**Закон де Моргана** в терминах событий:

$$\overline{A \cup B} = \bar{A} \cap \bar{B} \quad (48)$$

$$\overline{A \cap B} = \bar{A} \cup \bar{B} \quad (49)$$

Диаграммы Венна

**Свойства противоположного события:**

1.  $\overline{\bar{A}} = A$
2.  $A \cap \bar{A} = \emptyset$
3.  $A \cup \bar{A} = \Omega$

**Свойства бинарных операций над событиями.**

1. Коммутативность:
  - $A \cap B = B \cap A$ ;
  - $A \cup B = B \cup A$ .
2. Ассоциативность:

- $A \cap (B \cap C) = (A \cap B) \cap C$ ;
- $A \cup (B \cup C) = (A \cup B) \cup C$ .

3. Дистрибутивность.

- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ;
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ .

### Операция включения

$A \subset B$  — событие, которое заключается в том, что происхождение  $B$  влечёт  $A$ .

### Разность и симметрическая разность.

Разность событий  $A$  и  $B$  определяется как:

$$A \setminus B = A \cap \overline{B} \quad (50)$$

Симметрической разностью называется бинарная операция над событиями, такая, что

$$A \triangle B = (A \cup B) \cap (\overline{A} \cup \overline{B}) \quad (51)$$

Отрицание симметрической разности:

$$\overline{A \triangle B} = \overline{A} \triangle B = A \triangle \overline{B} = \overline{A} \triangle \overline{B} \quad (52)$$

### Поглощение.

1.  $A \cup (A \cap B) = A$
2.  $A \cap (A \cup B) = A$
3.  $\overline{A} \cup (A \cap B) = \overline{A} \cup B$
4.  $\overline{A} \cap (A \cup B) = \overline{A} \cap B$

### Декомпозиция бинарных операций.

1.  $A \cup B = A \triangle B \triangle AB$
2.  $A \setminus B = A \setminus (AB)$

### D.1.2. Аксиомы вероятности

1.  $\forall A \ P(A) \geq 0$  (неотрицательность);
2.  $P(\Omega) = 1$  (Вероятность достоверного события);
3.  $\forall A, B : A \cap B = \emptyset : P(A \cup B) = P(A) + P(B)$ . (Аддитивное свойство вероятности).



### D.1.3. Следствия из Аксиом

**Теорема о вероятности противоположных событий.**

$$P(A) + P(\overline{A}) = 1 \quad (53)$$

.

*Доказательство:* так как

$$\begin{cases} A \cup \overline{A} = \Omega \\ A \cap \overline{A} = \emptyset \end{cases} \quad (54)$$

то из аксиом 2 и 3:  $P(A \cup \overline{A}) = P(\Omega) = 1$ . ■

*Следствие из теоремы.*

Вероятность объединения  $n$  попарно независимых событий.

$$\forall A_1, A_2, \dots, A_n : \forall i, j : i \neq j : A_i \cap A_j = \emptyset :$$

$$P\left(\bigcup_{1 \leq i \leq n} A_i\right) = \sum_{i=1}^n P(A_i) \quad (55)$$

*Доказательство:* по индукции.  $n = 2$ : это аксиома 3.

Пусть верно для  $n \in \mathbb{N}$ . Тогда  $P\left(\bigcup_{1 \leq i \leq n} A_i\right) = \sum_{i=1}^n P(A_i)$  Докажем для  $n + 1$ :

$$\begin{aligned} P\left(\bigcup_{1 \leq i \leq n+1} A_i\right) &= P\left(\left[\bigcup_{1 \leq i \leq n} A_i\right] \cup A_{n+1}\right) = P\left(\bigcup_{1 \leq i \leq n} A_i\right) + \\ &+ P(A_{n+1}) = \sum_{i=1}^n P(A_i) + P(A_{n+1}) = \sum_{i=1}^{n+1} P(A_i) \quad \blacksquare \end{aligned} \quad (56)$$

## Е. Алгоритмы и структуры данных && программирование

### Е.1. Основные понятия

**Алгоритм** — точное или формализованное описание вычислительного процесса, ведущее от входных данных к искомому результату.

**Структуры данных** — множество элементов данных и связи между ними.

Физические данные существуют в памяти машины, а теоретические нет.

*Элементарные* данные не могут быть разделены на более мелкие части. Если же данные могут быть разделены на логически более мелкие части, то они называются *сложными*.

### Е.2. Анализ сложности и эффективности структур данных

Должны быть некие критерии *хорошего алгоритма*.

Два основных критерия, используемых на практике:

1. Быстродействие;
2. Объём потребляемой памяти.

Прямое измерение времени работы программной реализации измеряет далеко не только быстродействие алгоритма. На время выполнения влияют так же способ реализации, умения программиста, среда разработки и мощность компьютера.

Измерения скорости и памяти носят теоретический характер.

$T(n)$  — функция теоретического времени работы алгоритма.

$V(n)$  — функция теоретической пространственной сложности алгоритма.

Получить точную формулу нельзя, можно только получить скорость и порядок скорости изменения времени выполнения.

#### Е.2.1. О-символика

$$f(n) = O(g(n)) \Leftrightarrow \exists N, C > 0 : \forall n > N : |g(n)| \leq C \cdot |f(n)| \quad (57)$$

### Е.3. Дополнительные сведения

#### Е.3.1. Метод двух указателей

Задача на массиве  $a[n]$  решается методом двух указателей  $\Leftrightarrow$   
(Предикат из условия  $P(x) \equiv 1 : \forall x \in [L, R] \Rightarrow P(X) \equiv 1 \forall x \in [L', R'] \subset [L, R]$ )

## **Г. Анализ данных**