ШАД. Хэндбук поступающего

Автор: Даниил Скороходов

@neuralspeedster

07.12.2025

Содержание

A. Алгебра

A.1. Перестановки

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

$$S = S_n(\Omega) = \{\sigma : \Omega \to \Omega \mid \sigma - \text{биективно}\} \tag{1.1}$$

Элементы множества S называются *перестановками*(или *подстановками*) множества Ω.

Развёрнутая запись перестановки $\pi : i \to \pi(i)\ \forall i = 1, 2, ..., n$ имеет вид:

$$\begin{pmatrix} 1 & 2 & ... & n \\ \pi(1) & \pi(2) & ... & \pi(n) \end{pmatrix} \tag{1.2}$$

Её также называют стандартной двухрядной.

Определение. Перестановка

$$e = \begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix} \tag{1.3}$$

называется *единичной перестановкой.*

A.1.1. Умножение перестановок

Пусть $\pi, \sigma \in S$. Тогда их произведение $\pi\sigma$ находится из общего определения композиции преобразований. $\forall i = 1, ..., n$:

$$(\pi\sigma)(i) = \pi(\sigma(i)) \tag{1.4}$$

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:

$$(\pi\sigma)(1) = \pi(\sigma(1)) = \pi(4) = 1 \tag{1.5}$$

$$(\pi\sigma)(2) = \pi(\sigma(2)) = \pi(3) = 4 \tag{1.6}$$

$$(\pi\sigma)(3) = \pi(\sigma(3)) = \pi(2) = 3 \tag{1.7}$$

$$(\pi\sigma)(4) = \pi(\sigma(4)) = \pi(1) = 2 \tag{1.8}$$

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

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \tag{1.9}$$

A.1.1.1. Свойства произведения перестановок

Свойства произведения перестановок.

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 перестановка: $\forall \alpha \in S_n \ \exists \alpha^{-1} \in S_n : \alpha\alpha^{-1} = \alpha^{-1}\alpha = e$.

   Действительно, можно для α поменять местами строки:

$$\alpha = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} \tag{1.10}$$

$$\alpha^{-1} = \begin{pmatrix} j_1 & j_2 & \dots & j_n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}. \tag{1.11}$$

4. Некоммутативность. Вообще говоря, для $\alpha, \beta \in S_n$: $\alpha\beta \neq \beta\alpha$.

A.1.2. Количество перестановок

Мощность множества перестановок равна факториалу количества элементов Ω. Действительно, для каждого из n элементов множества Ω можно выбрать одно из n мест, затем для оставшихся $n-1$ элементов — одно из $n-1$ мест и так далее(согласно правилу произведения). В итоге получаем:

$$|S_n| = n(n-1)(n-2)...1 = n! \tag{1.12}$$

A.1.3. Циклы

Определение. Циклом длины $l \leq n$ называется такая перестановка $\sigma \in S_n$, что $\sigma\left(i_j\right) = \left(i_{j+1}\right) \ \forall j = 1, 2, ..., (l-1)$ и $\sigma(l) = i_1$, а все элементы, не указанные перечислением, остаются на своих местах.

Однорядная запись цикла:

$$(i_1, i_2, ..., i_l) \tag{1.13}$$

Определение. Орбитой цикла называется множество элементов, которые участвуют в цикле: $\{i_1, i_2, ..., i_l\}$.

Определение. Два цикла $\sigma = (i_1, i_2, ..., i_l)$ и $\tau = (j_1, j_2, ..., j_m)$ называются *независимыми*, если $\{i_1, i_2, ..., i_l\} \cap \{j_1, j_2, ..., j_m\} = \varnothing$.

Независимые циклы коммутативны: $\sigma\pi = \pi\sigma$.

A.1.4. Степень перестановки

Пусть $\pi \in S_n$. Тогда перестановка, равная π в степени $s \in \mathbb{Z}$ определяется так:

$$\pi^s = \begin{cases} \pi(\pi^{s-1}), & \text{если } s > 0 \\ e, & \text{если } s = 0 \\ (\pi^{-1})^{-s}, & \text{если } s < 0 \end{cases} \tag{1.14}$$

Свойства возведения в степень перестановок:

1. $\forall \sigma \in S_n, \forall k, l \in \mathbb{Z} : \sigma^k \sigma^l = \sigma^{k+l}$
2. $\left(\sigma^k\right)^l = \sigma^{k \cdot l}$

A.1.5. Орбита элемента

Определение. Орбитой числа $i \in \{1, ..., n\}$ под действием σ называется множество

$$O(i) \underset{\text{def}}{=} \left\{\sigma^k \mid k \in \mathbb{Z}\right\} \tag{1.15}$$

Среди элементов орбиты числа обязаны быть повторения:

$$\exists k, l \in \mathbb{Z}, k > l : \sigma^k(i) = \sigma^l(i) \tag{1.16}$$

Применим σ^{-l}:

$$\sigma^{k-l}(i) = \sigma^0(i) = i \tag{1.17}$$

Итак, существует положительная степень $k - l > 0$, такая, что перестановка σ в степени $k - l$ возвращает элемент на место. Тогда среди показателей положительных степеней можно выбрать наименьший.

$$m = \min_{p \in \mathbb{N}} \{p \mid \sigma^p(i) = i\} \tag{1.18}$$

Тогда для всех степеней, меньших m, орбита зацикливается и состоит всего из m чисел:

$$O(i) = \left\{i, \sigma(i), \sigma^2(i), ..., \sigma^{\{m-1\}}(i)\right\}. \tag{1.19}$$

A.1.5.1. Свойства орбит элементов

1. Разные орбиты не пересекаются: $O(i) \cap O(j) = \varnothing$, если $i \neq j$.

   Доказательство: □ Пусть $O(i) \cap O(j) \neq \varnothing$, тогда в пересечении этих орбит есть некоторое число k: $k \in O(i) \cap O(j)$, получим:

   $$k = \sigma^p(i) = \sigma^q(j) \tag{1.20}$$

   Если к левой и правой части равенства применить σ^{-p}, то получим:

   $$i = \sigma^{q-p}(j) \tag{1.21}$$

Теперь мы можем получить, что любой элемент орбиты i лежит в $O(j)$, а именно $\forall l \in \mathbb{Z}$:

$$\sigma^l(i) = \sigma^{l+q-p}(j) \in O(j) \tag{1.22}$$

Итак,

$$O(i) \subseteq O(j) \tag{1.23}$$

Аналогично, меняя i и j, местами, получаем:

$$O(j) \subseteq O(i) \tag{1.24}$$

Но это в точности означает, что $O(i) = O(j)$. Значит, если две орбиты пересекаются, то они совпадают. ■

2. Орбиты образуют разбиение множества чисел $\{1, ..., n\}$ на попарно непересекающиеся подмножества.

   Доказательство: □ Действительно, каждое число лежит в какой-то орбите, например, в своей. ■

A.1.6. Теорема о разложении перестановки в произведение независимых циклов

Теорема. Любая перестановка $\sigma \in S_n$ может быть представлена в виде произведения попарно независимых циклов:

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot ... \cdot \sigma_s, \tag{1.25}$$

Причём это разложение единственно с точностью до порядка множителей.

Доказательство: □ Запишем разбиение множества $\Omega = \{1, ..., n\}$ на непересекающиеся орбиты:

$$\Omega = \underbrace{O_1 \cup O_2 \cup ... \cup O_s}_{\substack{\text{орбиты, в которых} \\ > 1 \text{ элемента}}} \cup \underbrace{O_{s+1} \cup ... \cup O_t}_{\substack{\text{единичные орбиты} \\ \text{(если есть)}}}, \tag{1.26}$$

При действии перестановки $\sigma \in S_n$ элементы обязательно перемещаются внутри своих орбит.

Каждой орбите соответствует цикл, причём эти циклы независимы в силу того, что орбиты непересекающиеся. Тогда перестановка σ записывается в виде произведения:

$$\sigma = (i_1, i_2, ..., i_l) \cdot (j_1, j_2, ..., j_m) \cdot ... \cdot \big(k_1, k_2, ..., k_p\big) \tag{1.27}$$

Мы доказали существование разложения на независимые циклы. Докажем единственность. Пусть перестановка σ разложена в произведение попарно независимых циклов:

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot ... \cdot \sigma_s, \tag{1.28}$$

где $\sigma_1 = (i_1, i_2, ..., i_l), \sigma_2 = (j_1, j_2, ..., j_m), ..., \sigma_s = \big(k_1, k_2, ..., k_p\big)$. Из схемы действия σ видно, что орбиты перестановки σ на Ω это орбиты σ_1, σ_2, ..., σ_s и оставшиеся неподвижные точки.

Таким образом, по σ можно однозначно восстановить орбиты циклов $\sigma_1, \sigma_2, ..., \sigma_s$. А из них можно восстановить и сами циклы σ_i, потому что на своей орбите σ_i действует так же, как и сама σ. Что и требовалось доказать. ■

A.1.7. Транспозиции

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

Предложение. Любая перестановка может быть разложена в произведение транспозиций.

Доказательство: □ Разложим перестановку $\sigma \in S_n$ в произведение попарно независимых циклов:

$$\sigma = \sigma_1 \cdot \sigma_2 ... \cdot \sigma_s \tag{1.29}$$

Достаточно показать, что любой цикл можно разложить в произведение транспозиций. Пусть цикл σ_i выглядит так:

$$\sigma_i = (i_1, i_2, ...i_l) \tag{1.30}$$

Тогда такой цикл можно записать как произведение цикла длины $(l-1)$ и транспозиции двух последних номеров в орбите этого цикла:

$$\sigma_i = (i_1, i_2, ...i_{l-1}) \cdot (i_{l-1}, i_l) \tag{1.31}$$

Аналогино, можно разложить цикл длины $(l-1)$ в произведение цикла длины $(l-2)$ и транспозиции двух последних элементов. Продолжая далее этот алгоритм, мы дойдём до того, что в произведении останутся только транспозиции. Что и требовалось доказать. ■

A.1.8. Инверсии и знак перестановки

Определение. Назовём *инверсией(беспорядком)* в перестановке $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ пару (i_k, i_l), где $k < l$, но $i_k > i_l$.

Определение. Перестановка чётна, если количество инверсий в ней чётно.

Определение. Перестановка нечётна, если количество инверсий в ней нечётно.

Определение. Знаком перестановки σ называется число

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 \text{ , если } \sigma \text{ чётна} \\ -1 \text{ , если } \sigma \text{ нечётна} \end{cases} \tag{1.32}$$

Предложение. При транспозиции двух элементов перестановки её чётность меняется.

Доказательство. □ Пусть мы поменяли местами i_k и i_l.

1. Среди пар (i_p, i_q), где $p, q \notin \{k, l\}$, количество инверсий не меняется.
2. Среди пар (i_p, i_k), где $p < k \vee p > l$ не меняется.
3. Среди пар (i_p, i_l), где $p < k \vee p > l$ тоже не меняется.
4. Среди пар (i_q, i_k), где $k < q < l$, количество инверсий меняется на $\pm 1 \pm 1 \pm \dots \pm \pm 1$, таких пар $l - k - 1$.
5. Среди пар (i_q, i_l), где $k < q < l$, количество инверсий меняется на $\pm 1 \pm 1 \pm \dots \pm \pm 1$, таких пар $l - k - 1$.
6. В паре (i_k, i_l) инверсия либо появляется, либо исчезает.

Общее изменение количества инверсий равно $2(l - k - 1) + 1 \equiv 1 (\mathrm{mod}\, 2)$, поэтому чётность перестановки изменилась. ■

Следствие. Количество чётных и нечётных перестановок в S_n одинаково и равно $\frac{n!}{2}$.

Доказательство. □ Установим взаимно однозначное соответствие между чётными и нечётными перестановками. Для этого рассмотрим чётную перестановку $\sigma \in S_n$:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \underset{i_1 \leftrightarrow i_2}{\longrightarrow} \begin{pmatrix} 1 & 2 & \dots & n \\ i_2 & i_1 & \dots & i_n \end{pmatrix} \tag{1.33}$$

Следовательно, чётных и нечётных поровну. ■

Предложение. Если перестановка σ разложена в произведение N транспозиций, то можно найти её знак.

$$\sigma = \tau_1 \cdot \tau_2 ... \cdot \tau_N \Rightarrow \operatorname{sgn}(\sigma) = (-1)^N \tag{1.34}$$

Доказательство. □ Проведём индукцию по числу множителей.

1. База: $N = 0$. $\sigma = e \Rightarrow \operatorname{sgn}(\sigma) = 1$ — верно.

2. Шаг. Пусть

$$\sigma = \tau_1 \cdot \tau_2 ... \cdot \tau_{N-1} \cdot \tau_N \tag{1.35}$$

Обозначим $\sigma' = \tau_1 \cdot \tau_2 ... \cdot \tau_{N-1}$. Пусть $\tau_N = (k, l)$. Действие σ' на все числа, кроме k и l, такое же, как у σ. Для k и l под дейтсвием σ получаем:

$$k \to l \to i_l \tag{1.36}$$

$$l \to k \to i_K \tag{1.37}$$

Но σ' действует так: $k \to i_k$, $l \to i_l$, значит перестановки σ и σ' отличаются транспозиицей i_k и i_l, а значит их знаки различны по доказанному выше предложению.

$$\operatorname{sgn}(\sigma) = -\operatorname{sgn}(\sigma') \underset{\substack{\text{предп.} \\ \text{инд.}}}{=} -(-1)^{N-1} = (-1)^N. \tag{1.38}$$

Переход доказан и вместе с ним и утверждение $\forall N \in \mathbb{N}$. ■

Предложение. Мультипликативное свойство знака:

$$\operatorname{sgn}(\sigma \cdot \sigma') = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\sigma') \tag{1.39}$$

Доказательство. □ Пусть перестановки σ и σ' разложены на транспозиции:

$$\sigma = \tau_1 \cdot \tau_2 \cdot ... \cdot \tau_k \tag{1.40}$$

$$\sigma' = \pi_1 \cdot \pi_2 \cdot ... \cdot \pi_s. \tag{1.41}$$

Тогда, напрямую умножив их, получим

$$\begin{gathered} \operatorname{sgn}(\sigma\sigma') = \operatorname{sgn}(\tau_1 \cdot \tau_2 \cdot ... \cdot \tau_k \cdot \pi_1 \cdot \pi_2 \cdot ... \cdot \pi_s) = \\ = (-1)^{k+s} = (-1)^k \cdot (-1)^s = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\sigma'). \end{gathered} \tag{1.42}$$

■

Предложение. Знак обратной перестановки:

$$\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma) \tag{1.43}$$

Доказатательство. □ Согласно мультипликативности знака перестановки получаем:

$$\operatorname{sgn}(e) = \operatorname{sgn}(\sigma \cdot \sigma') = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\sigma') \tag{1.44}$$

Но $\operatorname{sgn}(e) = 1$, поэтому

$$\operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\sigma') = 1 \Rightarrow \operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma'). \tag{1.45}$$

Что и требовалось доказать. ■

A.2. Комплексные числа

Определение. Полем комплексных чисел $\mathbb{C}$ называется поле, удовлетворяющее следующим аксиомам:

1. $\mathbb{R} \subset \mathbb{C}$
2. Мнимая единица. $\exists i \in \mathbb{C} : i^2 = -1$
3. Аксиома минимальности. $(\mathbb{R} \subseteq K \subseteq \mathbb{C}) \wedge (i \in K) \Rightarrow K = \mathbb{C}$.

A.2.1. Алгебраическая форма записи

Теорема. $\forall z \in \mathbb{C}\ \exists! x, y \in \mathbb{R}$:

$$z = x + i \cdot y \tag{2.1}$$

Причём x называется *действительной частью* числа z и обозначается $\mathrm{Re}(z)$, а y — *мнимой частью* числа z и обозначается $\mathrm{Im}(z)$.

Доказательство. $\square$ Существавание. Пусть $K = \{x + i \cdot y \mid x, y \in \mathbb{R}\}$. Тогда

1. $\mathbb{R} \subset K$, так как $\forall x \in \mathbb{R} : x = (x + i \cdot 0) \in K$.
2. $i \in K$, так как $i = (0 + i \cdot 1) \in K$.
3. K — подполе $\mathbb{C}$. Докажем это:
   - 3.1. Замкнутость относительно сложения. Пусть $z_1 = x_1 + i \cdot y_1 \in K$, $z_2 = x_2 + i \cdot y_2 \in K$. Тогда
   $$z_1 + z_2 = (x_1 + x_2) + i \cdot (y_1 + y_2) \in K \tag{2.2}$$
   - 3.2. Замкнутость относительно умножения. Пусть $z_1 = x_1 + i \cdot y_1 \in K$, $z_2 = x_2 + i \cdot y_2 \in K$. Тогда
   $$z_1 z_2 = (x_1 x_2 - y_1 y_2) + i \cdot (x_1 y_2 + x_2 y_1) \in K \tag{2.3}$$
   - 3.3. Если $0 \neq z \in K$, то $z^{-1} \in K$. Пусть $z = x + i \cdot y$. Тогда
   $$z^{-1} = \frac{x - i \cdot y}{x^2 + y^2} = \left(\frac{x}{x^2 + y^2}\right) + i \cdot \left(-\frac{y}{x^2 + y^2}\right) \in K \tag{2.4}$$

   Таким образом, $\mathbb{R} \subset K \subseteq \mathbb{C}$, по аксиоме минимальности $K = \mathbb{C}$.

Единственность. Пусть $z = x_1 + i \cdot y_1 = x_2 + i \cdot y_2$. Тогда $(x_1 - x_2) + i \cdot (y_1 - y_2) = 0$. Следовательно, $x_1 - x_2 = 0$ и $y_1 - y_2 = 0$, то есть $x_1 = x_2$ и $y_1 = y_2$. $\blacksquare$

A.2.2. Единственность поля комплексных чисел

Теорема. Поле комплексных чисел единственно с точностью до изоморфизма.

Доказательство. □ Пусть $\mathbb{C}'$ — другое поле комплексных чисел, тогда оно удовлетворяет аксиомам:

1. $\mathbb{R}' \subset \mathbb{C}'$
2. $\exists i' \in \mathbb{C}' : (i')^2 = -1$
3. $(\mathbb{R} \subseteq K' \subseteq \mathbb{C}') \wedge (i' \in K') \Rightarrow K' = \mathbb{C}'$.

Заменив $\mathbb{R}'$ на изоморфное поле $\mathbb{R}$, можем считать, что $\mathbb{R} \subset \mathbb{C}'$. Рассмотрим отображение $\varphi : \mathbb{C} \to \mathbb{C}'$, определённое следующим образом:

$$\forall z = x + i \cdot y \in \mathbb{C} : \varphi(z) = x + i' \cdot y, \tag{2.5}$$

где $i' \in \mathbb{C}'$ — мнимая единица в $\mathbb{C}'$. Покажем, что φ — изоморфизм полей. Отображение φ биективно, в силу существования и единственности алгебраической формы комлпексного числа в обоих полях. Так же φ сохраняет операции сложения и умножения, так как операции над числами сводятся к операциям над их действительными и мнимыми частями, а они сохраняются изоморфизмом $\mathbb{R} \simeq \mathbb{R}'$. Таким образом, φ — изоморфизм полей. ■

A.2.3. Существование поля комплексных чисел

Теорема. Существует поле комплексных чисел, причём

$$\mathbb{C} = \mathbb{R}^2 \tag{2.6}$$

Доказательство. Рассмотрим множество всех упорядоченных пар действительных чисел $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$. Определим на этом множестве операции сложения и умножения следующим образом:

1. $\forall (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2 : (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$
2. $\forall (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2 : (x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$

Проверим, что $\mathbb{R}^2$ с такими операциями образует поле.

1. Коммутативность сложения и умножения очевидна.
2. Ассоциативность сложения очевидна.
3. Ассоциативность умножения. Пусть даны три элемента $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R}^2$. Действительно,

$$
\begin{aligned}
&((x_1, y_1) \cdot (x_2, y_2)) \cdot (x_3, y_3) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) \cdot (x_3, y_3) = \\
&= ((x_1x_2 - y_1y_2)x_3 - (x_1y_2 + x_2y_1)y_3, (x_1x_2 - y_1y_2)y_3 + (x_1y_2 + x_2y_1)x_3) = \\
&= (x_1(x_2x_3 - y_2y_3) - y_1(x_2y_3 + x_3y_2), x_1(x_2y_3 + x_3y_2) + y_1(x_2x_3 - y_2y_3)) = \\
&= (x_1, y_1) \cdot (x_2x_3 - y_2y_3, x_2y_3 + x_3y_2) = (x_1, y_1) \cdot ((x_2, y_2) \cdot (x_3, y_3))
\end{aligned} \tag{2.7}
$$

4. Дистрибутивность проверяется аналогично.

5. Нулевой элемент: $(0, 0)$

6. Единичный элемент: $(1, 0)$

7. Противоположный элемент: $\forall (x, y) \in \mathbb{R}^2 : -(x, y) = (-x, -y)$

8. Обратный элемент: Пусть $(x, y) \in \mathbb{R}^2$, причём $(x, y) \neq (0, 0)$. Тогда

$$
(x, y)^{-1} = \left(\frac{x}{x^2 + y^2}, -\frac{y}{x^2 + y^2} \right) \tag{2.8}
$$

   Таким образом, множество $\mathbb{R}^2$ с определёнными операциями образует поле. Теперь установим, что $\mathbb{R}^2 = \mathbb{C}$.

9. Рассмотрим $\mathbb{R}^2 \supset \mathbb{R} \times \{0\} = \{(x, 0) \mid x \in \mathbb{R}\}$. Это подполе $\mathbb{R}^2$, изоморфное $\mathbb{R}$ через отображение $\psi : \mathbb{R} \to \mathbb{R}^2$, $\forall x \in \mathbb{R} : \psi(x) = (x, 0)$.

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

   9.2. $(x_1, 0) \cdot (x_2, 0) = (x_1x_2, 0)$

10. Рассмотрим элемент $i = (0, 1) \in \mathbb{R}^2$. Легко видеть, что $i^2 = (0, 1) \cdot (0, 1) = (-1, 0)$.

11. Минимальность. Пусть $K \subset \mathbb{R}^2$ — подполе, содержащее $\mathbb{R} \times \{0\}$ и элемент $i = (0, 1)$. Тогда любой элемент $(x, y) \in \mathbb{R}^2$ можно записать как $(x, 0) + (0, 1) \cdot (y, 0)$, где $(x, 0), (y, 0) \in \mathbb{R} \times \{0\} \subset K$. Поскольку K — подполе, то $(x, y) \in K$. Таким образом, $K = \mathbb{R}^2$.

Таким образом, $\mathbb{R}^2$ является моделью поля комплексных чисел. ■

A.2.4. Геометрическая интерпретация комплексных чисел

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

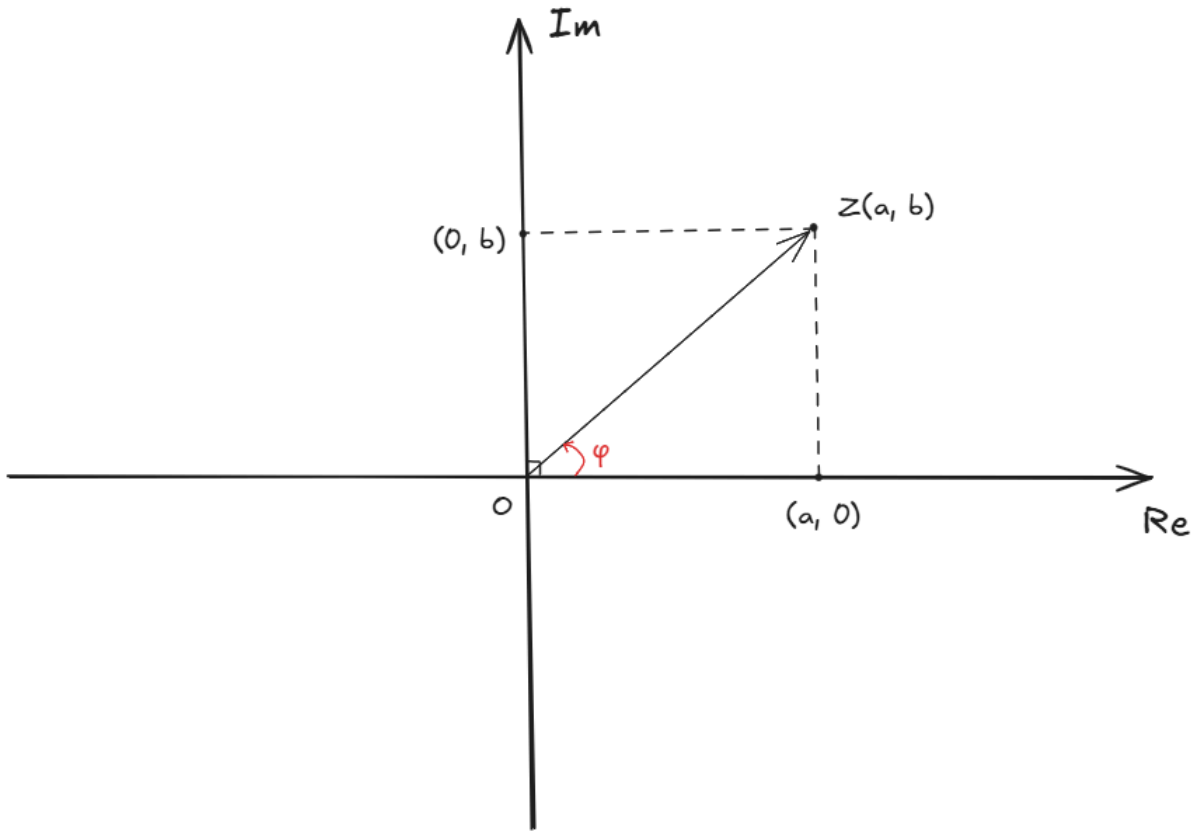


Рис. 1 - комплексная плоскость

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

A.2.5. Тригонометрическая форма записи

Определение. Величина $|z| = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}$ называется *модулем* z.

Определение. Многозначная функция $\operatorname{Arg}(z) = \varphi$, где φ — ориентированный угол между радиус-вектором z и положительным направлением оси абсцисс называется *аргументом комплексного числа.* Аргумент числа $(0, 0)$ не определён.

Для однозначности определяют $\arg(z) \in [0, 2\pi)$. Она однозначна.

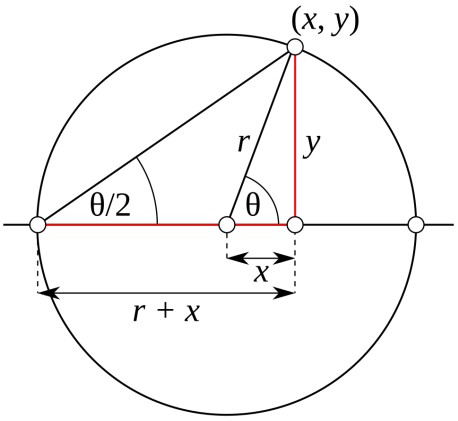
Пусть $z = x + yi$. Сделаем замену:

$$\begin{cases} r = |z| = \sqrt{x^2 + x^2} \\ \theta = \arg(z) \end{cases} \tag{2.9}$$

Теорема. Явное выражение для значения аргумента из $(-\pi, \pi]$

$$\operatorname{Arg}(z) = 2 \operatorname{arctg}\left(\frac{y}{x + \sqrt{x^2 + y^2}}\right) \tag{2.10}$$

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



$$\operatorname{tg}\left(\frac{\theta}{2}\right) = \frac{y}{x+r} \tag{2.11}$$

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

A.2.6. Формы записи комплексных чисел

1. Алгебраическая:

$$z = x + yi \tag{2.12}$$

2. Тригонометрическая:

$$z = r(\cos\varphi + i\sin\varphi) \tag{2.13}$$

3. Показательная:

$$z = re^{i\varphi} \tag{2.14}$$

Показательная форма есть просто следствие формулы Эйлера:

$$e^{i\varphi} = \cos\varphi + i\sin\varphi \tag{2.15}$$

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

$$\sin z = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \ldots = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n+1}}{(2n+1)!} \tag{2.16}$$

$$\cos z = 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \ldots = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n}}{(2n)!} \tag{2.17}$$

$$e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + ... = \sum_{n=0}^{\infty} \frac{z^n}{n!} \tag{2.18}$$

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, $i^n = i^{n-4}$.

A.2.7. Умножение комплексных чисел в тригонометрической форме

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:

$$\begin{gathered} z_1 z_2 = r_1 r_2(\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_2 + i\sin\varphi_2) = \\ = r_1 r_2(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 + i(\sin\varphi_1\cos\varphi_2 + \cos\varphi_1\sin\varphi_2)) = \\ = r_1 r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)) \end{gathered} \tag{2.19}$$

Итак,

$$\begin{cases} |z_1 z_2| = |z_1||z_2| \\ \arg(z_1 z_2) = \arg(z_1) + \arg(z_2) \end{cases} \tag{2.20}$$

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

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

$$z^n = r^n(\cos(n\varphi) + i\sin(n\varphi)) \tag{2.21}$$

Доказательство. □ докажем по индукции.

1. База: $n = 1$. Тогда $z^1 = z = r(\cos\varphi + i\sin\varphi)$. Это уже получено.
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

$$\begin{gathered} z^{n+1} = z^n z = r^n r(\cos(n\varphi + \varphi) + i\sin(n\varphi + \varphi)) = \\ = r^{n+1}(\cos((n+1)\varphi) + i\sin((n+1)\varphi)) \blacksquare \end{gathered} \tag{2.22}$$

Таким образом, формула верна для $n + 1 \Rightarrow$ она верна $\forall n \in \mathbb{N}$.

Чтобы доказать её для $n < 0$, достаточно написать $z^n = z^{-|n|}$. В случае $z \neq 0$ и $n = 0$ имеем $z^0 = 1$. ■

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 $\mathbb{R}^2 \to \mathbb{R}^2$ называется *поворотной гомотетией:* $H_O^{r_2,\varphi_2} = H_O^{r_2} \cdot R_O^{\varphi_2}$.

A.2.8. Извлечение корней

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

$\forall z \in \mathbb{C} : \left|(\sqrt[n]{z})\right| = n.$

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

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

1. Очевидно, что $|w_k| = \sqrt{r}$, где $\sqrt{r}$ — *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 $k \in \{k_0 + i \mid i = 0, 1, ...(n-1)\}$ будут получаться все n корней. Поэтому для удобства полагают $k_0 = 0$. ■

Теорема. Формула корней числа $z = r(\cos\varphi + i\sin\varphi)$ $\forall k \in \{0, 1, ..., n-1\}$:

$$w_k = \sqrt{r}\left(\cos\left(\frac{\varphi}{n} + 2\pi\frac{k}{n}\right) + i\sin\left(\frac{\varphi}{n} + 2\pi\frac{k}{n}\right)\right) \tag{2.23}$$

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

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 $\frac{2\pi}{n}$.

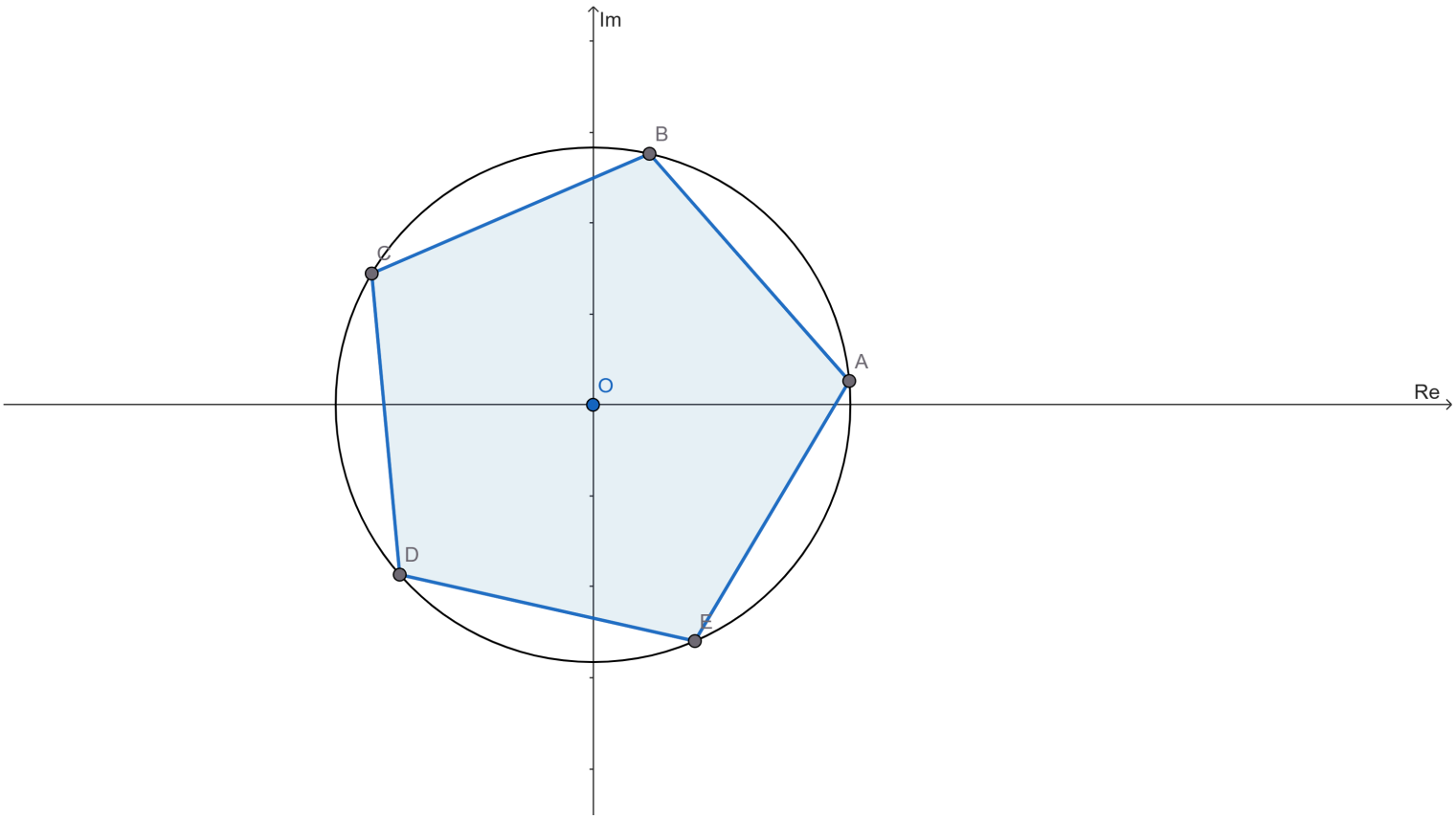


Рис. 2 — корни 5 степени из $z = 4 + 4i$

A.2.9. Корни из единицы

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

$$\sqrt[n]{1} = \varepsilon_k = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right) \tag{2.24}$$

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

Все корни есть вершины правильного n-угольника, вписанного в окружность единичного радиуса.

Свойства корней из единицы.

1. Если $\{w_k\}$ — корни n из комплексного числа z, то

$$w_k \cdot \varepsilon_l = w_{k+l(\mathrm{mod}\, n)} \tag{2.25}$$

2. $\varepsilon_k \cdot \varepsilon_l = \varepsilon_{k+l(\mathrm{mod}\, n)}$
3. $\varepsilon_k^{-1} = \varepsilon_{n-k(\mathrm{mod}\, n)}$

4. Из свойств (2) и (3) следует, что множество корней степени n единицы с операцией умножения образует подгруппу мультипликативной группы $\mathbb{C}^\times$ поля комплексных чисел.

$$\mathbb{U}_n = \{\varepsilon_k \mid k = 0, 1, ..., n-1\} \subset \mathbb{C}^\times \tag{2.26}$$

5. $\mathbb{U}_n \simeq \mathbb{Z}_n$ — эта группа изоморфна аддитивной группе вычетов по модулю n через отображение $\varphi : \mathbb{Z}_n \to \mathbb{U}_n$, $\forall k \in \mathbb{Z}_n : \varphi(k) = \varepsilon_k$.

Определение. Первообразным корнем степени n из единицы называется такой корень из единицы, не являющийся корнем из единицы степени $m < n$.

Любой корень из единицы является первообразным для какой-то степпени n.

Предложение. Число $\varepsilon_k = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$ ялвяется первообразным корнем степени n из единицы тогда и только тогда, когда $\gcd(k, n) = 1$.

Доказательство. □ Возьведём k-й корень из 1 в степень m:

$$\varepsilon_k^m = \varepsilon_{k\cdot m} = \cos\left(\frac{2\pi(k\cdot m)}{n}\right) + i\sin\left(\frac{2\pi(k\cdot m)}{n}\right) = 1 \Leftrightarrow n \mid (k\cdot m) \tag{2.27}$$

1. Пусть $\gcd(k, n) = 1$. Тогда $n \mid (k\cdot m) \Rightarrow n \mid m$. Следовательно, ε_k не является корнем из единицы степени $m < n$. Поэтому, ε_k — первообразный корень степени n из единицы.

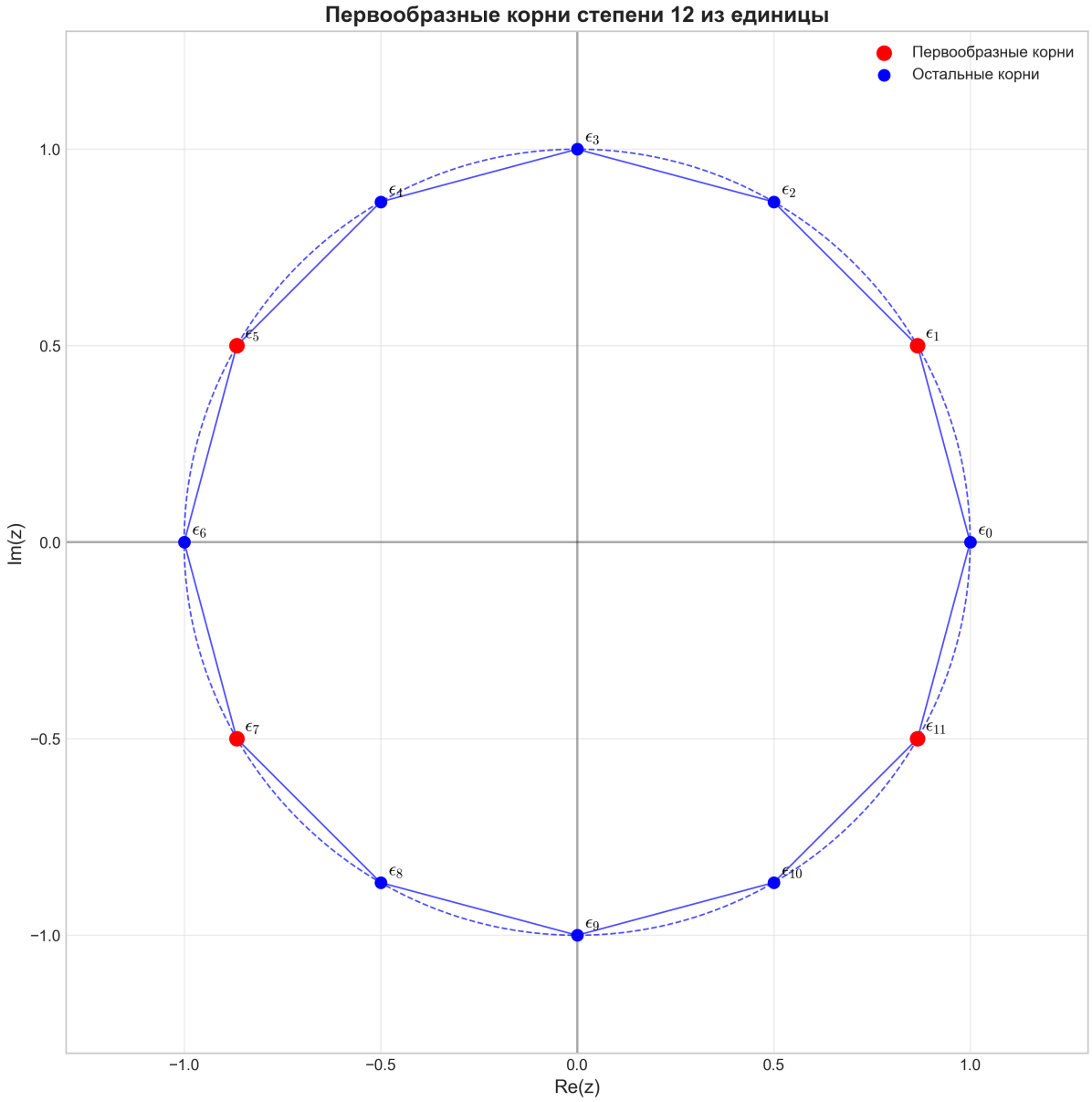
2. Пусть $k = d\cdot l$, $n = d\cdot m$, где $d = \gcd(k, n) > 1$. Тогда

$$\begin{gathered}\varepsilon_k^m = \varepsilon_{d\cdot l\cdot m} = \cos\left(\frac{2\pi(d\cdot l\cdot m)}{d\cdot m}\right) + i\sin\left(\frac{2\pi(d\cdot l\cdot m)}{d\cdot m}\right) = \\ = \cos(2\pi l) + i\sin(2\pi l) = 1\end{gathered} \tag{2.28}$$

Таким образом, ε_k является корнем из единицы степени $m < n$. Следовательно, ε_k не является первообразным корнем степени n из единицы. ■

Например, для $n = 12$ первообразными корнями из 1 являются $\varepsilon_1, \varepsilon_5, \varepsilon_7, \varepsilon_{11}$, так как $\gcd(1, 12) = 1$, $\gcd(5, 12) = 1$, $\gcd(7, 12) = 1$, $\gcd(11, 12) = 1$.

Количество первообразных корней степени n из единицы равно $\varphi(n)$, где φ — функция Эйлера.


Первообразные корни степени 12 из единицы
Первообразные корни
Остальные корни
ϵ_0
ϵ_1
ϵ_2
ϵ_3
ϵ_4
ϵ_5
ϵ_6
ϵ_7
ϵ_8
ϵ_9
ϵ_{10}
ϵ_{11}
1.0
0.5
0.0
−0.5
−1.0
Im(z)
−1.0
−0.5
0.0
0.5
1.0
Re(z)

A.3. Системы линейных алгебраический уравнений

Определение. Система линейных (алгебраических) уравнений имеет вид:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n = b_2 \\ \vdots \ ..... \\ a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n = b_m \end{cases} \tag{3.1}$$

где $x_1, x_2, ..., x_n$ - неизвестные, a_{ij} — коэфициенты для $i = 1, ..., m$ и $j = 1, ..., n$. И, наконец, b_i — свободные члены($i = 1, ..., n$).

Определение. Решением СЛУ называется упорядоченный набор чисел $(x_1^0, x_2^0, ..., x_n^0)$, при подстановке которого вместо неизвестных, все уравнения обращаются в равенства.

Определение. СЛУ называется совместной, если у неё $\exists$ решение.

Определение. СЛУ называется несовместной, если у неё $\nexists$ решений.

Определение. СЛУ называется определённой, если у неё $\exists!$ решение.

Определение. СЛУ называется неопределённой, если у неё $\exists > 1$ решения.

Определение. Матрицей коэффициентов системы линейных уравнений называется прямоугольная таблица, составленная из всех коэффициентов при неизвестных в уравнениях системы.

$$A = \begin{pmatrix} a_{11}x_1 & a_{12}x_2 & ... & a_{1n}x_n \\ a_{21}x_1 & a_{22}x_2 & ... & a_{2n}x_n \\ ... & ... & ... & \\ a_{m1}x_1 & a_{m2}x_2 & ... & a_{mn}x_n \end{pmatrix} \tag{3.2}$$

Определение. Расширенной матрицей системы линейных уравнений называется матрица, полученная из матрицы коэффициентов добавлением столбца свободных членов.

$$\tilde{A} = \begin{pmatrix} a_{11}x_1 & a_{12}x_2 & ... & a_{1n}x_n & b_1 \\ a_{21}x_1 & a_{22}x_2 & ... & a_{2n}x_n & b_2 \\ ... & ... & ... & ... & ... \\ a_{m1}x_1 & a_{m2}x_2 & ... & a_{mn}x_n & b_m \end{pmatrix} \tag{3.3}$$

A.3.1. Сложение и умножение строк

- Сложение двух строк:

$$(c_1, c_2, ..., c_n) + (d_1, d_2, ..., d_n) = (c_1 + d_1, c_2 + d_2, ..., c_n + d_n) \tag{3.4}$$

- Умножение строки на число:

$$\lambda(c_1, c_2, ..., c_n) = (\lambda c_1, \lambda c_2, ..., \lambda c_n) \tag{3.5}$$

A.3.2. Элементарные преобразования систем линейных уравнений и их матриц

Определение. Элементарными преобразованиями системы линейных уравнений называются следующие операции:

1. Элементарные преобразования I типа. Прибавляем к одному уравнению другое, умноженное на некоторое число.

   Символически:

$$(i)' = (i) + \lambda(j). \tag{3.6}$$

   В терминах матриц:

$$\widetilde{A'}_i = \tilde{A}_i + \lambda \cdot \tilde{A}_j \tag{3.7}$$

$$\widetilde{A'}_k = \tilde{A}_k, \ \forall k \neq i. \tag{3.8}$$

2. Элементарные преобразования II типа. Умножаем одно уравнение на некоторое число.

   Символически:

$$(i) \leftrightarrow (j). \tag{3.9}$$

   В терминах матриц:

$$\widetilde{A'}_i = \tilde{A}_j \tag{3.10}$$

$$\widetilde{A'}_j = \tilde{A}_i \tag{3.11}$$

$$\widetilde{A'}_k = \tilde{A}_k, \ \forall k \neq i, j. \tag{3.12}$$

3. Элементарные преобразования III типа. Умножение строки на ненулевое число.

   Символически:

$$(i)' = \lambda \cdot (i), \ \lambda \neq 0. \tag{3.13}$$

   В терминах матриц:

$$\widetilde{A'}_i = \lambda \cdot \tilde{A}_i, \ \lambda \neq 0 \tag{3.14}$$

$$\widetilde{A'}_k = \tilde{A}_k, \ \forall k \neq i. \tag{3.15}$$

Предложение. Элементарные преобразования системы линейных уравнений не изменяют множество её решений.

Доказательство. □ Если из сходной СЛУ мы получили новую систему с помощью элементарных преобразованиях, то уравнения новой системы следуют из уравнений исходной системы:

- преобразования I типа для решения системы сохраняют верное равенство;
- преобразования II типа меняют только порядок записи;
- преобразования III типа не изменяют верное равенство.

