Lomonosov Moscow
State University

Механико-математический факультет

Алгебра, 1 семестр, 2 поток

Преподаватель:	Куликова Ольга Викторовна
Студент:	Молчанов Вячеслав
Группа:	108
Контакт:	Мой телеграм для связи

Москва
Последняя компиляция: 26 декабря 2024 г.

Содержание

1 Система линейных уравнений

1.1 Матрица. Основные понятия

Определение. Матрица A размера $m \times n$ - это прямоугольная таблица с m строками и n столбцами:

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

a_{ij} - элемент матрицы и индексы:

- i - номер строками
- j - номер столбца

$M_{m\times n}(\mathbb{R})$ - Множество всех матриц размера $m \times n$ с элементами из $\mathbb{R}$

Матрица $m \times 1$ называется столбцом:

$$A = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix}$$

Если $A = (a_{ij})$ - квадратная, $a_{ij} = 0 \ \forall i \neq j$, то A называется диагональной.

$$A = \begin{pmatrix} a_{11} & & & 0 \\ & a_{22} & & \\ & & \ddots & \\ 0 & & & a_{nn} \end{pmatrix}$$

Если A - диагональноая и $a_{ii} = 1$, то A называется единичной.

$$A = \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$$

Если A - квадратная, то

- $A = \begin{pmatrix} a_{11} & & \\ & \ddots & \\ & & a_{nn} \end{pmatrix}$ главная диагональ
- $A = \begin{pmatrix} & & a_{1n} \\ & \dots & \\ a_{n1} & & \end{pmatrix}$ побочная диагональ

Определение. Если A - размера $m \times n$, $a_{ij} = 0 \ \forall i, j$, то A называется нулевой.

1.2 Система линейных (алгебраических) уравнений

$$(*) \begin{cases} a_{11}x_1 + ... + a_{1n}x_n = b_1 \\ a_{21}x_2 + ... + a_{2n}x_n = b_2 \\ \vdots \\ a_{n1}x_1 + ... + a_{nn}x_n = b_n \end{cases}$$

где $a_{ij}, b \in \mathbb{R}, x_1, ..., x_n$ - неизвестные.

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \qquad B = \begin{pmatrix} a_{11} \\ \vdots \\ b_n \end{pmatrix}$$

A - матрица коэффициентов, a_{ij} называется коэффициентом СЛУ.
B - столбец свободных членов, b_j - свободный член.

Определение. Расширенная матрица $\underset{m\times(n+1)}{(A|B)}$. Набор чисел $x_1^0, ..., x_n^0 \in \mathbb{R}$ называется решением системы $(*)$, если подстановка этих чисел вместо неизвестных в $(*)$ дает тождество в каждом уравнении. $(x_i^0 \longleftrightarrow x)$

Решить систему - это найти все решения системы. Любое конкретное решение называется частным.

Определение. Если СЛУ имеет решение, то она называется совместной, иначе - несовместной.

Определение. Совместная система, имеющая одно решение, называется определенной, иначе - неопределенной (более одного решения).

1.3 Элементарные преобразования над СЛУ

Определение. Элементарные преобразования над СЛУ:

1. Прибавить к одному уравнению другое уравнение, умноженное на число $\lambda \in \mathbb{R}$
2. Поменять местами два уравнения
3. Умножить уравнение на ненулевое число $\mu \in \mathbb{R}$

Утверждение. Эти преобразования обратимы.

Определение. Две системы линейных уравнений называются эквивалентными, если их множества решений совпадают.

Утверждение. Если одна СЛУ получена из другой СЛУ с помощью конечного числа элементарных преобразований, то эти системы эквивалентны.

Доказательство.

$\Longrightarrow$ $AX = B$ - исходная система, $\tilde{A}X = \tilde{B}$ преобразованная система.
Пусть $z_1, ..., z_n$ некотороое решение $AX = B$. Будем рассматривать $\tilde{A}X = \tilde{B}$, в ней ЭП III типа умножают строку на μ, имеем:

$$a_{i1}x_1 + ... + a_{in}x_n = b_i \text{ в } AX = B$$

$$\mu a_{i1}x_1 + ... + \mu a_{in}x_n = \mu b_i \text{ в } \tilde{A}X = \tilde{B}$$