Отсюда любое решение исходной системы является решением и новой системы. Теперь докажем, что любое решение новой системы является решением и исходной системы. Это происходит ввиду того, что $\forall$ элементарного преобразования $\exists$ обратное элементарное преобразование.

- Для I типа: $(i)' = (i) + \lambda(j) \Rightarrow (i) = (i)' - \lambda(j)$
- Для II типа: $(i)' = (j) \Rightarrow (i) = (j)'$
- Для III типа $(i)' = \lambda(i) \Rightarrow (i) = \frac{1}{\lambda}(i)'$

Применяя к обратным преобразованиям то же самое рассуждение, что и выше, мы и получим, что любое решение новой системы является решением и исходной системы. Следовательно, две системы эквивалентны. ■

A.3.3. Метод Гаусса решения систем линейных уравнений

Определение. Назовём *ведущим элементом* или же *лидером* числовой строки первый слева ненулевой элемент:

$$a_i : a_j = 0, \ \forall j < i. \tag{3.16}$$

Метод Гауса заключается в следующих шагах:

1. Выберем строку, лидер которой стоит на самой левой позиции.
2. Переставим эту строку с первой строкой с помощью элементарного преобразования II типа.
3. Обнулим коэфициент под лидером первой строки с помощью элементарного преобразования I типа.
4. Рассмотрим матрицу из всех строк, кроме первой: $\overline{A}$.
   - $\overline{A} = 0 \Rightarrow$ алгоритм завершается.
   - $\overline{A} \neq 0 \Rightarrow$ повторить шаги 1-4.

В итоге мы получим так называемую *ступенчатую матрицу.*

Определение. Ступенчатая матрица — это матрица, в которой:

- все ненулевые строки идут в начале
- все нулевые строки идут в конце
- лидер каждой ненулевой строки находится правее лидера предыдущей строки.

В качестве дополнительного шага, с помощью элементарных преобразований III типа мы можем сделать так, чтобы на местах лидеров всех строк были единицы. Получим так называемый *улучшенный ступенчатый вид матрицы.*

A.3.4. Ранг ступенчатой матрицы

Определение. Ранг ступенчатой матрицы — это количество ненулевых строк в ней.

Пусть A^* — ступенчатая матрица, $r = \text{rank}(A^*)$ и $\tilde{r} = \text{rank}\left(\widetilde{A^*}\right)$. Рассмотрим 2 случая:

1. $r < \tilde{r} \Rightarrow \tilde{r} = r + 1$. В $(r+1)$-м уравнении системы в левой части только нулевые коэфициенты, а в правой части лидер $(r+1)$-й строки матрицы $\widetilde{A^*}$. Выходит: $0 = b^*_{r+1}$ — противоречивое уравнение. Итак, если ранг матрицы меньше ранга расширенной матрицы, то СЛУ несовместна.

2. $r = \tilde{r}$. Пусть номера столбцов, содержащих лидеров столбцов равны $j_1, j_2, ..., j_r$. Назовём

   - $x_{j_1}, x_{j_2}, ..., x_{j_r}$ — главные неизвестные,
   - $\left(x_j\right), j \neq j_1, j_2, ..., j_r$ — свободные неизвестные.

   Обратный ход метода Гаусса. Рассмотрим r-е уравнение системы:

$$(r)\ a^*_{r,j_r} + ... = b^*_r \tag{3.17}$$

$$x_{j_r} = \frac{b^*_r - \sum_{j>j_r} a^*_{r_j} x_j}{a_{r_j}} \tag{3.18}$$

   Выразили неизвестную x_{j_r} через свободные неизвестные. Поднимемся на $(r-1)$-е уравнение.

$$(r-1) \Rightarrow x_{j_{r-1}} \text{ выражается через } x_j, j > j_{r-1}. \tag{3.19}$$

   И так далее, поднимаясь до первого уравнения. В итоге вы выражаем главные неизвестные через свободные, получая общее решение.

$$x_{j_k} = \sum_{j \neq j_1, ..., j_k} c_{kj} x_j + c_k,\ \forall k = 1, ..., r. \tag{3.20}$$

Подставляя конкретные значения для свободных неизвестных, мы получаем частное решение системы $\Rightarrow$ СЛУ совместна.

A.3.5. Критерий совместности и определённости системы

Теорема. Пусть матрица СЛУ имеет ранг r, расширенная матрица имеет ранг $\tilde{r}$, а число неизвестных равно n. Тогда СЛУ:

- совместна $\Leftrightarrow r = \tilde{r}$
- несовместна $\Leftrightarrow r < \tilde{r}$
- определена $\Leftrightarrow r = \tilde{r} = n$
- неопределена $\Leftrightarrow r = \tilde{r} < n$.

Доказательство. $\square$ Осталось доказать критерии определённости и неопределённости. Пусть СЛУ совместна. Количество свободных неизвестных равно количество неизвестных минус количество главных неизвестных: $(n - r)$.

- Если $n = r$, то свободных неизвестных нет, и тогда система определена. Если свободных неизвестных нет, то $r = n$.
- Если $n > r$, то свободные неизвестные есть, и тогда система неопределена.

$\blacksquare$

A.3.6. Однородные системы линейных уравнений

Определение. Однородная система линейных уравнений — это система вида:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n = 0 \\ \vdots \ ..... \\ a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n = 0 \end{cases} \tag{3.21}$$

Однородная система линейных уравнений всегда совместна: нулевое решение $x_1 = x_2 = ... = x_n = 0$.

Предложение. Однородная система линейных уравнений, в которой количество уравнений меньше количества неизвестных, всегда имеет ненулевое решение.

Доказательство. $\square$ Приведём однородную систему к ступенчатому виду. Тогда $r = \tilde{r}$, поскольку система всегда совместна. Ранг не превосходит количества строк системы: $r \leq m \underset{\text{по усл.}}{<} n$. По теореме Кронекера-Капелли, такая система неопределена, а значит кроме нулевого решения $\exists$ ненулевое. $\blacksquare$

A.4. Векторные пространства

Определение. Векторным пространством называется множество V, на котором заданы две алгебраические операции — сложение векторов и умножение векторов на числа — которые удовлетворяют следующим *аксиомам векторного пространства.*

1. Коммутативность сложения: $\forall u, v \in V$: $u + v = v + u$.
2. Ассоциативность сложения: $\forall u, v, w \in V$: $(u + v) + w = u + (v + w)$.
3. Нулевой вектор: $\exists 0 \in V$: $\forall v \in V$: $v + 0 = v$. (иногда обозначается $\vec{0}$)
4. Противоположный вектор: $\forall v \in V : \exists w \in V : v + w = 0$.
5. Ассоциативность умножения: $\forall \lambda, \mu \in \mathbb{R}, v \in V : \lambda \cdot (\mu \cdot v) = (\lambda\mu) \cdot v$.
6. Дистрибутивность умножения относительно сложения векторов: $\forall \lambda \in \mathbb{R}, u, v \in V : \lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v$.
7. Дистрибутивность умножения относительно сложения чисел: $\forall \lambda, \mu \in \mathbb{R}, v \in V : (\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$.
8. Аксиома нормировки: $\forall v \in V : 1 \cdot v = v$.

A.4.1. Примеры векторных пространств

1. $V = \{$все свободные геометрические векторы пространства$\}$. На этом множестве геометрически определяются операции сложения и умножения на числа.
   - Сложение по правилу параллелограмма.
   - Умножение на число: $\forall \lambda \in \mathbb{R}, v \in V$:

$$|\lambda v| = |\lambda||v| \tag{4.1}$$

$$\begin{cases} (\lambda v) \uparrow\uparrow v \text{ , если } \lambda > 0 \\ (\lambda v) \uparrow\downarrow v \text{ , если } \lambda < 0 \end{cases} \tag{4.2}$$

   - Противоположный вектор: $\forall v \in V : v + (-v) = \vec{0}$.
2. Арифметическое векторное пространство: $V = \mathbb{R}^n$. Элементы этого множества это упорядоченные наборы $(x_1, x_2, ..., x_n), x_i \in \mathbb{R} (i = 1, ..., n)$.
   - Сложение: $\forall u, v \in V : u + v = (u_1 + v_1, u_2 + v_2, ..., u_n + v_n)$.
   - Умножение на число: $\forall \lambda \in \mathbb{R}, v \in V : \lambda \cdot v = (\lambda v_1, \lambda v_2, ..., \lambda v_n)$.
   - Нулевой вектор: $(0, 0, ..., 0)$.
   - Противоположный вектор: $\forall v = (v_1, v_2, ..., v_n) \in V : -v = (-v_1, -v_2, ..., -v_n)$.
3. Пространство функций на множестве X: $V = \mathcal{F}(X, \mathbb{R}) = \{f : X \to \mathbb{R}\}$.

- сумма: $\forall f, g \in V, \forall x \in X : (f + g)(x) = f(x) + g(x)$.
- умножение на число: $\forall \lambda \in \mathbb{R}, f \in V, \forall x \in X : (\lambda \cdot f)(x) = \lambda \cdot (f(x))$.

A.4.2. Простейшие следствия из аксиом векторного пространства

1. Единственность нулевого вектора: $\exists! 0 \in V$.

   Доказательство. □ Пусть $0'$ — другой нулевой вектор. Рассмотрим их сумму: $0 + 0' = 0$ (так как $0'$ — нулевой вектор). Но $0 + 0' = 0'$ (так как 0 — нулевой вектор). Следовательно, $0 = 0'$. ■

2. Единственность противоположного вектора: $\forall v \in V : \exists! w \in V : v + w = 0$.

   Доказательство. □ Пусть $w' \neq w$ — другой вектор, противоположный v. Рассмотрим $w + v + w'$:

   $$(w + v) + w' = 0 + w' = w' \tag{4.3}$$

   $$w + (v + w') = w + 0 = w \tag{4.4}$$

   Следовательно, $w = w'$. Значит, противоположный вектор для данного только один. ■

   2.1. Поэтому противоположный вектор для $v \in V$ можно обозначить: $(-v)$.

3. $\forall v \in V : 0 \cdot v = \vec{0}$.

   Доказательство. □ $0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v$. Добавим к обеим частям равенства $-(0 \cdot v)$, тогда получим: $\vec{0} = 0 \cdot v$ ■

4. $\forall \lambda \in \mathbb{R} : \lambda \cdot \vec{0} = 0$.

   Доказательство. □ $\lambda \cdot \vec{0} = \lambda \cdot \left(\vec{0} + \vec{0}\right) = \lambda \cdot \vec{0} + \lambda \cdot \vec{0} \Rightarrow \lambda \cdot \vec{0} = 0$. ■

5. $\forall v \in V : (-1) \cdot v = -v$.

   Доказательство. □ $v + (-1) \cdot v = 1 \cdot v + (-1) \cdot v = (1 + (-1)) \cdot v = 0 \cdot v = \vec{0}$. ■

A.4.3. Линейные комбинации

Определение. Линейной комбинацией векторов $v_1, v_2, ..., v_n \in V$ с коэффициентами $\lambda_1, \lambda_2, ..., \lambda_n \in \mathbb{R}$ называется выражение вида:

$$\lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + ... + \lambda_n \cdot v_n \tag{4.5}$$

Её значение тоже вектор из V.

Определение. Тривиальной линейной комбинацией называется линейная комбинация, в которой все коэффициенты равны нулю: $\lambda_1 = \lambda_2 = ... = \lambda_n = 0$. Её значение равно нулю.

Определение. Система векторов $S = \{v_1, v_2, ..., v_n\}$ называется *зависимой*, если $\exists$ нетривиальная линейная комбинация этих векторов, равная нулю.

A.4.3.1. Примеры линейных комбинаций

1. $S = \{v\}$ линейно зависима $\Leftrightarrow v = 0$.

   Доказательство. $\square$

   - $\lambda \cdot v = \vec{0} \Rightarrow v = \frac{1}{\lambda} \cdot \vec{0} = \vec{0}$.
   - Обратно, $v = 0 \Rightarrow 1 \cdot v = \vec{0}$. $\blacksquare$

2. $S = \{v_1, v_2\}$ линейно зависима $\Leftrightarrow \exists \mu \in \mathbb{R} : v_1 = \mu \cdot v_2$.

   Доказательство. $\square$

   1) $\Rightarrow$ Пусть $\lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 = 0$ — нетривиальная линейная комбинация. Тогда $v_1 = -\frac{\lambda_2}{\lambda_1} \cdot v_2$ — векторы пропорциональны.

   2) $\Leftarrow$ Пусть $v_1 = \mu \cdot v_2$ для некоторого $\mu \in \mathbb{R}$. Тогда $v_1 + (-\mu) \cdot v_2 = 0$, что и означает зависимость векторов. $\blacksquare$

A.4.4. Свойства линейной зависимости

1. Если система векторов S линейно зависима и $S \subset S'$, то S' тоже линейно зависима.

   Доказательство. $\square$ Пусть $S = \{v_1, v_2, ..., v_m\}$, $S' = \{v_1, ..., v_m, v_{m+1}, ..., v_n\}$. Тогда $\exists$ нетривиальная линейная комбинация векторов из S, равная нулю:

   $$\lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + ... + \lambda_m \cdot v_m = 0 \tag{4.6}$$

   Добавим к ней векторы из $S' \setminus S$ с нулевыми коэффициентами:

   $$\lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + ... + \lambda_m \cdot v_m + 0 \cdot v_{m+1} + ... + 0 \cdot v_n = 0 \tag{4.7}$$

   Нетривиальная линейная комбинация векторов из S' равна нулю $\Rightarrow S'$ линейно зависима. $\blacksquare$

2. Если система векторов S линейно независима и $S' \subset S$, то S' тоже линейно независима.

Доказательство. □ Если бы S' была линейно зависима, то по свойству 1 S тоже была бы линейно зависима, что противоречит условию, поэтому S' линейно независима. ■

3. Система векторов S линейно зависима $\Leftrightarrow \exists v \in S$: v равен линейной комбинации векторов из $S \setminus \{v\}$.

   Доказательство. □

   1) $\Rightarrow$. Пусть $S = \{v_1, ..., v_n\}$ и $\exists \lambda_i (i = 1, ..., n)$:

   $$\lambda_1 v_1 + ... + \lambda_n = 0,\ \exists \lambda_j \neq 0. \tag{4.8}$$

   Отсюда получим:

   $$v_i = -\frac{\lambda_1}{\lambda_i} v_1 + ... + \left(-\frac{\lambda_{i-1}}{\lambda_i} v_{i-1}\right) + \left(-\frac{\lambda_{i+1}}{\lambda_i} v_{i+1}\right) + ... + \left(-\frac{\lambda_n}{\lambda_i} v_n\right) \tag{4.9}$$

   2) $\Leftarrow$. Пусть $v_i = \mu_1 v_1 + ... + \mu_{i-1} v_{i-1} + \mu_{i+1} v_{i+1} + ... + \mu_n v_n$. Перенесём всё в правую часть:

   $$\mu_1 v_1 + ... + \mu_{i-1} v_{i-1} + (-1) \cdot v_i + \mu_{i+1} v_{i+1} + ... + \mu_n v_n = 0. \tag{4.10}$$

   ■

4. Пусть S линейно независима, но $S \cup \{v\}$ линейно зависима $\Rightarrow v$ линейно выражается через S единственным способом.

   Доказательство. □ Обозначим $S = \{v_1, ..., v_n\}$. При добавлении v $\exists$ нетривиальная ЛК, равная нулю:

   $$\lambda_1 v_1 + ... + \lambda_n v_n + \lambda v = 0. \tag{4.11}$$

   Тогда $\lambda \neq 0$. Иначе, если бы $\lambda = 0$, мы получили бы

   $$\lambda_1 v_1 + ... + \lambda_n v_n = 0 \tag{4.12}$$

   Но это противоречит линейной независимости S. Отсюда мы можем выразить v:

   $$v = -\frac{\lambda_1}{\lambda} v_1 + ... + \left(-\frac{\lambda_i}{\lambda} v_i\right) \tag{4.13}$$

   Докажем единственность выражения через систему S. Пусть вектор v представляется двумя способами:

$$v = \alpha_1 v_1 + ... + \alpha_n v_n \tag{4.14}$$

$$v = \beta_1 v_1 + ... + \beta_n v_n \tag{4.15}$$

Отсюда, вычитая эти два равенства, получим

$$(\alpha_1 - \beta_1)v_1 + ... + (\alpha_n - \beta_n) = 0 \tag{4.16}$$

Система S линейно независима $\Rightarrow$ в этой ЛК все коэффициенты равны нулю: $\alpha_i - \beta_i = 0 \Rightarrow \alpha_i = \beta_i,\ i = 1, ..., n$. Значит вектор v выражается единственным способом. ■

5. Основная лемма о линейной зависимости. Пусть $S = \{v_1, ..., v_n\}$ и $T = \{w_1, ..., w_m\}$, причём система S линейно выражается через систему T и $n > m$. Тогда система S линейно зависима.

   Доказательство. □ Если S линейно выражется через T, то $\forall j = 1, ..., n$:

   $$v_j = a_{1j} w_1 + ... + a_{mj} w_j \tag{4.17}$$

   Рассмотрим произвольную ЛК векторов системы S:

   $$\begin{gathered} \lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_n v_n = \sum_{i=j}^{n} \lambda_j v_j = \sum_{j=1}^{n} \left(\lambda_j \cdot \sum_{i=1}^{m} a_{ij} w_i \right) = \\ = \sum_{\substack{i=1,...,m \\ j=1,...,n}} a_{ij} \lambda_j \cdot w_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij} \lambda_j \right) w_i. \end{gathered} \tag{4.18}$$

   Рассмотрим однородную систему линейных уравнений:

   $$\begin{cases} a_{11} x_1 + a_{12} x_2 + ... + a_{1n} x_n = 0 \\ a_{21} x_1 + a_{22} x_2 + ... + a_{2n} x_n = 0 \\ \vdots \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1} x_1 + a_{m2} x_2 + ... + a_{mn} x_n = 0 \end{cases} \tag{4.19}$$

   Здесь $m < n$, то есть число неизвестных больше числа уравнений. Мы знаем, что такая система всегда имеет ненулевое решение. $\exists (x_1^0, ..., x_n^0) = (\lambda_1, ..., \lambda_n)$, где хотя бы один из λ_i не равен нулю, такие, что $\forall i = 1, ..., m$:

   $$\sum_{j=1}^{m} a_{ij} \lambda_j = 0 \tag{4.20}$$

   Но $a_{ij}\lambda_j$ это коэффициенты ЛК в ((4.18)), значит эта ЛК равна нулю.

$$\lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_n v_n = 0 \tag{4.21}$$

И решение $(\lambda_1, ..., \lambda_n)$ ненулевое! $\Rightarrow$ система S линейно зависима! ■

A.4.5. Базис системы векторов

Возьмём ситему векторов $S \subseteq V$ в векторном пространстве V. Рассмотрим конечную подсистему $B \subseteq S$. Следующие 2 условия эквивалентны:

1. B — максимальная линейно независимая подсистема S.
2. B линейно независима и $\forall v \in S$ вектор v линейно выражается через B.

Доказательство. □ Пусть $B = \{v_1, ..., v_r\}$.

1. $(1) \Rightarrow (2)$.
   - Если $v \in B \Rightarrow v = v_i = 0 \cdot v_1 + ... + 1 \cdot v_1 + ... + 0 \cdot v_r$ — линейно выразили через B.
   - $v \in S \setminus B \Rightarrow B \cup \{v\}$ линейно зависима $\underset{\text{св. 4 ЛЗ}}{\Rightarrow}$ v линейно выражается через S.
2. $(2) \Rightarrow (1)$. $v \in S \setminus B \Rightarrow$ v линейно выражается через B $\underset{\text{св. 3 ЛЗ}}{\Rightarrow}$ система $B \cup \{v\}$ линейно зависима $\Rightarrow B$ — максимальная подсистема S. ■

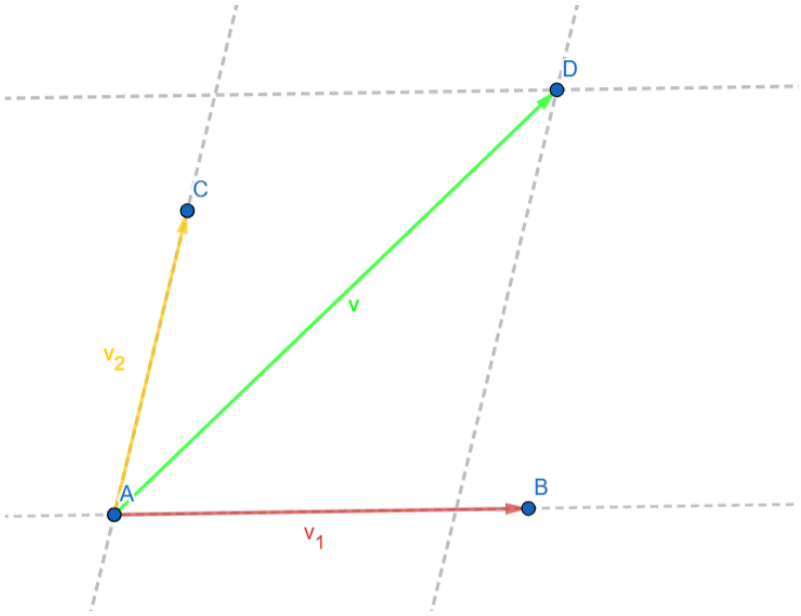
Определение. Конечная подсистема $B \subseteq S$, удовлетвлетворяющая любому из условий (1) или (2), называется *базисом* системы векторов S.

A.4.5.1. Примеры базисов

1. Рассмотрим

   $V = \{$множество всех геометрических векторов на одной прямой$\}$. Здесь $B = \{v\}$, где v — любой ненулевой вектор из V. Например, по второму определению можно выразить $\forall u \in V \ \exists k \in \mathbb{R} : u = k \cdot v$.

2. Пусть $V = \{$множество всех геометрических векторов на плоскости$\}$. Тогда $B = \{v_1, v_2\}$, где v_1 и v_2 неколлинеарны. Это множество является базисом, опять же, по определению 2: $\forall v \in V \ \exists \alpha_1, \alpha_2 \in \mathbb{R} : v = \alpha_1 v_1 + \alpha_2 v_2$.



3. Рассмотрим $V = \{$множество всех геометрических векторов в пространстве$\}$. Тогда $B = \{v_1, v_2, v_3\}$, где v_1, v_2 и v_3 некомпланарны. Это множество также является базисом, по определению 2: $\forall v \in V \ \exists \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R} : v = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3$.

4. Рассмотрим арифметическое векторное пространство $V = \mathbb{R}^n$. Назовём стандартным базисом систему векторов $B = \{e_1, ..., e_n\}$, где $e_i = (0, ..., 0, 1_i, 0, ..., 0)$ — вектор, у которого i-я координата равна 1, а все остальные равны 0.

   Докажем линейную независимость векторов B:

   $$\lambda_1 e_1 + \lambda_2 e_2 + ... + \lambda_n e_n = (\lambda_1, \lambda_2, ..., \lambda_n) \neq 0, \text{если } \exists \lambda_i \neq 0. \tag{4.22}$$

   Мы можем выразить любой вектор $x \in \mathbb{R}^n$:

   $$x = (x_1, x_2, ..., x_n) = x_1 e_1 + x_2 e_2 + ... + x_n e_n. \tag{4.23}$$

A.4.6. Единственность выражения через базисные векторы

Пусть задан базис $B = \{v_1, ..., v_n\}$ системы векторов S. Тогда $\forall v \in S \ \exists! \lambda_1, ..., \lambda_n \in \mathbb{R} : v = \lambda_1 v_1 + ... + \lambda_n v_n$.

Доказательство. □

Существование. $\Leftarrow$ (2) условие в определении базиса.

Единственность. Пусть есть два различных разложения по базису B:

$$v = \lambda_1 v_1 + ... + \lambda_n v_n = \mu_1 v_1 + ... + \mu_n v_n. \tag{4.24}$$

Тогда

$$(\lambda_1 - \mu_1)v_1 + ... + (\lambda_n - \mu_n)v_n = 0. \tag{4.25}$$

Так как есть хотя бы одна пара (λ_i, μ_i) различных коэффициентов, то мы получили, что нетривиальная линейная комбинация базисных векторов равна нулю, что противоречит линейной независимости базиса. Значит разложение единственно. ■

Определение. Пусть в базисе $B = \{v_1, ..., v_n\}$ системы векторов S вектор v выражется через базисные векторы:

$$v = \lambda_1 v_1 + ... + \lambda_n v_n. \tag{4.26}$$

Числа $\lambda_1, ..., \lambda_n$ называются *координатами* вектора v в базисе B.

A.4.7. Базис системы векторов из $\mathbb{R}^n$

Предложение.

1. $\forall S \subseteq \mathbb{R}^n \ \exists$ базис.
2. Во всех базисах системы S одинаковое количество векторов, причём не больше n.

Доказательство. □

1. Если $S = \varnothing$ или $S = \{0\} \Rightarrow B = \{0\}$. Иначе в системе есть ненулевой вектор $v_1 \in S \Rightarrow \{v_1\}$ линейно независима.
   1.1. Если система $\{v_1\}$ не максимальна, то расширим её до линейно независимой подсистемы, добавив вектор v_2. Если она снова не максимальна, добавим v_3 и так далее. Получим возрастающую цепочку линейно независимых подсистем:

   $$\{v_1\} \subset \{v_1, v_2\} \subset \{v_1, v_2, v_3\} \subset ... \subset \{v_1, v_2, ..., v_k\} \subset .... \subseteq S \subseteq \mathbb{R}^n \tag{4.27}$$

   Отсюда $\Rightarrow \forall \{v_1, ..., v_k\}$ линейно выражается через $\{e_1, ..., e_n\}$. По основной лемме о линейной зависимости, $k \leq n \Rightarrow$ цепочка конечна. $\exists r \leq n : B = \{v_1, ..., v_r\}$ — максимальная линейная независимая подсистема S, что и есть базис.
2. Докажем, что во всех базисах одинаковое количество векторов. Пусть $B' = \{w_1, ..., w_s\}$ — другой базис системы S. Тогда его можно выразить через первый. По основной лемме о линейной зависимости, $s \leq r$. Но и B можно выразить через B', поэтому $r \leq s$. Значит $r = s$. ■

A.4.8. Переход к новому базису

Пусть $(e_1, ..., e_n)$ и $(e'_1, ..., e'_n)$ — два базиса в V, причём $(e'_1, ..., e'_n) = (e_1, ..., e_n) \cdot C$.

Определение. Матрица C называется матрицей перехода от базиса $(e_1, ..., e_n)$ к базису $(e'_1, ..., e'_n)$.

В j-м стоблце матрицы C стоят координаты вектора e'_j в базисе $(e_1, ..., e_n)$.

Предложение. Пусть $v \in V$ и $v = x_1 e_1 + ... + x_n e_n$ и $v = x'_1 e'_1 + ... + x'_n e'_n$ — вектор v выражается в двух разных базисах, причём $(e'_1, ..., e'_n) = (e_1, ..., e_n) \cdot C$. Тогда

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = C \cdot \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} \tag{4.28}$$

Доказательство. □ С одной стороны, $v = (e_1, ..., e_n) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. С другой стороны,

$$v = (e'_1, ..., e'_n) \cdot \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} = \cdot (e_1, ..., e_n) \cdot C \cdot \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}. \tag{4.29}$$

Так как $(e_1, ..., e_n)$ — линейно независимы, то вектор представленный их линейной комбинацией, представляется так единственным способом, поэтому

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = C \cdot \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} \blacksquare \tag{4.30}$$

Эту формулу можно использовать для пересчёта координат вектора при переходе к новому базису.

A.4.9. Подпространство векторного пространства

Определение. Подпространством векторного пространства V называется непустое множество векторов $U \subseteq V$, которое удовлетворяет двум требованиям замкнутости:

1. $\forall x, y \in U : x + y \in U$
2. $\forall x \in U, \lambda \in \mathbb{R} : \lambda \cdot x \in U$

A.4.9.1. Свойства подпространства

Пусть U — подпространство векторного пространства V.

1. $\vec{0} \in U$.

   Доказательство. □ Так как U непусто, то $\exists u \in U$ и по второму свойству $0 \cdot u \in U$, но $0 \cdot u = \vec{0}$. ■

2. U само является векторным пространством относительно тех операций, что определены на множестве V.

3. Линейная оболочка системы векторов является подпространством. Пусть $S \subseteq V$. Линеная оболочка системы S обозначается $< S >$:

$$< S > \underset{\text{def}}{=} \{v = \lambda_1 v_1 + ... + \lambda_n v_n \mid \lambda_1, ..., \lambda_n \in \mathbb{R}, v_1, ..., v_n \in S\} \tag{4.31}$$

   3.1. $< S >$ является наименьшим подпространством, содержащим S.

   3.2. Если B — базис S, то B — базис $< S >$.

   3.3. $\dim < S >= \text{rk}\, S$.

A.4.10. Фундаментальная система решений

Предложение. Рассмотрим произвольную однородную систему линейных уравнений с матрицей коэффициентов A.

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n = 0 \\ \vdots \quad ..... \\ a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n = 0 \end{cases} \tag{4.32}$$

Тогда множество её решений $U \subseteq \mathbb{R}^n$ — подпространство, причём

$$\dim U = n - \text{rk}\, A. \tag{4.33}$$

Доказательство. □ Докажем, что U является подпространством.

1. В силу однородности системы, $\vec{0} = (0, ..., 0) \in U$

2. Пусть есть два решения системы: $y = (y_1, ..., y_n)$ и $z = (z_1, ..., z_n)$. Тогда $\forall i = 1, ..., m$:

$$\begin{aligned} a_{i1}y_1 + a_{i2}y_2 + ... + a_{in}y_n = 0, \\ a_{i1}z_1 + a_{i2}z_2 + ... + a_{in}z_n = 0. \end{aligned} \tag{4.34}$$

   Если мы сложим эти два равенства, то получим:

$$a_{i1}(y_1 + z_1) + a_{i2}(y_2 + z_2) + ... + a_{in}(y_n + z_n) = 0. \tag{4.35}$$

   Тогда $y + z \in U$(тоже является решением системы).

3. Пусть $\lambda \in \mathbb{R}$. Если $y \in U$, то, умножая все уравнения на λ, получаем $\forall i = 1, ..., m$:

$$a_{i1}(\lambda y_1) + a_{i2}(\lambda y_2) + ... + a_{in}(\lambda y_n) = 0. \tag{4.36}$$

Таким образом, $y \in U \Rightarrow \lambda \cdot y \in U \Rightarrow U$ является подпространством. ■

Определение. Базис пространства решений однородной системы линейных уравнений называется *фундаментальной системой решений.*

A.4.11. Пересечение и сумма подпространств

Пусть V — векторное пространство над полем F, $\dim V < \infty$. И пусть $U, W \subseteq V$. Тогда пересечение подпространств в теоретико-множественном смысле — тоже подпространство: $(U \cap W) \subseteq V$.

Доказательство. □ Проверяем:

1. $\vec{0} \in U, W \Rightarrow \vec{0} \in (U \cap W)$
2. $\forall x, y \in (U \cap W) : x, y \in U$ и $x, y \in W$. Поэтому $(x + y) \in U$ и $(x + y) \in W \Rightarrow (x + y) \in (U \cap W)$.
3. Пусть $\lambda \in F$. Тогда $\forall x \in (U \cap W) : x \in U, x \in W \Rightarrow \lambda \cdot x \in U, \lambda \cdot x \in W \Rightarrow \lambda \cdot x \in (U \cap W)$.

■

Определение. Суммой подпространств $U, W \subseteq V$ векторного пространства V называется множество

$$U + W := \{u + w \mid u \in U, w \in W\} \tag{4.37}$$

Предлоежение. Сумма подпространств — тоже подпространство в V.

Доказательство. □ Рассмотрим $u_1, u_2 \in U$, $w_1, w_2 \in W$. Надо проверить, что $[(u_1 + w_1) + (u_2 + w_2)] \in (U + W)$, но $(u_1 + w_1) + (u_2 + w_2) = (u_1 + u_2) + (w_1 + w_2)$. Аналогично проверяется замкнутость относительно умножения на скаляр: $\lambda \cdot (u + w) = \lambda \cdot u + \lambda \cdot w$. ■

Теорема. Пусть V — векторное пространство, U, W — подпространства V.

$$\dim(U \cap W) + \dim(U + W) = \dim U + \dim W \tag{4.38}$$

Доказательство. □ Пусть $\dim(U \cap W) = p$, $\dim U = q$, $\dim W = r$. Пусть $a = \{a_1, ..., a_p\}$ — базис в $U \cap W$. Так как $(U \cap W) \subseteq U$ и $(U \cap W) \subseteq W$, то a можно дополнить до базиса в U и W: $\exists b = \{b_1, ..., b_{q-p}\}$ и $\exists c = \{c_1, ..., c_{r-p}\}$, такие что $a \cup b$ — базис U и $a \cup c$ — базис W. Докажем, что $a \cup b \cup c$ — базис в $U + W$.

1. Покажем, что $< a \cup b \cup c >= U + W$.

   Если $v \in (U + W)$, то $v = u + w$, где $u \in U, w \in W$.

- $u \in < a \cup b > \subseteq < a \cup b \cup c >$.
- $w \in < a \cup c > \subseteq < a \cup b \cup c >$.
- $\Rightarrow (u + w) = v \in < a \cup b \cup c >$.
- $\Rightarrow (U + W) \subseteq < a \cup b \cup c >$.
- Обратно, $< a \cup b \cup c > \subseteq (U + W)$, так как $< a \cup b \cup c > = \underbrace{< a > + < b >}_{\in U} + \underbrace{< c >}_{\in W} \subseteq U + W$.

2. Проверим линейную независимость. Пусть $x = \alpha_1 a_1 + ... + \alpha_p a_p$, $y = \beta_1 b_1 + ... + \beta_{q-p} b_{q-p}$ и $z = \gamma_1 c_1 + ... + \gamma_{r-p} c_{r-p}$. Пусть

$$x + y + z = \vec{0} \Rightarrow z = (-x - y) \in U. \tag{4.39}$$

С другой стороны, по определению $z \in W$, а следовательно, $z \in (U \cap W)$. Поэтому $\exists \lambda_1, ..., \lambda_p$:

$$z = \lambda_1 a_1 + ... + \lambda_p a_p. \tag{4.40}$$

Итак,

$$\lambda_1 a_1 + ... + \lambda_p a_p - \gamma_1 c_1 - ... - \gamma_{r-p} c_{r-p} = \vec{0} \tag{4.41}$$

Но это ЛК векторов базиса $a \cup c$ пространства W. Поэтому $\lambda_1 = ... \lambda_p = \gamma_1 = ... = \gamma_{r-p} = 0$. Поэтому $z = \vec{0}$, остаётся

$$\alpha_1 a_1 + ... + \alpha_p a_p + \beta_1 b_1 + ... + \beta_{q-p} b_{q-p} = \vec{0} \tag{4.42}$$

Это линейная комбинация векторов базиса $(a \cup b)$ пространства U. Значит $\alpha_1 = ... \alpha_p = \beta_1 = ... = \beta_{q-p} = 0$.

Итак, $a \cup b \cup c$ — базис в $U + W$. Посчитаем размерность:

$$\begin{aligned} \dim(U + W) = |a| + |b| + |c| = p + (q - p) + (r - p) = q + r - p = \\ = \dim(U) + \dim(W) - \dim(U \cap W). \blacksquare \end{aligned} \tag{4.43}$$

A.5. Ранг системы векторов и ранг матрицы

A.5.1. Ранг системы векторов

Определение. Ранг системы векторов S — это количество векторов в любом её базисе. Обозначается $\operatorname{rk} S$.

Определение. Размерность векторного пространства V — это его ранг. Обозначается $\dim V$.

Определение. Конечномерные векторным векторным пространством называется векторное пространство, в котором существует конечный базис.

Например, $\dim \mathbb{R}^n = n$.

Взаимно однозначное соответствие между V и $\mathbb{R}^n$ позволяет отождествить их: $v \leftrightarrow (\lambda_1, ..., \lambda_n)$.

A.5.1.1. Свойства ранга системы векторов

1. $S \subseteq S' \Rightarrow \operatorname{rk} S \leq \operatorname{rk} S'$.

   Доказательство. □ Пусть B — базис S, тогда B — линейно независимая подсистема и S', а значит $B \subseteq B'$, где B' — базис системы S'. Значит $B \subseteq B' \Rightarrow \operatorname{rk} S \leq \operatorname{rk} S'$. ■

2. Если S линейно выражается через S', то $\operatorname{rk} S \leq \operatorname{rk} S'$.

   Доказательство. □ Пусть B — базис в системе S, а B' — базис в системе S'. Тогда поскольку S линейно выражается через S', то B можно выразить через B'. По основной лемме о линейной зависимости, $\operatorname{rk} S \leq \operatorname{rk} S'$. ■

3. Если две системы S и S' выражаются друг через друга(наз. *линейно эквивалентными.*), то $\operatorname{rk} S = \operatorname{rk} S'$.

A.5.2. Ранг матрицы

A.5.2.1. Определение горизонтального, вертикального и ступенчатого ранга

Пусть A — матрица размера $m \times n$.

$$A = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mn} \end{pmatrix} \tag{5.1}$$

Её строки(длины n) обозначим: $A_1, A_2, ..., A_m$.

Столбцы(высоты m): $A^{(1)}, A^{(2)}, ..., A^{(n)}$.

Определение. Горизонтальный ранг матрицы A это ранг системы её строк.

$$r_{\text{г}} \underset{\text{def}}{=} \text{rk}\{A_1, A_2, ..., A_m\} \tag{5.2}$$

Определение. Вертикальный ранг матрицы A это ранг системы её столбцов.

$$r_{\text{в}} \underset{\text{def}}{=} \text{rk}\left\{A^{(1)}, A^{(2)}, ..., A^{(n)}\right\} \tag{5.3}$$

Приведём матрицу A к ступенчатому виду с помощью элементарных преобразований строк, получим A^*.

Определение. Ступенчатым рангом назовём количество ненулевых строк в матрице A^*.

Определение. Матрица A^T называется транспонированной матрицей A. Она получается отражением элементов матрицы A относительно главной диагонали.

$$A^T = \begin{pmatrix} a_{11} & a_{21} & ... & a_{m1} \\ a_{12} & a_{22} & ... & a_{m2} \\ ... & ... & ... & ... \\ a_{1n} & a_{2n} & ... & a_{mn} \end{pmatrix} \tag{5.4}$$

Имеем $\forall i = 1..m, j = 1..n : a^T_{ij} = a_{ji}$.

$$r_{\text{г}}(A^T) = r_{\text{в}}(A), \tag{5.5}$$

$$r_{\text{в}}(A^T) = r_{\text{г}}(A). \tag{5.6}$$

A.5.2.2. Теорема о ранге матрицы

Теорема. Горизонтальный ранг матрицы равен вертикальному и равен ступенчатому рангу. Его можно обозначить $\text{rk}(A)$.

Доказательство. □

1. Докажем, что $r_{\text{г}}(A)$ не меняется при элементарных преобразованиях строк. Если мы получили с помощью ЭП строк новую матрицу A', то $\{A'_1, ..., A'_m\}$ выражается через $\{A_1, ..., A_m\}$ и наоборот. Значит эти системы линейно эквивалентны и их ранги равны.
2. Докажем, что $r_{\text{в}}(A)$ не меняется при элементарных преобразованиях строк. Рассотрим однородную систему линейных уравнений:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n = 0 \\ \vdots \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n = 0 \end{cases} \tag{5.7}$$

Если $(\lambda_1, ..., \lambda_n)$ — решение системы, то это равносильно тому, что $\forall i = 1, ..., m$:

$$a_{i1}\lambda_1 + a_{i2}\lambda_2 + ... + a_{in}\lambda_n = 0 \tag{5.8}$$

Перепишем это через столбцы:

$$A^{(1)}\lambda_1 + ... + A^{(n)}\lambda_n = 0 \tag{5.9}$$

Ненулевые решения этой системы $\Leftrightarrow$ линейная зависимость $A^{(1)}, ..., A^{(n)}$. Если мы перейдём с помощью ЭП строк к матрице A', то множество решений этой системы не изменится, и значит линейные зависимости между столбцами $A^{(1)}, ..., A^{(n)}$ такие же, как у $A'^{(1)}, ..., A'^{(n)}$. В частности, если $\left\{A^{(j_1)}, ..., A^{(j_r)}\right\}$ — базис системы столбцов A, то столбцы с теми же номерами новой матрицы A' также будут образовывать базис. То есть вертикальный ранг и той и другой системы равен r.

3. Горизонтальный и вертикальный ранг сохраняются при элементарных преобразованиях столбцов. Поскольку ЭП столбцов $A \Leftrightarrow$ ЭП строк A^T.

4. Приведём матрицу A с помощью ЭП строк приведем к улучшенному ступенчатому виду A^*. Теперь на местах лидеров строк стоят единицы, под ступеньками нули а над лидерами тоже нули. Обозначим столбцы, проходящие через лидеров строк $j_1, j_2, ..., j_r$. Её ступенчатый ранг равен r. Переставим(ЭП II типа) столбцы так, чтобы сначала шли только ненулевые строки. Обнулим все элементы, которые лежат не на главной диагонали с помощью ЭП I типа. Получим

$$A^{**} = \begin{pmatrix} 1 & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ ... & ... & 1 & ... \\ ... & ... & ... & ... \\ 0 & 0 & ... & 0 \end{pmatrix} \tag{5.10}$$

Первые $r \times r$ элементов это единичная матрица размера r. Итак, $r_{\text{г}}(A) = r_{\text{г}}(A^{**}) = r$. Первые r строк это просто векторы e_i стандартного базиса $\mathbb{R}^r$. Аналогично, $r_{\text{в}}(A) = r_{\text{в}}(A^{**}) = r$. ■

A.5.3. Свойства ранга матрицы

В вышеприведенном доказательстве мы установили следующие свойства ранга матрицы.

1. $\mathrm{rk}(A) \leq \min\{m, n\}$.
2. Ранг матрицы не меняется при элементарных преобразованиях строк и столбцов.
3. $\mathrm{rk}(A) = \mathrm{rk}(A^T)$.

A.6. Линейные отображения

Определение. Пусть даны два векторных пространства V и W. Отображение $\mathcal{A} : V \to W$ называется линейным, если выполнены два условия:

1. $x + y = x + y, \forall x, y \in V$.
2. $\lambda \cdot x = \lambda \cdot x, \forall \lambda \in \mathbb{R}, x \in V$.

По умолчанию будем считать, что линейные отображения действуют между арифметическими пространствами, то есть $\mathcal{A} : \mathbb{R}^n \to \mathbb{R}^m$.

A.6.1. Матрица линейного отображения

Определение. Матрицей A линейного отображения $\mathcal{A}$ называется матрица $m \times n$, такая, что

$$A^{(j)} = \mathcal{A}(e_i), \forall j = 1, ..., n, \tag{6.1}$$

где $e_1, ...e_n$ — векторы стандартного базиса пространства $\mathbb{R}^n$.

- Линейное отображение $\mathcal{A}$ однозначно определяется своей матрицей A.

  □ $\forall x \in \mathbb{R}^n : x = x_1 e_1 + ... + x_n e_n$. Но $\mathcal{A}(x) = \mathcal{A}(x_1 e_1) + ... + \mathcal{A}(x_n e_n) = x_1 \mathcal{A}(e_1) + ... + x_n \mathcal{A}(e_n)$. $\mathcal{A}(e_i)$ — это столбцы нужной матрицы A. Обратно, если $x = x_1 A^{(1)} + ... + x_n A^{(n)}$, то столбцы можно переписать как образы базисных векторов $\mathbb{R}^n$. ■

A.6.2. Алгебраические операции над линейными отображениями

1. Сложение. Пусть $\mathcal{A}, \mathcal{B} : \mathbb{R}^n \to \mathbb{R}^m$, тогда $\forall x \in \mathbb{R}^n$

$$\mathcal{C} = \mathcal{A} + \mathcal{B} \Leftrightarrow \mathcal{C}(x) = \mathcal{A}(x) + \mathcal{B}(x) \tag{6.2}$$

   Здесь $\mathcal{C}$ отображает $\mathbb{R}^n \to \mathbb{R}^m$.

2. Умножение на число. Пусть $\mathcal{A} : \mathbb{R}^n \to \mathbb{R}^m$ и $\lambda \in \mathbb{R}$, тогда $\forall x \in \mathbb{R}^n$:

$$\mathcal{C} = \lambda \cdot \mathcal{A} \Leftrightarrow \mathcal{C}(x) = \lambda \cdot \mathcal{A}(x) \tag{6.3}$$

   Здесь $\mathcal{C}$ отображает $\mathbb{R}^n \to \mathbb{R}^m$.

3. Умножение линейных отображений. Пусть $A : \mathbb{R}^n \to \mathbb{R}^m$ и $B : \mathbb{R}^p \to \mathbb{R}^n$. Тогда $\mathcal{C} : \mathbb{R}^p \to \mathbb{R}^m$:

$$\mathcal{C} = \mathcal{A} \cdot \mathcal{B} \Leftrightarrow \mathcal{C}(x) = \mathcal{A}(\mathcal{B}(x)), \forall x \in \mathbb{R}^p \tag{6.4}$$

A.6.3. Алгебраические операции над матрицами

1. Сложение. Пусть A, B - матрицы $m \times n$. Для всех столбцов $\forall j = 1, ..., n$:

$$C = A + B \Leftrightarrow C^{(j)} = A^{(j)} + B^{(j)} \tag{6.5}$$

Это следует из того, что для соответсвующих линейных отображений

$$C^{(j)} = \mathcal{C}(e_j) = \mathcal{A}(e_j) + \mathcal{B}(e_j) = A^{(j)} + B^{(j)}. \tag{6.6}$$

Или же

$$c_{ij} = a_{ij} + b_{ij}, \tag{6.7}$$

где $i = 1, ..., m; j = 1, ..., n$.

2. Умножение на число. Пусть A - матрица $m \times n$ и $\lambda \in \mathbb{R}$, тогда для всех столбцов $\forall j = 1, ..., n$:

$$C = \lambda \cdot A \Leftrightarrow C^{(j)} = \lambda \cdot A^{(j)} \tag{6.8}$$

Так как $\mathcal{C} = \lambda \cdot \mathcal{A}$, то для всех $j = 1, ..., n$:

$$C = \lambda \cdot A \Leftrightarrow \mathcal{C}(e_j) = \lambda \cdot \mathcal{A}(e_j) \tag{6.9}$$

Или же

$$C = \lambda \cdot A \Leftrightarrow c_{ij} = \lambda \cdot a_{ij}, \tag{6.10}$$

где $i = 1, ..., m; j = 1, ..., n$.

3. Умножение матриц. Пусть матрица A имеет размер $m \times n$ и B имеет размер $n \times p$.

$$C = A \cdot B \Leftrightarrow C^{(j)} = \mathcal{C}(e_j), \forall j = 1, ..., p \tag{6.11}$$

Так как $\mathcal{C} = \mathcal{A} \cdot \mathcal{B}$, то для всех $j = 1, ..., p$:

$$\begin{gathered} \mathcal{C}(e_j) = \mathcal{A}(\mathcal{B}(e_j)) = \mathcal{A}(B^{(j)}) = \mathcal{A}(b_{1j}e_1 + ... + b_{nj}e_n) = \\ = b_{1j}\mathcal{A}(e_1) + ... + b_{nj}\mathcal{A}(e_n) = b_{1j}A^{(1)} + ... + b_{nj}A^{(n)} \end{gathered} \tag{6.12}$$

Получаем поэлементно:

$$\begin{gathered} c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}, \\ \forall i = 1, ..., m; j = 1, ..., p \end{gathered} \tag{6.13}$$

Несложно доказать, что эти операции корректно определены на множестве линейных отображений.

A.6.4. Матричная запись линейного отображения

Пусть $\mathcal{A} : \mathbb{R}^n \to \mathbb{R}^m$ и

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n \tag{6.14}$$

тогда

$$y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{R}^m \tag{6.15}$$

$$y = \mathcal{A}(x) = \mathcal{A}(x_1 e_1 + ... + e_n x_n) = A^{(1)} x_1 + ... + A^{(n)} x_n \tag{6.16}$$

Для каждого элемента $y_i (i = 1, ..., m)$:

$$y_i = a_{i1} x_1 + ... + a_{in} x_n \tag{6.17}$$

Получаем **матричную запись** линейного отображения:

$$y = A \cdot x \tag{6.18}$$

Система линейных уравнений с матрицей коэффициентов A и столбцом свободных членов b и столбцом неизвестных x можно записать так:

$$A \cdot x = b \tag{6.19}$$

A.6.5. Свойства матричных операций

1. Коммутативность сложения:

$$A + B = B + A \tag{6.20}$$

2. Ассоциативность сложения:

$$(A + B) + C = A + (B + C) \tag{6.21}$$

3. Нулевая матрица:

$$O + A = A, \forall A \tag{6.22}$$

4. Ассоциативность умножения матрицы на число:

$$\lambda \cdot (\mu \cdot A) = (\lambda \cdot \mu) \cdot A \tag{6.23}$$

5. Дистрибутивность умножения матриц на числа относительно сложения:

5.1. Чисел:

$$(\lambda + \mu) \cdot A = \lambda \cdot A + \mu \cdot A \tag{6.24}$$

5.2. Матриц:

$$\lambda \cdot (A + B) = \lambda \cdot A + \lambda \cdot B \tag{6.25}$$

6. Умножение на нуль:

$$0 \cdot A = O \tag{6.26}$$

7. Умножение на нулевую матрицу:

$$\lambda \cdot O = O \tag{6.27}$$

8. Умножение на единицу:

$$1 \cdot A = A \tag{6.28}$$

9. Противоположная матрица:

$$A + (-A) = O \tag{6.29}$$

где $(-A) = (-1) \cdot A$.

- Таким образом, множество всех матриц $m \times n$ с операциями сложения и умножения на числа образует векторное пространство. Его элементы можно рассматривать как длинные векторы $m \times n$.

10. Ассоциативность умножения матриц:

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C \tag{6.30}$$

11. Некоммутативность. Вообще говоря,

$$A \cdot B \neq B \cdot A \tag{6.31}$$

12. Смешанная ассоциативность:

$$(\lambda \cdot A) \cdot B = \lambda \cdot (A \cdot B) \tag{6.32}$$

13. Дистрибутивность матричного умножения относительно сложения:

13.1. Левая дистрибутивность:

$$A \cdot (B + C) = A \cdot B + A \cdot C \tag{6.33}$$

13.2. Правая дистрибутивность:

$$(A + B) \cdot D = A \cdot D + B \cdot D \tag{6.34}$$

A.6.6. Взаимодействие транспонирования и алгебраических операций над матрицами

Прелоожение о транспонировании.

1. $(A+B)^T = A^T + B^T$
2. $(\lambda \cdot A)^T = \lambda \cdot A^T$
3. $(A \cdot B)^T = B^T \cdot A^T$

Доказательство. $\square$

1. Пусть $C = A + B$. Тогда $\forall i, j$:

$$c_{ij}^T = c_{ji} = a_{ji} + b_{ji} = a_{ij}^T + b_{ij}^T. \tag{6.35}$$

2. Пусть $C = \lambda \cdot A$, $\forall i, j$:

$$c_{ij}^T = c_{ji} = \lambda \cdot a_{ji} = \lambda \cdot a_{ij}^T. \tag{6.36}$$

3. Пусть $C = A \cdot B$, $\forall i, j$:

$$c_{ij}^T = c_{ji} = \sum_k a_{jk} \cdot b_{ki} = \sum_k a_{kj}^T \cdot b_{ik}^T = \sum_k b_{ik}^T \cdot a_{kj}^T \tag{6.37}$$

Отсюда $C^T = B^T \cdot A^T$. $\blacksquare$

A.6.7. Ранг произведения двух матриц

Теорема. Ранг произведения двух матриц не превосходит каждого из рангов сомножителей:

$$\operatorname{rk}(A \cdot B) \leq \min\{\operatorname{rk} A, \operatorname{rk} B\} \tag{6.38}$$

Доказательство. $\square$ Пусть $A \in \operatorname{Mat}_{m,n}$, $B \in \operatorname{Mat}_{n,p} \Rightarrow A \cdot B = C \in \operatorname{Mat}_{m,p}$. $\forall i, j$:

$$c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj} \tag{6.39}$$

$$C_i = \sum_{k=1}^{n} = a_{ik} \cdot B_k \tag{6.40}$$

Следовательно, система строк матрицы C линейно выражается через систему векторов B. Значит ранг системы строк матрицы C не превосходит ранга системы строк матрицы B. Значит, $\operatorname{rk} C \leq \operatorname{rk} B$. Аналогично, выражая систему стобцов $\left\{C^{(1)}, ..., C^{(p)}\right\}$ через столбцы матрицы A:

$$C^{(j)} = \sum_{k=1}^{n} A^{(k)} \cdot b_{kj} \tag{6.41}$$

Значит $\operatorname{rk} C \leq \operatorname{rk} A$. ■

Аналогично можно показать, что

$$\operatorname{rk}(A + B) \leq \min\{\operatorname{rk} A, \operatorname{rk} B\}. \tag{6.42}$$

A.6.8. Тождественное отображение

Определение. Отображение $\mathcal{E} : \mathbb{R}^n \to \mathbb{R}^n$ называется тождественным, если

$$\mathcal{E}(x) = x, \forall x \in \mathbb{R}^n. \tag{6.43}$$

Матрица тождественного отображения:

$$E = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 \end{pmatrix} \tag{6.44}$$

Это так называемая *единичная матрица* размера $n \times n$.

Её элементы можно описать символом Кронекера:

$$\delta_{ij} = \begin{cases} 1, \text{при } i = j \\ 0, \text{при } i \neq j \end{cases} \tag{6.45}$$

A.6.8.1. Основное свойство тождественного отображения и единичной матрицы

Основное свойство тождественного отображения $\forall \mathcal{A} : \mathbb{R}^n \to \mathbb{R}^m$

$$\mathcal{A} \cdot \mathcal{E} = \mathcal{A} \tag{6.46}$$

Аналогично, $\forall \mathcal{B} : \mathbb{R}^p \to \mathbb{R}^n$:

$$\mathcal{E} \cdot \mathcal{B} = \mathcal{B} \tag{6.47}$$

Из этого сразу следует основное свойство единичной матрицы:

$$A \cdot E = A, \forall A \in \operatorname{Mat}_{m,n} \tag{6.48}$$

$$E \cdot B = B, \forall B \in \operatorname{Mat}_{n,p} \tag{6.49}$$

A.6.9. Обратная матрица

Определение. Пусть $A \in \operatorname{Mat}_n$. Матрица $B \in \operatorname{Mat}_n$ называется обратной к матрице A, если

$$A \cdot B = B \cdot A = E. \tag{6.50}$$

Свойства обратной матрицы.

1. Если обратная матрица к данной существует, то она ровно одна.

   Доказательство. □ Пусть B и B' — две обратные матрицы к A.

   $$B \cdot A \cdot B' = (B \cdot A) \cdot B' = E \cdot B' = B' \tag{6.51}$$

   $$B \cdot A \cdot B' = B \cdot (A \cdot B') = B \cdot E = B \tag{6.52}$$

   Поэтому $B = B'$. ■

   1.1. Обратную матрицу к матрице A обозначают A^{-1}.

2. Если матрица $A \leftrightarrow \mathcal{A} : \mathbb{R}^n \to \mathbb{R}^n$, то $A^{-1} \leftrightarrow \mathcal{A}^{-1} : \mathbb{R}^n \to \mathbb{R}^n$. Кроме того, обратное отображение тоже линейно.

3. Матрица A обратима $\Leftrightarrow$ $\mathcal{A}$ обратимо $\Leftrightarrow$ $\mathcal{A}$ биективно.

Предложение. Если A, B обратимы, то $A \cdot B$ обратимо и $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$.

Доказательство. □ Рассмотрим $(A \cdot B) \cdot (B^{-1} \cdot A^{-1}) = A \cdot E \cdot A^{-1} = A \cdot A^{-1} = E$. Аналогично, в другом порядке получим при умножении E. Поэтому эти матрицы взаимно обратны. ■

Определение. Квадратная матрица $A \in \mathrm{Mat}_n$ называется *невырожденной*, если $\mathrm{rk}\, A = n$.

Теорема. Матрица $A \in \mathrm{Mat}_n$ обратима тогда и только тогда, когда она невырождена.

Доказательство. □

1. $\Rightarrow$. Пусть матрица A обратима. Тогда $A \cdot A^{-1} = E$. Мы знаем, что ранг произведения матриц не превосходит каждого из рангов сомножителей, значит

   $$\mathrm{rk}(A \cdot A^{-1}) \leq \min\{\mathrm{rk}\, A, \mathrm{rk}\, A^{-1}\} \tag{6.53}$$

   $$n \leq \mathrm{rk}\, A \tag{6.54}$$

   Поэтому $\mathrm{rk}\, A = n$. И матрица A невырождена.

2. $\Leftarrow$. Пусть $\mathrm{rk}\, A = n$. Тогда столбцы $\left\{A^{(1)}, \ldots, A^{(n)}\right\}$ линейно независимы. И они образуют базис в $\mathbb{R}^n$. Если бы эта система векторов была не максимальной, в ней было бы $> n$ векторов, но в любом пространстве V с $\dim V = n$ базис имеет ровно n векторов.

Тогда

$$\forall y \in \mathbb{R}^n \ \exists! x_1, ..., x_n : y = \sum_{i=1}^{n} x_i \cdot A^{(i)} \tag{6.55}$$

значит

$$\forall y \in \mathbb{R}^n \ \exists! x \in \mathbb{R}^n : y = \mathcal{A}(x), \tag{6.56}$$

где $\mathcal{A} : \mathbb{R}^n \to \mathbb{R}^n$ — линейное отображение. Значит A взаимно однозначно $\Rightarrow$ обратимо $\Rightarrow$ матрица этого отображения обратима.

■

A.6.10. Алгоритм нахождения обратной матрицы

Пусть A — невыроженная матрица. Запишем расширенную матрицу $(A \mid E)$ и приведём к улучшенному ступенчатому виду матрицу A. Её улучшенный ступенчатый вид будет E. Утверждается, что матрица, которая получена с помощью элементарных преобразований на месте E будет A^{-1}.

$$(A \mid E) \underset{\substack{\text{элементарные} \\ \text{преобразования} \\ \text{строк}}}{\longrightarrow} \left(E \mid A^{-1}\right) \tag{6.57}$$

Доказательство. □ $X = A^{-1}$ является решением уравнения $A \cdot X = E$. Это уравнение равносильно системе:

$$\begin{cases} A \cdot X^{(j)} = E^{(j)} \\ \forall j = 1, ..., n \end{cases} \tag{6.58}$$

Каждое из уравнений на $X^{(j)}$ есть матричная запись СЛАУ с матрицей коэффициентов A и свободным членом $E^{(j)}$. Решим её методом Гаусса:

$$\left(A \mid E^{(j)}\right) \underset{\substack{\text{элементарные} \\ \text{преобразования} \\ \text{строк}}}{\longrightarrow} \left(E \mid B^{(j)}\right) \tag{6.59}$$

Поэтому

$$A \cdot X^{(j)} = E^{(j)} \Leftrightarrow E \cdot X^{(j)} = B^{(j)}, \ \forall j = 1, ..., n. \tag{6.60}$$

$$A \cdot X = E \Leftrightarrow E \cdot X = B \tag{6.61}$$

Единственное решение этого уравнения есть $X = B$, и поэтому $B = A^{-1}$. ■

A.6.11. Элементарные матрицы

Определение. Элементарная матрица — это матрица размера $n \times n$, получаемая из E с помощью одного элементарного преобразования строк или столбцов.

3 типа элементарных матриц.

1. Применяем ЭП I типа к E: прибавим к $i-$й строке j-ю строку, умноженную на число λ.

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix} \overset{\text{ЭП I}}{\longrightarrow} U_{ij}(\lambda) = \begin{pmatrix} 1 & 0 & \dots & \dots & \dots & 0 \\ 0 & \dots & \dots & \dots & \dots & 0 \\ \dots & \dots & 1 & \lambda & \dots & 0 \\ \dots & \dots & \dots & 1 & \dots & 0 \\ 0 & 0 & \dots & \dots & \dots & 1 \end{pmatrix} \leftarrow i \text{ -я строка} \tag{6.62}$$

2. Применим к E элементарное преобразование II типа: переставим i-ю и j-ю строки.

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix} \overset{\text{ЭП II}}{\longrightarrow} U_{ij} = \begin{pmatrix} 1 & 0 & \dots & \dots & \dots & 0 \\ 0 & \dots & \dots & \dots & \dots & 0 \\ \dots & \dots & 0 & 1 & \dots & 0 \\ \dots & \dots & 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & \dots & \dots & 1 \end{pmatrix} \leftarrow i \text{ -я строка} \tag{6.63}$$

3. Применим к E элементарное преобразование III типа: умножим i-ю строку на число $\lambda \neq 0$.

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix} \overset{\text{ЭП III}}{\longrightarrow} U_i(\lambda) = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 \\ 0 & \dots & \dots & \dots & 0 \\ \dots & \dots & \lambda & \dots & 0 \\ 0 & 0 & \dots & \dots & 1 \end{pmatrix} \tag{6.64}$$

A.6.11.1. Основное свойство элементарных матриц

Пусть $A \in \mathrm{Mat}_{m,n}$. Применим к A одно элементарное преобразование строк и получим A', тогда

$$A' = U \cdot A, \tag{6.65}$$

где U — элементарная матрица, соответствующая применённому элементарному преобразованию строк.

Если же мы применим к A одно элементарное преобразование столбцов и получим A'', то

$$A'' = A \cdot V, \tag{6.66}$$

где V — элементарная матрица, соответствующая применённому элементарному преобразованию столбцов.

Доказательство. □ Докажем последовательно утверждения про строки и про столбцы.

1. Для всех трёх типов элементарных преобразований, строки A'_i являются линейными комбинациями строк A_i с коэффициентами λ_{ik}.

$$A_i = \sum_{k=1}^{m} \lambda_{ik} A_k \tag{6.67}$$

Так как элементарное преобразование то же самое, то

$$U_i = \sum_{k=1}^{m} \lambda_{ik} E_k = (\lambda_{i1}, ..., \lambda_{im}), \tag{6.68}$$

где $E_k = (0, ..., 1_k, ..., 0)$

$$a'_{ij} = \sum_{k=1}^{m} \lambda_{ik} a_{kj} = (\lambda_{i1}, ..., \lambda_{im}) \cdot \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} = U_i \cdot A^{(j)} \tag{6.69}$$

Поэтому $A' = U \cdot A$.

2. Столбцы $A''^{(j)}$ выражаются через столбцы $A^{(j)}$.

$$A''^{(j)} = \sum_{k=1}^{n} \mu_{kj} A^{(k)} \tag{6.70}$$

$$V^{(j)} = \sum_{k=1}^{n} \mu_{kj} E^{(k)} = \begin{pmatrix} \mu_{1j} \\ \vdots \\ \mu_{nj} \end{pmatrix} \tag{6.71}$$

Поэтому

$$a''_{ij} = \sum_{k=1}^{n} \mu_{kj} a_{ik} = \begin{pmatrix} a_{i1} \\ \vdots \\ a_{in} \end{pmatrix} \cdot \left(\mu_{1j}, ..., \mu_{nj}\right) = A_i \cdot V^{(j)} \tag{6.72}$$

Следовательно, $A'' = A \cdot V$. ■

Следствие. Элементарные матрицы обратимы, причём обратная матрица будет элементарной, полученной обратным элементарным преобразованием.

Доказательство. □ Пусть $E \to U$ — элементарная матрица, полученная преобразованиями строк. Тогда можно получить $U \to E$ обратным преобразованием. Но если применить это же обратное преобразование к E, то получим некую матрицу V.

$$U \leftrightarrow E \leftrightarrow V \tag{6.73}$$

Из основного свойства элементарных матриц:

$$E = V \cdot U \tag{6.74}$$

(получили матрицу E из матрицы U с помощью обратного элементарного преобразования V).

С другой стороны, можно получить E из матрицы V с помощью обратного к обратному ЭП, то есть умножением на U:

$$E = U \cdot V \tag{6.75}$$

Поэтому V обратна к U. Аналогично доказывается утверждение для столбцов. ■

A.6.11.2. Разложение невырожденной матрицы в произведение элементарных матриц

Теорема. Всякая невырожденная матрица раскладывается в произведение элементарных матриц.

Доказательство. □ Так как матрица A невырожденная, то с помощью элементарных преобразований строк можно привести её к единичной матрице E. По основному свойству элементарных матриц это означает, что существует последовательность элементарных матриц $U_1, U_2, ..., U_k$, таких что

$$U_k \cdot U_{k-1} \cdot ... \cdot U_1 \cdot A = E \tag{6.76}$$

где U_i получается с помощью i-го элементарного преобразования строк.

Так как для каждой из U_i существует обратная элементарная матрица U_i^{-1}, то умножив это равенство последовательно слева на обратные матрицы, получим

$$A = U_1^{-1} \cdot U_2^{-1} \cdot ... \cdot U_k^{-1} \cdot E = U_1^{-1} \cdot U_2^{-1} \cdot ... \cdot U_k^{-1} \tag{6.77}$$

Мы получили разложение A в произведение элементарных матриц, причём это матрицы тех преобразований, которые нужно получить, чтобы из единичной матрицы получить A. ■

A.7. Определители

Определение. Пусть задана квадратная матрица $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$. Её определитель это число, которое обозначают

$$\det A = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} \tag{7.1}$$

По определению оно равно

$$\det A = \sum_{\sigma \in S_n} a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdot \dots \cdot a_{n,\sigma(n)} \cdot \operatorname{sgn}(\sigma) \tag{7.2}$$

Где сумма ведётся по всем перестановкам $\sigma \in S_n$.

A.7.1. Свойства определителя

Каждая квадратная $n \times n$-матрица может рассматриваться как набор из n n-мерных векторов:

$$\det A = \det(A_1, A_2, \dots, A_n) \tag{7.3}$$

Определитель обладает свойствами:

1. Аддитивность:

$$\begin{aligned} \det(A_1, \dots, A'_k + A''_k, \dots A_n) = \det(A_1, \dots, A'_k, \dots A_n) + \\ + \det(A_1, \dots, A''_k, \dots, A_n) \end{aligned} \tag{7.4}$$

Доказатательство. □ Согласно определению определителя,

$$\det A = \sum_{(i_1, \dots, i_n)} a_{1,i_1} \cdot \dots \cdot a_{k,i_k} \cdot \dots \cdot a_{n,i_n} \cdot \operatorname{sgn}(i_1, \dots, i_n) \tag{7.5}$$

Но k-я строка распадается на сумму двух, поэтому $a_{k,i_k} = a'_{k,i_k} + a''_{k,i_k}$, раскрыв скобки, получим две суммы:

$$\begin{aligned} \det A = \sum_{(i_1, \dots, i_n)} a_{1,i_1} \cdot \dots \cdot a'_{k,i_k} \cdot \dots \cdot a_{n,i_n} \cdot \operatorname{sgn}(i_1, \dots, i_n) + \\ + \sum_{(i_1, \dots, i_n)} a_{1,i_1} \cdot \dots \cdot a''_{k,i_k} \cdot \dots \cdot a_{n,i_n} \cdot \operatorname{sgn}(i_1, \dots, i_n) = \\ = \det(A_1, \dots, A'_k, \dots A_n) + \det(A_1, \dots, A''_k, \dots, A_n). \blacksquare \end{aligned} \tag{7.6}$$

2. Однородность:

$$\det(A_1, ..., \lambda \cdot A_k, ...A_n) = \lambda \det(A_1, ..., A_k, ..., A_n) \tag{7.7}$$

Доказательство □ Левая часть равна:

$$\begin{gathered}\sum_{(i_1,...,i_n)} a_{1,i_1} \cdot ... \cdot \left(\lambda \cdot a_{k,i_k}\right) \cdot ... \cdot a_{n,i_n} \cdot \operatorname{sgn}(i_1, ..., i_n) = \\ = \lambda \sum_{(i_1,...,i_n)} a_{1,i_1} \cdot ... \cdot a_{k,i_k} \cdot ... \cdot a_{n,i_n} \cdot \operatorname{sgn}(i_1, ..., i_n) = \lambda \det A. \blacksquare\end{gathered} \tag{7.8}$$

3. Кососимметричность:

$$\det(A_1, ..., A_k, ..., A_l, ...A_n) = -\det(A_1, ..., A_l, ..., A_k, ...A_n) \tag{7.9}$$

Доказательство. □ Пусть матрица A' получена из матрицы A транспозицией двух строк с номерами k и l. Переставим в произведениях k-е и k-е элементы:

$$\begin{gathered}\det A = \sum_{\sigma \in S_n} a_{1,\sigma(1)} \cdot ... \cdot a_{k,\sigma(k)} \cdot ... \cdot a_{l,\sigma(l)} ... \cdot a_{n,\sigma(n)} \cdot \operatorname{sgn}(\sigma) = \\ = \sum_{\sigma \in S_n} a_{1,\sigma(1)} \cdot ... \cdot a_{l,\sigma(l)} \cdot ... \cdot a_{k,\sigma(k)} ... \cdot a_{n,\sigma(n)} \cdot \operatorname{sgn}(\sigma)\end{gathered} \tag{7.10}$$

Расммотрим перестановку $\pi = \sigma \cdot \tau$, где $\tau = (k, l)$ — транспозиция k и l. Она действует на все номера, кроме k и l так же, как и σ, кроме того, $\pi \in S_n$, если $\sigma \in S_n$.

$$\det A = \sum_{\pi \in S_n} a'_{1,\pi(1)} \cdot ... \cdot a'_{k,\pi(k)} \cdot ... \cdot a'_{l,\pi(l)} ... \cdot a'_{n,\pi(n)} \cdot \underbrace{\operatorname{sgn}(\sigma)}_{-\operatorname{sgn}(\pi)} = -\det A' \tag{7.11}$$

■

4. Определитель матрицы с нулевой строкой равен нулю:

$$\exists k : A_k = 0 \Rightarrow \det A = 0. \tag{7.12}$$

Доказательство. □

$$\begin{gathered}\det A = \det(A_1, ..., A_k, ..., A_n) = \det(A_1, ..., 0 \cdot A_k, ..., A_n) = \\ \underset{\text{св. 2}}{=} 0 \cdot \det(A_1, ..., A_k, ..., A_n) = 0. \blacksquare\end{gathered} \tag{7.13}$$

5. Если в определителе 2 строки совпадают, то определитель равен нулю:

$$\exists k \neq l : A_k = A_l \Rightarrow \det A = 0. \tag{7.14}$$

Доказательство. □ Переставим строки с местами k и l и воспользуемся косо-симметричностью:

$$\begin{gathered}\det A = \det(A_1, ..., A_k, ..., A_l, ...A_n) = -\det(A_1, ..., A_l, ..., A_k, ...A_n) = \\ = -\det A\end{gathered} \tag{7.15}$$

Но $\det A = -\det A \Rightarrow \det A = 0$. ■

6. Если в определителе две строки пропорциональны, то он равен нулю:

$$\exists k, l : k \neq l : A_l = \lambda \cdot A_k \Rightarrow \det A = 0 \tag{7.16}$$

Доказатательство. □

$$\begin{gathered}\det(A_1, ..., A_k, ..., A_l, ...A_n) = \det(A_1, ..., A_k, ..., \lambda \cdot A_k, ...A_n) = \\ = \lambda \det(A_1, ..., A_k, ..., A_k, ...A_n) = 0. \ ■\end{gathered} \tag{7.17}$$

7. Элементарные преобразования строк I типа не меняют определитель матрицы.

Доказатательство. □ Пусть матрица A' получена прибавлением l-й строки с коэфициентом λ к k-й строке матрицы A:

$$\begin{gathered}\det A' = \det(A_1, ..., A_k + \lambda \cdot A_l, ..., A_l, ..., A_n) = \\ = \det(A_1, ..., A_k, ..., A_l, ..., A_n) + \underbrace{\det(A_1, ..., \lambda \cdot A_l, ..., A_l, ..., A_n)}_{=0 \ \text{ по свойству 6}} = \\ = \det A. \ ■\end{gathered} \tag{7.18}$$

8. При транспонировании определитель матрицы не меняется:

$$\det A = \det A^T \tag{7.19}$$

Доказательство. □ Запишем по определению определитель транспонированной матрицы:

$$\det A^T = \sum_{\sigma \in S_n} a_{\sigma(1),1} \cdot ... \cdot a_{\sigma(n),n} \operatorname{sgn}(\sigma). \tag{7.20}$$

Пусть $\pi = \sigma^{-1}$. Тогда $\sigma(j) = i \Rightarrow \pi(i) = j$. Если σ пробегает все перестановки S_n по одному разу, то и π пробегает все перестановки S_n по одному разу. Кроме того, $\operatorname{sgn}(\pi) = \operatorname{sgn}(\sigma)$.

$$\det A^T = \sum_{\pi \in S_n} a_{1,\pi(1)} \cdot ... \cdot a_{n,\pi(n)} \cdot \underbrace{\operatorname{sgn}}_{\operatorname{sgn}(\pi)}(\sigma) = \det A. \ ■ \tag{7.21}$$

9. Свойства 1-7 верны, если рассматривать определитель как функцию набора столбцов матрицы.

Из 1 и 2 свойства следует линейность определителя по любой строке, то есть определитель — полилинейная кососимметричная функция строк матрицы. А из свойства 9 следует, что и от столбцов.

А.7.2. Вычисление определителя через приведение матрицы к треугольному виду

Мы можем привести элементарными преобразованиями строк любую квадратную матрицу A к ступенчатому виду, получив матрицу $A*$, у которой ниже главной диагонали будут только нули:

$$A \underset{\substack{\text{ЭП}\\ \text{строк}}}{\longrightarrow} A^* = \begin{pmatrix} \lambda_1 & \dots & \dots & \dots \\ 0 & \lambda_2 & \dots & \dots \\ \vdots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix} \tag{7.22}$$

Если по пути было сделано p перестановок строк и умножения строк производились на числа $\mu_1, \dots, \mu_N$, то определитель исходной матрицы так связан с определителем ступенчатой матрицы:

$$\det A = \det A^* \cdot (-1)^p \cdot \mu_1 \cdot \dots \cdot \mu_N \tag{7.23}$$

А.7.3. Определитель треугольной матрицы

Предложение. Определитель треугольной матрицы равен произведению элементов, стоящих на диагонали этой матрицы.

Доказательство. □ Пусть у нас есть треугольная квадратная матрица B с диагональю $(\lambda_1 \ \dots \ \lambda_n)$.

$$\det B = \begin{vmatrix} \lambda_1 & \dots & \dots & \dots \\ 0 & \lambda_2 & \dots & \dots \\ \vdots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{vmatrix} \tag{7.24}$$

Применим элементарное преобразование I типа: обнулим все элементы в n-м столбце выше единицы.

$$\det B = \lambda_n \cdot \begin{vmatrix} \lambda_1 & \dots & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{vmatrix} \tag{7.25}$$

Теперь вынесем множитель λ_{n-1} из предпоследней строки.

$$\det B = \lambda_n \cdot \lambda_{n-1} \begin{vmatrix} \lambda_1 & \dots & \dots & 0 \\ 0 & \lambda_2 & \dots & \dots \\ \vdots & \dots & 1 & 0 \\ 0 & 0 & \dots & 1 \end{vmatrix} \tag{7.26}$$

Теперь с помощью элементарных преобразований I типа обнулим все элементы $(n-1)$-го столбца выше единицы. Повторим эту процедуру до тех пор, пока на главной диагонали не останутся только единицы. Полученная матрица есть единичная.

$$\det B = \lambda_1 \cdot \dots \cdot \lambda_n \cdot \begin{vmatrix} 1 & \dots & \dots & 0 \\ \vdots & 1 & \dots & 0 \\ \vdots & \dots & \dots & \dots \\ 0 & \dots & \dots & 1 \end{vmatrix} \tag{7.27}$$

Но в разложении определителя единичной матрицы только одно ненулевое произведение: $1 \cdot 1 \cdot \dots \cdot 1 = 1$. Поэтому $\det B = \lambda_1 \cdot \dots \cdot \lambda_n$. ■

A.7.4. Определитель и другие кососимметричные полилинейные функции строк

Мы установили, что

$$\det A = (-1)^p \cdot \mu_1 \cdot \dots \cdot \mu_N \cdot \lambda_1 \cdot \dots \cdot \lambda_n \tag{7.28}$$

где p — количество перестановок строк, а $\mu_1, \dots, \mu_N$ — множители, на которые умножались строки.

Если $f(A)$ — любая кососимметричная полилинейная функция строк матрицы A, то аналогичными выкладками для неё можно получить

$$f(A) = (-1)^p \cdot \mu_1 \cdot \dots \cdot \mu_N \cdot \lambda_1 \cdot \dots \cdot \lambda_n \cdot f(E) \tag{7.29}$$

Поэтому функция f отличается от det лишь постоянным множителем.

$$f(A) = f(E) \cdot \det A \tag{7.30}$$

A.7.5. Разбиение матрицы на 4 блока

Предложение. Пусть матрицу A можно разбить на 4 блока:

$$A = \begin{pmatrix} B & D \\ O & C \end{pmatrix} \tag{7.31}$$

причём $B \in \mathrm{Mat}_k$, $C \in \mathrm{Mat}_{n-k}$, $D \in \mathrm{Mat}_{k,n-k}$, O — нулевая матрица. Тогда

$$\det A = \det B \cdot \det C \tag{7.32}$$

Доказатательство. □

1. Пусть матрица A — треугольная, $\Rightarrow B, C$ — тоже. Если $\operatorname{diag} B = (\beta_1, ..., \beta_k)$ и $\operatorname{diag} C = (\gamma_1, ..., \gamma_{n-k})$, то

$$\det A = \beta_1 \cdot ... \cdot \beta_k \cdot \gamma_1 \cdot ... \cdot \gamma_{n-k} = \det B \cdot \det C \tag{7.33}$$

2. В общем случае, мы можем привести A к треугольному виду. Путём элементарных преобразований первых k строк, так, чтобы B' стала ступенчатой.

$$A \underset{\substack{\text{ЭП } k \\ \text{строк}}}{\longrightarrow} A' = \begin{pmatrix} B' & D' \\ O & C \end{pmatrix} \underset{\substack{\text{ЭП } (n-k) \\ \text{строк}}}{\longrightarrow} A'' = \begin{pmatrix} B' & D' \\ O & C' \end{pmatrix} \tag{7.34}$$

При преобразованиях первых k строк имеем

$$\det A = \det A' \cdot (-1)^p \cdot \frac{1}{\mu_1} \cdot ... \cdot \frac{1}{\mu_q} \tag{7.35}$$

Если r — количество ЭП2, а ν_i — множители ЭП3, то

$$\det A' = \det A'' \cdot (-1)^r \cdot \frac{1}{\nu_1} \cdot ... \cdot \frac{1}{\nu_s} \tag{7.36}$$

Итак, соберём $\det A$:

$$\det A = \det A'' \cdot (-1)^{p+r} \cdot \frac{1}{\mu_1 \cdot ... \cdot \mu_q \cdot \nu_1 \cdot ... \cdot \nu_s} \tag{7.37}$$

Но матрица A'' треугольная, поэтому по доказанному в случае 1, имеем

$$\det A = \det B' \cdot (-1)^p \cdot \frac{1}{\mu_1 \cdot ... \cdot \mu_q} \cdot \det C' \cdot (-1)^r \cdot \frac{1}{\nu_1 \cdot ... \cdot \nu_s} = \det B \cdot \det C \tag{7.38}$$

■

A.7.6. Определитель Вандермонда

Определение. Определителем Вандермонда называется определитель матрицы

$$V(x_1, ..., x_n) = \begin{vmatrix} 1 & 1 & ... & 1 \\ x_1 & x_2 & ... & x_n \\ x_1^2 & x_2^2 & ... & x_n^2 \\ ... & ... & ... & ... \\ x_1^{n-1} & x_2^{n-1} & ... & x_n^{n-1} \end{vmatrix} \tag{7.39}$$

A.7.6.1. Вычисление определителя Вандермонда

Обнулим в первом столбце $V(x_1, ..., x_n)$ все элементы, кроме первого, вычитая из каждой строки предыдущую, умноженную на соответствующую степень x_1.

$$V(x_1, ..., x_n) = \begin{vmatrix} 1 & 1 & ... & 1 \\ 0 & x_2 - x_1 & ... & x_n - x_1 \\ 0 & x_2^2 - x_1 \cdot x_2 & ... & x_n^2 - x_1 \cdot x_n \\ ... & ... & ... & ... \\ 0 & x_2^{n-1} - x_1 \cdot x_2^{n-2} & ... & x_n^{n-1} - x_1 \cdot x_n^{n-2} \end{vmatrix} \tag{7.40}$$

Теперь, согласно предложению, мы можем разбить определитель на два блока, вынести множители по однородности определителя и получить рекурренту.

$$\begin{aligned} V(x_1, ..., x_n) &= 1 \cdot \begin{vmatrix} x_2 - x_1 & x_3 - x_1 & ... & x_n - x_1 \\ x_2^2 - x_1 \cdot x_2 & x_3^2 - x_1 \cdot x_3 & ... & x_n^2 - x_1 \cdot x_n \\ ... & ... & ... & ... \\ x_2^{n-1} - x_1 \cdot x_2^{n-2} & x_3^{n-1} - x_1 \cdot x_3^{n-2} & ... & x_n^{n-1} - x_1 \cdot x_n^{n-2} \end{vmatrix} = \\ &= (x_2 - x_1) \cdot ... \cdot (x_n - x_1) \cdot \begin{vmatrix} 1 & 1 & ... & 1 \\ x_2 & x_3 & ... & x_n \\ ... & ... & ... & ... \\ x_2^{n-1} & x_3^{n-1} & ... & x_n^{n-1} \end{vmatrix} = \\ &= (x_2 - x_1) \cdot ... \cdot (x_n - x_1) \cdot V(x_2, ..., x_n) \end{aligned} \tag{7.41}$$

Рассуждая по индукции, будем иметь

$$V(x_1, ..., x_n) = (x_2 - x_1) \cdot ... \cdot (x_n - x_{n-2}) \cdot \begin{vmatrix} 1 & 1 \\ x_{n-1} & x_n \end{vmatrix} \tag{7.42}$$

Итак,

$$V(x_1, ..., x_n) = \prod_{1 \le j < i \le n} (x_i - x_j) \tag{7.43}$$

A.7.6.2. Основное свойство определителя Вандермонда

В качестве следствия сразу получаем, что

Основное свойство определителя Вандермонда. Определитель Вандермонда равен нулю тогда и только тогда, когда среди чисел $x_1, ..., x_n$ есть равные.

$$V(x_1, ..., x_n) = 0 \Leftrightarrow \exists i \neq j : x_i = x_j \tag{7.44}$$

A.7.7. Критерий невырожденности матрицы

Теорема. Квадратная матрица A невырождена тогда и только тогда, когда $\det A \neq 0$.

Доказатательство. □ Пусть $A \in \mathrm{Mat}_n$. Приведём матрицу A с помощью ЭП строк к треугольному виду, получив A^*. Так как ранг не меняется, то матрица A невырождена $\Leftrightarrow$ матрица A^* невырождена, то есть $\mathrm{rk}\, A^* = n$. А это случается если и только если в $\mathrm{diag}\, A^* = (\lambda_1, ..., \lambda_n)$ все λ_i отличны от нуля. Но так как $\det A^* = \lambda_1 \cdot ... \cdot \lambda_n$, то $\det A \neq 0$, так как эти два определителя пропорцианальны. ■

A.7.8. Мультипликативное свойство определителя

Теорема. Пусть $A, B \in \mathrm{Mat}_n$. Тогда

$$\det(A \cdot B) = \det(A) \cdot \det(B) \tag{7.45}$$

Доказательство. □ Рассмотрим два случая

1. Если A вырождена. Тогда $A \cdot B$ тоже вырождена, так как $\mathrm{rk}(A \cdot B) \leq \mathrm{rk}\, A < n$. Аналогично, если B вырождена.
2. Пусть обе матрицы невырождены. Каждую невырожденную матрицу можно представить в виде произведения элементарных матриц

   $$A = U_1 \cdot ... \cdot U_N \tag{7.46}$$

   Тогда можно сказать, что $E \to A$ в ходе N элементарных преобразований строк. Следовательно

   $$A \cdot B = U_1 \cdot ... \cdot U_N \cdot B \tag{7.47}$$

   Значит матрица $A \cdot B$ получена с помощью *тех же* ЭП строк из матрицы B. Тогда

   $$\det A = \lambda \cdot \det E = \lambda \tag{7.48}$$

   где λ — коэффициент, получаемый при этих преобразованиях. Значит $\det(A \cdot B) = \lambda \cdot \det B = \det A \cdot \det B$. ■

A.7.9. Миноры и вычисление определителей

Определение. Выделим в матрице $A \in \mathrm{Mat}_{m,n}$ квадратную подматрицу $k \times k$ в строках с номерами $i_1, ..., i_k$ и столбцах с номерами $j_1, ..., j_k$.

$$A = \begin{pmatrix} a_{11} & \dots & \dots & \dots & a_{1n} \\ \vdots & \dots & \dots & \dots & \vdots \\ \vdots & \circ & \circ & \circ & \vdots \\ \vdots & \circ & \circ & \circ & \vdots \\ \vdots & \circ & \circ & \circ & \vdots \\ a_{m1} & \dots & \dots & \dots & a_{mn} \end{pmatrix} \tag{7.49}$$

Определитель выделенной подматрицы называется минором порядка k матрицы A.

$$M_{i_1,\dots,i_k}^{j_1,\dots,j_k} = \begin{vmatrix} a_{i_1,j_1} & \dots & a_{i_1,j_k} \\ \dots & \dots & \dots \\ a_{i_k,j_1} & \dots & a_{i_k,j_k} \end{vmatrix} \tag{7.50}$$

В частности, если $m = n$, рассмотрим миноры порядка $n - 1$.

Определение. Дополнительным минором к элементу a_{ij} называется определитель матрицы, полученной вычёркиеванием i-й строки и j-го столбца матрицы A. Обозначается M_{ij}.

Определение. Алгебраическим дополнением к элементу a_{ij} матрицы A называется число

$$A_{ij} = (-1)^{i+j} M_{ij} \tag{7.51}$$

. *Теорема.* Определитель матрицы A равен сумме произведений элементов любой строки (столбца) на соответствующие алгебраические дополнения.

$$\det A = a_{i1} \cdot A_{i1} + \dots + a_{in} \cdot A_{in} \tag{7.52}$$

$$\det A = a_{1j} \cdot A_{1j} + \dots + a_{nj} \cdot A_{nj} \tag{7.53}$$

Доказательство. □ Докажем разложение по столбцу.

$$A^{(j)} = \begin{pmatrix} a_{1j} \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ a_{2j} \\ \vdots \\ 0 \end{pmatrix} + \dots + \begin{pmatrix} 0 \\ 0 \\ \dots \\ a_{nj} \end{pmatrix} \tag{7.54}$$

По аддитивности определителя имеем:

$$\det A = \sum_{i=1}^{n} \begin{vmatrix} a_{11} & \dots & a_{1,(j-1)} & 0 & a_{1,(j+1)} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \\ a_{i1} & \dots & a_{i,(j-1)} & a_{ij} & a_{i,(j+1)} & \dots & a_{in} \\ \dots & \dots & \dots & \dots & \dots & \dots & \\ a_{n1} & \dots & a_{n,(j-1)} & 0 & a_{n,(j+1)} & \dots & a_{nn} \end{vmatrix} =$$

$$= \sum_{i=1}^{n} (-1)^{j-1} \cdot \begin{vmatrix} 0 & a_{11} & \dots & a_{1,(j-1)} & a_{1,(j+1)} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \\ a_{ij} & a_{i1} & \dots & a_{i,(j-1)} & a_{i,(j+1)} & \dots & a_{in} \\ \dots & \dots & \dots & \dots & \dots & \dots & \\ 0 & a_{n1} & \dots & a_{n,(j-1)} & a_{n,(j+1)} & \dots & a_{nn} \end{vmatrix} = \tag{7.55}$$

$$= \sum_{i=1}^{n} (-1)^{i+j-2} \cdot \begin{vmatrix} a_{ij} & a_{i1} & \dots & a_{i,j-1} & a_{i,j+1} & \dots & a_{in} \\ 0 & a_{11} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & a_{n1} & \dots & a_{n,(j-1)} & a_{n,(j+1)} & \dots & a_{nn} \end{vmatrix} = \sum_{i=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot M_{ij}$$

Итак, для разложения по столбцам:

$$\det A = \sum_{i=1}^{n} a_{ij} \cdot A_{ij} \tag{7.56}$$

Чтобы получить разложение по строкам, достаточно заметить, что

$$\det A = \det A^T = \sum_{j=1}^{n} a_{ji}^T \cdot A_{ji}^T = \sum_{i=1}^{n} a_{ij} \cdot A_{ij} \ \blacksquare \tag{7.57}$$

A.7.10. Лемма о фальшивом разложении определителя

Пусть $i \neq j$, тогда

$$a_{i1} \cdot A_{j1} + \dots + a_{in} \cdot A_{jn} = 0 \tag{7.58}$$

$$a_{1i} \cdot A_{1j} + \dots + a_{ni} \cdot A_{nj} = 0 \tag{7.59}$$

Доказательство. Рассмотрим матрицу, где вместо j строки будет i-я строка той же матрицы A.

$$\det A' = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = 0 \tag{7.60}$$

Но если разложить его по j-й строке, то получим сумму:

$$\det A' = a_{i1} \cdot A_{j1} + ... + a_{in} \cdot A_{jn} = 0 \tag{7.61}$$

Аналогично доказывается для столбцов. ■

A.7.11. Формула обратной матрицы

Определение. Назовём присоединённой матрицей к квадратной матрице A, обозначаемой $A^\vee$ называется транспонированная матрица алгебраических дополнений матрицы A.

$$A^\vee = \begin{pmatrix} A_{11} & A_{21} & ... & A_{n1} \\ A_{12} & A_{22} & ... & A_{n2} \\ ... & ... & ... & ... \\ A_{1n} & A_{2n} & ... & A_{nn} \end{pmatrix} \tag{7.62}$$

Элементы $a^\vee_{ij} = A_{ji}$.

Теорема. Пусть матрица A обратима. Тогда обратная матрица может быть вычислена по формуле

$$A^{-1} = \frac{1}{\det A} \cdot A^\vee \tag{7.63}$$

Доказатательство. □ Рассмотрим $A \cdot A^\vee$: её элемент на месте (i, j) равен

$$a_{i1}a^\vee_{1j} + a_{i2}a^\vee_{2j} + ... + a_{in}a^\vee_{nj} = a_{i1} \cdot A_{j1} + a_{i2} \cdot A_{j2} + ... + a_{in} \cdot A_{jn} \tag{7.64}$$

Если $i = j$, то эта сумма равна $\det A$, а при $i \neq j$, по лемме о фальшивом разложении определителя, она равна нулю. Поэтому

$$A \cdot A^\vee = \begin{pmatrix} \det A & 0 & ... & 0 \\ 0 & \det A & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & \det A \end{pmatrix} = \det A \cdot E \tag{7.65}$$

Аналогично, в порядке $A^\vee \cdot A$ для элемента на позиции (i, j) имеем

$$a^\vee_{i1} \cdot a_{1j} + a^\vee_{i2} \cdot a_{2j} + ... + a^\vee_{in} \cdot a_{nj} = A_{1i} \cdot a_{1j} + A_{2i} \cdot a_{2j} + ... + A_{ni} \cdot a_{nj} \tag{7.66}$$

При $i = j$ это разложение $\det A$ по столбцу i, а если $i \neq j$, по лемме о фальшивом разложении определителя, сумма равна нулю. Следовательно,

$$A^\vee \cdot A = \det A \cdot E \tag{7.67}$$

Если матрица A обратима, то $\det A \neq 0$, и мы получаем, что

$$A \cdot \left(\frac{1}{\det A} \cdot A^{\vee} \right) = \left(\frac{1}{\det A} \cdot A \right) \cdot A^{\vee} = E \tag{7.68}$$

что и означает требуемое. ■

А.7.12. Метод Крамера решения СЛУ

Пусть у нас есть квадратная СЛУ

$$\begin{cases} a_{11}x_1 + ... + a_1 n x_n = b_1 \\ \vdots \ ..... \ \vdots \\ a_{n1}x_1 + ... + a_{nn}x_n = b_n \end{cases} \tag{7.69}$$

Её матричная запись будет

$$A \cdot x = b, \tag{7.70}$$

где $A = \begin{pmatrix} a_{11} & ... & a_1 n \\ ... & .... & ... \\ a_{n1} & ... & a_{nn} \end{pmatrix}, x = \begin{pmatrix} x_1 \\ ... \\ x_n \end{pmatrix}, b = \begin{pmatrix} b_1 \\ ... \\ b_n \end{pmatrix}.$

Обозначим $\Delta = \det A$. Обозначим Δ_j определитель матрицы, которая получается заменой j-го столбца в матрице коэффициентов на столбец свободных членов($j = 1, ..., n$).

$$\Delta = \begin{vmatrix} a_{11} & ... & a_1 n \\ ... & ... & ... \\ a_{n1} & ... & a_{nn} \end{vmatrix} \tag{7.71}$$

$$\Delta_j = \begin{vmatrix} a_{11} & ... & a_1(j-1) & b_1 & a_1(j+1) & ... & a_1 n \\ ... & ... & ... & ... & ... & ... & \\ a_{n1} & ... & a_{n,(j-1)} & b_n & a_{n,(j+1)} & ... & a_{nn} \end{vmatrix} \tag{7.72}$$

Правило крамера.