Выносим μ из второго уравнения:

$$\mu(a_{i1}x_1 + ... + a_{in}x_n) = \mu b_i$$

Получаем, что $z_1, ..., z_n$ решение для $\tilde{A}X = \tilde{B}$. Для II типа ЭП очевидно. Теперь рассмотрим I тип, будем к i-ой строчке прибавлять j-ую с коэффициентом λ, получаем:

$$\begin{aligned}(a_{i1} + \lambda a_{j1})x_1 + ... + (a_{in} + \lambda a_{jn})x_n = \\ = a_{i1}x_1 + \lambda a_{j1}x_1 + ... + a_{in}x_n + \lambda a_{jn}x_n = \\ = a_{i1}x_1 + ... + a_{in}x_n + \lambda(a_{j1}x_1 + ... + a_{jn}x_n) = b_i + \lambda b_j\end{aligned}$$

Таким образом, любое решение старой СЛУ - это и решение новой, то есть множество решений не уменьшилось. (со столбцами все то же самое)

$\Longleftarrow$ В обратную сторону аналогично (для доказательства эквивалентности), используя обратимость элементарных преобразований.

□

Мораль в том, что мы можем работать с расширенной матрицей $(A|B)$.

1.4 Элементарные преобразования над матрицами

Элементарные преобразования над строками:

$$A = \begin{pmatrix} \overline{a_1} \\ \overline{a_2} \\ \vdots \\ \overline{a_i} \end{pmatrix}, \text{ где } \overline{a_i} - \text{строка}$$

- ЭП1: $\overline{a_i} \to \overline{a_i} + \lambda\overline{a_i}$
- ЭП2: $\overline{a_i} \longleftrightarrow \overline{a_j}$
- ЭП3: $\overline{a_i} \to \mu\overline{a_i},\ \mu \neq 0$

Определение. Лидер строки (ведущий элемент) - это 1-й ненулевой элемент слева.
Пример: $(0, 0, \underbrace{3}_{\text{лидер}}, 4, 5, 0, 0, 7)$

Определение. Матрица A размера $m \times n$ называется ступенчатой, если

1. Номера лидеров ненулевых строк строго возрастают с увеличением номера строки.
2. Все нулевые строки стоят внизу (в конце).

Теорема. Любую матрицу A размера $m \times n$ за конечное число элементарных преобразований над строками можно привести к ступенчатому виду.

Доказательство. Индукция по n:
Если A - нулевая, то A - ступенчатого вида. Если $A \neq 0$: найдем первый ненулевой столбец (начиная слева). Пусть j - номер первого ненулевого столбца

и $a_{ij} \neq 0$:

$$A = \begin{pmatrix} 0 & 0 & & \\ \vdots & \vdots & & \\ & & a_{ij} & \\ \vdots & \vdots & & \\ 0 & 0 & & \end{pmatrix}$$

Меняем 1-ю и i-ю строку местами и получаем, что a_{ij} стал лидером первой строки. Считаем, что сразу $a_{1j} \neq 0$:

$$A = \begin{pmatrix} 0 & 0 & a_{ij} & * \\ \vdots & \vdots & * & * \\ & & \vdots & \\ \vdots & \vdots & \vdots & \\ 0 & 0 & \vdots & \end{pmatrix}$$

Вычитаем из кажкой k-й строки, начиная со 2-ой, 1-ю строку, умноженную на число $\frac{a_{kj}}{a_{1j}}$. Получаем вид:

$$\tilde{A} = \left(\begin{array}{c|ccc} a_{ij} & * & \cdots & * \\ \hline 0 & * & \cdots & * \\ \vdots & * & \cdots & * \\ 0 & * & \cdots & * \end{array}\right)$$

К правой части матрицы (без 1 столбца и 1 строки) применяем индукцию и проводим матрицу к ступенчатому виду. □

Замечание. Этот метод называется методом Гаусса.

1.5 Решение СЛУ методом Гаусса

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

Элементарные преобразования над $AX = B \Longleftrightarrow$ элементарные преобразования над $(A|B)$.

СЛУ $AX = B$ ступенчатая $\Longrightarrow (A|B)$ имеет ступенчатый вид.

Утверждение. Решение СЛУ ступенчатого вида.