1. Квадратная СЛУ определена в том и только в том случае, когда $\det A \neq 0$, причём

$$x_j = \frac{\Delta_j}{\Delta} \tag{7.73}$$

2. Если $\Delta = 0$, но $\exists j : \ \Delta_j \neq 0$, то СЛУ несовместна.

Доказательство. □ Заметим, что A это матрица $n \times n$, тогда как $\tilde{A} = A \mid b$ это матрица $n \times (n+1)$. Тогда

$$\operatorname{rk} A \leq \operatorname{rk} \tilde{A} \leq n \tag{7.74}$$

1. Критерий определённости. Система линейных уравнений определена тогда и только тогда, когда $\operatorname{rk} A = \operatorname{rk} \tilde{A} = n \Leftrightarrow \operatorname{rk} A = n$ (последняя равносильность следует из неравенства выше). Значит это равносильно тому, что A невырождена, что эквивалентно $\Delta \neq 0$.

2. Условие несовместности. Пусть $\Delta = 0$, но $\exists j: \ \Delta_j \neq 0$. Отсюда следует, что столбцы матрицы j линейно независимы.

$$\operatorname{rk}\left\{A^{(1)}, ..., A^{(j-1)}, b, A^{(j+1)}, ..., A^{(n)}\right\} = n \tag{7.75}$$

   При добавлении ещё одной строки ранг может только увеличиться:

$$\operatorname{rk}\left\{A^{(1)}, ..., A^{(j-1)}, b, A^{(j+1)}, ..., A^{(n)}\right\} \leq \operatorname{rk} \tilde{A} \tag{7.76}$$

   Значит $\operatorname{rk} \tilde{A} = n$ и $\operatorname{rk} A < n$, поэтому, по теореме Кронекера-Капелли, система несовместна.

3. Доказательство формул Крамера. Предположим, что $\Delta \neq 0$. Значит у матрицы коэффициентов есть обратная: $A^{-1} = \frac{1}{\det A} \cdot A^{\vee}$. Если $A \cdot x = b$, то

$$x = A^{-1} \cdot b = \frac{1}{\det A} \cdot A^{\vee} \cdot b \tag{7.77}$$

   Распишем каждое неизвестное, $\forall j = 1, .., n$:

$$x_j = \frac{a^{\vee}_{j1} \cdot b_1 + a^{\vee}_{j2} \cdot b_2 + ... + a^{\vee}_{jn} \cdot b_n}{\det A} = \frac{b_1 \cdot A_{1j} + b_2 \cdot A_{2j} + ... + b_n \cdot A_{nj}}{\det A} = \frac{\Delta_j}{\Delta} \tag{7.78}$$

■

A.7.13. Теорема о ранге матрицы

Теорема. Ранг произвольной матрицы равен наибольшему порядку её ненулевого минора.

Доказательство. □ Пусть r — наибольший порядок ненулевого минора $M^{j_1,...,j_r}_{i_1,...,i_r} \neq 0$ матрицы A. Переставим строки и столбцы в матрице A. От этого миноры могут лишь поменять знак, но не равенство или неравенство нулю. А именно переставим так, чтобы $M^{1,...,r}_{1,...,r} \neq 0$, — минор занимал первые r строк и r столбцов. Тогда $M^{1,...,r}_{1,...,r} = \det \overline{A} \neq 0$. Пусть

$$\overline{A}_i = (a_{i1}, ..., a_{ir}) \tag{7.79}$$

Матрица $\overline{A}$ невырождена $\Rightarrow$ её строки линейно независимы, значит $\left\{\overline{A}_1, ..., \overline{A}_r\right\}$ образуют базис в $\mathbb{R}^n \Rightarrow \forall i > r \ \exists!(\lambda_1, ..., \lambda_r)$:

$$\overline{A}_i = \lambda_1 \overline{A}_1 + ... + \lambda_r \overline{A}_r \tag{7.80}$$

Так как $\left\{\overline{A_1}, ..., \overline{A_r}\right\}$ линейно независимы, то линейно независимы и строки $\left\{\overline{A_1}, ..., \overline{A_r}\right\}$. Если бы это было не так, то $\exists \mu_1, ..., \mu_r \neq 0$:

$$\mu_1 \overline{A}_1 + ... + \mu_r \overline{A}_r = 0 \tag{7.81}$$

что неверно.

$\forall i, j > r$ Рассмотрим $M^{1,...,r,j}_{1,...,r,i}$ — он называется окаймляющим минором, и он обязательно равен нулю. Рассмотрим соответствующую матриу $\overline{\overline{A}}$. Её строки линейно независимы, а $\left\{\overline{\overline{A}}_1, ..., \overline{\overline{A}}_{r+1}\right\}$ уже линейно зависимы.

$$\overline{\overline{A}}_{r+1} = \lambda'_1 \overline{\overline{A}}_1 + ... + \lambda'_r \overline{\overline{A}}_r \tag{7.82}$$

Поэтому для более коротких строк верно

$$\overline{A}_{r+1} = \lambda'_1 \overline{A}_1 + ... + \lambda'_r \overline{A}_r \tag{7.83}$$

В силу единственности выражения строки в базисе,

$$\lambda'_1 = \lambda_1, ..., \lambda'_r = \lambda_r \tag{7.84}$$

Следовательно $\forall i = 1, ..., n$:

$$a_{ij} = \lambda_1 a_{1j} + ... + \lambda_r a_{rj} \Rightarrow A_i = \lambda_1 A_1 + ... + \lambda_r A_r \tag{7.85}$$

И поэтому $\{A_1, ..., A_r\}$ образует базис системы строк матрицы A, поэтому ранг матрицы A равен r. ■

A.8. Основы теории групп и основные алгебраические структуры

Определение. **Группа** — это множество G, на котором задана бинарная операция $(*)$, т. е. отображение $G \times G \to G$, которое удовлетворяет следующим свойствам(аксиомы группы):

1. Ассоциативность: $\forall a, b, c \in G : (a * b) * c = a * (b * c)$.
2. Существование нейтрального элемента: $\exists e \in G : \forall g \in G : e * g = g * e = g$.
3. Существование обратного элемента: $\forall g \in G : \exists h \in G : g * h = h * g = e$.

A.8.1. Следствия из аксиом группы

1. Единственность нейтрального элемента: $\forall g \in G\ \exists! e \in G : e * g = g * e = g$.

   Доказательство. □ Предположим, что есть два нейтральных элемента: e и e'. Тогда так как e — нейтральный элемент,

   $$e' * e = e \tag{8.1}$$

   Аналогично, в силу нейтральности элемента e',

   $$e' * e = e' \tag{8.2}$$

   Поэтому $e \equiv e'$. ■

2. Единственность обратного элемента: $\forall g \in G\ \exists! h \in G : g * h = h * g = e$. *Доказательство.* □ Предположим, что для некоторого элемента g существуют два обратных элемента: h и h'. Тогда

   $$h' * g * h = (h' * g) * h = e * h = h \tag{8.3}$$

   Но в силу ассоциативности, скобки можно расставить иначе:

   $$h' * g * h = h' * (g * h) = h' * e = h' \tag{8.4}$$

   Поэтому $h \equiv h'$. ■

   2.1. Поэтому обозначим обратный элемент к g как g^{-1}.

A.8.1.1. Абелевы группы

Определение. Группа G называется коммутативной(абелевой), если

$$\forall a, b \in G : a * b = b * a. \tag{8.5}$$

A.8.2. Примеры групп и не групп

1. $\mathbb{N}$ с умножением чисел — не группа, так как нарушена аксиома 3.
2. Множество перестановок S_n с операцией умножения(композиции) — это группа.
   - Называется симметрической группой степени n.

3. Арифметическое векторное пространство $\mathbb{R}^n$ с операцией $+$. Это абелева группа.

A.8.3. Подгруппа

Определение. Пусть G — группа. Множество $H \subseteq G$ называется подгруппой группы G, если

1. $H \neq \varnothing$
2. $a, b \in H \Rightarrow a * b \in H$
3. $a \in H \Rightarrow a^{-1} \in H$.

Замечания

1. В любой подгруппе есть нейтральный элемент.

   Доказательство. □ Пусть H — подгруппа G, по свойству 1 из определения подгруппы $H \neq \varnothing$, значит существует элемент $h \in H$. По свойству 3 определения, $h^{-1} \in H$. Следовательно, по свойству 2, $h * h^{-1} = e \in H$. ■

2. Подгруппа H сама является группой относительно операции на самой группе G, ограниченной на H.

Например,

1. Множество чётных перестановок $A_n \subset S_n$. Это подгруппа S_n.
   - A_n называется знакопеременной группой степени n.
2. $S_n \setminus A_n$ не является подгруппой S_n, так как произведение двух нечётных перестановок является чётной перестановкой.

A.8.4. Кольца

А что такое кольцо?

Определение. Кольцо — это множество K с двумя бинарными операциями — сложения и умножения, которое удовлетворяет следующим аксиомам:

1. Коммутативность сложения: $\forall a, b \in K : a + b = b + a$.
2. Ассоциативность сложения: $\forall a, b, c \in K : (a + b) + c = a + (b + c)$.
3. Нулевой элемент: $\exists 0 \in K : \forall a \in K : a + 0 = a$.
4. Существование противоположного элемента: $\forall a \in K : \exists (-a) \in K : a + (-a) = 0$.

   Говоря коротко, $(K, +)$ — абелева группа. Такая группа называется аддитивной группой кольца K.

5. Дистрибутивность умножения относительно сложения.

5.1. Левая дистрибутивность, $\forall a, b, c \in K$:

$$a \cdot (b + c) = a \cdot b + a \cdot c \tag{8.6}$$

5.2. Правая дистрибутивность, $\forall a, b, c \in K$:

$$(a + b) \cdot c = a \cdot c + b \cdot c \tag{8.7}$$

A.8.4.1. Классы колец

1. Коммутативные: $\forall a, b \in K : a \cdot b = b \cdot a$.
2. Ассоциативные: $\forall a, b, c \in K : (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. С единицей: $\exists 1 \in K : \forall a \in K : a \cdot 1 = 1 \cdot a = a$.
4. И другие.

A.8.4.2. Примеры колец

1. $(\mathbb{Z}, +, \cdot)$ — коммутативное ассоциативное кольцо с единицей
2. $(\mathrm{Mat}_n, +, \cdot)$ — некоммутиавное ассоциативное кольцо с единицей.
3. $\{$геометрические векторы в пространстве$\}$ с операцией сложения и векторного произведения — некоммутативное неассоциативное кольцо без единицы.

A.8.5. Следствия из аксиом кольца

Пусть K — кольцо с единицей. Первые два свойства следуют из теории групп, так как $(K, +)$ — абелева группа.

1. Единственность нулевого элемента.
2. Единственность противоположного элемента.
3. Единственность 1.
4. $0 \cdot a = a \cdot 0 = 0, \forall a \in K$.

   Доказательство. □ Пусть $a \in K$. Тогда

   $$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \tag{8.8}$$

   Добавим $-(0 \cdot a)$ к обеим частям равенства:

   $$0 = 0 \cdot a \tag{8.9}$$

   Что и требовалось(аналогично с нулевым элементом справа). □
5. $(-1) \cdot a = a \cdot (-1) = -a, \forall a \in K$. *Доказательство.* □

   $$a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = (1 + (-1)) \cdot a = 0 \cdot a = 0 \tag{8.10}$$

Аналогично с умножением справа. ■

Далее кольца будем предполагать ассоциативными и с единицей.

A.8.6. Обратный элемент в кольце

Определение. Пусть K — ассоциативное кольцо с единицей. Назовём элемент $a \in K$ обратимым, если $\exists b \in K : a \cdot b = b \cdot a = 1$.

Обозначение: a^{-1}.

Не у каждого элемента в кольце есть обратный, то если он есть, то он единственный.

Замечание. Если $|K| > 1$, то 0 необратим.

Доказательство. □ Пусть $|K| > 1$.

1. Во-первых, $1 \neq 0$. Если бы это было не так, то $\forall a \in K : a = a \cdot 1 = a \cdot 0 = 0$.
2. $\forall b \in K : 0 \cdot b = b \cdot 0 = 0 \neq 1$.

На что бы мы не умножили 0, результат всегда будет 0, а не 1. Следовательно, 0 не может иметь обратного элемента. ■

Предложение. Положим $K^\times = \{a \mid a \text{ обратим}\}$

1. $a, b \in K \Rightarrow a \cdot b \in K$
2. $K^\times$ с операцией умножения — группа, называемая мультипликативной группой кольца K.

Доказательство. □

1. Докажем, что $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. Действительно,

$$(a \cdot b) \cdot (b \cdot a)^{-1} = a \cdot \left(b \cdot b^{-1}\right) \cdot a^{-1} = a \cdot 1 \cdot a^{-1} = a \cdot a^{-1} = 1. \tag{8.11}$$

   Итак, произведение двух обратимых элементов обратимо.

2. $1 \in K$, кроме того, $a, b \in K^\times \Rightarrow a \cdot b \in K^\times$ и, наконец, $\left(a^{-1}\right)^{-1} = a$.

Исходя из этих свойств $K^\times$ — группа относительно умножения. ■

Например,

1. $\mathbb{Z}^\times = \{-1, +1\}$
2. $\mathrm{Mat}_n^\times = \{A \mid \mathrm{rk}(A) = n\} = \{A \mid \det A \neq 0\} = GL_n$ — так называется *полная матричная группа.*

A.8.7. Делители нуля

Определение. Элемент $a \in K$, $a \neq 0$ называется левым делителем нуля, если $\exists b \in K$ и $b \neq 0: \ a \cdot b = 0$.

Определение. Элемент $a \in K$, $a \neq 0$ называется правым делителем нуля, если $\exists b \in K$ и $b \neq 0: \ b \cdot a = 0$.

Примеры:

1. В $\mathbb{Z}$ нет делителей нуля!
2. В Mat_n есть делители нуля: $A = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 \end{pmatrix}$ и $B = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 1 \end{pmatrix}$, для которых $A \cdot B = 0$.

Предложение.

1. Делители нуля необратимы.
2. Если $a, b, c \in K$, причём $a \neq 0$ и a не является левым делителем нуля, то
$$a \cdot b = a \cdot c \Rightarrow b = c. \tag{8.12}$$
3. Если $a, b, c \in K$, причём $a \neq 0$ и a не является правым делителем нуля, то
$$b \cdot a = c \cdot a \Rightarrow b = c. \tag{8.13}$$

Доказательство. □ Пусть a обратим и $a \cdot b = 0$. Умножим это равенство слева на a^{-1}:

$$a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 \tag{8.14}$$

Отсюда $b = 0$. Аналогично можно доказать, что $b \cdot a = 0 \Rightarrow b = 0$. Поэтому делители нуля необратимы.

Теперь предположим что $a \cdot b = a \cdot c$. Прибавим к левой и правой части $-(a \cdot c)$:

$$a \cdot b - a \cdot c = 0 \tag{8.15}$$

$$a \cdot (b - c) = 0 \tag{8.16}$$

Но a не является делителем нуля слева, следовательно, $b - c = 0$, то есть $b = c$. Аналогично доказывается пункт 3. ■

A.8.8. Поля

Определение. Поле — это коммутативное, ассоциативное кольцо K с единицей, в котором $|K| > 1$ и все ненулевые элементы обратимы.

Например,

1. $\mathbb{Z}$ — не поле.

2. $\mathbb{R}$ — поле.

Определение. Пусть K — кольцо или поле. Подмножество $L \subseteq K$ называется подкольцом или подполем, если

1. $L \neq \varnothing$

2. $a, b \in L \Rightarrow a + b \in L, a \cdot b \in L$.

3. $a \in L \Rightarrow (-a) \in L$.
   - в частности, $0 \in L$.

4. Для полей дополнительно требуется $|L| > 1$.

5. Для полей дополнительно требуется $a \in L, a \neq 0 \Rightarrow a^{-1} \in L$.
   - В частности, $1 \in L$.

Подкольцо/подполе само является кольцом/полем относительно операций, ограниченном на этом подкольце/подполе.

Например,

$$\underset{\text{подкольцо}}{\mathbb{Z}} \subset \underset{\text{подполе}}{\mathbb{Q}} \subset \underset{\text{поле}}{\mathbb{R}} \tag{8.17}$$

В теории СЛАУ, матриц, определителей для чисел кроме $\mathbb{R}$ можно рассматривать любое поле.

А.8.9. Кольца вычетов

Определние. Числа $a, b \in \mathbb{Z}$ называются сравнимыми по модулю $m \in \mathbb{Z} \setminus \{0\}$, если они имеют равные остатки при делении на m, или, что одно и то же, $m \mid (a - b)$. Обозначается $a \equiv b (\mathrm{mod}\, m)$, кратко можно написать $a \underset{m}{\equiv} b$.

Определение. Для $k \in \mathbb{Z}$ множество

$$\overline{k} \underset{\text{def}}{=} \{a \in \mathbb{Z} \mid a \equiv k \ (\mathrm{mod}\, m)\} \tag{8.18}$$

называется *классом вычетов* числа k по модулю m.

Замечание. Существует m различных остатков при делении на m, поэтому существует лишь m различных классов вычетов по модулю m.

Замечание 2. Таким образом, множество всех возможных классов вычетов по модулю m образует разбиение $\mathbb{Z}$ на m непересекающихся подмножеств.

Определение. Кольцо вычетов по модулю m — это множество всех классов вычетов по модулю m с операциями сложения и умножения, определёнными следующим образом:

1. $\overline{a} + \overline{b} = \overline{a + b}$
2. $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$

Обозначение: $\mathbb{Z}_n$.

Кольцо вычетов по модулю m является коммутативным ассоциативным кольцом с единицей.

Предложение.

1. $\overline{k} \in \mathbb{Z}_m$ — делитель нуля $\Leftrightarrow k \nmid m$ и $\gcd(k, m) > 1$.
2. $\overline{k} \in \mathbb{Z}_m^\times \Leftrightarrow \gcd(k, m) = 1$ (критерий обратимости вычета).

Доказательство. □

1. $\overline{k}$ — делитель нуля $\Leftrightarrow \left(\overline{k} \neq \overline{0}\right) \wedge \left(\exists \overline{l} \neq \overline{0} : \overline{k} \cdot \overline{l} = \overline{0}\right)$. Из первого условия k не делится на m, а из второго

$$\exists l \nmid m : (k \cdot l) \vdots m \tag{8.19}$$

   Значит у k и l есть обшие делители, так как иначе одно из чисел должно было делиться на m нацело.

   Обратно, пусть $\gcd(k, m) > 1$ и при этом k не делится на m. Тогда можно написать, что $k = k' \cdot d$ и $m = m' \cdot d$ для некоторого общего делителя d, меньшего m, но большего 1.

   Пусть $l = m'$. Тогда $k \cdot l = k' \cdot d \cdot m' = k' \cdot m$. Значит это делитель нуля.

2. $\overline{k} \in \mathbb{Z}_m^\times \Rightarrow \overline{k} \neq \overline{0}$ и $\overline{k}$ не делитель нуля. По пункту 1, это равносильно тому, что

$$\begin{cases} k \nmid m \\ \gcd(k, m) = 1 \end{cases} \tag{8.20}$$

   Обратно, пусть $\overline{k} \neq \overline{0}$ и $\overline{k}$ — неделитель нуля. Рассмотрим произведения

$$\overline{k} \cdot \overline{0},\ \overline{k} \cdot \overline{1},\ \ldots,\ \overline{k} \cdot \overline{m-1} \tag{8.21}$$

   Таких произведений m штук. Если два таких произведения совпали:

$$\overline{k} \cdot \overline{i} = \overline{k} \cdot \overline{j} \Rightarrow \overline{i} = \overline{j}. \tag{8.22}$$

Следовательно, множество таких произведений это просто $\mathbb{Z}_m$. В частности, $\overline{1} \in \mathbb{Z}_m$, поэтому $\exists \overline{k}, \overline{l} \in \mathbb{Z}_m : \overline{k} \cdot \overline{l} = \overline{1}$. Обратимость даказана.

■

Следствие. $\mathbb{Z}_m$ — поле $\Leftrightarrow$ m — простое число.

Доказательство. □ $\mathbb{Z}_m$ коммутативно, ассоциативно и содержит единицу, поэтому осталось показать, что любой ненулевой вычет обратим. $\mathbb{Z}_m$ — поле $\Leftrightarrow \mathbb{Z}_m^{\times} = \mathbb{Z}_m \setminus \{\overline{0}\}$. А это случается тогда и только тогда, когда все числа от 1 до $(m-1)$ взаимно просты с m, а это то же самое, что число m — простое. ■

A.8.10. Характеристика поля

Определение. Пусть K — произвольное поле. Назовём характеристикой поля число

$$\operatorname{char} K = \begin{cases} \min\left\{ p \in \mathbb{N} \mid \underbrace{\overline{1} + \ldots + \overline{1}}_{p \text{ раз}} = \overline{0} \right\}, \exists p \\ 0, \text{иначе} \end{cases} \tag{8.23}$$

Например,

1. $\operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{Q} = 0$.
2. $\operatorname{char} \mathbb{Z}_p = p$, если p — простое число.

Теорема. Характеристика любого поля либо равна нулю, либо простое число.

Доказательство. □ Пусть $\operatorname{char} K = p > 1$ и p не простое. Тогда $p = k \cdot l$, причём $1 < k, l < p$.

$$\underbrace{1 + \ldots + 1}_{k} \neq 0 \tag{8.24}$$

$$\underbrace{1 + \ldots + 1}_{l} \neq 0 \tag{8.25}$$

Но при перемножениии эти сумм получим

$$\underbrace{1 + \ldots + 1}_{k \cdot l = p} \underset{\text{характ.}}{=} 0 \tag{8.26}$$

Значит в K есть делитель нуля, но это противоречие, так как в поле нет делителя нуля(они необратимы), а в поле все элементы обратимы. ■

Предложение. Если $\operatorname{char} K = p > 0$, то $\forall x, y \in K$:

$$(x+y)^p = x^p + y^p. \tag{8.27}$$

Доказательство. □ Согласно биному Ньютона,

$$(x+y)^p = x^p + C_p^1 x^{p-1} y + ... + C_p^k x^{p-k} y^k + ... + y^p \tag{8.28}$$

Поскольку $C_p^k = \frac{p!}{k!(p-k)!}$ целое, и числитель делится на p, а знаменатель нет, то C_p^k делится на p. Следовательно, все члены бинома Ньютона, кроме первого и последнего, равны нулю в поле характеристики p:

$$C_n^k = \underbrace{1 + ... + 1}_{p} + ... + \underbrace{1 + ... + 1}_{p} = 0 \tag{8.29}$$

Поэтому остаются только x^p и y^p. ■

Следсвствие. Если $\operatorname{char} K = p > 0$, то $\forall x, y \in K$:

$$(x_1 + ... + x_n)^p = x_1^p + ... + x_n^p \tag{8.30}$$

A.8.11. Малая теорема Ферма

Пусть p — простое число. Тогда $\forall n \in \mathbb{Z}$:

$$n^p \equiv n \pmod p \tag{8.31}$$

Доказательство. □ Рассмотрим $\mathbb{Z}_p$: Надо доказать, что

$$\overline{n^p} = \overline{n} \tag{8.32}$$

Тогда по ((8.30)) имеем:

$$\overline{n} = \overline{1} + ... + \overline{1} \Rightarrow \overline{n^p} = \overline{1}^p + ... + \overline{1}^p = \overline{1} + ... + \overline{1} = \overline{n} \tag{8.33}$$

Что и требовалось доказать. ■

A.9. Кольцо многочленов

Определение. Пусть K — ассоциативное, коммутативное кольцо с единицей. Кольцом многочленов от одной переменной над K называется кольцо $K[x]$, удовлетворяющее следующим условиям:

1. Кольцо многочленов должно содержать кольцо K или подкольцо, изоморфное K.

$$K[x] \supset K \tag{9.1}$$

2. Существует элемент x, называемый переменной:

$$K[x] \supset x \notin K \tag{9.2}$$

3. $\forall f \neq 0$ $\exists!$ представление f в виде:

$$f = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n, \tag{9.3}$$

причём $a_i \in K$, $a_n \neq 0$.

Определение. Степенью многочлена f называется наибольший показатель степени переменной x в его разложении. Обозначение: $\deg f$.

Замечание. У нулевого мночголена степени нет, или её формально можно считать равной $-\infty$.

Определение. $a_0, a_1, ..., a_n$ называются коэффициентами многочлена f. Коэффициент a_n называется старшим коэффициентом.

Определение. Стеепени $x^0, x^1, ..., x^n$ называются мономами или одночленами.

Замечание. Если $c_0 + c_1 x + ... + c_n x^n = 0$, то $c_0 = c_1 = ... = c_n = 0$. Если бы это было не так, то взяв

$$f = a_0 + a_1 x + ... + a_n x^n \neq 0, \tag{9.4}$$

тогда для f найдётся другое представление

$$f = (a_0 + c_0) + (a_1 + c_1)x + ... + (a_n + c_n)x^n, \tag{9.5}$$

что противоречит единственности представления многочлена.

Замечание. Если разрешить

$$f = \sum_{k=0}^{\infty} a_k x^k, \tag{9.6}$$

так, чтобы только конечное число коэффициентов было ненулевыми, то свойство 3 можно сформулировать так: $\forall f \neq 0\ \exists!$ представление f в виде бесконечной суммы.

A.9.1. Единственность кольца многочленов

Теорема. Кольцо многочленов $K[x]$ единственно с точностью до изоморфизма.

Доказательство. □ Пусть $f = \sum_{n\geq 0} a_n x^n \in K[x]$ и $g = \sum_{n\geq 0} b_n x^n \in K[x]$. Тогда их сумма равна

$$f + g = \sum_{n\geq 0} (a_n + b_n) x^n, \tag{9.7}$$

а произведение равно

$$f \cdot g = \sum_{k\geq 0} a_k x^k \cdot \sum_{l\geq 0} b_l x^l = \sum_{k,l\geq 0} a_k b_l x^{k+l} = \sum_{n\geq 0} \left(\sum_{\substack{(k,l):\\ k+l=n}} a_k b_l \right) x^n. \tag{9.8}$$

Коэффициенты в суммах и произведениях зависят только от коэффициентов сомножителей. Пусть $K[y]$ — другое кольцо многочленов. Построим изоморфизм $\varphi : K[x] \xrightarrow{\sim} K[y]$ следующим образом:

$$\varphi\left(\sum_{n\geq 0} a_n x^n \right) = \sum_{n\geq 0} a_n y^n. \tag{9.9}$$

1. Проверим, что φ биективно. Так как многочлены имеют единстенное представление в виде комбинации коэффициентов, у у многочленов из $K[x]$ и $K[y]$ при отображении φ один и тот же набор коэффициентов, то элемент и его образ однозначно соответствуют друг другу.
2. Проверим, что φ — гомоморфизм. Так как результат операций сложения и умножения многочленов зависит только от коэффициентов, то при отображении φ сумма и произведение сохраняются.

Таким образом, кольца $K[x]$ и $K[y]$ изоморфны. ■

A.9.2. Существование кольца многочленов

Определение. Последовательность $a_0, a_1, ..., a_k, ...$ элементов кольца K называется финитной, если $\exists N \in \mathbb{N} : \forall n > N\ a_n = 0$.

Обозначим K^∞ множество всех финитных последовательностей элементов кольца K.

Определим на K^∞ операцию суммы. $\forall a, b \in K^\infty$:

$$(a_0, a_1, ..., a_n, ...) + (b_0, b_1, ..., b_n, ...) = (a_0 + b_0, a_1 + b_1, ..., a_n + b_n, ...). \quad (9.10)$$

$$a \cdot b = \Bigg(a_0 \cdot b_0, a_0 \cdot b_1 + a_1 \cdot b_0, a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0, ..., \sum_{(k,l):k+l=n} a_k \cdot b_l, ... \Bigg). \quad (9.11)$$

Проверим свойства кольца на K^∞.

1. Коммутативность сложения и умножения следует из коммутативности в K.
2. Ассоциативность сложения следует из ассоциативности в K.
3. Ассоциативность умножения. Пусть $a, b, c \in K^\infty$, $f = a \cdot b$, $g = (a \cdot b) \cdot c$, $u = b \cdot c$, $v = a \cdot (b \cdot c)$. Тогда мы хотели бы доказать, что $g = v$. Рассмотрим n-ый коэффициент g:

$$g_n = \sum_{\substack{(k,l):\\ k+l=n}} f_k \cdot c_l = \sum_{\substack{k,l\geq 0\\ k+l=n}} \left(\sum_{\substack{i,j\geq 0\\ i+j=k}} a_i \cdot b_j \right) \cdot c_l = \sum_{\substack{i,j,l\geq 0\\ i+j+l=n}} a_i \cdot b_j \cdot c_l. \quad (9.12)$$

$$v_n = \sum_{\substack{(i,m):\\ i+m=n}} a_i \cdot u_m = \sum_{\substack{i,m\geq 0\\ i+m=n}} a_i \cdot \left(\sum_{\substack{j,l\geq 0\\ j+l=m}} b_j \cdot c_l \right) = \sum_{\substack{i,j,l\geq 0\\ i+j+l=n}} a_i \cdot b_j \cdot c_l. \quad (9.13)$$

   Таким образом, $g_n = v_n$ для всех $n \in \mathbb{N}$, значит, $g = v$.

4. Дистрибутивность умножения относительно сложения. $a \cdot (b + c) = a \cdot b + a \cdot c$. Пусть $f = a \cdot (b + c)$, $g = a \cdot b + a \cdot c$. Рассмотрим n-ый коэффициент f:

$$f_n = \sum_{\substack{(k,l):\\ k+l=n}} a_k \cdot (b + c)_l = \sum_{\substack{(k,l):\\ k+l=n}} a_k \cdot (b_l + c_l) = \sum_{\substack{(k,l):\\ k+l=n}} a_k \cdot b_l + \sum_{\substack{(k,l):\\ k+l=n}} a_k \cdot c_l \quad (9.14)$$

$$g_n = (a \cdot b)_n + (a \cdot c)_n = \sum_{\substack{(k,l):\\ k+l=n}} a_k \cdot b_l + \sum_{\substack{(k,l):\\ k+l=n}} a_k \cdot c_l. \quad (9.15)$$

   Таким образом, $f_n = g_n$ для всех $n \in \mathbb{N}$, значит, $f = g$.

5. Нулевой элемент: $0 = (0, ..., 0, ...)$

6. Противоположный элемент: для $a = (a_0, a_1, ..., a_n, ...)$ его противоположный элемент равен $-a = (-a_0, -a_1, ..., -a_n, ...)$.

7. Единичный элемент: $1 = (1, 0, 0, ..., 0, ...)$.

   Поэтому K^∞ является ассоциативным, коммутативным кольцом с единицей.

8. $K^\infty \supset (a_0, 0, 0, ..., 0, ...)$. Если сложить две такие последовательности, то получится $(a_0 + b_0, 0, 0, ..., 0, ...)$. Если перемножить, то получится $(a_0 \cdot b_0, 0, 0, ..., 0, ...)$. Таким образом, множество таких последовательностей изоморфно K.

9. Пусть $x = (0, 1, 0, 0, ..., 0, ...)$ — переменная.

10. $x^n = (0, 0, ..., 1, 0, ..., 0, ...)$, где 1 стоит на n-ой позиции.

    Докажем по индукции. □ База: $n = 0$. Тогда $x^0 = (1, 0, 0, ..., 0, ...) = 1$. Пусть верно для $n \in \mathbb{N}$: $x^n = (0, 0, ..., 1, 0, ..., 0, ...)$. Тогда

$$\begin{gathered} x^{n+1} = x^n \cdot x = (0, 0, ..., 1, 0, ..., 0, ...) \cdot (0, 1, 0, 0, ..., 0, ...) = \\ = (0, 0, ..., 0, 1, 0, ..., 0, ...) = x^{n+1} \ \blacksquare \end{gathered} \tag{9.16}$$

11. $\forall a = (a_0, a_1, ..., a_n, ...) \in K^\infty$:

$$\begin{gathered} a = (a_0, 0, 0, ..., 0, ...) + (0, a_1, 0, ..., 0, ...) + ... + (0, 0, ..., a_n, 0, ...) = \\ = a_0 x^0 + a_1 x^1 + ... + a_n x^n + ... \end{gathered} \tag{9.17}$$

    причём коэффициенты этой линейной комбинации определены однозначно по представлению a.

Поэтому K^∞ является моделью кольца многочленов над K и значит $K[x]$ существует.

A.9.3. Алгебраические свойства многочленов

Определение. Кольцо K называется целостным, если K — ассоциативное, коммутативное кольцо с единицей и без делителей нуля.

1. Кольцо $\mathbb{Z}$ целостно.

2. Любое поле есть область целостности.

Теорема. Если $f, g \in K[x]$, $f, g \neq 0$ и K — область целостности, то $f \cdot g \neq 0$ и

$$\deg(f \cdot g) = \deg f + \deg g \tag{9.18}$$

Доказательство. □ Пусть $f = a_0 + a_1x + ... + a_nx^n$, $g = b_0 + b_1x + ... + b_mx^m$, где $a_n \neq 0, b_m \neq 0$.

$$f \cdot g = \sum_{\substack{i=0,...,n \\ j=0,...,m}} a_i \cdot b_j x^{i+j} = a_n \cdot b_m x^{n+m} + \sum_{\substack{(i,j): \\ i+j<n+m}} a_i \cdot b_j x^{i+j} \neq 0, \tag{9.19}$$

причём $\deg(f \cdot g) = n + m = \deg f + \deg g$. ■

Замечание. Если счиать $\deg 0 = -\infty$, то теорема верна для нулевого многочлена.

Следствие. $K[x]$ над областью целостности K тоже является областью целостности, причём его группа обратимых по умножению элементов равна группе обратимых элементов $K^\times$.

$$K[x]^\times = K^\times \tag{9.20}$$

Доказательство. □

1. Так как произведение ненулевых многочленов ненулевое, то в $K[x]$ нет делителей нуля, значит, $K[x]$ — область целостности.
2. Пусть $f \in K[x]^\times$. Тогда существует $g \in K[x]$: $f \cdot g = 1$. По теореме выше $\deg(f \cdot g) = \deg f + \deg g$. Так как $\deg 1 = 0$, то $\deg f + \deg g = 0$. Следовательно, $\deg f = \deg g = 0$ и $f, g \in K$. Поэтому если многочлен f обратим в $K[x]$, то он лежит и обратим в K, то есть $f \in K^\times$. ■

A.9.4. Кольцо многчленов над полем

Всякий многочелен $f = a_0 + a_1x + ... + a_nx^n \in K[x]$ определяет функцию $f : K \to K$ по правилу $f(t) = a_0 + a_1t + ... + a_nt^n$. Такие функции называются полиномиальными.

A.9.4.1. Задача полиномиальной интерполяции

Пусть даны n различных элементов $x_1, ..., x_n \in K$, где K — поле, и ещё n элементов $y_1, ..., y_n \in K$. Требуется найти полиномиальную функцию $f : K \to K$, такую что $f(x_i) = y_i, \forall i = 1, ..., n$.

A.9.4.2. Теорема об интерполяции

Теорема. Пусть K — поле, $x_1, ..., x_n \in K$ — различные элементы, $y_1, ..., y_n \in K$ — произвольные элементы. Тогда существует единственный многочлен $f \in K[x]$ степени меньше n, такой что $f(x_i) = y_i$, $\forall i = 1, ..., n$.

Доказательство. □ Пусть $f(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$.

$$\begin{cases} f(x_1) = a_0 + a_1 x_1 + ... + a_{n-1} x_1^{n-1} = y_1 \\ f(x_2) = a_0 + a_1 x_2 + ... + a_{n-1} x_2^{n-1} = y_2 \\ ... \\ f(x_n) = a_0 + a_1 x_n + ... + a_{n-1} x_n^{n-1} = y_n \end{cases} \tag{9.21}$$

— система линейных уравнений относительно неизвестных $a_0, a_1, ..., a_{n-1}$. Определитель матрицы этой системы есть определитель Вандермонда с точностью до транспонирования:

$$\Delta = \begin{vmatrix} 1 & x_1 & x_1^2 & ... & x_1^{n-1} \\ 1 & x_2 & x_2^2 & ... & x_2^{n-1} \\ ... & & & & \\ 1 & x_n & x_n^2 & ... & x_n^{n-1} \end{vmatrix} = \prod_{(1 \le i < j \le n)} (x_j - x_i) \neq 0. \tag{9.22}$$

Так как все x_i различны, то определитель $\Delta \neq 0$ и система имеет единственное решение. ■

По правилу Крамера, решение системы можно записать явно:

$$a_j = \frac{\Delta_j}{\Delta}, \tag{9.23}$$

где в Δ_j мы заменили $(j+1)$-ый столбец матрицы Δ на столбец свободных членов:

$$\Delta_j = \begin{vmatrix} 1 & x_1 & ... & x_1^{j-1} & y_1 & x_1^{j+1} & ... & x_1^{n-1} \\ 1 & x_2 & ... & x_2^{j-1} & y_2 & x_2^{j+1} & ... & x_2^{n-1} \\ ... & & & & & & & \\ 1 & x_n & ... & x_n^{j-1} & y_n & x_n^{j+1} & ... & x_n^{n-1} \end{vmatrix} = \sum_{i=1}^{n} \left(y_i \cdot \prod_{\substack{(1 \le m \le n \\ m \neq i)}} (x_m - x_i) \right). \tag{9.24}$$

Тогда многочлен интерполяции можно записать в виде:

$$f(x) = \sum_{i=1}^{n} \left(y_i \cdot \prod_{\substack{(1 \le m \le n \\ m \neq i)}} \left(\frac{x - x_m}{x_i - x_m} \right) \right). \tag{9.25}$$

Этот многочлен называется интерполяционным многочленом Лагранжа.

Предложение. Пусть K — бесконечное поле, $f = \sum_{k \ge 0} a_k x^k$, $g = \sum_{k \ge 0} b_k x^k \in K[x]$. Тогда имеет место эквивалентность функционального и формального равенства:

$$f(c) = g(c) \ \forall c \in K \Leftrightarrow f = g \tag{9.26}$$

Доказательство. □ Из формального равенства очевидно следует функциональное равенство. Докажем обратное.

$$f = a_0 + a_1 x + ... + a_n x^n, g = b_0 + b_1 x + ... + b_m x^n. \tag{9.27}$$

Выберем $n+1$ различных элементов $x_0, x_1, ..., x_n \in K$, так как поле K бесконечно. Обозначим $y_i = f(x_i) = g(x_i)$, $\forall i = 0, 1, ..., n$. Так как $\deg f \leq n$, $\deg g \leq n$, то по теореме об интерполяции многочлен f единственен, следовательно, $f = g$. ■

A.9.5. Деление многочленов с остатком

Теорема. Пусть K — поле, $\forall f, g \in K[x]$, $g \neq 0$ $\exists! q, r \in K[x]$:

$$\begin{gathered} f = q \cdot g + r, \\ \deg r < \deg g \end{gathered} \tag{9.28}$$

условие на степени можно убрать, если $\deg 0 = -\infty$. Многочлен q называется частным, r — остатком от деления f на g. Если $r = 0$, то говорят, что $g \mid f$ (g делит f).

Доказательство. □

1. Существование. Если $f = 0$, то $q = 0, r = 0$.

   Пусть $f \neq 0$, $\deg f = n$, $\deg g = m$. Если $n < m$, то $q = 0$, $r = f$. Тогда $f = a_0 + a_1 x + ... + a_n x^n$ и $g = b_0 + b_1 x + ... + b_m x^m$, где $a_n \neq 0$, $b_m \neq 0$. Проведём индукцию по n.

   1.1. Если $n < m$, то $q = 0, r = f$.

   1.2. Пусть $n \geq m$. Тогда умножим g на одночлен cx^{n-m}, где $c = \frac{a_n}{b_m}$. Тогда старшие члены f и $cx^{n-m} \cdot g$ совпадут и их можно вычесть:

   $$\tilde{f} = f - cx^{n-m} \cdot g = a'_0 + a'_1 x + ... + a'_{n-1} x^{n-1}, \tag{9.29}$$

   где $\deg \tilde{f} < n$. Если $\deg \tilde{f} = 0$, то $g \mid f : q = \frac{a_n}{b_m} x^{n-m}, r = 0$.

   Если же $\deg \tilde{f} > 0$, то по предположению индукции существуют $\tilde{q}, r$ такие, что

   $$\begin{gathered} \tilde{f} = \tilde{q} \cdot g + r, \\ \deg r < \deg g. \end{gathered} \tag{9.30}$$

   Сам многочлен f можно записать как

   $$f = \tilde{f} + cx^{n-m} \cdot g = (\tilde{q} + cx^{n-m}) \cdot g + r. \tag{9.31}$$

2. Единственность. Пусть существуют $q_1, r_1, q_2, r_2 \in K[x]$ такие, что

$$\begin{aligned} f &= q_1 \cdot g + r_1, \\ \deg r_1 &< \deg g, \end{aligned} \tag{9.32}$$

и

$$\begin{aligned} f &= q_2 \cdot g + r_2, \\ \deg r_2 &< \deg g. \end{aligned} \tag{9.33}$$

Тогда

$$(q_1 - q_2) \cdot g = r_2 - r_1. \tag{9.34}$$

Степень многочлена в правой части $\deg(r_2 - r_1) < \deg g$. А степень многочлена в левой части $\deg((q_1 - q_2) \cdot g) \geq \deg g$, если $q_1 \neq q_2$. Противоречие. Следовательно, $q_1 = q_2$ и $r_1 = r_2$. ■

A.9.6. Теорема Безу

Теорема. Пусть K — поле, $f \in K[x]$, $x_0 \in K$. Тогда при делении f на многочлен $x - x_0$ получается остаток $f(x_0)$:

$$f(x) = q(x) \cdot (x - x_0) + f(x_0) \tag{9.35}$$

Доказательство. □ По теореме о делении с остатком, существуют $q, r \in K[x]$ такие, что

$$\begin{aligned} f(x) &= q(x) \cdot (x - x_0) + r, \\ \deg r &< \deg(x - x_0) = 1. \end{aligned} \tag{9.36}$$

Значит остаток это константа: $r \in K$. Подставим $x = x_0$:

$$f(x_0) = q(x_0) \cdot (x_0 - x_0) + r = r. \blacksquare \tag{9.37}$$

Следствие. Пусть K — поле, $f \in K[x]$. Тогда $x_0 \in K$ является корнем многочлена f, если и только если $(x - x_0) \mid f(x)$.

Определение. Кратность значения x_0 многочлена $f \in K[x]$ это такое наибольшее целое число $k \geq 0$, что $(x - x_0)^k \mid f(x)$.

Это тоже самое, что $f(x) = (x - x_0)^k \cdot q(x)$, где $q(x_0) \neq 0$.

Кратность, равная нулю, означает, что x_0 не является корнем многочлена.

Определение. Корень многочлена называетсся простым, если его кратность равна единице.

Определение. Корень многочлена называется кратным, если его кратность больше единицы.

A.9.7. Теорема о количестве корней ненулевого многочлена

Теорема. Пусть K — поле, $f \in K[x]$, $f \neq 0$. Тогда число корней многочлена f с учётом кратности не больше $\deg f$.

Доказательство. □ Индукция по степени многочлена. Если $n = \deg f = 0$, то f — константа и корней нет.

Если f не имеет корней, то утверждение верно. Иначе возьмём корень $x_0 \in K$ многочлена f и возьмём $g \in K[x]$, для которого $g(x_0)! - 0$. Пусть так же кратность корня x_0 равна k_0.

$$f(x) = (x - x_0)^{k_0} \cdot g(x), \tag{9.38}$$

причём $\deg g = \deg f - k_0$. По предположению индукции многочлен g имеет лишь конечное число корней $x_1, x_2, ..., x_m$ с кратностями $k_1, k_2, ..., k_m$, причём $k_1 + ... + k_m \leq n - k_0$ по предположению индукции. Тогда многочлен f имеет корни $x_0, x_1, x_2, ..., x_m$ с кратностями $k_0, k_1, k_2, ..., k_m$. Следовательно, $k_0 + k_1 + ... + k_m \leq k_0 + (n - k_0) = n$. ■

A.9.8. Производная многочлена

Определение. Пусть $f = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \in K[x]$. Его формальная производная определяется как

$$f' = a_1 + 2a_2 x + 3a_3 x^2 + ... + n a_n x^{n-1} = \sum_{k=1}^{n} k a_k x^{k-1}. \tag{9.39}$$

при $K = \mathbb{R}$ формальная производная совпадает с обычной производной полиномиальной функции $f(x)$

$$f'(x_0) = \lim_{\varepsilon \to 0} \frac{f(x_0 + \varepsilon) - f(x_0)}{\varepsilon}. \tag{9.40}$$

Свойства производной многочлена:

1. Производная суммы многочленов равна сумме производных:

$$(f + g)' = f' + g' \tag{9.41}$$

2. Константу можно выносить за знак производной:

$$(c \cdot f)' = c \cdot f' \tag{9.42}$$

первые два свойства назваются свойствами линейности.

3. Производная произведения многочленов подчиняется правилу Лейбница:

$$(f \cdot g)' = f' \cdot g + f \cdot g' \tag{9.43}$$

Доказательство. □ Пусть $f = \sum_{k\geq 0} a_k x^k$ и $g = \sum_{l\geq 0} b_l x^l$. Тогда

$$f \cdot g = \sum_{k,l\geq 0} a_k b_l x^{k+l} \tag{9.44}$$

$$\begin{gathered}(f \cdot g)' = \sum_{k,l\geq 0} (k+l) a_k b_l x^{k+l-1} = \sum_{k,l\geq 0} k a_k b_l x^{k+l-1} + \sum_{k,l\geq 0} l a_k b_l x^{k+l-1} = \\ = \sum_{k\geq 0} k a_k x^{k-1} \cdot \sum_{l\geq 0} b_l x^l + \sum_{k\geq 0} a_k x^k \cdot \sum_{l\geq 0} l b_l x^{l-1} = f' \cdot g + f \cdot g'. \blacksquare\end{gathered} \tag{9.45}$$

4. Производная произведения нескольких многочленов:

$$(f_1 \cdot f_2 \cdot \ldots \cdot f_k)' = \sum_{i=1}^{k} (f_1 \cdot \ldots \cdot f_{i-1} \cdot f_i' \cdot f_{i+1} \cdot \ldots \cdot f_k) \tag{9.46}$$

Доказательство. □ Индукция по числу сомножителей. База: $k = 2$ — верно по правилу Лейбница. Пусть верно для $k \in \mathbb{N}$. Тогда для $k+1$:

$$\begin{gathered}(f_1 \cdot f_2 \cdot \ldots \cdot f_k \cdot f_{k+1})' = (f_1 \cdot f_2 \cdot \ldots \cdot f_k)' \cdot f_{k+1} + (f_1 \cdot f_2 \cdot \ldots \cdot f_k) \cdot f_{k+1}' = \\ = \left(\sum_{i=1}^{k} (f_1 \cdot \ldots \cdot f_{i-1} \cdot f_i' \cdot f_{i+1} \cdot \ldots \cdot f_k) \right) \cdot f_{k+1} + (f_1 \cdot f_2 \cdot \ldots \cdot f_k) \cdot f_{k+1}' = \\ = \sum_{i=1}^{k+1} (f_1 \cdot \ldots \cdot f_{i-1} \cdot f_i' \cdot f_{i+1} \cdot \ldots \cdot f_{k+1}). \blacksquare\end{gathered} \tag{9.47}$$

5. Производная степени многочлена:

$$\left(f^k\right)' = k \cdot f^{k-1} \cdot f' \tag{9.48}$$

Доказательство. □ Индукция по k. База: $k = 1$ — верно. Пусть верно для $k \in \mathbb{N}$. Тогда для $k+1$:

$$\left(f^{k+1}\right)' = \left(f^k \cdot f\right)' = \left(f^k\right)' \cdot f + f^k \cdot f' = k \cdot f^{k-1} \cdot f' \cdot f + f^k \cdot f' = (k+1) \cdot f^k \cdot f'. \blacksquare \tag{9.49}$$

6. Производная степени линейного двучлена:

$$\left((x - x_0)^k\right)' = k \cdot (x - x_0)^{k-1} \tag{9.50}$$

A.9.9. Высшая производная многочлена

Определение. Высшей производной k-го порядка многочлена f называется многочлен, определяемый индуктивно:

$$\begin{gathered} f^{(k)} = \left(f^{(k-1)}\right)', \\ f^{(0)} = f. \end{gathered} \tag{9.51}$$

Предложение. Пусть дано поле K.

1. x_0 является кратным корнем многочлена $f \in K[x]$ тогда и только тогда, когда он являтеся корнем многочлена f и его первой производной.
2. Если $\operatorname{char} K = 0$, то x_0 является корнем кратности k многочлена $f \in K[x]$ тогда и только тогда, когда

$$\begin{gathered} f(x_0) = f'(x_0) = f^{(2)}(x_0) = \ldots = f^{(k-1)}(x_0) = 0, \\ f^k(x_0) \neq 0. \end{gathered} \tag{9.52}$$

Доказательство. □ Пусть кратность корня x_0 многочлена f равна k. Тогда

$$f(x) = (x - x_0)^k \cdot g(x), g(x_0) \neq 0. \tag{9.53}$$

Продифференцируя f, получаем

$$f'(x) = k(x - x_0)^{k-1} \cdot g(x) + (x - x_0)^k \cdot g'(x) = (x - x_0)^{k-1} \cdot (k \cdot g(x) + (x - x_0) \cdot g'(x)). \tag{9.54}$$

Пусть $h = k \cdot g(x) + (x - x_0) \cdot g'(x)$.

1. Если $k > 1$, то $k - 1 > 0$ и поэтому $(x - x_0) \mid f'(x)$, то есть x_0 — корень многочлена f'.
2. Если $k = 1$, то $f'(x) = h(x)$ и $h(x_0) = k \cdot g(x_0) = g(x_0) \neq 0$, то есть x_0 не является корнем многочлена f'.

Теперь докажем второе утверждение. $h(x_0) = k \cdot g(x_0)$, так как $\operatorname{char} K = 0$, то $k \cdot g(x_0) \neq 0$. Значит кратность корня x_0 многочлена f' равна $k - 1$. Повторяя этот процесс, получаем, что $f(x_0) = f'(x_0) = \ldots = f^{(k-1)}(x_0) = 0, f^{(k)}(x_0) \neq 0$. ■

A.9.10. Разложение многочлена на линейные множители над полем

Предложение. Если K — поле, то $\forall x_0 \in K$

$$K[x] = K[x - x_0] \tag{9.55}$$

то есть $\forall$ многочлен $f \in K[x]$ можно единственным способом представить в виде

$$\begin{gathered} f(x) = a_0 + a_1(x - x_0) + a_2(x - x_0)^2 + \ldots + a_n(x - x_0)^n, \\ a_i \in K. \end{gathered} \tag{9.56}$$

Доказательство. □

1. Существование. Пусть $f = a_0 + a_1 x + \ldots + a_n x^n, a_n \neq 0$. Обозначим $y = x - x_0$. Тогда

$$f(x) = a_0 + a_1(y + x_0) + a_2(y + x_0)^2 + \ldots + a_n(y + x_0)^n. \tag{9.57}$$

   Раскроем скобки и приведём подобные слагаемые по степеням y.

$$\begin{gathered} f(x) = c_0 + c_1 y + c_2 y^2 + \ldots + c_n y^n, \\ c_i \in K. \end{gathered} \tag{9.58}$$

2. Единственность. Индукция по $n = \deg f$. Если $n = 0$, то $f = a_0 = c_0$. Пусть верно для степеней меньше $n \in \mathbb{N}$, представим, что

$$f(x) = c_0 + c_1(x - x_0) + c_2(x - x_0)^2 + \ldots + c_n(x - x_0)^n = c_n x^n + \ldots \tag{9.59}$$

   Поэтому $c_n = a_n$. Рассотрим разность

$$f(x) - c_n(x - x_0)^n = c_0 + c_1(x - x_0) + c_2(x - x_0)^2 + \ldots + c_{n-1}(x - x_0)^{n-1} \tag{9.60}$$

   Так как f задан, то разность задана однозначно. По предположению индукции коэффициенты $c_0, c_1, \ldots, c_{n-1}$ определены однозначно, поэтому весь набор определён однозначно. ■

Теорема. Пусть $f(x) = \sum_{l \geq 0} c_l (x - x_0)^l$, тогда

$$c_k \cdot k! = f^{(k)}(x_0) \tag{9.61}$$

Доказательство. □ Посмотрим, что будет при дифференцировании линейного двучлена:

$$\left((x-x_0)^l\right)^{(k)} = \begin{cases} 0, l < k \\ k!, l = k \\ l(l-1)...(l-k+1)(x-x_0)^{l-k}, l > k. \end{cases} \tag{9.62}$$

Продифференцируем f k раз:

$$f^{(k)}(x) = \sum_{l \geq 0} c_l \left((x-x_0)^l\right)^{(k)} = c_k k! + \sum_{l>k} c_l l(l-1)...(l-k+1)(x-x_0)^{l-k}. \tag{9.63}$$

Подставим $x = x_0$ и получим желаемое равенство. ■

Следствие. Если K — поле, $\operatorname{char} K = 0$, $f \in K[x]$ и $\deg f = n$, то

$$f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(x_0)}{k!} \cdot (x-x_0)^k \tag{9.64}$$

(формула Тейлора для многочленов).

Доказательство. □ Так как $\operatorname{char} K = 0$, $k! \neq 0$, и на него можно разделить многочлен, записанный в форме из теоремы выше. ■

A.10. Теория делимости в кольцах многочленов

Определение. Пусть A — область целостности и $a, b \in A$, $a, b \neq 0$. Говорят, что $b \mid a$ (b делит a), если $\exists c \in A : a = b \cdot c$.

Определение. Если $a \mid b$ и $b \mid a$, то эти элементы называются ассоциированными.

Обозначение: $a \sim b$.

A.10.1. Свойства ассоциированности

Пусть A — область целостности и рассматриваемые элементы лежат в ней.

1. $a \sim b \Leftrightarrow a = b \cdot u$, где $u \in A^\times$.

   Доказательство. $\square$

   - $\Rightarrow$. $(a \mid b) \wedge (b \mid a) \Leftrightarrow b = a \cdot v$ и $a = b \cdot u$. Отсюда $b = b \cdot u \cdot v$, и так так как в кольце A нет делителей нуля, то можно сократить на b и получить $u \cdot v = 1 \Rightarrow u, v \in A^\times$.
   - $\Leftarrow$. $a = b \cdot u, u \in A^\times \Rightarrow a \cdot u^{-1} = b \Rightarrow (a \mid b) \wedge (b \mid a) \Rightarrow a \sim b$. $\blacksquare$

2. Ассоциированность — отношение эквивалентности.

   Доказательство. $\square$

   - Рефлексивность. $a \sim a$.
   - Симметричность. $a \sim b \Rightarrow a = b \cdot u, u \in A^\times \Rightarrow b = a \cdot u^{-1}, u^{-1} \in A^\times \Rightarrow b \sim a$.
   - Транизитивность. $a \sim b \sim c \Rightarrow a = b \cdot u, b = c \cdot v \Rightarrow a = c \cdot u \cdot v \Rightarrow a \sim c$, где $u, v \in A^\times$. $\blacksquare$

3. Ассоциированность не влияет на делимость. Пусть $a \sim a'$, $b \sim b'$. Тогда $b \mid a \Leftrightarrow b' \mid a'$.

   Доказательство. $\square$ Так как отношение ассоциированности симметрично, то достаточно доказать в одну сторону.

   Если $a \sim a'$ и $b \sim b'$, то $a = a' \cdot u$, $b = b' \cdot v$, где $u, v \in A^\times$. Если $b \mid a$, то $a = b \cdot c$. Тогда $a' \cdot u = b' \cdot v \cdot c$. Тогда, умножив на u^{-1}, получим $a' = b' \cdot \left(v \cdot c \cdot u^{-1}\right)$. $\blacksquare$

Например,

1. В $\mathbb{Z} : a \sim b \Leftrightarrow a = \pm b$, так как в $\mathbb{Z}$ обратимы только $\{-1, 1\}$.
2. $K[x]$ над полем K: $f \sim g \Leftrightarrow f = g \cdot \lambda$, $\lambda \in K^\times$.

A.10.2. Наибольший общий делитель

Определение. Пусть $a, b \in A$, $a, b \neq 0$, где A — область целостности. Наибольший общий делитель(НОД) элементов a и b это такой элемент $d \in A$, что

1. Он делит оба элемента: $d \mid a$ и $d \mid b$.
2. Он наибольший в том смысле, что любой общий делитель a и b делит и его тоже: $\forall c \in A \setminus \{0\} : \ c \mid a, c \mid b \Rightarrow c \mid d$.

Обозначение. $\gcd(a, b)$.

Определение. Элементы области целостности $a, b \in A$ называются взаимно простыми, если $\gcd(a, b) = 1$, то есть a и b не имеют общих делителей, кроме обратимых элементов.

Теорема. Если $\gcd(a, b)$ существует, то он определён однозначно с точностью до ассоциированности.

Доказательство. □ Пусть d и d' — два наибольших общих делителя a и b. Тогда $d, d' \mid a, b$. Тогда $d' \mid d$ и $d \mid d'$ по свойству 2 НОД. Значит $d \sim d'$. ■

A.10.3. Евклидовы кольца

Определение. Целостное кольцо A называется евклидовым, если на множестве его ненулевых элементов задана функция

$$N : A \setminus \{0\} \to \mathbb{Z}_+ = \{0, 1, 2, ...\}, \tag{10.1}$$

которая обладает следующими свойствами:

1. Монотонность: $N(a \cdot b) \geq N(a)$, причём $N(a \cdot b) \Leftrightarrow b \in A^\times$.
2. $\forall a, b \in A, b \neq 0 \ \exists q, r \in A : a = b \cdot q + r$, причём $N(r) < N(b)$ или $r = 0$.

Если считать, что $N(0) = -\infty$, то случай $r = 0$ можно не оговаривать.

Например,

1. Для $A = \mathbb{Z}$: $N(a) = |a|$.
2. $A = K[x]$: $N(f) = \deg f$.
3. Кольцо гауссовых целых чисел $\mathbb{Z}[i] = \{x + i \cdot y \mid x, y \in \mathbb{Z}\}$, $N(z) = |z|^2$.

Теорема. В еклидовом кольце $\forall a, b \neq 0 \ \exists \gcd(a, b)$.

Доказательство. □ Алгоритм Евклида:

1. Делим с остатком: $a = b \cdot q_1 + r_1$. Если $r_1 = 0$, то конец. Иначе переходим на шаг 2.
2. $b = r_1 \cdot q_2 + r_2$
3. $r_1 = r_2 \cdot q_3 + r_3$

$\vdots$

$(k+1).\ r_{k-1} = r_k \cdot q_{k+1} + r_{k+1}.$

$\vdots$

$(s-1).\ r_{s-1} = r_s \cdot q_{s+1}.$

Этот алгоритм конечен, поскольку $N(b) > N(r_1) > N(r_2) > ... > N(r_{k+1})$ и все нормы целые неотрицательные, значит спуск не может быть бесконечным!

Тогда $r_{s-1} = \gcd(a, b)$. Действительно,

1. $r_s \mid r_{s-1} \Rightarrow r_s \mid r_{s-2} \Rightarrow ... \Rightarrow r_s \mid r_{k+1}, r_k \Rightarrow r_s \mid r_{k-1} \Rightarrow ... \Rightarrow r_s \mid r_2, r_1 \Rightarrow r_s \mid b \Rightarrow r_s \mid a.$
2. $c \mid a, b \Rightarrow c \mid r_1 = a - b \cdot q_1 \Rightarrow c \mid r_2 = b - r_1 \cdot q_2 \Rightarrow ... \Rightarrow c \mid r_{k-1}, r_k \Rightarrow c \mid r_{k+1} \Rightarrow ... \Rightarrow c \mid r_s.$

Поэтому оба свойства НОД выполнены. ■

Следсвие алгоритма Евклида. $\gcd(a, b) = u \cdot a + v \cdot b$, где $u, v \in A$ — элементы того же евклидова кольца.

Доказательство □ Докажем, что $r_k = u_k \cdot a + v_k \cdot v$.

Индукция по k.

1. $k = 1$: $r_1 = 1 \cdot a - q_1 \cdot b$.
2. Шаг: $r_{k+1} = r_{k-1} - r_k \cdot q_{k+1} = u_{k-1} \cdot a + v_{k-1} \cdot b - (u_k \cdot a + v_k \cdot b) = (u_{k-1} - u_k \cdot q_{k+1}) \cdot a + (v_{k-1} - v_k \cdot q_{k+1}) \cdot b$.

При $k = s$ получаем выражение для $r_s = \gcd(a, b)$. ■

Определение. Элемент p целостного кольца A называется простым если $p \neq 0$, $p \notin A^\times$, $\nexists p = a \cdot b$, где $a, b \notin A^\times$.

В кольце многочленов над полем K многочлен $p \in K[x]$ будет простым, если $p \neq 0, \deg p > 0, \nexists p = f \cdot g$, где $0 < \deg f, \deg g < \deg p$. То есть такие многочлены не разлагаются в произведение двух множителей меньшей степени.

Определение. Простые элементы в $K[x]$ называются неприводимыми многочленами.

Простой элемент $p \in A$ в кольце целостности имеет ровно 2 делителя с точностью до ассоциированности: p и 1.

B. Математический анализ

B.1. Числовые последовательности

Отображение $\mathbb{N} \to \mathbb{R}$ называется числовой последовательностью. Последовательность можно записать как $a_1, a_2, ...a_n, ...$, где $\forall n \in \mathbb{N} : a_n \in \mathbb{R}$ или же

$$\{a_n\}_{n=1}^{\infty} \tag{11.1}$$

Членом последовательности с номером n называется пара (n, a_n).

B.1.1. Предел последовательности

Число $a \in \mathbb{R}$ называется пределом последовательности $\{a_n\}$, если

$$\forall \varepsilon > 0 \ \exists N \in \mathbb{N} : \forall n > N : |a_n - a| < \varepsilon \tag{11.2}$$

Если a — предел последовательности $\{a_n\}$, то пишут

$$\lim_{n \to \infty} a_n = a. \tag{11.3}$$

Можно дать более общее определение, если ввести следующие обозначения.

1. $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$
2. $\hat{\mathbb{R}} = \overline{\mathbb{R}} \cup \{\infty\}$
3. Понятие эпсилон-окрестности элемента $a \in \hat{\mathbb{R}}$.

   3.1. Если $a \in \mathbb{R}$, то

$$u_\varepsilon(a) \underset{\text{def}}{=} (a - \varepsilon, a + \varepsilon) \tag{11.4}$$

   3.1. Если $a = -\infty$, то

$$u_\varepsilon(a) \underset{\text{def}}{=} \left(-\infty, -\frac{1}{\varepsilon}\right) \tag{11.5}$$

   3.2. Если $a = +\infty$, то

$$u_\varepsilon(a) \underset{\text{def}}{=} \left(\frac{1}{\varepsilon}, +\infty\right) \tag{11.6}$$

   3.3. Если $a = \infty$, то

$$u_\varepsilon(a) \underset{\text{def}}{=} \left(-\infty, -\frac{1}{\varepsilon}\right) \cup \left(\frac{1}{\varepsilon}, +\infty\right) \tag{11.7}$$

Тогда $a \in \hat{\mathbb{R}}$ называется пределом последовательности $\{a_n\}$, если

$$\forall \varepsilon > 0 \ \exists N \in \mathbb{N} : \forall n > N : a_n \in u_\varepsilon(a) \tag{11.8}$$

B.1.2. Ограниченность

Последовательность $\{a_n\}$ называется *ограниченной сверху*, если $\exists M \in \mathbb{R} : \forall n \in \mathbb{N} : a_n \leq M$.

Последовательность $\{a_n\}$ называется *ограниченной снизу*, если $\exists m \in \mathbb{R} : \forall n \in \mathbb{N} : a_n \geq m$.

Последовательность $\{a_n\}$ называется *ограниченной*, если она ограничена сверху и снизу.

Теорема. Если последовательность $\{a_n\}$ сходится, то она ограничена.

Доказательство. □ Пусть $a_n \to a$. По определению сходимости $\forall \varepsilon > 0\ \exists N \in \mathbb{N} : \forall n > N : |a_n - a| < \varepsilon$. В частности, для $\varepsilon = 1$:

$$\exists N \in \mathbb{N} : \forall n > N : |a_n - a| < 1. \tag{11.9}$$

Тогда вне 1-окрестности числа a лежит конечное число членов a_n, поэтому мы можем явно предъявить ограничивающие сверху и снизу константы M и m соответственно:

$$M = \max(\{a_n \mid n \leq N\} \cup \{a + 1\}) \tag{11.10}$$

$$m = \min(\{a_n \mid n \leq N\} \cup \{a - 1\}) \tag{11.11}$$

Поэтому последовательность ограничена сверху и снизу, и поэтому она ограничена.

■

Контрпример для обратного утверждения(ограничена ⇒ сходится?): последовательность $a_n = (-1)^n$ не сходится, но ограничена.

B.1.3. Единственность предела

Лемма. Если $a, b \in \overline{\mathbb{R}}$ и $a \neq b$, то

$$\exists \varepsilon > 0 : u_\varepsilon(a) \cap u_\varepsilon(b) = \varnothing \tag{11.12}$$

Доказательство: □ Не умаляя общности рассуждений, предположим, что $a < b$.

1. Пусть $a, b \in \mathbb{R}$. Возьмём $\varepsilon = \frac{b-a}{3} \Rightarrow \forall x \in u_\varepsilon(a), y \in u_\varepsilon(b)$:

$$x < a + \varepsilon < b - \varepsilon < y \tag{11.13}$$

2. $a = -\infty, b \in \mathbb{R}$.

$$b - \varepsilon > -\frac{1}{\varepsilon} \Leftrightarrow b > -\varepsilon^2 + b\varepsilon > -1 \tag{11.14}$$

$$\varepsilon^2 - b\varepsilon - 1 < 0 \tag{11.15}$$

Это неравенство всегда имеет *положительное* решение относительно ε, поскольку дискриминант квадратного трёхчлена в левой части всегда положителен, а по теореме Виета, произведение корней отрицательно, а значит больший корень положителен.

3. $b = +\infty$, $a \in \mathbb{R}$.

$$a + \varepsilon < \frac{1}{\varepsilon} \Leftrightarrow a < \varepsilon^2 + a\varepsilon < 1 \tag{11.16}$$

$$\varepsilon^2 + a\varepsilon - 1 > 0 \tag{11.17}$$

Это неравенство всегда имеет *положительное* решение относительно ε.

4. $a = -\infty$, $b = +\infty$. В этом случае $\forall \varepsilon > 0$

$$-\frac{1}{\varepsilon} < 0 < \frac{1}{\varepsilon} \tag{11.18}$$

Поэтому $\forall x \in u_\varepsilon(a), y \in u_\varepsilon(b) : x < 0 < y$.

В случаях 2 и 3 показано, что для любого действительного числа существует подходящее значение ε, при котором любое число из его окрестности заведомо больше или меньше соответственно любого числа из окрестности $-\infty$ или $+\infty$. ■

Из вышедоказанной леммы можно получить такую теорему.

Теорема. У любой последовательности $\{a_n\}$, сходящейся в $\overline{\mathbb{R}}$ может быть только один предел.

B.1.4. Свойства пределов, связанные с неравенствами

Выведем некоторые свойства пределов.

1. Пусть $a, b \in \mathbb{R}$. Тогда верно следующее(знак $<$ можно заменить на $>$).

$$\lim_{n\to\infty} a_n = a < b \Rightarrow \exists N \in \mathbb{N} : \forall n > N : a_n < b. \tag{11.19}$$

Доказательство. □ Пусть $\lim a_n = a < b$. По определению предела $\forall \varepsilon > 0\ \exists N \in \mathbb{N} : \forall n > N : |a_n - a| < \varepsilon$. В частности, для $\varepsilon = \frac{b-a}{2}$:

$$\exists N \in \mathbb{N} : \forall n > N : |a_n - a| < \varepsilon. \tag{11.20}$$

Следовательно, $\forall n > N : a_n < a + \varepsilon = a + \frac{b-a}{2} = \frac{a+b}{2} < b$. ■

2. Пусть $\lim a_n = a$.

$$\exists N \in \mathbb{N} : \forall n > N : a_n \leq b \Rightarrow a \leq b. \tag{11.21}$$

Доказательство. □ Предположим, что

$$[\exists N \in \mathbb{N} : \forall n > N : a_n \leq b] \wedge \neg(a \leq b) \tag{11.22}$$

Поскольку тогда $a > b$, то по свойству 1, начиная с некоторого номера, $a_n > b$, но по предположению $a_n \leq b$. Это противоречие. ■

3. Теорема о промежуточной последовательности(о двух милиционерах).

Пусть даны три последовательности a_n, b_n, c_n, такие что $\exists N \in \mathbb{N} : \forall n > N : a_n \leq b_n \leq c_n$. Тогда

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} c_n = a \in \overline{\mathbb{R}} \Rightarrow \lim_{n\to\infty} b_n = a \tag{11.23}$$

Доказательство. □ Пусть $\lim a_n = a$, $\lim c_n = a$. Тогда по определению предела

$$\forall \varepsilon > 0 \ \exists N_1 \in \mathbb{N} : \forall n > N_1 : a_n \in u_\varepsilon(a) \tag{11.24}$$

$$\forall \varepsilon > 0 \ \exists N_2 \in \mathbb{N} : \forall n > N_2 : c_n \in u_\varepsilon(a). \tag{11.25}$$

Тогда $\exists N_3 = \max\{N_1, N_2, N\}$($N$ из условия теоремы, то есть тот номер, начиная с которого верно неравенство). Имеем $\forall n > N_3$:

$$u_\varepsilon(a) \ni a_n \leq b_n \leq c_n \in u_\varepsilon(a) \tag{11.26}$$

Поэтому $\forall n > N_3 : b_n \in u_\varepsilon(a)$, а это и есть определение предела $\lim b_n = a$. ■

B.1.5. Бесконечно малые последовательности

Определение. Последовательность α_n называется бесконечно малой(БМ), если

$$\lim_{n\to\infty} \alpha_n = 0 \tag{11.27}$$

Свойства бесконечно малых последовательностей:

1. Если α_n и β_n - бесконечно малые последовательности, то $\alpha_n + \beta_n$ - бесконечно малая последовательность.

   Доказательство. □ Пусть $\lim \alpha_n = 0$, $\lim \beta_n = 0$. Тогда по определению предела

   $$\forall \varepsilon > 0 \ \exists N_1 \in \mathbb{N} : \forall n > N_1 : |\alpha_n| < \varepsilon \tag{11.28}$$

   $$\forall \varepsilon > 0 \ \exists N_2 \in \mathbb{N} : \forall n > N_2 : |\beta_n| < \varepsilon. \tag{11.29}$$

Обозначим $N = \max\{N_1, N_2\}$. Тогда $\forall n > N : |\alpha_n + \beta_n| \leq |\alpha_n| + |\beta_n| < 2\varepsilon$, что и означает, что $\lim(\alpha_n + \beta_n) = 0$. ■

2. Если α_n - бесконечно малая последовательность, а a_n - ограничена, то $\alpha_n \cdot a_n$ — бесконечно малая последовательность.

   Доказательство. □ Пусть $\lim \alpha_n = 0$, a_n ограничена, то есть $\exists M > 0 : \forall n \in \mathbb{N} : |a_n| < M$. Тогда для последовательности $\beta_n = \alpha_n \cdot a_n$ имеем

$$|\beta_n| = |\alpha_n| \cdot |a_n| \underset{(n>N)}{<} \varepsilon \cdot M. \tag{11.30}$$

   Тогда b_n - бесконечно малая последовательность. ■

Утверждение. Если α_n — бесконечно малая последовательность, то

$$\lim_{n\to\infty} a_n = a \Leftrightarrow \exists \alpha_n = a_n - a \tag{11.31}$$

Доказательство. □

1. $\Rightarrow$. По определению предела

$$\forall \varepsilon > 0 \ \exists N \in \mathbb{N} : \forall n > N : |a_n - a| < \varepsilon. \tag{11.32}$$

   Обозначим $\alpha_n = a_n - a$. Тогда $\forall n > N : |\alpha_n| < \varepsilon$, следовательно, $\lim \alpha_n = 0$.

2. $\Leftarrow$. По определению бесконечно малой последовательности,

$$\forall \varepsilon > 0 \exists N \in \mathbb{N} : \forall n > N : |\alpha_n| < \varepsilon. \tag{11.33}$$

   Подставляя сюда $\alpha_n = a_n - a$, получаем, что $a_n \to a$.

■

B.1.6. Арифметические свойства пределов

Сначала докажем лемму о сохранении знака.

Лемма о сохранении знака. Пусть $\lim b_n = b \neq 0$. Тогда $\exists N \in \mathbb{N} : \forall n > N$:

$$\left[|b_n| > \frac{|b|}{2}\right] \wedge [\operatorname{sign}(b_n) = \operatorname{sign}(b)] \tag{11.34}$$

Доказательство. □ В определении предела для b_n мы возьмём $\varepsilon = \frac{|b|}{2}$. Для $b > 0$ получим $\exists N \in \mathbb{N} : \forall n > N : |b_n - b| < \frac{b}{2}$, что эквивалентно

$$-\frac{b}{2} < b_n - b < \frac{b}{2} \Rightarrow b_n > \frac{b}{2} > 0 \tag{11.35}$$

Отсюда следует требуемое. Если $b < 0$, то аналогично получаем $b_n < -\frac{b}{2} < 0$. ■

После доказательства леммы о сохранении знака можно перейти к теореме об арифметических свойствах пределов.

Теорема. Пусть $\lim a_n = a$, $\lim b_n = b$, тогда

1. $$\exists \lim_{n\to\infty} (a_n + b_n) = a + b \tag{11.36}$$
2. $$\exists \lim_{n\to\infty} (a_n - b_n) = a - b \tag{11.37}$$
3. $$\exists \lim_{n\to\infty} (a_n \cdot b_n) = a \cdot b \tag{11.38}$$
4. Если $b \neq 0$ и $\forall n \in \mathbb{N} : b_n \neq 0$, то
$$\exists \lim_{n\to\infty} \left(\frac{a_n}{b_n}\right) = \frac{a}{b} \tag{11.39}$$

Доказательство. □ Докажем последовательно все 4 утверждения. Общий план состоит в том, чтобы доказывать, что разность последовательности и её предполагаемого предела — бесконечно малая последовательность. Обозначим $\alpha_n = a_n - a$, а также $\beta_n = b_n - b$.

1. $a_n + b_n - (a + b) = (a_n - a) + (b_n - b) = \alpha_n + \beta_n$ — это сумма двух бесконечно малых последовательностей, следовательно, такая последовательность сама БМ, следовательно $\lim(a_n + b_n) = a + b$.
2. $a_n - b_n - (a - b) = (a_n - a) - (b_n - b) = \alpha_n - \beta_n$. Разность двух БМ также бесконечно малая: легко установить, что если b_n — бесконечно малая последовательность, то $(-b_n)$ — тоже БМ. Итак, мы получили разность двух бесконечно малых последовательностей, следовательно, такая последовательность сама БМ, следовательно $\lim(a_n - b_n) = a - b$.
3. $a_n \cdot b_n - a \cdot b = a_n \cdot b_n - (a \cdot b) \underbrace{+a_n \cdot b - a_n \cdot b}_{\text{добавили } 0} = b \cdot (a_n - a) + a_n \cdot (b_n - b) = b \cdot \alpha_n + a_n \cdot \beta_n$. Получили сумму двух бесконечно малых, поскольку каждое слагаемое это произведение ограниченной на бесконечно малую(a_n ограничена, так как сходится!). Значит $a_n \cdot b_n - a \cdot b$ — бесконечно малая последовательность, следовательно $\lim(a_n \cdot b_n) = a \cdot b$.
4. Для частного оценим модуль разности последовательности и значения предела.

$$\left|\frac{a_n}{b_n}-\frac{a}{b}\right| = \left|\frac{a_n\cdot b - a\cdot b_n}{b_n\cdot b}\right| = \left|\frac{a_n\cdot b - a\cdot b + a\cdot b - a\cdot b_n}{b_n\cdot b}\right| = \\ = \left|\frac{b\cdot\alpha_n - a\cdot\beta_n}{b_n\cdot b}\right| \underset{\substack{\text{лемма о}\\ \text{сохр. знака}}}{<} \frac{|b\cdot\alpha_n - a\cdot\beta_n|}{\frac{|b|^2}{2}} \tag{11.40}$$

Для наглядности напишем полученное выражение и посмотрим, что вышло:

$$\left|\frac{a_n}{b_n}-\frac{a}{b}\right| < \underbrace{\frac{2}{b^2}}_{\text{огр.}}\cdot\underbrace{(b\cdot\alpha_n - a\cdot\beta_n)}_{\text{бесконечно малая}} \tag{11.41}$$

Последовательность, которая по модулю асимптотически меньше бесконечно малой, сама является бесконечно малой, следовательно $\lim\left(\frac{a_n}{b_n}\right) = \frac{a}{b}$.

Таким образом, теорема доказана. ■

B.1.7. Монотонные последовательности

Последовательность $\{a_n\}$ называется *возрастающей*, если $\forall \in \mathbb{N} : a_{n+1} \geq a_n$.

Последовательность $\{a_n\}$ называется *строго возрастающей*, если $\forall \in \mathbb{N} : a_{n+1} > a_n$.

Последовательность $\{a_n\}$ называется *убывающей*, если $\forall \in \mathbb{N} : a_{n+1} \leq a_n$.

Последовательность $\{a_n\}$ называется *строго убывающей*, если $\forall \in \mathbb{N} : a_{n+1} < a_n$.

Для обозначеняя возрастания последовательности $\{a_n\}$ будем писать $a_n \uparrow$, а для убывания $a_n \downarrow$.

B.1.7.1. Теорема Вейерштрасса

Теорема. Если последовательность возрастает, то у неё есть предел в $\overline{\mathbb{R}}$, а точнее

1. Если последовательность возрастает и ограничена сверху, то у неё есть предел $\mathbb{R}$.
2. Если последовательность возрастает и не ограничена сверху, то она сходится к $+\infty$.

Доказательство. □ Рассмотрим последовательность $x_n \uparrow$ и положим $a = \sup(x_n)$. Тогда мы можем записать, что

$$\forall n \in \mathbb{N} : x_n \leq a \tag{11.42}$$

(по определению точной верхней грани). А также

$$\forall \varepsilon > 0\ \exists n_\varepsilon : x_{n_\varepsilon} \in u_\varepsilon(a) \tag{11.43}$$

Теперь по определению возрастающей последовательности $\forall \varepsilon > 0\ \exists n_\varepsilon \in \mathbb{N} :$

$$\forall n > n_\varepsilon : x_n \geq x_{n_\varepsilon} \tag{11.44}$$

Получили двойное неравенство $\forall n > n_\varepsilon$:

$$x_{n_\varepsilon} \leq x_n \leq a \tag{11.45}$$

Значит, начиная с некоторого номера, все x_n лежат в ε-окрестности a. Что и требовалось доказать. ■

Абсолютно аналогично можно доказать, что если последовательность убывает и ограничена снизу, то у неё есть предел.

B.1.8. Кто растёт быстрее?

Пусть $k \in \mathbb{N}$ и $q > 1$. Расмотрим 4 последовательности:

$$n^k,\ q^n,\ n!\ n^n \tag{11.46}$$

1. Сравнение степенной и показательной последовательности. Рассмотрим последовательность

$$x_n = \frac{n^k}{q^n} \tag{11.47}$$

$$x_{n+1} = \frac{(n+1)^k}{q^{n+1}} \tag{11.48}$$

Рассмотрим отношение соседних членов:

$$\frac{x_{n+1}}{x_n} = \frac{\left(\frac{n+1}{n}\right)^k}{q} \tag{11.49}$$

Поскольку $\left(\frac{n+1}{n}\right)^k \underset{n\to\infty}{\to} 1 < q$, то начиная с некоторого номера N, $\forall n > N$: $\left(\frac{n+1}{n}\right)^k < q$, поэтому начиная с этого номера $\frac{x_{n+1}}{x_n} < 1$, а значит последовательность $\{x_n\}$ убывает, начиная с этого номера.

Кроме того, последовательность $\{x_n\}$ ограничена снизу нулём: $x_n > 0\ \forall n \in \mathbb{N}$. По теореме Вейерштрасса, последовательность x_n имеет предел.

Пусть $\lim x_n = a$. Тогда $\lim x_{n+1} = a$. Предположим, что $a \neq 0$. Тогда

$$\lim_{n\to\infty}\left(\frac{x_{n+1}}{x_n}\right) = \frac{a}{a} = 1 \tag{11.50}$$

Но с другой стороны

$$\lim_{n\to\infty}\left(\frac{x_{n+1}}{x_n}\right) = \lim_{n\to\infty} = \frac{\left(\frac{n+1}{n}\right)^k}{q} = \frac{1}{q} \neq 1 \tag{11.51}$$

Получили противоречие $\Rightarrow a = 0$. Итак,

$$\lim_{n\to\infty}\frac{n^k}{q^n} = 0$$

2. Сравним $n!$ и q^n. Рассмотрим последовательность $x_n = \frac{q^n}{n!}$. Тогда следующий член равен

$$x_{n+1} = \frac{q^{n+1}}{(n+1)!} \tag{11.52}$$

$$\frac{x_{n+1}}{x_n} = \frac{q}{n+1} \underset{\substack{\uparrow \\ \text{с некоторого} \\ \text{номера}}}{<} 1 \tag{11.53}$$

Поэтому последовательность x_n, начиная с некоторого номера, убывает. Кроме того, она ограничена снизу нулём. Поэтому пусть $a = \lim x_n = \lim x_{n+1}$. Предположим, что $a \neq 0$. Тогда $\lim\left(\frac{x_{n+1}}{x_n}\right) = 1$, но это противоречит тому, что

$$\lim_{n\to\infty}\left(\frac{x_{n+1}}{x_n}\right) = \lim_{n\to\infty}\left(\frac{q}{n+1}\right) = 0. \tag{11.54}$$

В силу противоречия, $a = 0$, поэтому доказано, что

$$\lim_{n\to\infty}\frac{q^n}{n!} = 0$$

3. Сравним $n!$ и n^n. Рассмотрим последовательность $x_n = \frac{n!}{n^n}$. Найдем отношение соседних членов:

$$x_{n+1} = \frac{(n+1)!}{(n+1)^{n+1}} \tag{11.55}$$

$$\frac{x_{n+1}}{x_n} = \frac{n+1}{\frac{(n+1)^{n+1}}{n^n}} = \frac{1}{\left(1+\frac{1}{n}\right)^n} \leq 1 \tag{11.56}$$

Значит последовательность x_n убывает и ограничена снизу нулём. Пусть $a = \lim x_n = \lim x_{n+1}$. Предположив, что $a \neq 0$ получим

$$\lim_{n\to\infty}\frac{x_{n+1}}{x_n} = 1 \tag{11.57}$$

С другой стороны,

$$\lim_{n\to\infty}\frac{x_{n+1}}{x_n}=\lim_{n\to\infty}\frac{1}{\left(1+\frac{1}{n}\right)^n}=\frac{1}{e}<1. \tag{11.58}$$

В силу противоречия получаем $a=0$ и доказываем

$$\lim_{n\to\infty}\frac{n!}{n^n}=0$$

Получили «иерархию роста»: $x^k \to q^n \to n! \to n^n$. В последнем утверждении было использовано число e.

B.1.9. Число e

Определение. Числом e называеся следующий предел последовательности

$$e=\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n \tag{11.59}$$

B.1.9.1. Первое доказательство существования e

□ Рассмотрим последовательность $x_n=\left(1+\frac{1}{n}\right)^{n+1}$. Согласно неравенству Бернулли:

$$x_n=\left(1+\frac{1}{n}\right)^{n+1}\geq 1+\frac{n+1}{n}>2 \tag{11.60}$$

То есть последовательность x_n ограничена снизу. Теперь посмотрим на отношение соседних членов:

$$\begin{gathered}\frac{x_{n+1}}{x_n}=\frac{\left(1+\frac{1}{n+1}\right)^{n+2}}{\left(1+\frac{1}{n}\right)^{n+1}}=\frac{\left(\frac{n+2}{n+1}\right)^{n+2}}{\left(\frac{n+1}{n}\right)^{n+1}}= \\ =\frac{n+2}{n+1}\cdot\left(\frac{n^2+2n}{(n+1)^2}\right)^{n+1}\end{gathered} \tag{11.61}$$

Оценим величину, обратную ко второму множителю по неравенству Бернулли:

$$\left(\frac{n^2+2n+1}{n^2+2n}\right)^{n+1}=\left(1+\frac{1}{n^2+2n}\right)^{n+1}\geq 1+\frac{n+1}{n^2+2n} \tag{11.62}$$

То есть

$$\left(\frac{n^2+2n+1}{n^2+2n}\right)^{n+1}\geq\frac{n^2+3n+1}{n^2+2n} \tag{11.63}$$

Перевернём это неравенство:

$$\left(\frac{n^2+2n}{n^2+2n+1}\right)^{n+1} \leq \frac{n^2+2n}{n^2+3n+1} \tag{11.64}$$

Получаем оценку для отношения соседних членов:

$$\frac{x_{n+1}}{x_n} \leq \frac{n+2}{n+1} \cdot \frac{n^2+2n}{n^2+3n+1} = \frac{n^3+4n^2+4n}{n^3+4n^2+4n+1} < 1 \tag{11.65}$$

Итак, мы доказали, что последовательность x_n убывает и ограничена снизу числом 2, поэтому по теореме Вейерштрасса у неё есть предел

$$e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^{n+1} = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^{n} \tag{11.66}$$

И в силу последнего равенства, этот же предел есть у исходной последовательности из определения числа e. ■

B.1.9.2. Второе доказательство существования e

□ Будем исследовать последовательность $a_n = \left(1+\frac{1}{n}\right)^n$ напрямую. Согласно биному Ньютона:

$$a_n = \sum_{k=0}^{n} C_n^k \left(\frac{1}{n}\right)^k = 1 + C_n^1 \cdot \frac{1}{n} + ... + C_n^n \cdot \frac{1}{n^n} \tag{11.67}$$

$$a_{n+1} = \sum_{k=0}^{n+1} C_{n+1}^k \left(\frac{1}{n+1}\right)^k = 1 + C_{n+1}^1 \cdot \frac{1}{n+1} + ... + C_{n+1}^{n+1} \cdot \frac{1}{(n+1)^{n+1}} \tag{11.68}$$

Сравним $k-$ е слагаемые в этих двух суммах, имея в виду, что

$$C_n^k = \frac{n!}{k!(n-k)!} = \frac{(n-k+1)\cdot ... \cdot n}{k!}. \tag{11.69}$$

$$\begin{gathered} C_n^k \cdot \frac{1}{n^k} = \frac{1}{k!} \cdot \frac{n-k+1}{n} \cdot \frac{n-k+2}{n} \cdot ... \cdot \frac{n}{n} \leq \\ \leq \frac{1}{k!} \cdot \frac{n-k+2}{n+1} \cdot \frac{n-k+3}{n+1} \cdot ... \cdot \frac{n+1}{n+1} = C_{n+1}^k \cdot \frac{1}{(n+1)^k} \end{gathered} \tag{11.70}$$

Следовательно, $a_{n+1} \geq a_n$, так как каждое слагаемое в a_{n+1} не меньше соответствующего слагаемого в a_n. Таким образом, последовательность a_n возрастает. Теперь докажем, что она ограничена сверху:

$$a_n = \sum_{k=0}^{n} C_n^k \cdot \frac{1}{n^k} = 1 + 1 + \frac{n(n-1)}{2} \cdot \frac{1}{n^2} + \frac{n(n-1)(n-2)}{6} \cdot \frac{1}{n^3} + ... \\ + \frac{1}{n^n} \leq 2 + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + ... + \frac{1}{n!} \leq 2 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + ... + \frac{1}{2^{n-1}} \tag{11.71}$$

Мы смогли оценить a_n сверху суммой двойки и геометрической прогрессии, которая точно меньше 1. Поэтому получаем:

$$a_n < 3 \tag{11.72}$$

По теореме Вейерштрасса, возрастающая ограниченная сверху последовательность имеет предел. Обозначим его e. ■

Из этих двух доказательств мы установили, что

$$2 < e < 3 \tag{11.73}$$

B.1.10. Подпоследовательность

Определение 1. Пусть задана последовательность $\{x_n\}$. Возьмём возрастающую последовательность натуральных чисел: $\{n_k\} \uparrow$ и $n_k \in \mathbb{N}\ \forall k \in \mathbb{N}$. Тогда последовательность $\left\{x_{n_k}\right\}$ называется подпоследовательностью последовательности $\{x_n\}$.

Определение 2. Число a называется частичным пределом последовательности $\{x_n\}$, если существует такая подпоследовательность $\left\{x_{n_k}\right\}$, что

$$a = \lim_{k \to \infty} x_{n_k} \tag{11.74}$$

Определение 2′. Число a называется частичным пределом последовательности $\{x_n\}$, если

$$\forall \varepsilon > 0\ \forall M \in \mathbb{N} : |\{x_n \mid x_n \in u_\varepsilon(a)\}| > M \tag{11.75}$$

Утверждение. Определения 2 и 2′ эквивалентны.

Доказательство. □

1. $2 \Rightarrow 2'$. По определению предела последовательности, $\forall \varepsilon > 0$, начиная с некоторого номера n_k, все члены последовательности будут лежать в ε-окрестности a. Значит, за пределами ε-окрестности лежит только конечное число членов исходной последовательноси $\{x_n\}$, что и утверждает $2'$.
2. $2' \Rightarrow 2$. Рассмотрим окрестность точки a с $\varepsilon = 1$. Возьмём произвольный член последовательности x_n с номером n_1, такой, что $x_{n_1} \in u_\varepsilon(a)$. Теперь рассмотрим более малую окрестность, $\varepsilon = \frac{1}{2}$. Выберем в ней такой x_{n_2}, что $n_2 > n_1$. Далее

аналогично выбираем x_{n_3} в $\frac{1}{3}$-окрестности a такой, что $n_3 > n_2$, и так далее. То есть, мы строим подпоследовательность

$\left\{x_{n_k}\right\}$, такую что

$$a - \frac{1}{k} < x_{n_k} < a + \frac{1}{k} \tag{11.76}$$

При $k \to \infty$ получаем по теореме о двух милиционерах, что

$$\lim_{k\to\infty} x_{n_k} = a. \tag{11.77}$$

Что и требовалось доказать. ■

B.1.10.1. Теорема Больцано-Вейерштрасса

Теорема Больцано-Вейерштрасса. Каждая ограниченная последовательность имеет сходящуюся подпоследовательность.

Доказательство. □ Пусть последовательность $\{x_n\}$ ограничена, тогда все члены последовательности лежат на отрезке $[m_1, M_1]$. Если разбить данный отрезок пополам, то хотя бы на одном из них будет бесконечное количество членов $\{x_n\}$. Действительно, если это не так, то на обоих подотрезках лежит конечное число членов, что противоречит ограниченности $\{x_n\}$. Поделим пополам отрезок $[m, M]$ и выберем тот отрезок $[m_2, M_2] \subset [m_1, M_1]$, на котором лежит бесконечное число членов. И так далее, каждый следующий отрезок $[m_k, M_k]$ вложен в предыдущий и имеет в два раза меньшую длину.

Полученная конструкция есть *система стягивающихся отрезков*. По теореме Кантора, у всех этих отрезков есть только одна общая точка. Обозначим её a. Пусть $x_{n_k} \in [m_k, M_k]$, так как на каждом отрезке бесконечно много членов, то последовательность $\{n_k\}$ можно сделать возрастающей.

Для каждого члена подпоследовательности x_{n_k} выполняется неравенство:

$$\left|x_{n_k} - a\right| < \frac{M_1 - m_1}{2^{k-1}} \tag{11.78}$$

Что равносильно двойному неравенству:

$$a - \frac{M_1 - m_1}{2^{k-1}} < x_{n_k} < a + \frac{M_1 - m_1}{2^{k-1}} \tag{11.79}$$

При стремлении $k \to \infty$ получаем по теореме о промежуточной последовательности, что

$$\lim_{k\to\infty} x_{n_k} = a. \tag{11.80}$$

Таким образом, мы явно построили сходящуюся подпоследовательность ограниченной последоваательности и теорема доказана. ■

B.1.11. Критерий Коши сходимости числовых последовательностей

Определение. Последовательность $\{x_n\}$ называется *фундаментальной*, если

$$\forall \varepsilon > 0 \ \exists N \in \mathbb{N} : \forall m, n > N : |x_n - x_m| < \varepsilon \tag{11.81}$$

Критерий Коши. Последовательность $\{x_n\}$ сходится тогда и только тогда, когда она является фундаментальной.

Доказательство. □ Докажем каждое утверждение по отдельности.

1. сход. $\Rightarrow$ фунд. По определению предела,

$$\forall \varepsilon > 0 \ \exists N \in \mathbb{N} : \forall n \geq N : |x_n - a| < \varepsilon \tag{11.82}$$

   Но тогда, начиная с N, для всех $m, n \geq N$, поскольку $x_n, x_m \in u_\varepsilon(a)$, выполняется неравенство

$$|x_n - x_m| < 2\varepsilon, \tag{11.83}$$

   что и означает, что последовательность является фундаментальной.

2. фунд. $\Rightarrow$ сход. Сначала докажем, что из фундаментальности следует ограниченность. Пусть $\{x_n\}$ фундаментальна, тогда для фиксированного $\varepsilon > 0$, и любого фиксированного номера $m \geq N$, все члены с номереми $n \geq N$ лежат в интервале $(x_m - \varepsilon, x_m + \varepsilon)$. Поскольку вне интервала лежит только конечное число членов, то последовательность $\{x_n\}$ ограничена.

   По теореме Больцано-Вейерштрасса, существует сходящаяся подпоследовательность $\left\{x_{n_k}\right\}$, пусть её предел равен a. Тогда

$$\forall \varepsilon > 0 \exists n_\varepsilon \in \mathbb{N} : \forall k \geq n_\varepsilon : \left|x_{n_k} - a\right| < \varepsilon \tag{11.84}$$

   Возьмём любой член x_m такой, что $m \geq n_\varepsilon$. Мы знаем, что $\forall n \geq \max\{n_\varepsilon, N\}$:

$$|x_n - x_m| < \varepsilon \tag{11.85}$$

   В частности и для $n = n_k$. Тогда получаем

$$|x_m - a| \leq \left|x_{n_k} - a\right| + \left|x_{n_k} - x_m\right| < \varepsilon + \varepsilon = 2\varepsilon \tag{11.86}$$

И это выполняется для любого $\varepsilon > 0$, начиная с некоторого номера для любых m, поэтому последовательность $\{x_n\}$ сходится к a.

■

B.2. Предел функции

Определение. Проколотой ε-окрестностью точки x называется множество

$$\mathring{u}_\varepsilon(x) = (x-\varepsilon, x) \cup (x, x+\varepsilon) \tag{12.1}$$

B.2.1. Определение предела по Коши

Пусть функция f определена в некоторой проколотой окрестности точки x: $\mathring{u}(x)$.

Определение. Число A называется пределом функции f в точке a, если

$$\forall \varepsilon > 0 \ \exists \delta > 0 : \forall x \in \mathring{u}_\delta(a) \Rightarrow |f(x) - A| < \varepsilon \tag{12.2}$$

B.2.2. Определение предела по Гейне

Пусть функция f определена в некоторой проколотой окрестности точки x: $\mathring{u}(x)$.

Определение. Число A называется пределом функции f в точке a, если

$$\forall \{x_n\} : x_n \in \mathring{u}(a) : \lim_{n\to\infty} x_n = a \Rightarrow \exists \lim_{n\to\infty} f(x_n) = A \tag{12.3}$$

B.2.3. Эквивалентность определений Коши и Гейне

Утверждение. Определения предела по Коши и по Гейне эквивалентны.

Доказательство. □ Докажем две импликации:

1. [Коши $\Rightarrow$ Гейне]. Пусть мы знаем, что существует предел по Коши, тогда

   $$\lim_{x\to a} f(x) = A \tag{12.4}$$

   есть то же самое, что и

   $$\forall \varepsilon > 0 \ \exists \delta > 0 : \forall x \in \mathring{u}_\delta(a) \Rightarrow |f(x) - A| < \varepsilon \tag{12.5}$$

   Запишем, что $x_n \to a$, если $x_n \in \mathring{u}(a)$:

   $$\forall \delta > 0 \ \exists N \in \mathbb{N} : \forall n \geq N : 0 < |x_n - a| < \delta \tag{12.6}$$

   Объединяя эти два утверждения, получим, что

   $$\forall \varepsilon > 0 \ \exists N \in \mathbb{N} : \forall n \geq N : |f(x_n) - A| < \varepsilon \tag{12.7}$$

   Итак, мы получили, что если $x_n \in \mathring{u}(a)$ и $x_n \to a$, то $f(x_n) \to A$, что и требовалось доказать.
2. [Гейне $\Rightarrow$ Коши]. Предположим, что определение по Гейне выполнено, а определение по Коши — нет. Запишем отрицание определения по Коши:

   $$\exists \varepsilon > 0 : \ \ \forall \delta > 0 : \exists x \in \mathring{u}_\delta(a) \Rightarrow |f(x) - A| \geq \varepsilon \tag{12.8}$$

   Возьмём $\delta = \frac{1}{n}$:

$$\exists \varepsilon > 0 : \exists x_n : 0 < |x_n - a| < \frac{1}{n} \Rightarrow |f(x_n) - A| \geq \frac{1}{n} \tag{12.9}$$

Из $0 < |x_n - a| < \frac{1}{n}$ по теореме о промежуточной последовательности следует, что $\lim x_n = a$ и $x_n \neq a$. Тогда по определению предела по Гейне получаем, что

$$\lim_{n \to \infty} f(x_n) = A. \tag{12.10}$$

Но, из ((12.9)) мы знаем, что $\exists \varepsilon > 0$, что $|f(x_n) - A| \geq \varepsilon$, что противоречит тому, что $A = \lim f(x_n)$. Следовательно, если верно определение по Коши, то верно определение по Гейне.

Что и требовалось доказать. ■

B.2.4. Теорема о промежуточной функции

Теорема. Пусть функции f, g, h определены в $\mathring{u}_\varepsilon(a)$ и $\forall x \in \mathring{u}_\varepsilon(a)$:

$$f(x) \leq g(x) \leq h(x) \tag{12.11}$$

и существуют пределы:

$$\lim_{x \to a} f(x) = \lim_{x \to a} h(x) = A. \tag{12.12}$$

Тогда

$$\lim_{x \to a} g(x) = A \tag{12.13}$$

Доказательство. □ Рассмотрим любую последовательность $\{x_n\}$, такую что

$$\forall \{x_n\} : x_n \in \mathring{u}_\varepsilon(a) : \lim_{n \to \infty} x_n = a. \tag{12.14}$$

Определим для неё последовательности:

$$f_n = f(x_n), g_n = g(x_n), h_n = h(x_n). \tag{12.15}$$

Так как функции f и h стремятся к A при стремлении x к a, то по определению предела по Гейне имеем:

$$A = \lim_{n \to \infty} f_n = \lim_{n \to \infty} h_n \tag{12.16}$$

В силу неравенства ((12.11)) получаем, что

$$f_n \leq g_n \leq h_n \tag{12.17}$$

И, наконец, по теореме о промежуточной последовательности, получаем, что $g_n \to A$, что согласно определению предела функции по гейне, означает

$$\lim_{x \to a} g(x) = A \tag{12.18}$$

Что и требовалось доказать. ■

B.2.5. Арифметические свойства пределов функции

Теорема. Пусть для функций f и g выполняются условия

$$\lim_{x \to a} f(x) = A \quad \text{и} \quad \lim_{x \to a} g(x) = B \tag{12.19}$$

Тогда

1. Предел суммы равен сумме пределов

$$\lim_{x \to a} (f(x) + g(x)) = A + B \tag{12.20}$$

2. Предел произведения равен произведению пределов

$$\lim_{x \to a} (f(x) \cdot g(x)) = A \cdot B \tag{12.21}$$

3. Если $\forall x \in \mathring{u}(a) : g(x) \neq 0$ и $B \neq 0$, то предел частного равен частному пределов

$$\lim_{x \to a} \frac{f(x)}{g(x)} = \frac{A}{B} \tag{12.22}$$

Доказательство: $\square$ $\forall \{x_n\} : x_n \in \mathring{u}(a)$:

$$\lim_{n \to \infty} x_n = a \Rightarrow \exists \lim_{n \to \infty} f(x_n) = A \tag{12.23}$$

$$\lim_{n \to \infty} x_n = a \Rightarrow \exists \lim_{n \to \infty} g(x_n) = B \tag{12.24}$$

Введём последовательности $f_n = f(x_n), g_n = g(x_n)$ и разберёмся с каждым пунктом.

1. Пользуясь тем, что предел суммы последовательностей равен сумме пределов, получаем

$$\lim_{n \to \infty} (f_n + g_n) = \lim_{n \to \infty} f_n + \lim_{n \to \infty} g_n = A + B \tag{12.25}$$

Но по определению предела по Гейне отсюда получаем, что

$$\lim_{x \to a} (f(x) + g(x)) = A + B \tag{12.26}$$

2. Пользуясь тем, что предел произведения последовательностей равен произведению пределов, получаем

$$\lim_{n\to\infty}(f_n \cdot g_n) = \lim_{n\to\infty} f_n \cdot \lim_{n\to\infty} g_n = A \cdot B \tag{12.27}$$

Но по определению предела по Гейне отсюда получаем, что

$$\lim_{x\to a}(f(x) \cdot g(x)) = A \cdot B \tag{12.28}$$

3. Пользуясь тем, что предел частного последовательностей равен частному пределов и $B \neq 0$, получаем

$$\lim_{n\to\infty}\left(\frac{f_n}{g_n}\right) = \frac{\lim f_n}{\lim g_n} = \frac{A}{B} \tag{12.29}$$

Но по определению предела по Гейне отсюда получаем, что

$$\lim_{x\to a}\frac{f(x)}{g(x)} = \frac{A}{B}. \tag{12.30}$$

Что и требовалось доказать. ■

Примечание. Свойство предела разности, аналогичное свойству предела суммы, можно получить либо аналогично, либо применив пункты 1 и 2 теоремы об арифметических свойствах пределов функции.

B.2.6. Критерий Коши существования предела функции

Теорема (критерий Коши). Пусть функция f определена в $\mathring{u}(x_0), x_0 \in \overline{\mathbb{R}}$. Предел функции f в точке x_0 существует тогда и только тогда, когда выполняется условие

$$\forall\varepsilon > 0 : \exists\delta > 0 : \forall x', x'' \in \mathring{u}_\delta(x_0) : |f(x') - f(x'')| < \varepsilon. \tag{12.31}$$

Доказательство. □

1. $\Rightarrow$. Пусть $f(x) \to A$ при $x \to x_0$. Запишем дважды определение предела по Коши: $\forall\varepsilon > 0 \exists\delta > 0 : \forall x', x'' \in \mathring{u}_\delta(x_0)$:

$$|f(x') - A| < \varepsilon \tag{12.32}$$

$$|f(x'') - A| < \varepsilon \tag{12.33}$$

Отсюда получаем, что

$$|f(x') - f(x'')| \leq |f(x') - A| + |f(x'') - A| < 2\varepsilon \tag{12.34}$$

что и есть условие Коши.

2. $\Leftarrow$. Пусть мы знаем, что

$$\forall \varepsilon > 0 : \exists \delta > 0 : \forall x', x'' \in \mathring{u}_\delta(x_0) : |f(x') - f(x'')| < \varepsilon. \tag{12.35}$$

Возьмём произвольную последовательность x_n такую, что $\lim x_n = x_0$ и $x_n \in \mathring{u}(x_0)$. Тогда по определению предела последовательности

$$\exists N \in \mathbb{N} : \forall n \geq N : x_n \in \mathring{u}_\delta(x_0) \tag{12.36}$$

Согласно условию Коши, получаем, что

$$\forall m, n \geq N : |f(x_m) - f(x_n)| < \varepsilon. \tag{12.37}$$

Значит, согласно критерию Коши сходимости числовых последовательностей, мы получаем, что $\{f(x_n)\}$ сходится, пусть

$$A = \lim_{n \to \infty} f(x_n) \tag{12.38}$$

Теперь докажем, что для любой последовательности $\{x_n\} : f(x_n) \to A$. Предположим противное: пусть для некоторой последовательности $\{x'_n\} : x'_n \in \mathring{u}(x_0)$ и $f(x'_n) \to B \neq A$. Тогда для последовательности $\{x_1, x'_1, x_2, x'_2, ...\}$ мы получим, что она сходится к x_0. Расмотрим последовательность

$$\{f(x_1), f(x'_1), f(x_2), f(x'_2), ...\} \tag{12.39}$$

Она расходится, поскольку у неё есть два частичных предела A и B, которые не равны друг другу. Но она должна сходиться, поскольку мы доказали выше, что любая такая последовательность сходится. Получили противоречие, значит все последовательности $\{x_n\}$, сходящиеся к x_0, все члены которых лежат в проколотой окрестности x_0, имеют один и тот же предел A. Согласно определению предела по Гейне,

$$\lim_{x \to a} f(x) = A \tag{12.40}$$

Что и требовалось доказать. ■

B.3. Кратные интегралы

B.3.1. Двойные интегралы

B.3.1.1. Определение двойного интеграла

Пусть тело (V) в $\mathbb{R}^3$ ограничено сверху поверхностью $z = f(x, y)$. С боков ограничено цилиндрической поверхностью с образующей, параллельной оси z, а снизу плоской фигурой D на плоскости $z = 0$. Требуется найти объём тела V.

Разобьём D на малые фигуры $(\sigma_i),\ i = 1, ..., n$. Внутри каждой фигуры рассмотрим точку $(\xi_i, \eta_i) \in \sigma_i$. Тогда объём i-того столбика равен

$$|V_i| = f(\xi_i, \eta_i) \cdot |\sigma_i| \tag{13.1}$$

Приближённо можно написать, что

$$|V| \approx S_n = \sum_{i=1}^{n} f(\xi_i, \eta_i) \cdot |\sigma_i| \tag{13.2}$$

Полученная сумма называется интегральной. Будем неограниченно увеличивать мощность разбиения: $n \to \infty$. При стремлении макисмального диаметра фигуры σ_i к нулю:

$$\lambda = \max_{i=1,...n} d(\sigma_i) \tag{13.3}$$

получим, что объём $|V|$ равен пределу

$$|V| = \lim_{\lambda \to 0} \left[\sum_{i=1}^{n} f(\xi_i, \eta_i) \cdot |\sigma_i| \right] \tag{13.4}$$

Определение. Если существует предел интегральной сумммы S_n при стремлении максимального диаметра разбиения области $D \subset \mathbb{R}^2$ к нулю, не зависящий от способа разбиения области, то этот предел называется *двойным интегралом* функции f по области D.

$$\iint\limits_D f(x, y) dx dy \underset{\text{def}}{=} \lim_{\lambda \to 0} \left[\sum_{i=1}^{n} f(\xi_i, \eta_i) \cdot |\sigma_i| \right] \tag{13.5}$$

Условие существования двойного интеграла. Если функция f непрерывна на ограниченной замкнутой области D, то она интегрируема на D.

B.3.1.2. Суммы Дарбу

Пусть область D разбита на конечное число подмножеств $\sigma_i,\ i = 1, ..., n$. Обозначим

$$M_i = \sup_{\sigma_i} f(x, y) \tag{13.6}$$

$$m_i = \inf_{\sigma_i} f(x, y) \tag{13.7}$$

1. Верхняя сумма Дарбу:

$$S = \sum_{i=1}^{n} M_i \cdot |\sigma_i| \tag{13.8}$$

2. Нижняя сумма Дарбу:

$$s = \sum_{i=1}^{n} m_i \cdot |\sigma_i| \tag{13.9}$$

Для любого разбиения справедливо, что

$$s \leq S_n \leq S \tag{13.10}$$

Свойства сумм Дарбу:

1. При добавлении новых фигур σ_i и линий в разбиение D нижняя сумма Дарбу не убывает, а верхняя — не возрастает.
2. Любая нижняя сумма Дарбу не превосходит любой верхней суммы Дарбу, даже для разных разбиений.

Определение. Колебанием функции $f(x, y)$ на области D называется число

$$S - s = \sum_{i=1}^{n} (M_i - m_i) \cdot |\sigma_i| \tag{13.11}$$

Критерий интегрируемости Римана. Для того, чтобы ограниченная функция f была интегрируема по области D *необходимо и достаточно*, чтобы

$$\lim_{\lambda \to 0} S - s = 0 \tag{13.12}$$

B.3.1.3. Свойства двойного интеграла

Пусть функции $f(x, y)$ и $g(x, y)$ интегрируемы в D.

1. Линейность. $\forall \alpha, \beta \in \mathbb{R}$:

$$\iint\limits_D (\alpha f(x,y) + \beta g(x,y))d\sigma = \alpha \iint\limits_D f(x,y)d\sigma + \beta \iint\limits_D g(x,y)d\sigma \quad (13.13)$$

2. Аддитивнось по области. $\forall D_1, D_2 : (D_1 \cup D_2 = D) \wedge (\text{int}(D_1) \cap \text{int}(D_2) = \varnothing)$:

$$\iint\limits_D f(x,y)d\sigma = \iint\limits_{D_1} f(x,y)d\sigma + \iint\limits_{D_2} f(x,y)d\sigma \quad (13.14)$$

3. Интегрирование неравенств. Если $f(x,y) \leq g(x,y)$, то

$$\iint\limits_D f(x,y)d\sigma \leq \iint\limits_D g(x,y)d\sigma \quad (13.15)$$

3.1. Следствие. Если $m \leq f(x,y) \leq M$, то

$$m \cdot |D| \leq \iint\limits_D f(x,y)d\sigma \leq M \cdot |D| \quad (13.16)$$

3.1. Следствие.

$$\left| \iint\limits_D f(x,y)d\sigma \right| \leq \iint\limits_D |f(x,y)|d\sigma \quad (13.17)$$

4. Теорема о среднем. Если функция $f(x,y)$ непрерывна в замкнутой связной области D, то $\exists(\xi,\eta) \in D$:

$$f(\xi,\eta) = \frac{1}{|D|} \iint\limits_D f(x,y)d\sigma \quad (13.18)$$

Доказательство. По теореме Вейерштрасса, на связной замнкутой области D функция f ограничена, поэтому $\exists m, M \in \mathbb{R} : \ \forall (x,y) \in D : \ m \leq f(x,y) \leq M$. Используя следствие (3.1), можно написать, что

$$m \leq \frac{1}{|D|} \iint\limits_D f(x,y)d\sigma \leq M \quad (13.19)$$

По теореме Больцано-Коши (о промежуточном значении), непрерывная функция f принимает на D все значения между m и M, в частности $\exists(\xi,\eta) \in D$, для которой выполнено требуемое. ■

5. Интеграл от единицы равен площади области интегрирования.

$$\iint\limits_D dxdy = |D| \tag{13.20}$$

B.3.1.4. Сведение двойного интеграла к повторному

B.3.2. Тройные интегралы

B.3.2.1. Определение тройного интеграла

B.4. Криволинейные и поверхностные интегралы

B.4.1. Криволинейный интеграл I рода

Пусть в пространстве задана некоторая простая кривая $C \subset \mathbb{R}^3$. Пусть A и B — начальные и конечные точки кривой C. Разобьём участок кривой между A и B точками $P_1, P_2, ..., P_n$. Составим для функции $f(x, y, z)$ интегральную сумму. Обозначим $\Delta s_i = |P_i P_{i+1}|$.

$$S_n = \sum_{i=1}^{n} f(P_i) \cdot \Delta s_i \tag{14.1}$$

Пусть $\lambda = \max\left(\left|P_i P_{i+1}\right|\right)$ — максимальная длина отрезка ломанной $P_1 P_2 ... P_n$.

Определение. Если существует предел при стремлении максимальной длины отрезка разбиения к нулю, который не зависит от способа разбиения, то он называется криволинейным интегралом I рода по кривой C функции $f(x, y, z)$ и обозначается:

$$\int\limits_{(C)} f(x, y, z) ds = \lim_{\lambda \to 0} \sum_{i=1}^{n} f(P_i) \cdot \Delta s_i \tag{14.2}$$

Свойства криволинейного интеграла I рода:

1. Значение криволинейного интеграла I рода не зависит от направления обхода кривой C:

$$\int\limits_{(AB)} f(x, y, z) ds = \int\limits_{(BA)} f(x, y, z) ds \tag{14.3}$$

2. Константу можно вынести за знак интеграла, $\forall k \in \mathbb{R}$:

$$\int\limits_{(C)} k f(x, y, z) ds = k \int\limits_{(C)} f(x, y, z) ds \tag{14.4}$$

3. Интеграл суммы функций равен сумме их интегралов:

$$\int\limits_{(C)} (f(x, y, z) + g(x, y, z)) ds = \int\limits_{(C)} f(x, y, z) ds + \int\limits_{(C)} g(x, y, z) ds \tag{14.5}$$

4. Аддитивность по кривой. Если точка $D \in C$ лежит между A и B, то

$$\int\limits_{(AB)} f(x, y, z) ds = \int\limits_{(AD)} f(x, y, z) ds + \int\limits_{(DB)} f(x, y, z) ds \tag{14.6}$$

5. Интеграл от единицы. Пусть l_{AB} — длина участка кривой между A и B.

$$\int\limits_{(AB)} ds = l_{AB} \tag{14.7}$$

B.4.1.1. Вычисление криволинейного интеграла I рода

Пусть кривая C задана параметрически: $x = x(t),\ y = y(t),\ z = z(t),\ t \in [t_1, t_2]$. При $\lambda \to 0$ участок кривой $\Delta s \to \Delta l$, где $\Delta l = \sqrt{(\Delta x)^2 + (\Delta z)^2 + (\Delta z)^2}$ — отрезок ломаной, который можно выразить через проекции на координатные оси. Переходя к дифференциалам, получим:

$$\Delta x \to dx = x'_t dt \tag{14.8}$$

И аналогично для Δy и Δz. Поэтому

$$\begin{gathered} ds = \sqrt{(dx)^2 + (dy)^2 + (dz)^2} = \sqrt{(x'_t dt)^2 + (y'_t dt)^2 + (z'_t dt)^2} = \\ = \sqrt{(x'_t)^2 + (y'_t)^2 + (z'_t)^2}\, dt \end{gathered} \tag{14.9}$$

Тогда криволинейный интеграл I рода можно вычислить по формуле:

$$\int\limits_{(C)} f(x,y,z)ds = \int\limits_{t_1}^{t_2} f(x(t), y(t), z(t))\sqrt{(x'_t)^2 + (y'_t)^2 + (z'_t)^2}\, dt \tag{14.10}$$

Здесь существенно использовано то, что $dt > 0$.

B.4.2. Криволинейный интеграл II рода

Пусть в пространстве задана некоторая простая кривая $C \subset \mathbb{R}^3$. Пусть A и B — начальные и конечные точки кривой C. Разобьём участок кривой между A и B точками $P_1, P_2, ..., P_n$. Спроецируем точки $P_1, ..., P_n$ на ось Ox и обозначим проекции этих точек как $x_1, x_2, ..., x_n$. Обозначим $\Delta x_i = x_i - x_{i-1}$. И пусть $\lambda = \max(\Delta x_i)$. Рассмотрим интегральную сумму

$$S_n = \sum_{i=1}^{n} f(P_i) \cdot \Delta x_i \tag{14.11}$$

Определение. Если существует предел при стремлении максимальной длины отрезка разбиения к нулю, который не зависит от способа разбиения, то он называется криволинейным интегралом II рода по кривой C функции f и обозначается:

$$\int\limits_{AB} f(P)dx = \lim_{\lambda \to 0} \sum_{i=1}^{n} f(P_i) \cdot \Delta x_i \tag{14.12}$$

Аналогично можно спроецировать точки $P_1, ..., P_n$ на ось Oy и Oz и обозначить проекции этих точек как $y_1, y_2, ..., y_n$ и $z_1, z_2, ..., z_n$. Получив аналогичные интегральные суммы и соответствующие криволинейные интегралы II рода. При этом можно интегрировать по этой кривой *другие функции.*

Определение. Криволинейный интеграл II рода общего вида по кривой C равен сумме криволинейных интегралов по каждой из координат и равен

$$\begin{gathered}\int\limits_{AB} f(P)dx + g(P)dy + h(P)dz \underset{\text{def}}{=} \int\limits_{AB} f(P)dx + \int\limits_{AB} g(P)dy + \\ + \int\limits_{AB} h(P)dz\end{gathered} \tag{14.13}$$

Свойства криволинейного интеграла II рода(почти аналогичны I):

1. Значение криволинейного интеграла II рода *зависит* от направления обхода кривой C:

$$\int\limits_{AB} f(P)dx = -\int\limits_{BA} f(P)dx \tag{14.14}$$

2. Константу можно вынести за знак интеграла, $\forall k \in \mathbb{R}$:

$$\int\limits_{AB} kf(P)dx = k\int\limits_{AB} f(P)dx \tag{14.15}$$

3. Интеграл суммы функций равен сумме их интегралов:

$$\int\limits_{AB} (f(P) + g(P))dx = \int\limits_{AB} f(P)dx + \int\limits_{AB} g(P)dx \tag{14.16}$$

4. Аддитивность по кривой. Если точка $D \in C$ лежит между A и B, то

$$\int\limits_{AB} f(P)dx = \int\limits_{AD} f(P)dx + \int\limits_{DB} f(P)dx \tag{14.17}$$

B.4.2.1. Вычисление криволинейного интеграла II рода

Очевидно, можно получить формулу для вычисления криволинейного интеграла II рода обшего вида, подставив параметризацию и расписав дифференциалы:

Если кривая C задана параметрически: $x = x(t), y = y(t), z = z(t), t \in [t_1, t_2]$, то

$$\int\limits_{AB} f(P)dx + g(P)dy + h(P)dz = \\ = \int\limits_{t_1}^{t_2} (f(x(t), y(t), z(t))x'_t + g(x(t), y(t), z(t))y'_t + h(x(t), y(t), z(t))z'_t)dt \tag{14.18}$$

B.4.2.2. Связь с криволинейным интегралом I рода

Если $\cos\alpha, \cos\beta, \cos\gamma$ — направляющие косинусы касательной к кривой C(зависящие от точки на кривой, конечно же), то проецируя отрезки Δs на соответствующие оси и переходя к дифференциалам, получаем

$$\int\limits_{AB} f(P)dx + g(P)dy + h(P)dz = \\ = \int\limits_{AB} (f(P)\cos\alpha + g(P)\cos\beta + h(P)\cos\gamma)ds \tag{14.19}$$

B.5. Гамма-функция и бета-функция

B.5.1. Гамма-функция

Определение. Гамма-функция $\Gamma(x)$ определяется для всех положительных вещественных чисел $x > 0$ интегралом

$$\Gamma(x) = \int_0^\infty t^{x-1} e^{-t} dt \tag{15.1}$$

B.5.1.1. Свойства гамма-функции

1. Основное свойство гамма-функции.

$$\Gamma(x+1) = x\Gamma(x) \tag{15.2}$$

Доказательство. □ Подставим $(x+1)$ в гамма-функцию:

$$\Gamma(x+1) = \int_0^\infty t^x e^{-t} dt \tag{15.3}$$

Интегрируем по частям:

$$u = t^x \Rightarrow du = xt^{x-1}dt \tag{15.4}$$

$$dv = e^{-t}dt \Rightarrow v = -e^{-t} \tag{15.5}$$

$$\begin{gathered} \int_0^\infty t^x e^{-t} dt = -t^x e^{-t} \mid_0^\infty + x \int_0^\infty t^{x-1} e^{-t} dt = \\ = -\lim_{t\to\infty} t^x e^{-t} + x \int_0^\infty t^{x-1} e^{-t} dt = 0 + x\Gamma(x) = x\Gamma(x) \end{gathered} \tag{15.6}$$

■

2. Значение гамма-функции в натуральных числах. $\forall n \in \mathbb{N}$

$$\Gamma(n) = (n-1)! \tag{15.7}$$

Доказательство. □ Сначала найдём $\Gamma(1)$:

$$\Gamma(1) = \int_0^\infty t^{1-1} e^{-t} dt = \int_0^\infty e^{-t} dt = -e^{-t} \mid_0^\infty = 1 \tag{15.8}$$

Используя основное свойство гаммма-функции, находим:

$$\Gamma(2) = 1 \cdot \Gamma(1) = 1 = 1! \tag{15.9}$$

$$\Gamma(3) = 2 \cdot \Gamma(2) = 2 = 2! \tag{15.10}$$

Теперь строго обобщим по индукции: пусть верно, что $\Gamma(n) = (n-1)!$. Докажем, что верно $\Gamma(n+1) = n!$. По основному свойству гамма-функции: $\Gamma(n+1) = n\Gamma(n) = n(n-1)! = n!$. Поскольку база индукции проверена, то требуемое доказано. ■

3. Ещё одно интегральное представление.

$$\Gamma(x) = \int\limits_0^\infty 2t^{2x-1}e^{-t^2}dt \tag{15.11}$$

Доказательство. □ Сделаем в интеграле $\int_0^\infty t^{x-1}e^{-t}dt$ замену:

$$u = \sqrt{t} \Rightarrow \begin{cases} t \to 0 \Rightarrow u \to 0 \\ t \to \infty \Rightarrow u \to \infty \end{cases} \tag{15.12}$$

$$t = u^2 \Rightarrow dt = 2udu \tag{15.13}$$

$$\int\limits_0^\infty t^{x-1}e^{-t}dt = \int\limits_0^\infty \left(u^2\right)^{x-1}e^{-u^2} \cdot 2udu = \int\limits_0^\infty 2u^{2x-1}e^{-u^2}du \tag{15.14}$$

Поскольку $\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt$, то требуемое доказано. ■

4. Значения в положительных полуцелых аргументах. $\forall n \in \mathbb{N}_0$:

$$\Gamma\left(n + \frac{1}{2}\right) = \frac{(2n)!}{4^n n!}\sqrt{\pi} \tag{15.15}$$

Доказательство. □ Используем факт ((15.43)) о том, что $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$. Теперь, используя основное свойство гамма-функции, найдём значение в произвольной полуцелой точке:

$$\begin{gathered} \Gamma\left(n + \frac{1}{2}\right) = \frac{1}{2} \cdot \frac{3}{4} \cdot \ldots \cdot \frac{2n-1}{2} \cdot \Gamma\left(\frac{1}{2}\right) = \\ = \frac{1 \cdot 3 \cdot \ldots \cdot (2n-1)}{2^n} \cdot \sqrt{\pi} = \frac{(2n-1)!!}{2^n}\sqrt{\pi} = \frac{(2n)!}{4^n n!}\sqrt{\pi}. \blacksquare \end{gathered} \tag{15.16}$$

5. Свойство дополнения. $\forall x \in (0,1)$:

$$\Gamma(x) \cdot \Gamma(1-x) = \frac{\pi}{\sin(\pi x)} \tag{15.17}$$

6. Логарифмическая выпуклость гамма-функции. $\forall x_1, ..., x_n > 0, \forall \alpha_1, ..., \alpha_n \in [0, 1], \ \sum \alpha_i = 1$:

$$\Gamma\left(\sum_{i=1}^{n} \alpha_i x_i\right) \leq \prod_{i=1}^{n} [\Gamma(x_i)]^{\alpha_i} \tag{15.18}$$

Доказательство. □

$$\ln(\Gamma(x)) = \ln\left(\int_0^\infty t^{x-1} e^{-t} dt\right) = \ln\left(\int_0^\infty f(t; x) dt\right) \tag{15.19}$$

$$\frac{d \ln(\Gamma(x))}{dx} = \frac{\Gamma'(x)}{\Gamma(x)} \tag{15.20}$$

$$\frac{d^2 \ln(\Gamma(x))}{dx^2} = \frac{\Gamma''(x) \cdot \Gamma(x) - [\Gamma'(x)]^2}{(\Gamma(x))^2} \tag{15.21}$$

Сейчас мы будем доказывать, что числитель этого выражения положителен для всех $x > 0$.

$$\Gamma'(x) = \int_0^\infty t^{x-1} e^{-t} (\ln t) dt \tag{15.22}$$

$$\Gamma''(x) = \int_0^\infty t^{x-1} e^{-t} (\ln t)^2 dt \tag{15.23}$$

Введём *линейно независимые* функции f и g на $(0, \infty)$:

$$f(t) = t^{\frac{x-1}{2}} e^{-\frac{t}{2}} \tag{15.24}$$

$$g(t) = t^{\frac{x-1}{2}} e^{-\frac{t}{2}} \ln t \tag{15.25}$$

Запишем неравенство Коши-Буняковского для интегралов:

$$\left[\int_0^\infty f(t) g(t) dt\right]^2 \leq \left(\int_0^\infty f(t)^2 dt\right) \cdot \left(\int_0^\infty g(t)^2 dt\right) \tag{15.26}$$

$$\left[\int_0^\infty t^{x-1} e^{-t} (\ln t) dt\right]^2 \leq \left(\int_0^\infty t^{x-1} e^{-t} dt\right) \cdot \left(\int_0^\infty t^{x-1} e^{-t} (\ln t)^2 dt\right) \tag{15.27}$$

Остаётся заметить, что слева стоит квадрат производной гамма-функции, а справа произведение гамма-функции и её второй производной. Итак, верно неравенство

$$\Gamma''(x) \cdot \Gamma(x) - [\Gamma'(x)]^2 > 0 \tag{15.28}$$

Следовательно, вторая производная логарифма гамма-функции положительна, значит логарифм гамма-функции выпуклая функция, а значит для неё верно неравенство Йенсена. $\forall x_1, ..., x_n > 0, \forall \alpha_1, ..., \alpha_n \in [0, 1], \ \sum \alpha_i = 1$:

$$\ln\left(\Gamma\left(\sum_{i=1}^{n} \alpha_i x_i\right)\right) \leq \sum_{i=1}^{n} \alpha_i \ln(\Gamma(x_i)) \tag{15.29}$$

Пользуясь монотонностью экспоненты, получаем исходное неравенство, потенцируя обе части.

$$\Gamma\left(\sum_{i=1}^{n} \alpha_i x_i\right) \leq \prod_{i=1}^{n} [\Gamma(x_i)]^{\alpha_i} \tag{15.30}$$

Что и требовалось доказать. ■

B.5.2. Бета-функция

Определение. Бета-функция $\mathrm{B}(x, y)$ определяется для всех положительных вещественных чисел $x > 0$, $y > 0$ интегралом

$$\mathrm{B}(x, y) = \int_0^1 t^{x-1}(1-t)^{y-1} dt \tag{15.31}$$

B.5.2.1. Свойства бета-функции

Альтернативное интегральное представление можно получить, если сделать замену $t = \sin^2 u$. Тогда $(1 - t) = \cos^2 u$ и $dt = 2 \sin u \cos u$. При $t = 0 \Rightarrow u = 0$ и $t = 1 \Rightarrow u = \frac{\pi}{2}$.

Итак,

$$\mathrm{B}(x, y) = \int_0^{\frac{\pi}{2}} 2 \cdot (\sin u)^{2x-1} (\cos u)^{2y-1} du \tag{15.32}$$

Ясно, что бета-функция обладает симметричностью относительно перестановки аргументов, поскольку на $[0, 1]$ графики функций t и $(1 - t)$ симметричны относительно $t = \frac{1}{2}$, и значит при траснпозиции аргументов значение интеграла не меняется. Ана-

логичный вывод можно получить при анализе тригонометрической интегральной формы.

$$\mathrm{B}(x,y) = \mathrm{B}(y,x) \tag{15.33}$$

Найдем значение $\mathrm{B}\left(\frac{1}{2},\frac{1}{2}\right)$:

$$\mathrm{B}\left(\frac{1}{2},\frac{1}{2}\right) = \int\limits_0^{\frac{\pi}{2}} 2\cdot(\sin t)^{2\cdot\frac{1}{2}-1}(\cos t)^{2\cdot\frac{1}{2}-1}dt = \int\limits_0^{\frac{\pi}{2}} 2dt = \pi \tag{15.34}$$

B.5.3. Связь гамма-функции и бета-функции

Теорема. Для любых $a, b > 0$ справедливо

$$\mathrm{B}(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)} \tag{15.35}$$

Доказательство. □

$$\Gamma(a) = \int\limits_0^{\infty} 2x^{2a-1}e^{-x^2}dx \tag{15.36}$$

$$\Gamma(b) = \int\limits_0^{\infty} 2y^{2b-1}e^{-y^2}dy \tag{15.37}$$

$$\Gamma(a)\cdot\Gamma(b) = \int\limits_0^{\infty} y^{b-1}e^{-y}dy \int\limits_0^{\infty} x^{a-1}e^{-x}dx \tag{15.38}$$

Произведение этих интегралов можно воспринимать как повторный, поэтому запишем теперь его как двойной по области $D = \{(x,y) \mid x,y \geq 0\}$.

$$\Gamma(a)\cdot\Gamma(b) = \iint\limits_D 4x^{2a-1}y^{2b-1}e^{-x^2-y^2}dxdy \tag{15.39}$$

Перейдём в полярные координаты:

$$\begin{cases} x = r\cos\varphi \\ y = r\sin\varphi \\ dxdy = rdrd\varphi \end{cases} \tag{15.40}$$

$$\Gamma(a)\cdot\Gamma(b)=\iint\limits_D 4r^{2a+2b-1}(\cos\varphi)^{2a-1}(\sin\varphi)^{2b-1}e^{-r^2}drd\varphi=$$
$$=\int\limits_0^{\frac{\pi}{2}}2(\cos\varphi)^{2a-1}(\sin\varphi)^{2b-1}d\varphi\int\limits_0^{\infty}2r^{2(a+b)-1}e^{-r^2}dr \tag{15.41}$$

Поскольку границы внутреннего интеграла не зависят от φ, то можно считать данную запись произведением двух отдельных интегралов! Но интеграл по φ, согласно ((15.32)), есть бета-функция, а интеграл по r — гамма-функция. Окончательно имеем:

$$\Gamma(a)\cdot\Gamma(b)=\mathrm{B}(b,a)\cdot\Gamma(a+b)\Rightarrow\mathrm{B}(b,a)=\frac{\Gamma(a)\cdot\Gamma(b)}{\Gamma(a+b)} \tag{15.42}$$

■

Следствие 1. Из этого соотношения так же видно, что $\mathrm{B}(a,b)=\mathrm{B}(b,a)$.

Следствие 2. Гамма-функция в $\frac{1}{2}$ и интеграл Эйлера-Пуассона.

$$\Gamma\left(\frac{1}{2}\right)=\int\limits_{-\infty}^{+\infty}e^{-x^2}dx=\sqrt{\pi} \tag{15.43}$$

Доказательство. □ Запишем, используя связь ((15.35)):

$$\mathrm{B}\left(\frac{1}{2},\frac{1}{2}\right)=\frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(\frac{1}{2}\right)}{\Gamma\left(\frac{1}{2}+\frac{1}{2}\right)} \tag{15.44}$$

Учитывая, что $\mathrm{B}\left(\frac{1}{2},\frac{1}{2}\right)=\pi$ и $\Gamma(1)=1$, получим:

$$\left[\Gamma\left(\frac{1}{2}\right)\right]^2=\pi \tag{15.45}$$

Следовательно, $\Gamma\left(\frac{1}{2}\right)=\sqrt{\pi}$. Но с другой стороны,

$$\Gamma\left(\frac{1}{2}\right)=2\int\limits_0^{\infty}e^{-x^2}dx=\int\limits_{-\infty}^{\infty}e^{-x^2}dx \tag{15.46}$$

■

B.6. Числовые ряды

Определение. Выражение $a_1 + a_2 + ... + a_n + ...$ называют **рядом** с общим членом a_n и обозначают

$$\sum_{n=1}^{\infty} a_n \tag{16.1}$$

Определение. Элементы последовательности $\{a_n\}$ называются членами ряда.

Определение. n-ой частичной суммой ряда с общим членом $\{a_i\}$ называется сумма

$$s_n = \sum_{i=1}^{n} a_i \tag{16.2}$$

Определение. Если последовательность частичных сумм $\{s_n\}$ для ряда с общим членом $\{a_n\}$ имеет предел, то ряд называется сходящимся. Если последовательность частичных сумм предела не имеет, то ряд называется расходящимся.

Определение. Суммой ряда называется предел последовательности его частичных сумм.

$$s = \lim_{n \to \infty} s_n \tag{16.3}$$

Если ряд сходится, то найдя его сумму, пишут

$$\sum_{n=1}^{\infty} a_n = s \tag{16.4}$$

Остатком ряда называется разность между n-й частичной суммой и суммой ряда.

$$r_n = s - s_n \tag{16.5}$$

Свойства рядов:

1. Отбрасывание конечного количества членов ряда не влияет на его сходимость.
2. Для сходящегося ряда остаток стремится к нулю при $n \to \infty$.
3. Если все члены сходящегося ряда умножить на константу $c \in \mathbb{R} \setminus \{0\}$, то ряд из умноженных членов так же сходится, а его сумма равна $c \cdot s$.
4. Если ряды $A = (a_1 + a_2 + ...)$ и $B = (b_1 + b_2 + ...)$ сходятся, то ряд, для которого $c_n = a_n + b_n$

$$C = c_1 + c_2 + ... \tag{16.6}$$

тоже сходится, причём $C = A + B$.

B.6.1. Необходимый признак сходимости ряда

Теорема(необходимый признак сходимости ряда). Если ряд сходится, то его общий член стремится к нулю при неограниченном возрастании n.

$$\sum_{n=1}^{\infty} a_n \text{ сходится} \Rightarrow \lim_{n\to\infty} a_n = 0 \tag{16.7}$$

Доказательство. □ Пусть для сходящегося ряда

$$\sum_{n=1}^{\infty} a_n \tag{16.8}$$

определена последовательность частичных сумм $\{s_n\}$. Пусть

$$s = \lim_{n\to\infty} s_n \tag{16.9}$$

Заметим, что $a_n = s_n - s_{n-1}$. Тогда

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} (s_n - s_{n-1}) = s - s = 0 \tag{16.10}$$

Что и требовалось доказать. ■

B.6.2. Признаки сходимости положительных рядов

Пусть, начиная с некоторого номера N, $\forall n \geq N : a_n \geq 0$. Тогда ряд $\sum_{n=1}^{\infty} a_n$ назовём *положительным.*

Основная теорема сходимости. Положительный ряд всегда имеет сумму. Если последовательность частичных сумм ограничена сверху, то ряд сходится, иначе расходится.

Доказательство. □ Поскольку $a_n \geq 0$ начиная с некоторого номера N, то $\forall n \geq N$: $s_{n+1} = s_n + a_{n+1} \geq s_n$. Следовательно последовательность $\{s_n\}$ мотонно не убывает. Так как по условию теоремы $\{s_n\}$ ограничена сверху, то у неё есть предел $\Rightarrow$ ряд из членов $\{a_n\}$ сходится. Если же последовательность $\{s_n\}$ не ограничена сверху, то у неё нет предела и ряд расходится. ■

B.6.2.1. Теоремы сравнения

Теорема 1. Пусть даны два положительных ряда

$$\sum_{n=1}^{\infty} a_n \tag{16.11}$$

и

$$\sum_{n=1}^{\infty} b_n \tag{16.12}$$

Если $\forall n \geq N : a_n \leq b_n$, то

- Из сходимости ряда $\{b_n\}$ следует сходимость ряда $\{a_n\}$.
- Из расходимости ряда $\{a_n\}$ следует расходимость ряда $\{b_n\}$.

Доказательство. □ Не умаляя общности рассуждений считаем $0 \leq a_n \leq b_n \ \forall n \in \mathbb{N}$, так как конечное число слагаемых ряда можно отбросить. Пусть A_n, B_n - частичные суммы рядов $\{a_n\}$ и $\{b_n\}$. Если ряд $\{b_n\}$ сходится, то по основной теореме о сходимости существует такая константа L, что

$$B_n \leq L \tag{16.13}$$

учитывая, что $A_n \leq B_n$, получаем $A_n \leq L$. Это и означает что ряд $\{a_n\}$ сходится. ■

Теорема 2. Если существует предел $\lim_{n\to\infty}\left(\frac{a_n}{b_n}\right) = K$ и при этом $(0 \leq K \leq +\infty)$, то

1. Если $K < +\infty$, то из сходимости $\{b_n\}$ следует сходимость $\{a_n\}$
2. Если $K > 0$, то из расходимости $\{b_n\}$ следует расходимость $\{a_n\}$
3. Если $0 < K < +\infty$, то ряды $\{a_n\}$ и $\{b_n\}$ сходятся и расходятся одновременно.

Доказательство. □

1. Пусть $\sum b_n$ сходится и $K < +\infty$. Тогда по определению предела последовательности, для всех достаточно больших n $\exists \varepsilon > 0$, такой, что

$$\frac{a_n}{b_n} - K < \varepsilon \tag{16.14}$$

   Следовательно, $a_n < (K + \varepsilon)b_n$. По первой теореме сравнения, из сходимости b_n следует сходимость a_n.

2. Пусть $\sum b_n$ расходится и $K > 0$. Тогда $\lim \frac{b_n}{a_n}$ обязательно конечен. Предположим, что ряд $\sum a_n$ сходится, тогда по только что доказанному п. 1 ряд $\sum b_n$ должен сходиться. Получили противоречие, и значит при расходимости $\sum b_n$ ряд $\sum a_n$ расходится.

Пересекая оба случая, получаем истинность пункта 3. ■

Теорема 3. Если для положиетльных рядов, начиная с некоторого номера, верно, что

$$\frac{a_{n+1}}{a_n} \leq \frac{b_{n+1}}{b_n} \tag{16.15}$$

,

то их сходимости $\sum b_n$ следует сходимость $\sum a_n$, а из расходимости $\sum a_n$ следует расходимость b_n.

Доказательство. □ Не умаляя общности можно сказать, что неравенство из условия теоремы верно для всех $n \in \mathbb{N}$. Тогда

$$\frac{a_2}{a_1} \leq \frac{b_2}{b_1}; \frac{a_3}{a_2} \leq \frac{b_3}{b_2}; ... \frac{a_n}{a_{n-1}} \leq \frac{b_n}{b_{n-1}}. \tag{16.16}$$

Перемножим все эти неравенства и получим

$$\frac{a_n}{a_1} \leq \frac{b_n}{b_1} \Leftrightarrow a_n \leq \left(\frac{a_1}{b_1}\right) b_n \tag{16.17}$$

.

Это означает по первой теореме, что из сходимости b_n следует сходимость a_n, а из расходимости a_n следует расходимость b_n. ■

B.6.2.2. Радикальный признак Коши

Радикальный признак Коши. Пусть $0 < q < 1$. Составим для ряда $\sum a_n$ выражение

$$b_n = \sqrt[n]{a_n} \tag{16.18}$$

Если для достаточно больших n выполянется $b_n < q$, где постоянная $q < 1$, то ряд $\sum a_n$ сходится. Если же $b_n \geq 1$, то ряд расходится.

Доказательство. □ геометрическая прогрессия $\sum q^n$ сходится при $q < 1$. Сравним ряд $\sum a_n$ с геометрической прогрессией. Если $\sqrt[n]{a_n} < q$ для достаточно больших n, то

$$a_n < q^n \tag{16.19}$$

По первой теореме сравнения, ряд $\sum a_n$ сходится. Если же, начиная с некоторого номера, $a_n \geq 1$, то либо из сравнения с расходяшимся рядом $(1 + 1 + 1 + ...)$, либо из нарушения необходимого признака сходимости, получаем, что ряд $\sum a_n$ расходится.

Радикальный признак Коши в предельной форме. Пусть для положительного ряда $\sum a_n$

$$\lim_{n \to \infty} \sqrt[n]{a_n} = l \tag{16.20}$$

1. Если $l < 1$, то ряд $\sum a_n$ сходится.
2. Если $l > 1$, то ряд $\sum a_n$ расходится.
3. Если $l = 1$, то ряд может как сходиться, так и расходиться.

Доказательство. □

1. Пусть $l < 1$. Возьмём такое $\varepsilon > 0$, что $l + \varepsilon < 1$. Тогда по определению предела, для достаточно больших n будет верно, что

$$\sqrt[n]{a_n} < l + \varepsilon < 1 \tag{16.21}$$

   По радикальному признаку Коши ряд $\sum a_n$ сходится.

2. Пусть теперь $l > 1$. Тогда существует такое q, что $1 < q < l$. По определению предела, для достаточно больших n будет верно, что

$$\sqrt[n]{a_n} \geq q \geq 1 \tag{16.22}$$

   По радикальному признаку Коши ряд $\sum a_n$ расходится. ■

B.6.2.3. Признак Даламбера

Признак Даламбера. Для положительного ряда $\sum a_n$ определим величину

$$D_n = \frac{a_{n+1}}{a_n} \tag{16.23}$$

Если для достаточно больших n выполнено $D_n \leq q < 1$, где q - постоянное число, то ряд сходится. Если же $D_n \geq 1$, то ряд расходится.

Доказательство. □

1. Пусть $D_n \leq q < 1$ для достаточно больших n. Рассмотрим геометрическую прогрессию $\sum q^n$. Она сходится при $q < 1$. Сравним ряд $\sum a_n$ с ней, имея в виду, что $\frac{q^{n+1}}{q^n} = q$.

$$\frac{a_{n+1}}{a_n} \leq q = \frac{q^{n+1}}{q^n} \tag{16.24}$$

   По третьей теореме сравнения, из сходимости ряда $\sum q^n$ следует сходимость ряда $\sum a_n$.

2. Пусть теперь $D_n \geq 1$ для достаточно больших n. Тогда либо из сравнения с расходящимся рядом $(1 + 1 + 1 + ...)$, либо из нарушения необходимого признака сходимости, получаем, что ряд $\sum a_n$ расходится. ■

Признак Даламбера в предельной форме. Пусть для положительного ряда $\sum a_n$

$$\lim_{n\to\infty}\left(\frac{a_{n+1}}{a_n}\right) = D \tag{16.25}$$

.

1. Если $D < 1$, то ряд $\sum a_n$ сходится.
2. Если $D > 1$, то ряд $\sum a_n$ расходится.
3. Если $D = 1$, то ряд может как сходиться, так и расходиться.

Доказательство. □

1. Пусть $D < 1$. Возьмём такое $\varepsilon > 0$, что $D + \varepsilon < 1$. Тогда по определению предела, для достаточно больших n будет верно, что

$$\frac{a_{n+1}}{a_n} < D + \varepsilon < 1 \tag{16.26}$$

   По признаку Даламбера ряд $\sum a_n$ сходится.

2. Пусть теперь $D > 1$. Тогда существует такое q, что $1 < q < D$. По определению предела, для достаточно больших n будет верно, что

$$\frac{a_{n+1}}{a_n} \geq q \geq 1 \tag{16.27}$$

   По признаку Даламбера ряд $\sum a_n$ расходится. ■

B.6.2.4. Признак Раабе

Признак Раабе. Для положительного ряда $\sum a_n$ определим величину

$$R_n = n\left(1 - \frac{a_{n+1}}{a_n}\right) \tag{16.28}$$

Если для достаточно больших n выполнено $R_n \geq r > 1$, где r - постоянное число, то ряд сходится. Если же $R_n \leq 1$, то ряд расходится.

Доказательство. □

1. Пусть $R_n \geq r > 1$ для достаточно больших n. Это эквивалетно тому, что

$$\frac{a_{n+1}}{a_n} \leq 1 - \frac{r}{n} \tag{16.29}$$

   Используем лемму:

$$\lim_{n\to\infty} \frac{\left(1 - \frac{1}{n}\right)^s - 1}{-\frac{1}{n}} = s \tag{16.30}$$

   Мозьмём такое число s, что $1 < s < r$. Тогда для достаточно больших n будет верно, что

$$\frac{\left(1-\frac{1}{n}\right)^s-1}{-\frac{1}{n}}<r \Leftrightarrow 1-\frac{r}{n}<\left(1-\frac{1}{n}\right)^s \tag{16.31}$$

Полученное неравенство эквивалентно такому:

$$\frac{a_{n+1}}{a_n}<\left(\frac{n-1}{n}\right)^s=\frac{\frac{1}{n^s}}{\frac{1}{(n-1)^s}} \tag{16.32}$$

Справа стоит отношение следующего члена *сходящегося* обобщённого гармонического ряда $H_s(s>1)$, поэтому по третьей теореме сравнения из сходимости ряда H_s следует сходимость ряда $\sum a_n$.

2. Пусть теперь $R_n \leq 1$ для достаточно больших n. Имеем:

$$n\left(1-\frac{a_{n+1}}{a_n}\right)\leq 1 \Leftrightarrow \frac{a_{n+1}}{a_n}\geq \frac{1}{1+\frac{1}{n}}=\frac{n}{n+1}=\frac{\frac{1}{n+1}}{\frac{1}{n}} \tag{16.33}$$

Справа стоит отношение следующего члена *расходящегося* гармонического ряда H_1. Поэтому по третьей теореме сравнения из расходимости ряда H_1 следует расходимость ряда $\sum a_n$. ■

Признак Раабе в предельной форме. Пусть для положительного ряда $\sum a_n$

$$\lim_{n\to\infty} n\left(1-\frac{a_{n+1}}{a_n}\right)=R \tag{16.34}$$

1. Если $R>1$, то ряд $\sum a_n$ сходится.
2. Если $R<1$, то ряд $\sum a_n$ расходится.
3. Если $R=1$, то ряд может как сходиться, так и расходиться.

Признак Раабе существенно сильнее признака Даламбера.

B.6.2.5. Интегральный признак Маклорена-Коши

Интегральный признак Маклорена-Коши. Пусть ряд можно представить в виде

$$\sum_{n=1}^{\infty} a_n \equiv \sum_{n=1}^{\infty} f(n) \tag{16.35}$$

где $f(n)$ — значение при $x=n$ непрерывной положительной монотонно убывающей функции $f(x)$ на полуинтервале $[1,+\infty)$.

Тогда ряд $\sum a_n$ сходится тогда и только тогда, когда сходится интеграл

$$\int_1^{\infty} f(x)dx \text{ сходится} \Leftrightarrow \sum_{n=1}^{\infty} a_n \text{ сходится} \tag{16.36}$$

Доказательство. □ Рассмотрим произвольную первообразную функцию $F(x)$ для $f(x)$ на полуинтервале $[1, +\infty)$:

$$F(x) = \int_1^x f(t)dt \tag{16.37}$$

Ясно, что $0 < f(x) = F'(x)$, поэтому $F(x) \nearrow$. Поскольку $f(x)$ монотонно убывает, то для $x : n \leq x \leq n+1$:

$$a_{n+1} = f(n+1) \leq f(x) \leq f(n) = a_n \tag{16.38}$$

$$a_{n+1} \leq \int_n^{n+1} f(t)dt \leq a_n \tag{16.39}$$

Мы получиили оценку для общего члена такого ряда:

$$\sum_{n=1}^{\infty} \int_n^{n+1} f(t)dt \tag{16.40}$$

Его n-я частичная сумма равна

$$s_n = \int_1^{n+1} f(t)dt = F(n+1) - F(1) \underset{\text{сход.}}{\sim} F(n+1) \tag{16.41}$$

Итак, проанализируем предел

$$L = \lim_{x \to \infty} F(x) \tag{16.42}$$

- Если $L < \infty$, то ряд $\sum a_{n+1}$ сходится по первой теореме сравнения как меньший либо равный сходящемуся ряду. И из сходимости $\sum a_{n+1}$ следует сходимость $\sum a_n$.
- Если $L = \infty$, то ряд $\sum a_n$ расходится по первой теореме сравнения как больший либо равный расходящемуся ряду.

Таким образом, ряд $\sum a_n$ сходится тогда и только тогда, когда сходится интеграл $\int_1^{\infty} f(x)dx$. ■

B.6.3. Сходимость произвольных рядов

Пусть задан ряд $\sum a_n$, где члены a_n имеют произвольные знаки. Вопрос его сходимости сводится к сходимости последовательности частичных сумм $\{s_n\}_{n=1}^{\infty}$:

$$s_1, s_2, ...s_n, s_{n+1}, ...s_{n+m}, .. \tag{16.43}$$

Ряд $\sum a_n$ сходится тогда и только тогда, когда последовательность $\{s_n\}$ фундаментальна, то есть

$$\forall \varepsilon > 0 \; \exists N : \forall n > N, \forall m \in \mathbb{N} : \left| s_{n+m} - s_n \right| < \varepsilon \tag{16.44}$$

B.6.3.1. Абсолютная сходимость

Абсолютная сходимость. Ряд $\sum a_n$ называется абсолютно сходящимся, если сходится ряд $\sum |a_n|$.

Теорема Коши. Если ряд $\sum a_n$ сходится абсолютно, то он сходится.

Доказательство. □ Из абсолютной сходимости мы знаем, что начиная с некоторого номера и для всех $m \in \mathbb{N}$:

$$\forall \varepsilon > 0 : \; \left| \sum_{i=0}^{m} \left| a_{n+i} \right| \right| < \varepsilon \tag{16.45}$$

Поскольку подмодульное выражение неотрицательно, то отбрасываем модуль:

$$\sum_{i=0}^{m} \left| a_{n+i} \right| < \varepsilon \tag{16.46}$$

Но с другой стороны, используем неравенство треугольника:

$$\left| \sum_{i=0}^{m} a_{n+i} \right| \leq \sum_{i=0}^{m} \left| a_{n+i} \right| < \varepsilon \tag{16.47}$$

Значит, ряд $\sum a_n$ сходится. ■

Кроме того, если ряд $\sum a_n$ сходится абсолютно, то ряды

$$\sum_{k=1}^{\infty} b_k \quad \text{и} \quad \sum_{m=1}^{\infty} c_m, \tag{16.48}$$

где b_k - положительные члены ряда $\sum a_n$ в порядке следования, а c_m - модули отрицательных членов ряда $\sum a_n$ в порядке следования, *сходятся.* И имеет место

$$\sum_{n=1}^{\infty} a_n = \sum_{k=1}^{\infty} b_k - \sum_{m=1}^{\infty} c_m \tag{16.49}$$

B.6.3.2. Знакопеременные ряды и признак Лейбница

Ряд $\sum a_n$ называется знакопеременным, если $\forall n \in \mathbb{N}: \ a_n \cdot a_{n+1} < 0$.

Не умаляя общности, можно давать такое определение для всех $n \in \mathbb{N}$, так как конечное число членов ряда можно отбросить и перенумеровать оставшиеся с сохранением сходимости.

То же самое можно написать и так:

$$\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty} (-1)^n c_n, \tag{16.50}$$

где $c_n > 0$.

Признак Лейбница. Пусть ряд $\sum a_n$ является знакопеременным. Если все члены ряда убывают по абсолютной величине и стремятся к нулю, то ряд $\sum a_n$ сходится.

Доказательство. □ Пусть $c_n = |a_n|$, и S_{2m} - частичная сумма чётного порядка:

$$S_{2m} = c_1 - c_2 + c_3 - ... + c_{2m-1} - c_{2m} \tag{16.51}$$

$$S_{2m} = (c_1 - c_2) + (c_3 - c_4) + ... + (c_{2m-1} - c_{2m}) \tag{16.52}$$

Поскольку $c_i > c_{i+1}$, то S_{2m} с ростом m возрастает.

$$S_{2m} = c_1 - (c_2 - c_3) - ... - (c_{2m-2} - c_{2m-1}) - c_{2m} \tag{16.53}$$

Выходит, что S_{2m} ограничена сверху c_1. Тогда последовательность S_{2m} сходится как возрастающая и ограниченная сверху.

$$\lim_{m \to \infty} S_{2m} = S \tag{16.54}$$

Для суммы нечётного порядка имеем $S_{2m-1} = S_{2m} + c_{2m}$.

Поэтому, используя, что $c_{2m} \to 0$:

$$\lim_{m \to \infty} S_{2m-1} = S \tag{16.55}$$

Последовательности как чётных, так и нечётных сумм данного ряда сходятся к одному числу, следовательно, ряд сходится. ■

C. Комбинаторика

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

C.1. Основные правила комбинаторики

C.1.1. Првила 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: □ Пусть $A = \{a_1, ..., a_m\}$ и $B = \{b_1, ..., b_n\}$ Тогда

$$A \cup B = \{a_1, ..., a_m, b_1, ..., b_n\} \tag{17.1}$$

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

Правило произведения. Если элемент множества A можно выбрать m способами и вслед за ним элемент множества B можно выбрать n способами, то количество способов выбрать упорядоченную пару элементов $(a \in A, b \in B)$ равно $m \cdot n$.

Обобщённые правила суммы и произведения:

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

C.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 $\left\lceil \frac{n}{m} \right\rceil$ объектов.

Доказательство. □ Обозначим $k = \left\lceil \frac{n}{m} \right\rceil$ 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: $k-1 = \left\lceil \frac{n}{m} \right\rceil - 1 < \frac{n}{m}$. Имеем:

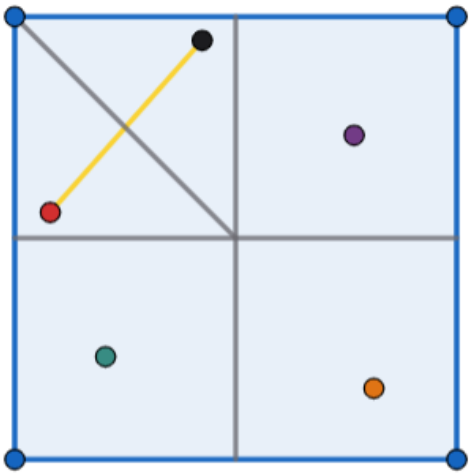
$$\begin{cases} n \leq m \cdot (k-1) \\ n > m \cdot (k-1) \end{cases} \tag{17.2}$$

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

C.1.3. Примеры

1. В квадрате со стороной два случайным образом выбрали 5 точек. Доказать, что расстояние между любыми двумя из них не больше $\sqrt{2}$.

   Решение. □ Разобьём квадрат на 4 одинаковых единичных квадрата. По принципу Дирихле, найдётся единичный квадрат, в котором не меньше двух точек.



   Внутри единичного квадрата точки расположены на расстоянии не большем, чем диагональ, равная $\sqrt{2}$. ■

C.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 называаются 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 $\varnothing$. $\forall A : \ \varnothing \subset A$

C.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. $A \triangle B = (A \setminus B) \cup (B \setminus A)$

C.2.2. Свойства бинарных операций над множествами

1. Коммутативность объедиения и пересечения:
   - $A \cup B = B \cup A$
   - $A \cap B = B \cap A$.
2. Ассоциативность объедиения и пересечения:
   - $(A \cup B) \cup C = A \cup (B \cup C)$
   - $(A \cap B) \cap C = A \cap (B \cap C)$.
3. Дистрибутивность объедиения и пересечения:
   - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
   - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

C.2.3. Кортеж

Кортежем называется упорядоченная n-ка элементов. Обозначается как

$$(a_1, a_2, ..., a_n) \text{ или } \ \langle a_1, a_2, ..., a_n \rangle \tag{18.1}$$

.

Более строго, можно индуктивно сопоставить кортежи множествам:

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

Тогда:

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

Альтернативно, можно дать такое определение:

$$\langle a_1, a_2, ..., a_n\rangle = f : [n] \to \{a_1, a_2, ..., a_n\} \tag{18.2}$$

C.2.4. Декартово произведение

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

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\} \tag{18.3}$$

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 объедиения и пересечения(по левому и по правому множителю):
   - $A \times (B \cup C) = A \times B \cup A \times C$
   - $A \times (B \cap C) = A \times B \cap A \times C$
   - $(B \cup C) \times A = B \times A \cup C \times A$
   - $(B \cap C) \times A = B \times A \cap C \times A$

C.2.5. Возведение множества в степень множества

Определение. Для множеств $A, B : A^B$ — множество всех отображений $B \to A$

Определение. Булеаном множества A называется множество всех подмножеств A и обозначается 2^A.

Каждое подмножество $S \subseteq A \leftrightarrow \chi_S : A \to \{0, 1\}$

$$\chi_S(x) = \begin{cases} 1, x \in S \\ 0, x \notin S \end{cases} \tag{18.4}$$

C.2.6. Частичный порядок

Определение. Бинарное отношение называется частичным порядком, если

1. Рефлексивность:

$$x \leq x \tag{18.5}$$

2. Антисимметричность:

$$(x \leq y \land y \leq x) \to x = y \tag{18.6}$$

3. Транзитивность:

$$(x \leq y \land y \leq z) \to x \leq z \tag{18.7}$$

Определение. Линейным порядком называется условие

$$\forall x, y : (x \leq y \lor y \leq x) \tag{18.8}$$

Определение. Строгим порядком называется условие

$$x < y \coloneqq (x \leq y \land x \neq y) \tag{18.9}$$

Определение. Обратный порядок.

$$x \geq y \coloneqq (y \leq x) \tag{18.10}$$

C.3. Перестановки, сочетания и размещения

Существуют две градации выбора из множества A.

1. Выбор с учётом порядка и без учёта порядка.
2. Выбор с возвращением и без возвращения.

Определение. Размещением называется выбор с учётом порядка. Обозначается A_n^k для выбора без возвращения и $\overline{A_n^k}$ для выбора с возвращением.

Определение. Сочетанием называется выбор без учёта порядка. Обозначается C_n^k для выбора без возвращения и $\overline{C_n^k}$ для выбора с возвращением.

Предложение. Число размещений с повторениями равно

$$\overline{A_n^k} = n^k \tag{19.1}$$

□ По правилу произведения мы выбираем с возвращением по n элементов k раз. ■

Предложение. Число размещений без повторений равно

$$A_n^k = n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!} \tag{19.2}$$

Предложение. Число сочетаний без повторений равно

$$C_n^k = \frac{A_n^k}{k!} = \frac{n!}{(n-k)!k!} \tag{19.3}$$

Определение. Перестановкой из k называется размещение A_k^k.

Предложение. Число перестановок из k равно

$$P_k = A_k^k = k! \tag{19.4}$$

Теорема. Число сочетаний с повторениями равно

$$\overline{C_n^k} = C_{n+k-1}^k = \frac{(n+k-1)!}{k!(n-1)!} \tag{19.5}$$

Доказательство. □ Каждой выборке длины k можно взаимно однозначо сопоставить последовательность 0 и 1 длины $n+k-1$, где для входящих в неё элементов исходного множества будет количество единиц, равное количеству вхождений, а между буквами стоять перегородки в виде нулей. Последовательностей к k единицами ровно C_{n+k-1}^k. ■

C.3.1. Тождества с биномиальными коэффициентами

1. Симметричность:

$$C_n^k = C_n^{n-k} \tag{19.6}$$

Доказательство. □ Между сочетаниями из n по k и из n по $n-k$ существует взаимно однозначное соответствие: каждому сочетанию из k элементов соответствует дополнение до n элементов, состоящее из $n-k$ элементов, поэтому $C_n^k = C_n^{n-k}$. ■

2. Бином Ньютона. $\forall x, y \in \mathbb{R}$, $\forall n \in \mathbb{N}$:

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k} \tag{19.7}$$

Доказательство. □ Всего в произведении n скобок, и из каждой можно выбрать либо x, либо y.

$$\underbrace{(x+y)\cdot \ldots \cdot (x+y)}_{n \text{ скобок}} \tag{19.8}$$

Если мы k раз выбрали x, то y будет $(n-k)$ раз, а всего степень $x^k y^{n-k}$ встретится ровно столько раз, сколькими способами можно выбрать из n скобок k, то есть C_n^k, и это верно $\forall k = 0, \ldots, n$. ■

3. Сумма двух чисел в треугольнике Паскаля:

$$C_n^k = C_{n-1}^k + C_{n-1}^{k-1} \tag{19.9}$$

Доказательство. □ Рассмотрим множество всех k-сочетаний из $\{a_1, \ldots, a_n\}$. Их всего C_n^k. Но с другой стороны, это множество можно разбить на два непересекающихся подмножества: первое содержит a_1, а второе не содержит. Мощность первого равна C_{n-1}^k, а второго C_{n-1}^{k-1}, поэтому $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$. ■

В силу этого свойства биномиальные коэффициенты можно быстро выписать в треугольник Паскаля:

$$\begin{array}{c} 1 \\ 1\ 1 \\ 1\ 2\ 1 \\ 1\ 3\ 3\ 1 \\ 1\ 4\ 6\ 4\ 1 \\ \ldots\ldots\ldots\ldots \end{array} \tag{19.10}$$

4. Сумма чисел в одной строке треугольника Паскаля

$$C_n^0 + C_n^1 + ... + C_n^n = 2^n \tag{19.11}$$

Доказательство 1. □ Подставим в ((19.7)) $x = y = 1$, и получим

$$(1+1)^n = C_n^0 \cdot 1 \cdot 1 + ... + C_n^n \cdot 1 \cdot 1 \tag{19.12}$$

Что и требовалось доказать. ■

Доказательство 2. □ Количество строк из 0 и 1 длины n равно 2^n, для всех $k = 0, ..., n$ последовательностей с k единиц будет C_n^k, поэтому суммируя по всем k, получим, что сумма биномиальных коэффициентов равна 2^n. ■

5. Сумма квадратов биномиальных коэффициентов.

$$\left(C_n^0\right)^2 + \left(C_n^1\right)^2 + ... + \left(C_n^n\right)^2 = C_{2n}^n \tag{19.13}$$

Докахательство. □ Рассмотрим множество $\{a_1, ..., a_n, a_{n+1}, ..., a_{2n}\}$. Здесь C_{2n}^n n-сочетаний. Пусть k — количество объектов из n-сочетания, попавших в первые n. Значит в другой половине множества $(n-k)$ объектов. Всего способов выбрать k из левой половины и $(n-k)$ из правой: $C_n^k \cdot C_n^{n-k} = \left(C_n^k\right)^2$. Значит всего n-сочетаний есть

$$\sum_{k=0}^{n} \left(C_n^k\right)^2 = C_{2n}^n \tag{19.14}$$

■

6. Знакопеременная сумма биномиальных коэффициентов. Если $n \neq 0$, то

$$C_n^0 - C_n^1 + ... + (-1)^n C_n^n = 0 \tag{19.15}$$

C.3.2. Перестановки с повторениями

Определение. Последовательность из n_1 объектов типа $a_1, ... n_k$ объектов типа a_k, где все объекты задействованы, называется перестановкой с повторениями.

Предложение. Если есть n_1 объектов типа $a_1, ... n_k$ объектов типа a_k, то количество перестановок с повторениями равно

$$P(n_1, ..., n_k) = \frac{(n_1 + ... + n_k)!}{n_1! \cdot n_2! \cdot ... \cdot n_k!} \tag{19.16}$$

Доказательство. □ Согласно правилу произведения, обозначив $n = n_1 + ... + n_k$, имеем

$$P(n_1, ..., n_k) = C_n^{n_1} \cdot C_{n-n_1}^{n_2} \cdot ... \cdot C_{n_k}^{n_k} \tag{19.17}$$

■

C.3.3. Полиномиальная формула

Найдём по аналогии с биномом Ньютона разложение для $(x_1 + ... + x_k)^n$.

$$(x_1 + ... + x_k)^n = \underbrace{(x_1 + ... + x_k) \cdot ... \cdot (x_1 + ... + x_k)}_{n} \tag{19.18}$$

Пусть n_1 — число скобок, из которых берётся x_1, n_2 — число скобок, из которых берётся x_2, ..., n_k — число скобок, из которых берём x_k. Про эти числа можно сказать, что

$$\begin{cases} n_1 + ... + n_k = n \\ n_i \geq 0 \ \forall i = 1, ..., k \end{cases} \tag{19.19}$$

После раскрытия скобок и приведения подобных слагаемых получим, что при каких-то $n_1, n_2, ..., n_k$ будет такой полиномиальный коэффициент:

$$P(n_1, ..., n_k) \cdot x^{n_1} \cdot x^{n_2} \cdot ... \cdot x^{n_k} \tag{19.20}$$

Итак, полиномиальная формула получается суммой по всем таким слагаемым

$$(x_1 + ... + x_k)^n = \sum_{\substack{(n_1,...,n_k): \\ n_1+...+n_k=n \\ \forall i \ n_i \geq 0}} P(n_1, ..., n_k) \cdot x_1^{n_1} \cdot ... \cdot x_k^{n_k} \tag{19.21}$$

Следствие. Сумма полиномиальных коэффициентов равна

$$\sum_{\substack{(n_1,...,n_k): \\ n_1+...+n_k=n \\ \forall i \ n_i \geq 0}} P(n_1, ..., n_k) = k^n \tag{19.22}$$

C.3.4. Ещё одно тождество с биномиальными коэффициентами

Предложение.

$$C_{n+m-1}^{n-1} + C_{n+m-2}^{n-1} + ... + C_{n-1}^{n-1} = C_{n+m}^{n} \tag{19.23}$$

Доказательство. □ Рассмотрим множество $\{a_1, ..., a_n, a_{n+1}\}$ и все m сочетания с повторениями из него. С одной стороны, их

$$\overline{C_{n+1}^{m}} = C_{n+m}^{m} = C_{n+m}^{n} \tag{19.24}$$

С другой стороны, пусть $k = 0, ..., m$. Посчитаем все m-сочетания с повторениями, в которых ровно k раз встречается a_1. Их всего

$$\overline{C_n^{m-k}} = C_{n+m-k-1}^{m-k} = C_{n+m-k-1}^{n-1} \tag{19.25}$$

Суммируя по всем k, получим равенство из предложения. ■

Следствие 1. Сумма многих арифметических прогрессий. Подставляя $n = 3$, имеем

$$\frac{(m+2)(m+1)}{2} + \frac{(m+1)m}{2} + ... + \frac{2 \cdot 1}{2} = \frac{(m+3)(m+2)(m+1)}{6} \tag{19.26}$$

Следствие 1.1. Из ((19.26)) можно получить формулу суммы квадратов первых n натуральных чисел.

□

$$\frac{(m+1)^2}{2} + \frac{m+1}{2} + \frac{m^2}{2} + \frac{m}{2} + ... + \frac{1^2}{2} + \frac{1}{2} = \frac{(m+3)(m+2)(m+1)}{6} \tag{19.27}$$

Откуда

$$\frac{1}{2} \cdot (1^2 + ... + (m+1)^2) + \frac{1}{2} \cdot (1 + ... + (m+1)) = \frac{(m+3)(m+2)(m+1)}{6} \tag{19.28}$$

Выразим сумму квадратов

$$(1^2 + ... + (m+1)^2) = 2 \cdot \frac{(m+3)(m+2)(m+1)}{6} - 2 \cdot \frac{(m+2)(m+1)}{4} \tag{19.29}$$

итак

$$1^2 + ... + (m+1)^2 = \frac{(m+1)(m+2)(2m+3)}{6} \tag{19.30}$$

Теперь можно заменить $m + 1 = n$. ■

Аналогично, можно последовательно получать формулы суммы 3. 4, 5... степеней первых n натуральных чисел.

C.4. Формула включений-исключений

Теорема. Пусть даны объекты $\{a_1, ..., a_N\}$ и свойства $\{\alpha_1, ..., \alpha_n\}$. Обозначим $N(\alpha_i)$ количество объектов, обладающих свойством α_i. За $N(\alpha_i, \alpha_j)$ — количество объектов, обладающих свойствами α_i, α_j и так далее. За α_i' обзначим отрицание свойства α_i. Утверждается, что

$$N(\alpha_1', ..., \alpha_n') = N(\alpha_1) + ... + N(\alpha_n) - N(\alpha_1, \alpha_2) - ... - N(\alpha_{n-1}, \alpha_n) + \\ + ... + (-1)^n N(\alpha_1, ..., \alpha_n)$$

(слагаемых для набора из k свойств ровно C_n^k).

Доказательство. □ Докажем индукцией по n.

1. База. При $n = 1 : N(\alpha') = N - N(\alpha)$ — тривиально.
2. Предположение индукции. Пусть $\forall k \leq n, n \geq 1$ доказано, что

$$N(\alpha_1', ..., \alpha_k') = N(\alpha_1) + ... + N(\alpha_k) - N(\alpha_1, \alpha_2) - ... - N(\alpha_{k-1}, \alpha_k) + \\ + ... + (-1)^k N(\alpha_1, ..., \alpha_k) \tag{20.1}$$

3. Шаг индукции. Пусть $k = n + 1$. Для объектов $\{a_1, ..., a_N\}$ и свойств $\alpha_1, ..., \alpha_n, \alpha_{n+1}$ докажем утверждение. Применим к $a_1, ..., a_N, \alpha_1, ..., \alpha_n$ предположение индукции.

   Рассмотрим среди $a_1, ..., a_N$ те и только те объекты, которые обладают свойством α_{n+1}: их $N(\alpha_{n+1}) = M$. Тогда $\{b_1, ..., b_M\} \subseteq \{a_1, ..., a_N\}$. Применим предположение индукции к $b_1, ..., b_M, \alpha_1, ..., \alpha_n$

$$M(\alpha_1', ..., \alpha_n') = M - M(\alpha_1) - ... - M(\alpha - n) + ... + \\ + (-1)^n M(\alpha_1, ..., \alpha_n) \tag{20.2}$$

   Но

$$M(\alpha_1', ..., \alpha_n') = N(\alpha_1', ..., \alpha_n', \alpha_{n+1}) \tag{20.3}$$

   Поэтому вычитая одно из другого получим

$$N(\alpha_1', ..., \alpha_n') - N(\alpha_1', ..., \alpha_n', \alpha_{n+1}) = N - N(\alpha_1) - ... - N(\alpha_n) - \\ - N(\alpha_{n+1}) + N(\alpha_1, \alpha_2) + ... + N(\alpha_n, \alpha_{n+1}) - ... + (-1)^{n+1} N(\alpha_1, ..., \alpha_n, \alpha_{n+1}) \tag{20.4}$$

   Но $N(\alpha_1', ..., \alpha_n') - N(\alpha_1', ..., \alpha_n', \alpha_{n+1}) = N(\alpha_1', ..., \alpha_{n+1}')$. ■

C.4.1. Применение ФВИ

Рассмотрим множество $A = \{a_1, ..., a_n\}$ и число $m < n$. Рассмотрим все возможные m-размещения с повторениями: их $N = n^m$. Обозначим α_i свойство «a_i не входит в размещение». Тогда $N(\alpha_i) = (n-1)^m$, $N\big(\alpha_i, \alpha_j\big) = (n-2)^m$, ... $N(\alpha_1, ..., \alpha_n) = (n-n)^m$. Кроме того,

$$N(\alpha'_1, ..., \alpha'_n) = 0 \tag{20.5}$$

так как такое m-размещение должно содержать все n объектов, но $m < n$. По ФВИ имеем:

$$\sum_{k=0}^{n} (-1)^k C_n^k (n-k)^m = 0 \tag{20.6}$$

C.4.2. Вероятность беспорядка

Рассотрим такие перестановки n-элементного множества, где каждый элемент оказывается не на своём месте. Какова вероятность случайно получить такую перестановку(беспорядок)?

Решение. □ Всего $N = n!$ перестановок. Обозначим α_i — элемент i на своём месте. Ясно, что $N(\alpha_i) = (n-1)!$. Тогда Число беспорядков равно по ФВИ

$$N(\alpha'_1, ..., \alpha'_n) = n! - n \cdot (n-1)! + C_n^2 \cdot (n-2)! - ... + (-1)^n C_n^n \cdot 0! \tag{20.7}$$

Поэтому искомая вероятность равна

$$p_n = \frac{N(\alpha'_1, ..., \alpha'_n)}{n!} = \frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - ... + (-1)^n \frac{1}{n!} \approx e^{-1} \tag{20.8}$$

При $n \to \infty$ $p_n \to \frac{1}{e} \approx 0,36787$. ■

C.5. Функция Мёбиуса

Определение. Функцией Мёбиуса называется функция $\mu : \mathbb{N} \to \{-1, 0, 1\}$, по определению равная

$$\mu(n) = \begin{cases} 1, \text{ если } n = 1 \\ (-1)^s, \text{ если } n = p_1 \cdot ... p_s \\ 0, \text{ иначе} \end{cases} \tag{21.1}$$

где $p_1, ..., p_s$ — различные простые числа.

Лемма. Сумма значений функции Мёбиуса по делителям числа равна

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, \text{ если } n = 1 \\ 0, \text{ иначе} \end{cases} \tag{21.2}$$

Доказательство. □ Если $n = 1$, то утверждение тривиально. Пусть $n \geq 2$. Тогда согласно основной теореме арифметики, можно написать каноническое разложение

$$n = p_1^{\alpha_1} \cdot ... \cdot p_s^{\alpha_s} \tag{21.3}$$

Отсюда следует, что

$$d \mid n \Leftrightarrow d = p_1^{\beta_1} \cdot ... \cdot p_s^{\beta_s}, \tag{21.4}$$

где $0 \leq \beta_i \leq \alpha_i$ для всех $i = 1, ..., s$. ■

Тогда

$$\sum_{d \mid n} \mu(d) = \sum_{\beta_1 = 0}^{\alpha_1} ... \sum_{\beta_s = 0}^{\alpha_s} \mu\left(p_1^{\beta_1} \cdot ... \cdot p_s^{\beta_s}\right) \tag{21.5}$$

эту сумму можно переписать так

$$\sum_{\beta_1 = 0}^{1} ... \sum_{\beta_s = 0}^{1} \mu\left(p_1^{\beta_1} \cdot ... \cdot p_s^{\beta_s}\right) = C_s^0 + (-1) \cdot C_s^1 + C_s^2 + ... + (-1)^s C_s^s = 0. \tag{21.6}$$

C.5.1. Формула обращения Мёбиуса

Пусть $f(n)$ — функция натурального аргумента. Пусть $g(n) = \sum_{d \mid n} f(d)$. Тогда можно выразить f через g:

$$f(n) = \sum_{d \mid n} \mu(d) \cdot g\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \cdot g(d) \tag{21.7}$$

Доказательство. □ Запишем сумму значений g

$$\sum_{d \mid n} \mu(n) g\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu(d) \cdot \left(\sum_{d' \mid \frac{n}{d}} f(d') \right) = \sum_{(d,d'):d \cdot d' \mid n} \mu(d) \cdot f(d') =$$

$$= \sum_{d \mid n} f(d) \cdot \left(\sum_{d' \mid \frac{n}{d}} \mu(d') \right) = f(n) \cdot 1 + \sum_{\substack{d \mid n \\ d<n}} f(d) \cdot \underbrace{\left(\sum_{d' \mid \frac{n}{d}} \mu(d') \right)}_{0 \text{ по лемме}} = \tag{21.8}$$

$$= f(n)$$

Что и требовалось доказать. ■

C.5.2. Решение комбинаторной задачи

Пусть дан алфавит $X = \{b_1, ..., b_r\}$, n — длина слова. Надо найти $T_r(n)$ — количество всех возможных циклических слов длины n над алфавитом мощности r.

□ Пусть $a_1, ..., a_n$ — нециклическое слово, а $(a_1, ..., a_n)$ — циклическое слово, то есть класс эквивалентности обычных слов.

Если сделать n циклических сдвигов, то слово перейдёт в себя.

Определение. Назовём периодом линейного слова минимальное натуральное число d такое, что после d циклических сдвигов получается исходное слово. То есть $\sigma^d(a_1, ..., a_n) = (a_1, ..., a_n)$, где $\sigma \in S_n$ и при этом является циклом.

Лемма 1. У линейной последовательности длины n период d является делителем n.

Доказательство. □ Предположим, что $d \nmid n$. Тогда $n = d \cdot k + r$, где $1 \leq r \leq d - 1$. Применим $k \cdot d$ циклический сдвиг, и получим исходное слово $a_1, ..., a_n$. Далее применим ещё r сдвигов, и получается. что всего было сделано n сдвигов и должно получиться $a_1, ..., a_n$. Но d — минимальное число сдвигов, а $r < d$ — противоречие. ■

Лемма 2. Если длина линейного слова n и период d, то слово имеем вид:

$$\underbrace{\underbrace{a_1, ..., a_d}_{\text{блок периода } d} , a_1, ..., a_d, ...a_1, ..., a_d}_{\frac{n}{d} \text{ блоков}} \tag{21.9}$$

Обозначим V множество всех линейных последовательностей длины n над алфавитом X. Тогда $|V| = r^n$. Рассмотрим делители числа n: $1 = d_s < d_2 < ... < d_s = n$.

Пусть $V \supset V_i$ — множество всех линейных слов периода d_i. Тогда

$$V = \bigsqcup_{i=1}^{s} V_i \Rightarrow r^n = |V_1| + ... + |V_s| \tag{21.10}$$

Пусть W_i — множество всех линейных последовательностей длины d_i и периода d_i. Тогда $|W_i| = |V_i|$.

$$r^n = |W_1| + ... + |W_s| \tag{21.11}$$

Пусть U_i — множество всех циклических слов, которые можно получить из слов W_i. Тогда $d_i \cdot |U_i| = |W_i|$.

Если обозначить $M(d_i) := |U_i|$, то

$$r^n = \sum_{d \mid n} d \cdot M(d) \tag{21.12}$$

Чтобы воспользоваться формулой обращения Мёбиуса, можно сказать, что $g(n) = r^n$ и $f(n) = n \cdot M(n)$. Тогда

$$n \cdot M(n) = \sum_{d \mid n} \mu(d) \cdot r^{\frac{n}{d}} \tag{21.13}$$

Итак, мы получили $M(n)$ — количество циклических слов, которые получаются из линейных слов длины n и периода n:

$$M(n) = \frac{1}{n} \sum_{d \mid n} \mu(d) \cdot r^{\frac{n}{d}} \tag{21.14}$$

Теперь для любого циклического слова, в силу его разбиения на d-блоки, мы находим искомое значение $T_r(n)$:

$$T_r(n) = \sum_{d \mid n} M(d) = \sum_{d \mid n} \frac{1}{d} \cdot \left(\sum_{d' \mid d} \mu(d') \cdot r^{\frac{d}{d'}} \right) \tag{21.15}$$

C.5.3. Функция Мёбиуса на ЧУМе

Определение. Пусть $(P, \preccurlyeq)$ — частично упорядоченное множество, в котором верно, что $\forall x \in P \ \exists$ лишь конечное число $y : y \preccurlyeq x$. Тогда для $x, y \in P : x \preccurlyeq y$ функция Мёбиуса $\mu(x, y)$ определяется следующим образом:

$$\begin{gathered} \mu(x, x) = 1, \\ \mu(x, y) = - \sum_{x \preccurlyeq z \prec y} \mu(x, z), \text{если } x \prec y \end{gathered} \tag{21.16}$$

Теорема. Если $(P, \preccurlyeq) = (\mathbb{N}, |)$, то

$$\mu(x, y) = \mu\left(\frac{y}{x}\right) \tag{21.17}$$

Доказательство. □ Индукция по величине $\frac{x}{y}$.

1. База $\mu(x,x) = \mu\left(\frac{x}{x}\right) = 1$.
2. Предположим, что это верно и сделаем шаг индукции. Пусть отношение имеет каноническое разложение

$$y = x \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s} \tag{21.18}$$

Запишем обобщённую функцию Мёбиуса

$$\mu(x,y) = -\sum_{x \preccurlyeq z \prec y} \mu(x,z) \tag{21.19}$$

Распишем $z = x \cdot p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$, где $\forall i\ 0 \le \beta_i \le \alpha_i$, причём $\exists i : \beta_i < \alpha_i$, так как $z \prec y$ строго! Тогда

$$\mu(x,y) = -\sum_{x \preccurlyeq z \prec y} \mu\left(\frac{z}{x}\right) = -\sum_{\substack{(\beta_1,\ldots,\beta_s):\\ \forall i:\ 0 \le \beta_i \le \alpha_i,\\ \exists i : \beta_i < \alpha_i}} \mu\left(p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}\right) \tag{21.20}$$

2.1. Если все $\alpha_i = 1$, то

$$\mu(x,y) = -\sum_{\substack{(\beta_1,\ldots,\beta_s):\\ \forall i:\ 0 \le \beta_i \le 1,\\ \exists i : \beta_i < 1}} \mu\left(p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}\right) = -(C_s^0 - C_s^1 + \ldots \tag{21.21}$$

$$\ldots + (-1)^{s-1} C_s^{s-1}) = -(-(-1)^s C_s^s) = (-1)^s = \mu\left(\frac{y}{x}\right).$$

2.2. Если $\exists i : \alpha_i \ge 2$, то в суммировани в выкладке ((21.21)) появляется $(-1)^s C_s^s$, из-за чего сумма равна нулю, что и есть $\mu\left(\frac{y}{x}\right)$.

■

C.5.4. Обращение Мёбиуса на ЧУМе

Теорема. Пусть на $(P, \preccurlyeq)$ верно $g(y) = \sum_{x \preccurlyeq y} f(x)$. Тогда

$$f(y) = \sum_{x \preccurlyeq y} g(x) \cdot \mu(x,y) \tag{21.22}$$

Доказательство. □

$$\sum_{x \preccurlyeq y} \mu(x,y) \cdot \left(\sum_{z \preccurlyeq x} f(z)\right) = \sum_{z \preccurlyeq y} f(z) \cdot \left(\sum_{z \preccurlyeq x \preccurlyeq y} \mu(x,y)\right) \underset{\text{лемма}}{=} \sum_{z \preccurlyeq y} f(z) \cdot \mathbf{1}_{\{y=z\}}, \tag{21.23}$$

где $\mathbf{1}_{\{y=z\}}$ — индикатор.

Тогда

$$\sum_{x \preccurlyeq y} g(x) \cdot \mu(x, y) = f(y) \cdot 1 + \sum_{z \prec y} f(z) \cdot \mathbf{1}_{\{y=z\}} = f(y). \tag{21.24}$$

■

Теперь докажем лемму, использованную в доказательстве теоремы.

Лемма. Сумма значений функции Мёбиуса равна индикатору:

$$\sum_{z \preccurlyeq x \preccurlyeq y} \mu(x, y) = \mathbf{1}_{\{y=z\}} \tag{21.25}$$

Доказательство. □ Если $z = y$, то

$$\sum_{z \preccurlyeq x \preccurlyeq y} \mu(x, y) = \mu(y, y) = 1 = \mathbf{1}_{\{y=z\}}. \tag{21.26}$$

Если $z \prec y$, то рассмотрим два случая:

1. Между z и y нет других элементов. Тогда

$$\begin{aligned} \sum_{z \preccurlyeq x \preccurlyeq y} \mu(x, y) = \mu(y, y) + \sum_{z \preccurlyeq x \prec y} \mu(x, y) = 1 + \mu(z, y) = \\ = 1 - \sum_{z \preccurlyeq u \prec y} \mu(z, u) = 1 - \mu(z, z) = 0. \end{aligned} \tag{21.27}$$

2. Индукция по длине длиннейшей цепочки значков $\prec$ между z и y.

$$\begin{aligned} \sum_{z \preccurlyeq x \preccurlyeq y} \mu(x, y) = 1 + \sum_{z \preccurlyeq x \prec y} \mu(x, y) = 1 - \sum_{z \preccurlyeq x \prec y} \sum_{x \preccurlyeq u \preccurlyeq y} \mu(x, u) = \\ = 1 - \sum_{z \preccurlyeq u \prec y} \underbrace{\sum_{z \preccurlyeq x \preccurlyeq u} \mu(x, u)}_{\mathbf{1}_{\{z=u\}} \text{ по предп. инд.}} = 1 - 1 = 0. \blacksquare \end{aligned} \tag{21.28}$$

С.5.5. Пример применения обращения Мёбиуса на ЧУМе для доказательства ФВИ

Обозначим $\mathcal{R}_n = \{1, ..., n\}$. Рассмотрим ЧУМ $\left(2^{\mathcal{R}_n}, \subseteq\right)$.

Рассмотрим произвольные множества $A_1, ..., A_n$, необязательно элементы $2^{\mathcal{R}_n}$, и пусть $A = A_1 \cup A_2 \cup ... \cup A_n$.

Пусть $I \subseteq \mathcal{R}_n$.

Определим $f(I)$ как количество элементов из A, которые принадлежат всем множествам A_i при $i \notin I$ и могут как принадлежать, так и не принадлежать $A_i, i \in I$.

$$f(I) = \left| \bigcap_{i \notin I} A_i \right| \tag{21.29}$$

И пусть $g(I)$ это количество элементов из A, которые принадлежат всем множествам A_i при $i \notin I$ и не принадлежат ни одному A_i при $i \in I$.

Тогда можно разбить пересечение множеств на части:

$$f(I) = \sum_{I' \subseteq I} g(I') \tag{21.30}$$

И, используя формулу обращения Мёбиуса на ЧУМе, получаем

$$g(I) = \sum_{I' \subseteq I} f(I') \cdot \mu(I', I) \tag{21.31}$$

📕 *Лемма.* На ЧУМе $\left(2^{\mathcal{R}_n}, \subseteq\right)$ функция Мёбиуса имеет вид

$$\mu(I', I) = (-1)^{|I| - |I'|} \tag{21.32}$$

докажем её позже.

Если $I = \mathcal{R}_n$, то $g(I) = 0$, поэтому

$$0 = \sum_{I' \subseteq \mathcal{R}_n} f(I') \cdot (-1)^{n - |I'|} \cdot \left| \bigcap_{i \notin I'} A_i \right| = f(\mathcal{R}_n) + \sum_{I' \subset R_n} (-1)^{n - |I'|} \cdot \left| \bigcap_{i \notin I'} A_i \right| \tag{21.33}$$

Откуда можно найти мощность объединения, так как $f(\mathcal{R}_n) = \left| \bigcup_{i=1}^{n} A_i \right|$

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{I' \subset \mathcal{R}_n} (-1)^{n - |I'| + 1} \cdot \left| \bigcap_{i \notin I'} A_i \right| \tag{21.34}$$

Преобразуем через дополнение, получая ФВИ

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{\substack{J \neq \varnothing \\ J \subseteq \mathcal{R}_n}} (-1)^{|J| + 1} \cdot \left| \bigcap_{j \in J} A_j \right| \tag{21.35}$$

Доказательство леммы. □ Докажем индукцией по $|I| - |I'|$.

1. База. $|I| - |I'| = 0$. Тогда $\mu(I', I) = 1 = (-1)^0$. ✅
2. Шаг индукции. Пусть предположение верно, и мы знаем, что $I' \subset I$. Тогда

$$\mu(I', I) = - \sum_{I' \subseteq J \subset I} \mu(I', J) \tag{21.36}$$

Так как $|J| - |I'| < |I| - |I'|$, то по предположению индукции

$$\mu(I', J) = (-1)^{|J|-|I'|} \tag{21.37}$$

Поэтому

$$\begin{gathered}\mu(I', I) = -\sum_{I' \subseteq J \subset I} (-1)^{|J|-|I'|} = -\sum_{k=|I'|}^{|J|-1} (-1)^{k-|I'|} \cdot C_{|I|-|I'|}^{k-|I'|} = \\ = -\sum_{l=0}^{|I|-|I'|-1} (-1)^l \cdot C_{|I|-|I'|}^l = -\Big(-(-1)^{|I|-|I'|}\Big) = (-1)^{|I|-|I'|}. \blacksquare\end{gathered} \tag{21.38}$$

C.6. Разбиение чисел в суммы

Мы хотим для заданного $n \in \mathbb{N}$ подсчитать, сколькими способами можно сделать разбиение $n = x_1 + x_2 + ... + x_t$, где $x_i \in \mathbb{N}$.

Пусть $\forall i\ x_i \in \{n_1, ..., n_k\}$ Пусть $f(n; n_1, ..., n_k)$ — количество всех упорядоченных разбиений числа n на слагаемые $n_1, ..., n_k$.

Теорема. Рекуррента для $f(n; n_1, ..., n_k)$ имеет вид

$$f(n; n_1, ..., n_k) = f(n - n_1; n_1, ..., n_k) + ... + f(n - n_k; n_1, ..., n_k) \tag{22.1}$$

$$f(0; n_1, ..., n_k) = 1,\ \ f(-n; n_1, ..., n_k) = 0 \tag{22.2}$$

Следствие.

$$f(n; 1, 2, ..., n) = 2^{n-1} \tag{22.3}$$

Если же порядок не важен, вычислим по-другому. Пусть $F(n; n_1, ..., n_k)$

Теорема. Рекуррента для $F(n; n_1, ..., n_k)$ имеет вид

$$F(n; n_1, ..., n_k) = F(n - n_1; n_1, ..., n_k) + F(n; n_2, ..., n_k), \tag{22.4}$$

$$\begin{gathered} F\left(0; n_{i_1}, ..., n_{i_l}\right) = 1,\ \ F\left(-n; n_{i_1}, ..., n_{i_l}\right) = 0 \\ F(m; \varnothing) = 0 \end{gathered} \tag{22.5}$$

Обозначим $p(n) = F(n; 1, ..., n)$

Теорема(Харди-Рамануджана). Асимптотика $p(n)$ имеет вид:

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\frac{1}{\pi} \cdot \sqrt{\frac{2}{3}} \cdot \sqrt{n}} \tag{22.6}$$

C.6.1. Диаграмма Юнга

Пусть $n = x_1 + ... + x_t$, причём порядок неважен. Можно считать, что $x_1 \leq x_2 \leq ... \leq x_t$.

C.6.2. Теорема Эйлера о разбиениях

Пусть нам дано формальное произведение

$$(1 + x)(1 + x^2)(1 + x^3)... = 1 - x^2 - x^3 + x^5 + x^6 - x^8 - x^9 + x^{11} + ... \tag{22.7}$$

Теорема Эйлера. Коэффициент при x^n, если $n = \frac{3k^2 \pm k}{2}$ равен $(-1)^k$, иначе равен нулю.

Найдём коэффициент при $(x^n) : \left(-x^{k_1}\right) \cdot \left(-x^{k_2}\right) \cdot \ldots \cdot \left(-x^{k_t}\right) = (-1)^t x^{k_1+k_2+\ldots+k_t}$, $n = k_1 + \ldots + k_t$. Если n_e — число чётных слагаемых, n_o — нечётных.

Переформулировка. Тогда $n_e - n_o = (-1)^k$, где $n = \frac{3k^2 \pm k}{2}$, иначе $n_e = n_o$.

C.7. Линейнные рекуррентные соотношения

Пусть даны коэффициенты $a_0, a_1, ..., a_k \in \mathbb{C}$ и последовательность $\{y_n\}_0^\infty$. Линейным рекуррентным соотношением порядка k с постоянными коэффициентами называется соотношение $\forall n$:

$$a_k y_{n+k} + a_{k-1} y_{n+k-1} + ... + a_1 y_{n+1} + a_0 y_n = 0 \tag{23.1}$$

чтобы это имело смысл, необходимо, чтобы $a_k \neq 0$. Будем говорить, что это рекуррента k-го порядка, если $a_0 \neq 0$. Чтобы однозначно задать последовательность, необходимо задать k начальных значений $y_0, y_1, ..., y_{k-1}$.

C.7.1. Случай второго порядка

Если $k = 2$, мы полагаем $a_2 \neq 0$ и $a_0 \neq 0$ и хотим решить

$$a_2 y_n + a_1 y_{n-1} + a_0 y_{n-2} = 0 \tag{23.2}$$

🛠 Алгоритм. Чтобы решить рекурренту второго порядка, составим квадратное уравнение

$$a_2 x^2 + a_1 x + a_0 = 0 \tag{23.3}$$

и получим из него корни λ_1, λ_2.

Теорема. Пусть $\lambda_1 \neq \lambda_2$. Тогда

1. $\forall c_1, c_2 \in \mathbb{C}$ последовательность $y_n = c_1 \lambda_1^n + c_2 \lambda_2^n$ удовлетворяет исходной рекурренте.
2. Если последовательность $\{y_n\}_1^\infty$ удовлетворяет исходной рекурренте, то $\exists c_1, c_2 \in \mathbb{C}$: $y_n = c_1 \lambda_1^n + c_2 \lambda_2^n$.

Доказательство. □

1. Подставим эту линейную комбинацию в исходное соотношение.

$$\begin{gathered} a_2\left(c_1\lambda_1^{n+2} + c_2\lambda_2^{n+2}\right) + a_1\left(c_1\lambda_1^{n+1} + c_2\lambda_2^{n+1}\right) + a_0(c_1\lambda_1^n + c_2\lambda_2^n) = \\ = c_1\lambda^n(a_2\lambda_1^2 + a_1\lambda_1 + a_0) + c_2\lambda^n(a_2\lambda_2^2 + a_1\lambda_2 + a_0) \end{gathered} \tag{23.4}$$

   поэтому λ_1, λ_2 — это корни квадратного уравнения.

2. $\{y_n\}_1^\infty$ удовлетворяет исходной рекурренте. Составим СЛУ из 2 уравнений

$$\begin{cases} c_1 + c_2 = y_0 \\ c_1\lambda_1 + c_2\lambda_2 = y_1 \end{cases} \tag{23.5}$$

так как $\lambda_1 \neq \lambda_2$, то система определена, и пусть решения будут $(c_1^\star, c_2^\star)$. Рассмотрим последовательность $y_n^\star = c_1^\star \lambda_1^n + c_2^\star \lambda_2^n$, и ясно, что это та же самая последовательность, что и y_n.■

Теорема. Пусть $\lambda_1 = \lambda_2 = \lambda$. Тогда

1. $\forall c_1, c_2 \in \mathbb{C}$ последовательность $y_n = (c_1 n + c_2)\lambda^n$ удовлетворяет исходной рекурренте.
2. Если последовательность y_n удовлетворяет исходной рекурренте, то $\exists c_1, c_2$: $y_n = (c_1 n + c_2)\lambda^n$.

Доказательство. □

1. Подставим $y_n = (c_1 n + c_2)\lambda^n$ в рекурренту:

$$\begin{gathered} a_2(c_1(n+2)+c_2)\lambda^{n+2} + a_1(c_1(n+1)+c_2)\lambda^{n+1} + a_0(c_1 n + c_2)\lambda^n = \\ = c_1 n\lambda^{n(a_2\lambda^2+a_1\lambda+a_0)} + c_2\lambda^n(a_2\lambda^2 + a_1\lambda + a_0) + c_1\lambda^{n+1}(2a_2\lambda + a_1) = 0 \end{gathered} \tag{23.6}$$

2. Аналогично проверяется, что решение единственно. ■

C.7.2. Общий случай

Пусть дана рекуррента k-го порядка

$$a_k y_{n+k} + a_{k-1} y_{n+k-1} + \ldots + a_1 y_{n+1} + a_0 y_n = 0 \tag{23.7}$$

Составим с коэфициентами a_i характеристическое уравнение.

$$a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0 = 0 \tag{23.8}$$

Согласно основной теореме алгебры, у этого уравнения ровно k корней над полем $\mathbb{C}$, пусть $a_k(x-\lambda_1)(x-\lambda_2)\cdot\ldots\cdot(x-\lambda_k) = 0$.

Теорема. За $\mu_1, \ldots, \mu_r$ обозначим все различные числа среди $\lambda_1, \ldots, \lambda_k$. Обозначим $k_1, \ldots, k_r$ кратности корней характеристического многочлена. Тогда $k = k_1 + \ldots + k_r$. Обозначим $P_m(n) = c_m n^m + \ldots + c_1 n + c_0$, причём $\deg P_m \leq n$.

1. $\forall P_{k_1-1}(n), \ldots P_{k_r-1}$ последовательность

$$y_n = P_{k_1-1}(n)\mu_1^n + \ldots + P_{k_r-1}(n)\mu_r^n \tag{23.9}$$

удовлетворяет исходному соотношению.

2. Если $\{y_n\}_1^\infty$ удовлетворяет исходной рекурренте, то $\exists P_{k_1-1}(n), \ldots, P_{k_r-1}(n)$:

$$y_n = P_{k_1-1}(n)\mu_1^n + \ldots + P_{k_r-1}(n)\mu_r^n. \tag{23.10}$$

C.8. Формальные степенные ряды и производящие функции

Определение. Формальный степенной ряд — это последовательность $a_1, a_2, ..., a_n, ...$ Можно представлять его как формальное выражение $a_1 + a_2x + a_3x^2 + ...$

Обозначим $\mathcal{F}$ множество всех формальных степенных рядов.

Операции над формальными степенными рядами

1. $A + B = (a_0 + b_0, a_1 + b_1, ...)$
2. $\lambda \cdot A = (\lambda a_0, \lambda a_1, ...)$
3. $A \cdot B = (a_0b_0, a_0b_1 + a_1b_0, ..., a_0b_n + ... + a_nb_0, ...)$
4. $\frac{A}{B} = C \Leftrightarrow B \cdot C = A$. Для этого надо $b_0 \neq 0$

Такая структура называется алгеброй.

C.8.1. Примеры

1. Разделим формальные степенные ряды: 1 на $1 - x$:

$$\frac{1}{1-x} = 1 + x + x^2 + ... \tag{24.1}$$

2. Рассмотрим отношение $\left(\frac{1}{1-x^2}\right)^2$. Согласно предыдущему тождеству имеем:

$$\left(\frac{1}{1-x^2}\right)^2 = \left(1 + x^2 + x^4 + x^6 + ...\right)^2 = 1 + 2x^2 + 3x^4 + ... + (n+1)x^{2n} \tag{24.2}$$

Но с другой стороны,

$$\left(\frac{1}{1-x}\right)^2\left(\frac{1}{1+x}\right)^2 = (1 + x + x^2 + ...)^2(1 - x + x^2 + .. + (-1)^n x^n)^2 =$$
$$= (1 + 2x + 3x^2 + ... + (n+1)x^n + ...)(1 - 2x + 3x^2 + ... + (-1)^n(n+1)x^n ...) = \tag{24.3}$$
$$= ... + x^n(1 \cdot (-1)^n \cdot (n+1) + 2 \cdot (-1)^{n-1} \cdot n + ... + (n+1) \cdot (-1)^0 \cdot (n+1-n)).$$

Тогда

$$\sum_{k=0}^{n}(k+1) \cdot (-1)^n \cdot (n+1-k) = \begin{cases} 0, \text{если } \ 2 \nmid n \\ 2l, \text{иначе} \end{cases} \tag{24.4}$$

C.8.2. Производящие функции

Определение. Производящая функция последовательности $\{a\}_0^\infty$ это степенной ряд

$$f(x) = \sum_{n=0}^{\infty} a_n x^n \tag{24.5}$$

в аналитическом смысле.

Теорема(Коши-Адамара). Пусть

$$\rho = \left(\overline{\lim_{n\to\infty}} \sqrt[n]{|a_n|}\right)^{-1} \tag{24.6}$$

тогда $\forall x_0 : |x_0| < \rho$ ряд $\sum a_n x^n$ сходится, а $\forall x_0 : |x_0| > \rho$ ряд $\sum a_n x^n$ расходится.

Причём ряд можно почленно дифференцировать внутри области сходимости.

Примеры применения производящих функций:

1. Найдём сумму:

$$\sum_{k=0}^{n} k^2 C_n^k \cdot \left(\frac{2}{3}\right)^k \tag{24.7}$$

Рассмотрим сумму $\sum_{k=0}^{n} k^2 C_n^k x^k$. Введём функцию f:

$$f(x) = \sum_{k=0}^{n} C_n^k x^k = (1+x)^n. \tag{24.8}$$

Её производная равна

$$f'(x) = \sum_{k=0}^{n} k C_n^k x^{k-1}. \tag{24.9}$$

Домножим на x и возьмём производную ещё раз:

$$(x \cdot f'(x))' = \left(\sum_{k=0}^{n} k C_n^k x^k\right)' = \sum_{k=0}^{n} k^2 C_n^k x^{k-1} \tag{24.10}$$

Тогда

$$x \cdot (x \cdot f'(x))' = \sum_{k=0}^{n} k^2 C_n^k x^k. \tag{24.11}$$

Имея в виду, что $f'(x) = ((1+x)^n)' = n(1+x)^{n-1}$ и $f''(x) = n \cdot (n-1) \cdot (1+x)^{n-2}$, получим

$$\begin{gathered} x \cdot (x \cdot f'(x))' = x \cdot (f'(x) + x \cdot f''(x)) = \\ = x \cdot n \cdot (1+x)^{n-1} + x^2 \cdot n \cdot (n-1) \cdot (1+x)^{n-2} \end{gathered} \tag{24.12}$$

подставляем $x = \frac{2}{3}$ и получаем ответ для такой задачи.

2. Пусть F_n — последовательность чисел Фибоначчи с $F_0 = 0, F_1 = 1$. Найдём

$$\sum_{n=0}^{\infty} n^2 \cdot F_n \cdot \left(\frac{1}{3}\right)^n \tag{24.13}$$

Введём производящую функцию для чисел Фибоначчи:

$$f(x) = F_0 + F_1 x + F_2 x^2 + \ldots \tag{24.14}$$

$$x \cdot f(x) = x \cdot F_0 + F_1 x^2 + \ldots + F_n x^{n+1} + \ldots \tag{24.15}$$

$$x^2 f(x) = x^2 \cdot F_0 + F_1 x^3 + \ldots + F_n x^{n+2} + \ldots \tag{24.16}$$

Сложим $x \cdot f(x)$ и $x^2 f(x)$:

$$x \cdot f(x) + x^2 f(x) = F_0 x + (F_0 + F_1)x^2 + (F_1 + F_2)x^3 + \ldots + (F_{n-2} + F_{n-1})x^n + \ldots \tag{24.17}$$

Итак,

$$xf(x) + x^2 f(x) = f(x) - x \Rightarrow f(x) = \frac{x}{1 - x - x^2} \tag{24.18}$$

Теперь аналогично выражаем степенной ряд через производящую функцию и получаем ответ.

C.8.3. Числа Каталана

Определение. Числами Каталана называются элементы последовательности $\{T_n\}_0^\infty$, определённые рекуррентой:

$$\begin{gathered} T_n = T_0 T_{n-1} + T_1 T_{n-2} + \ldots + T_{n-1} T_0, \\ T_0 = 1 \end{gathered} \tag{24.19}$$

Теорема. Формула для чисел Каталана

$$T_n = \frac{1}{n+1} C_{2n}^n \tag{24.20}$$

Доказатательство. □ Запишем производящую функцию для этой последовательности, работая с ней как с формальным степенным рядом

$$f(x) = T_0 + T_1 x + T_2 x^2 + \ldots \tag{24.21}$$

Рассмотрим квадрат производящей функции:

$$\begin{gathered} f^2(x) = T_0^2 + (T_0 T_1 + T_1 T_0) \cdot x + \ldots + (T_0 T_n + \ldots + T_n T_0)x^n + \ldots = \\ = T_1 + T_2 x + \ldots + T_{n+1} x^n + \ldots \end{gathered} \tag{24.22}$$

$$xf^2(x) = f(x) - 1 \tag{24.23}$$

отсюда

$$x \cdot f_{1,2} = \frac{1 \pm \sqrt{1-4x}}{2} \tag{24.24}$$

Вариант с плюсом не подходит, так как при x = 0 получается противоречие. Итак, ПФ чисел Каталана равна

$$f(x) = \frac{1 - \sqrt{1-4x}}{2x}. \tag{24.25}$$

Можно показать, что корень из формального степенного ряда, определённый по правилу $B = \sqrt{A} \Leftrightarrow B \cdot B = A$, работает для $(1+x)^{\frac{1}{2}}$ так:

$$(1+x)^{\frac{1}{2}} = 1 + C^1_{\frac{1}{2}}x + C^2_{\frac{1}{2}}x^2 + ... \tag{24.26}$$

То есть формальный степенной ряд совпадает с рядом Тейлора для функции $\sqrt{1+x}$.

Напишем ряд для $\sqrt{1-4x}$ и посмотрим на коэфициенты при степенях больше нуля

$$\sqrt{1-4x} = ... + C^n_{\frac{1}{2}}(-4)^n x^n + ... \tag{24.27}$$

$$\begin{gathered} C^n_{\frac{1}{2}}(-4)^n = \frac{\frac{1}{2} \cdot \left(\frac{1}{2}-1\right) \cdot ... \cdot \left(\frac{1}{2}-n+1\right) \cdot (-4)^n}{n!} = \frac{(-1)^n \cdot 4^n}{2^n \cdot n!} \cdot (-1)^{n-1} \cdot (2n-3)!! = \\ = -\frac{2^n}{n!} \cdot \frac{(2n-2)!}{2 \cdot 4 \cdot 6 \cdot ... \cdot (2n-2)} = -\frac{2^n}{n!} \cdot \frac{(2n-2)!}{2^{n-1} \cdot (n-1)!} = -2 \cdot \frac{(2n-2)!}{n!(n-1)!} = -\frac{2}{n} C^{n-1}_{2n-2} \end{gathered} \tag{24.28}$$

Итак, коэфициент при x^n у функции $f(x)$ будет $\left(-\frac{1}{2}\right) \cdot \left(-\frac{2}{n}\right) C^{n-1}_{2n-2} = \frac{1}{n} C^{n-1}_{2n-2} = T_{n-1}$. ■

C.9. Основы теории графов

Определение. Граф — это пара множеств (V, E), где элементы $v \in V$ называются вершинами, а элементы $e \in E$ — рёбрами, причём $E \subseteq V^2$.

Определение. Граф $G(V, E)$ называется простым, если

1. $\forall x \in V : (x, x) \notin E$ (нет петель).
2. $\forall x, y \in V : (x, y) = (y, x)$ (неориентированный).
3. $E \subseteq 2^V$ (нет кратных рёбер).

Определение.

1. Граф с ориентацией называется орграфом.
2. Граф, где есть петли, называется псевдографом.
3. Граф, где есть кратные рёбра, называается мультиграфом.

Будем считать, что граф = простой граФ.

Определение. Маршрут в графе — это последовательность $v_1e_1v_2e_2...v_ne_nv_{n+1}$, где все $v_i \in V$, и все $e_i \in E$.

Определение. Маршрут $v_1e_1v_2e_2...v_ne_nv_{n+1}$ называется замкнутым, если $v_1 = v_{n+1}$.

Определение. Если в замкнутом маршруте все рёбра e_i разные, то он называется циклом, а если все вершины($\Rightarrow$ рёбра) кроме v_1 и v_{n+1} разные, то он называется простым циклом.

Определение. Если в незамкнутом маршруте $v_1e_1v_2e_2...v_ne_nv_{n+1}$ все рёбра разные, то он называется цепью(путём). Если дополнительно все вершины разные, то он называется простой цепью или простым путём.

Определение. Граф называется связным, если между любыми двумя его вершинами существует маршрут.

Определение. Степенью вершины $v \in V$ называется число рёбер, инцидентных с ней. Обозначается $\deg v$.

Очевидно, что для любого графа $G(V, E)$

$$\sum_{v \in V} \deg v = 2 \cdot |E|. \tag{25.1}$$

C.9.1. Деревья

Определение. Дерево — это связный граф без циклов.

Определение. Лист дерева — вершина степени 1. У любого дерева с больше чем одной вершиной есть листья.

Теорема. Пусть $G(V, E)$ — граф. Следующие 4 утверждения попарно эквиваленты:

1. G — дерево.
2. $\forall v, w \in V$ $\exists!$ цепь, соединяющая v и w.
3. G связен и $|E| = |V| - 1$.
4. G ацикличен и $|E| = |V| - 1$.

Эквивалентность можно очевидно доказать по циклу $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 1$.

Теорема(Формула Кэли). Пусть t_n — число деревьев на n вершинах. Тогла $t_n = n^{n-2}$.

Доказательство. □ Будем использовать коды Прюфера. Для любого дерева с больше чем одной вершиной поступим по такому алгоритму. Пусть у нас есть дерево на n вершинах.

1. Выберем из всех листьев текущего дерева лист с наименьшим номером.
2. Удалим выбранный лист и инцидентное ему ребро. Запишем в код справа номер единственного соседа удалённого листа.
3. Повторить с пункта 1, пока в дереве не останется 2 вершины.

Получили для данного дерева код длины $(n-2)$. Алгоритм декодирования выглядит так:

1. Запишем код Прюфера p_{n-2} и под ним кортеж из первых n натуральных чисел $s_n = (1, ..., n)$.
2. Будем для каждого следующего числа $x \in p_{n-2}$ будем искать в s_n наименьший номер y, которого нет в p_{n-2}. Записываем в ответ пару (x, y) — это ребро. Удаляем из p_n номер x и из s_n номер y.
3. Повторяем шаг 2 с получившимися s_n и p_{n-2} при $n \to (n-1)$, пока p_n не пуст.
4. Когда p_n пуст, остаётся в s_n только 2 ребра, выписываем их в ответ.

Можно доказать, что такое отображение из множества деревьев в множество из n^{n-2} кодов биективно. Отсюда следует формула Кэли. ■

Определение. Лесом называется ациклический граф, который состоит из одного или нескольких непересекающихся деревьев.

Теорема. Пусть $F(n,k)$ — количество лесов на n вершинах из k компонент связности. Тогда

$$F(n,k) = k \cdot n^{n-k-1} \tag{25.2}$$

C.9.2. Унициклические графы

Определение. Связный граф называется унициклическим, если в нём ровно один простой цикл.

Определение. Обозначим $C(n,k)$ связных количество графов на n вершинах, в которых ровно k рёбер.

- Если $k < n-1$, то граф не связен и $C_{n,k} = 0$
- Если $k = n-1$, то $C(n,n-1) = t_n = n^{n-2}$ (количество деревьев).
- Если $k = n$, то $C(n,n)$ — количество унициклических графов.

Найдём $C(n,n)$. Так как петель и кратных ребёр нет, то минимальный цикл это треугольник.

$$C(n,n) = \sum_{k=3}^{n} C_n^k \cdot \frac{(k-1)!}{2} \cdot F(n,k), \tag{25.3}$$

где $F(n,k)$ — количество лесов на n вершинах с k компонентами связности.

Итак,

Теорема. Количество унициклических графов на n вершинах равно

$$C(n,n) = \sum_{k=3}^{n} C_n^k \frac{(k-1)!}{2} \cdot k \cdot n^{n-k-1} \tag{25.4}$$

D. Теория вероятностей

D.1. Основные понятия

Определение. Случайный эксперимент это эксперимент, который обладает тремя свойствами

1. Повторяемость.
2. Отсутствие детерминистической регулярности.
3. Статистическая устойчивость частот.

Определение. Элементарным исходом w_i называется результат случайного эксперимента. Все Элементарные исходы образуют пространство элементарных исходов конечное или бесконечное множество Ω, причём элементарные исходы не могут происходить одновременно.

Определение. Вероятностным пространством называется тройка $(\Omega, \mathcal{F}, \mathbf{P})$, где $\Omega -$ множество, $\mathcal{F} -$ множество

$$\mathcal{F} = \{A \mid A \subseteq \Omega\}, \tag{26.1}$$

удовлетворяющее требованиям:

1. $\mathcal{F}$ замкнуто относительно операций $\cap, \cup, \setminus$ и $\triangle$.
2. $\forall A_1, A_2, ... \in \mathcal{F}$:

$$\bigcup_{n=1}^{\infty} A_n \in \mathcal{F}, \tag{26.2}$$

а $\mathbf{P} -$ функция: $\mathcal{F} \to [0, 1]$, удовлетворяющая требованиям:

1. $\mathbf{P}(\Omega) = 1$
2. $\forall A_1, ..., A_n, ... \in \mathcal{F}$:

$$\mathbf{P}\left(\bigsqcup_{n=1}^{\infty} A_n\right) = \sum_{n=1}^{\infty} \mathbf{P}(A_n) \tag{26.3}$$

D.2. Случайная величина

Будем обозначать случайные величины прописными греческими буквами($\xi, \eta, ..$).

1. Для дискретных случайных величин множество значений или конечно, или бесконечно, но счётно.
2. Для непрерывных случайных величин множество значений равномощно $\mathbb{R}$.

Универсальным законом распределения и непрерывных, и дискретных случайных величин является *функция распределения*(ф. р.).

По определению, функция распределения F_ξ для случайной величины ξ определяется как вероятность события $\{\xi < x\}$.

$$F_\xi := P(\xi < x) \tag{27.1}$$

D.2.1. Свойства функции распределения случайной величины

Пусть ξ - случайная величина.

1. $0 \leq F_\xi(x) \leq 1, \ \forall x \in \mathbb{R}$,
2. $F_\xi(-\infty) = F_\xi(\xi < -\infty) = 0$,
3. $F_\xi(+\infty) = F_\xi(\xi < \infty) = 1$,
4. $F_\xi \nearrow$ (функция распределения монотонно не убывает на всей области определения).

   □ Пусть $x_1 < x_2$ и x_1, x_2 входят в область значений случайной величины ξ. Тогда $F_\xi(x_2) = P(\xi < x_2) = P(\{\xi < x_1\} \cup \{x_1 \leq \xi < x_2\}) = P(\xi < x_1) + P(x_1 \leq \xi < x_2) \geq P(\xi < x_1) = F_\xi(x_1)$ ■

D.3. Основные распределения

D.3.1. Непрерывные распределения

D.3.1.1. Нормальное распределение

Нормальное распределение задается функцией плотности

$$p(x) = \frac{1}{\sqrt{2\pi} \cdot \sigma} e^{-\frac{(t-\mu)^2}{2\sigma^2}} \tag{28.1}$$

Функция распределения $\xi \sim N(\mu, \sigma)$

$$F_\xi(x) = P(\xi < x) = \frac{1}{\sqrt{2\pi} \cdot \sigma} \int\limits_{-\infty}^{x} e^{-\frac{(t-\mu)^2}{2\sigma^2}} dt \tag{28.2}$$

Определим для стандартного нормального распределения $\xi \sim N(0, 1)$

$$\Phi(x) = F_\xi(x) = \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{x} e^{-\frac{t^2}{2}} dt \tag{28.3}$$

Напомним, что функция лапласа $\Phi_0(x)$ определяется как

$$\Phi_0(x) = \frac{1}{\sqrt{2\pi}} \int\limits_{0}^{x} e^{-\frac{t^2}{2}} dt \tag{28.4}$$

Тогда

$$\Phi(x) = \frac{1}{2} + \Phi_0(x) \tag{28.5}$$

$$\begin{gathered} F_\xi(x) = \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{x} e^{-\frac{t^2}{2}} dt = \left[\frac{t-\mu}{\sigma} = z\right] = \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{\frac{x-\mu}{\sigma}} e^{-\frac{z^2}{2}} dz = \\ = \Phi\left(\frac{x-\mu}{\sigma}\right) = \frac{1}{2} + \Phi_0\left(\frac{x-\mu}{\sigma}\right) \end{gathered} \tag{28.6}$$

Вероятность попадания в заданный интервал. Пусть $\xi \sim N(\mu, \sigma)$. Найдём $P(\xi \in [\alpha, \beta])$

$$\begin{gathered} P(\xi \in [\alpha, \beta]) = F_\sigma(\beta) - F_\sigma(\alpha) - \Phi\left(\frac{\beta - m}{\sigma}\right) - \Phi\left(\frac{\alpha-\mu}{\sigma}\right) = \\ = \Phi_0\left(\frac{\beta - m}{\sigma}\right) - \Phi_0\left(\frac{\alpha-\mu}{\sigma}\right) \end{gathered} \tag{28.7}$$

Для симметричного интервала получим:

$$P(|\xi - \mu| \leq \delta) = 2\Phi_0\left(\frac{\delta}{\sigma}\right) \tag{28.8}$$

«Правило 3-х сигм». Пусть $\delta = 3\sigma$

$$P(|\sigma - \mu| < 3\sigma) = 2\Phi_0(3) \approx 0.9974 \tag{28.9}$$

D.3.1.2. Сводная таблица для нормального распределения

D.3.2. Универсальный двумерный закон распределения

Для двух случайных величин совместная функция распределения.

$$F_{\xi,\eta}(x, y) = P(\xi < x, \eta < y) = P(\{\xi < x\} \cap \{\eta < y\}) \tag{28.10}$$

Свойства двумерной функции распределения

1. $0 \leq F_{\xi,\eta}(x, y) \leq 1, \ \forall x, y \in \mathbb{R}$
2. Значения на бесконечности

$$F_{\xi,\eta}(+\infty, +\infty) = P(\Omega) = 1 \tag{28.11}$$

$$F_{\xi,\eta}(-\infty, -\infty) = P(\varnothing) = 0 \tag{28.12}$$

3. Формулы согласованности

$$F_{\xi,\eta}(x, +\infty) = P(\xi < x) = F_\xi(x) \tag{28.13}$$

$$F_{\xi,\eta}(+\infty, y) = P(\eta < y) = F_\eta(y) \tag{28.14}$$

4. Монотонное возрастание.

$$F_{\xi,\eta}(x, y) \nearrow \text{ на } \mathbb{R}^2 \tag{28.15}$$

5. Вероятность попадания в прямоугольную область. Если

$$\begin{cases} x_1 \leq x \leq x_2 \\ y_1 \leq y \leq y_2 \end{cases} \tag{28.16}$$

то вероятность попадания в данный прямоугольник

$$\begin{gathered} P(x_1 \leq \xi \leq x_2, y_1 \leq \eta \leq y_2) = \\ = F(x_2, y_2) - F(x_1, y_2) - F(x_2, y_1) + F(x_1, y_1) \end{gathered} \tag{28.17}$$

D.3.3. Независимость случайных величин

Определение. Случайные величины ξ, η называются независимыми, если события $A = \{\xi < x\}$ и $B = \{\eta < y\}$ независимы $\forall x, y \in \mathbb{R}$.

Из определения независимости СВ ясно, что

$$P(A) \cdot P(B) = P(A \cap B) \tag{28.18}$$

Условие независимости двух случайных величин.

$$F_{\xi,\eta} = F_{\xi}(x) + F_{\eta}(y) \Leftrightarrow \xi, \eta \text{ независимы} \tag{28.19}$$

D.3.4. Дискретная система случайных величин

Можно построить двумерную таблицу, аналогичную ряду распределения.

ξ^{η}	y_1	y_2	$\dots$	y_n
y_1	p_{11}	p_{12}	$\dots$	p_{1n}
y_2	p_{21}	p_{22}	$\dots$	p_{2n}
$\vdots$	$\dots$	$\dots$	$\dots$	$\dots$
y_m	p_{m1}	p_{m2}	$\dots$	p_{mn}

Условие независимости для дискретных случайных величин.

E. Алгоритмы и структуры данных && программирование

E.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*

E.1.1. Анализ сложности и эффективности алгоритмов

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 компъютера.

Измеренеия 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.

E.2. Асимптотические оценки функций

Далее при анализе алгоритмов будем полагать, что все функции асимптотически положительны.

1. Функция $f(n)$ принадлежит О-большому от функции $g(n)$, если существуют такие положительные константы C и N, что для всех $n > N$ функция $f(n)$ ограничена сверху функцией $g(n)$, умноженной на константу C.

$$f(n) = O(g(n)) \Leftrightarrow \exists N, C > 0 : \forall n > N : f(n) \leq C \cdot (g(n) \tag{30.1}$$

2. Функция $f(n)$ принадлежит Омега-большому от функции $g(n)$, если существуют такие положительные константы C и N, что для всех $n > N$ функция $f(n)$ ограничена снизу функцией $g(n)$, умноженной на константу C.

$$f(n) = \Omega(g(n)) \Leftrightarrow \exists N, C > 0 : \forall n > N : f(n) \geq C \cdot g(n) \tag{30.2}$$

3. Функция $f(n)$ принадллежит тетта-большому от функции $g(n)$, если существуют такие положительные константы C_1, C_2 и N, что для всех $n > N$ функция $f(n)$ ограничена сверху и снизу функцией $g(n)$, умноженной на константы C_1 и C_2 соответственно.

$$\begin{gathered} f(n) = \Theta(g(n)) \Leftrightarrow \exists N, C_1, C_2 > 0 : \forall n > N : \\ C_1 \cdot g(n) \leq f(n) \leq C_2 \cdot g(n) \end{gathered} \tag{30.3}$$

4. Функция $f(n)$ принадлежит о-малому от функции $g(n)$, если предел отношения f и g равен нулю при неограниченном возрастании n.

$$f(n) = o(g(n)) \Leftrightarrow \lim_{n \to \infty} \frac{f(n)}{g(n)} = 0 \tag{30.4}$$

5. Функция $f(n)$ принадлежит омега-малому от функции $g(n)$, если предел отношения g и f равен нулю при неограниченном возрастании n.

$$f(n) = \omega(g(n)) \Leftrightarrow \lim_{n \to \infty} \frac{g(n)}{f(n)} = 0 \tag{30.5}$$

E.2.1. Свойства сравнений функций

1. Транзитивность.
   - из $f(n) = \Theta(g(n))$ и $g(n) = \Theta(h(n))$ следует $f(n) = \Theta(h(n))$
   - из $f(n) = O(g(n))$ и $g(n) = O(h(n))$ следует $f(n) = O(h(n))$
   - из $f(n) = \Omega(g(n))$ и $g(n) = \Omega(h(n))$ следует $f(n) = \Omega(h(n))$

- из $f(n) = o(g(n))$ и $g(n) = o(h(n))$ следует $f(n) = o(h(n))$
- из $f(n) = \omega(g(n))$ и $g(n) = \omega(h(n))$ следует $f(n) = \omega(h(n))$

2. Рефлексивность.
   - $f(n) = \Theta(f(n))$
   - $f(n) = O(f(n))$
   - $f(n) = \Omega(f(n))$
3. Симметричность.
   - $f(n) = \Theta(g(n)) \Rightarrow g(n) = \Theta(f(n))$
4. Перестановочная симметрия.
   - $f(n) = O(g(n)) \Leftrightarrow g(n) = \Omega(f(n))$
   - $f(n) = o(g(n)) \Leftrightarrow g(n) = \omega(f(n))$

E.3. Бинарный поиск

Классический бинарный поиск это алгоритм поиска на отсортированном массиве со значениями в диапазоне $[a; b]$. Ниже приведён псевдокод для этого алгоритма.

```
fun binary_search(array, x):
  n = array.len()
  l, r = 0, n-1
  while l <= r:
    mid = (l + r) / 2
    if arr[mid] == x:
      return mid
    if array[mid] < x:
      l = mid + 1
    else:
      r = mid - 1
  return -1
```

Временная сложность данного алгоритма равна $O(\log n)$.

E.3.1. Вариант с поиском границ

1. Если требуется найти **левую** границу, когда требуемое условие выполняется, то можно использовать такой алгоритм.

   ```
   fun left_binary_search(l, r, check, checkparams):
     while l < r:
       mid = (l + r)/2
       if check(mid, checkparams):
         r = mid
       else:
         l = mid + 1
     return l
   ```

2. Если требуется найти **правую** границу, когда требуемое условие выполняется, то можно использовать такой алгоритм.

```
fun right_binary_search(l, r, check, checkparams):
  while l < r:
    mid = (l + r + 1)/2
    if check(mid, checkparams):
      l = mid
    else:
      r = mid - 1
  return l
```

На практике, лучше проверять реализацию бинпоиска на 2-х числах!

E.4. Динамическое программирование

Динамическое программирование(ДП) позволяет решать задачи, комбинируя решения вспомогательных задач.

Два варианта задач для решения методом динамического программирования:

- подсчёт количества способов;
- оптимизация(максимум или минимум).

Этапы решения задачи методом ДП.

1. Описание структуры оптимального решения;
2. Реккурентное соотношение для значения, соответствующего оптимальному решению(включая базу динамики);
3. Вычисление значения, соответствующего оптимальному решению методом восходящего анализа.
4. Составление оптимального решения, полученного на предыдущих этапах.

E.4.1. Простые примеры ДП

E.4.1.1. Ступеньки

За один шаг можно подняться на одну или две ступеньки. За посещение каждой из ступенек дают a_i рублей. Необходимо найти максимальную сумму за подъём на вершину лестницы из n ступенек.

Решение: Пусть $dp[i]$ - максимальная сумма за подъём на i-ю ступеньку. Тогда

$$dp[i] = a[i] + \max(dp[i-1], dp[i-2]) \tag{32.1}$$

База динамики. $dp[0] = 0$, $dp[1] = a[1]$. Ответ: $dp[n]$ ■.

Полученное решение имеет временную и пространственную сложность $\Theta(n)$. Пример таблицы для данной задачи(0 добавлен в качестве нулевого элемента).

$a[i]$	0	10	-5	-20	-10	20	30	-10	10
$dp[i]$	0	10	5	-10	-5	15	45	35	55

E.4.1.2. Ступеньки с сертификатом

За один шаг можно подняться на одну или две ступеньки. За посещение каждой из ступенек дают a_i рублей. Необходимо найти максимальную сумму за подъём на вершину лестницы из n ступенек. Вывести *номера ступенек*, по которым мы шагали.

Решение: Пусть $dp[i]$ - максимальная сумма за подъём на i-ю ступеньку. Выделим массив $prev[n]$, в i-том элементе которого будем хранить номер ступепньки, с которой мы попали на i-ю ступеньку. Тогда

$$dp[i] = a[i] + \max(dp[i-1], dp[i-2]) \tag{32.2}$$

$$prev[i] = \underset{i}{\operatorname{argmax}}(dp[i-1], dp[i-2]) \tag{32.3}$$

База динамики. $dp[0] = 0$, $dp[1] = a[1]$ и теперь добавляется $prev[1] = 0$. Ответ: $dp[n]$ ■.

Пример таблицы для данной задачи:

$a[i]$	0	10	-5	-20	-10	20	30	-10	10
$dp[i]$	0	10	5	-10	-5	15	45	35	55
$prev[i]$	0	0	1	1	2	4	5	6	6

E.4.1.3. Наибольшая возрастающая подпоследовательность

Задача: найти длину наибольшей возрастающей подпоследовательности в массиве a.

- *подпоследовательность* — подпоследовательность, полученная вычёркиванием некоторых элементов из исходной(необязательно подряд идущих);
- *возрастающая* — $\forall i \in \overline{1..n} : a_{i+1} > a_i$.
- *наибольшая* — максимальная по длине среди всех подходящих подпоследовательностей.

Решение. Пусть $dp[i]$ - длина наибольшей возрастающей подпоследовательности, заканчивающейся на i-ом элементе. Будем для очереднего элемента $a[i]$ запускать внутренний цикл на отрезке от 0 до $i-1$ и проверять, можно ли продлить возрастающую подпоследовательность элементом $a[i]$. Если да, то берём максимум из всех подходящих $dp[j]$ $(j < i)$. Если нет, то записываем $prev[i] = -1$ и $a[i] = 1$. Ответ на задачу: $\max(dp[i])$.

К сожалению, временная сложность этого решения $\Theta(n^2)$. Пример таблицы ниже. Жёлтым выделены индексы НВП, зелёным максимум динамики(ответ), а красным те элементы, у которых нет предшественников.

индекс	0	1	2	3	4	5	6
$a[i]$	4	10	5	12	3	24	7
$dp[i]$	1	2	2	3	1	4	3
$prev[i]$	-1	0	0	1	-1	3	2

Приведём решение за $O(n \log n)$.

E.4.1.4. Покупка билетов

В очереди за билетами стоит n людей. $i-$ й человек может купить себе билет за A_i секунд. Себе и следующему за B_i секунд. Себе, следующему и ещё одному за ним за C_i секунд. Найти минимальное время, за которое все люди будут с билетами.

Решение. Пусть $dp[i]$ - минимальное время обилечивания первых i людей. Тогда реккурентное соотношение будет иметь вид:

$$\begin{aligned} dp[i] = \max(&dp[i-1] + A_i, \\ &dp[i-2] + B_i, \\ &dp[i-3] + C_i) \end{aligned} \tag{32.4}$$

В качестве базы динамики запишем 3 виртуальных человека с бесконечным временем покупки, чтобы начинать использовать реккуренту с $n = 1$ и определим для них динамику, равную 0. Сложность решения по времени равна $\Theta(n)$.

Пример таблицы для этой задачи ниже.

№	A_i	B_i	C_i	$dp[i]$
-2	∞	∞	∞	0
-1	∞	∞	∞	0
0	∞	∞	∞	0
1	5	10	15	5
2	2	10	15	7
3	5	5	5	12
4	20	20	1	12
5	20	1	1	12

E.4.1.5. Представление числа минимальной последовательностью операций

Дано целое число $N \leq 10^4$. Представить его в виде арифметического выражения *миинимальной длины*, в котором используются только операции сложения, умножения и скобки, а все числа не превосходят K.

Решение. Пусть $dp[i]$ - минимальная длина арифметического выражения для числа i.

E.4.2. Двумерное динамическое программирование

E.4.2.1. Наибольшая общая подпоследовательность

Наибольшая общая подпоследовательность (НОП) двух последовательностей - это максимальная по длине подпоследовательность, которую можно получить вычеркиванием некоторых элеменнтов из первой и из второй последовательности.

Задача. Даны две последовательности a и b. Найти НОП для этих последовательностей.

Решение. Пусть $dp[i][j]$ - длина НОП для первых i элементов последовательности a и первых j элементов последовательности b. Обозначим $n = |a|,\ m = |b|$.

1. Если $a[i] = b[j]$, то $dp[i][j] = dp[i-1][j-1] + 1$ (если элементы совпали, то мы берём данный элемент в НОП).
2. Иначе, как минимум один из элементов $a[i]$ или $b[j]$ не входит в НОП. Тогда $dp[i][j] = \max(dp[i-1][j], dp[i][j-1])$.

Итак,

$$dp[i][j] = \begin{cases} 0, \text{если } i \cdot j = 0 \\ dp[i-1][j-1] + 1, \quad \text{если } a[i] = b[j] \\ \max(dp[i-1][j], dp[i][j-1]), \quad \text{если } a[i] \neq b[j] \end{cases} \tag{32.5}$$

Длина НОП равна $dp[n-1][m-1]$. Для восстановления ответа поднимаемся по таблице dp в обратном порядке по следующему алгоритму:

1. Если $a[i] = b[j]$, то добавляем этот элемент в НОП и переходим к $dp[i-1][j-1]$.
2. Иначе, переходим к $dp[i-1][j]$ или $dp[i][j-1]$, а точнее к тому из них, который имеет большее значение.

Сложность нахождения длины НОП по времени равна $\Theta(n \cdot m)$. Для восстановления ответа потребуется ещё $O(n + m)$ времени.

E.4.2.2. Расстояние Левенштейна

Расстояние Левенштейна(редакционное расстояние) между двумя строками - это минимальное количество операций (вставка, удаление, замена), необходимых для преобразования одной строки в другую.

Задача. Даны две строки s и t. Найти расстояние Левенштейна между ними.

Решение. Пусть $dp[i][j]$ - расстояние Левенштейна между первыми i символами строки s и первыми j символами строки t. Обозначим $n = |s|,\ m = |t|$.

1. Если $s[i] = t[j]$, то $dp[i][j] = dp[i-1][j-1]$.
2. Иначе, $dp[i][j] = \min(dp[i-1][j] + 1, dp[i][j-1] + 1, dp[i-1][j-1] + 1)$.

Итак, расстояние Левенштейна между строками s и t равно $dp[n-1][m-1]$. Этот алгоритм работает за $\Theta(n \cdot m)$.

F. Анализ данных