Пусть $AX = B$ - ступенчатая

$$(A|B) = \left(\begin{array}{cccc|c} a_{11} & & & & b_1 \\ & a_{22} & & & \vdots \\ & & \ddots & & \vdots \\ & & & a_{sn} & b_s \\ & & & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & b_{\widetilde{s}} \end{array}\right)$$

$\widetilde{s}$ - ненулевые строки расширенной матрицы

s - число ненулевых строк

$$\widetilde{s} = \begin{bmatrix} s \\ s+1 \end{bmatrix}$$

1 случай: $\widetilde{s} \neq s$ $(\widetilde{s} = s + 1)$

Рассмотрим последнюю ненулевую строку:

$$\left(\begin{array}{cccc|c} a_{11} & & & & b_1 \\ & a_{22} & & & \vdots \\ & & \ddots & & \vdots \\ & & & a_{sn} & b_s \\ 0 & \cdots & \cdots & 0 & b_{s+1} \end{array}\right)$$

$0x_1 + ... + 0x_n = b_{s+1} \Longrightarrow$ решений у этого уравнения нет $\Longrightarrow$ СЛУ не имеет решения, т.е. несовместна.

Далее $\widetilde{s} = s$

Заметим, что $\widetilde{s} = s \leq n$ (n-количество столбцов)

2 случай: $\widetilde{s} = s = n$

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{22}x_2 + \cdots + a_{1n}x_n = b_2 \\ \ddots \quad \vdots \\ a_{nn}x_n = b_n \end{cases}$$

Такая СЛУ называется строготреугольной.

Из n-го уравнения однозначно находится $x_n = \frac{b_n}{a_{nn}}$ Подставляем во все оставшиеся уравнения $x_n = \frac{b_n}{a_{nn}} \Longrightarrow$ исключаем x_n. Получаем строго треугольную систему с меньшим количество неизвестных.

Далее из (n-1)-го уравнения находим x_{n-1} и т.д. $\Longrightarrow$ СЛУ имеет единственное решение т.е. является определенной.

3 случай: $\widetilde{s} \underbrace{<}_{\text{хотим}} n$

$$\left(\begin{array}{ccccccc|c} 0 & 0 & |\underline{a_{1k_1}} & * & \cdots & \cdots & * & * \\ 0 & 0 & 0 & |\underline{a_{2k_2}} & * & \cdots & * & * \\ & & & & \ddots & & & \vdots \end{array}\right)$$

$a_{1k_1}, ..., a_{sk_s}$ - лидеры;

$x_{k_1}, ..., x_{k_s}$ - главные неизвестные (неизвестные, соответствующие лидерам)

Оставшиеся неизвестные назовем свободными.

Перекинем в правую часть СЛУ слагаемые, соответствующие свободным неизвестным $\Longrightarrow$ получаем относительно главных неизвестных строго треугольную СЛУ.

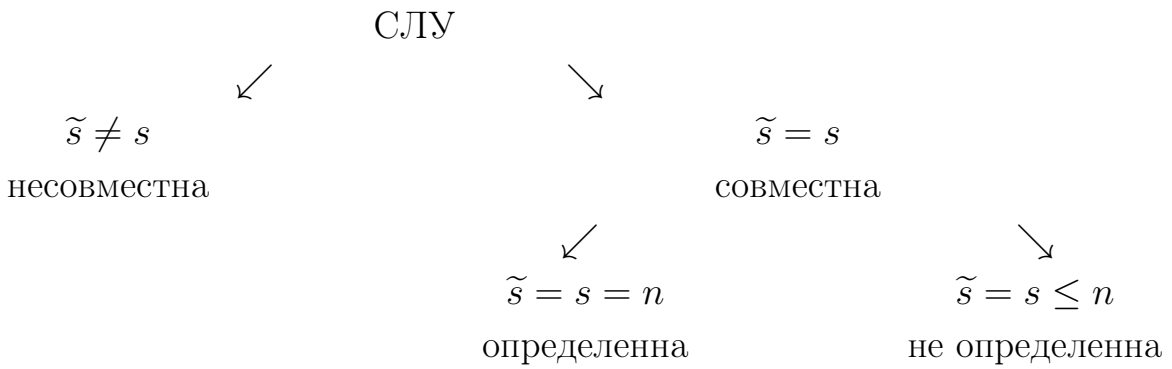
Как в случае 2, однозначно выражаются главные неизвестные через свободные $\Longrightarrow$ с точностью до нумерации получаем:

$$\begin{cases} x_1 = c_{1,s+1}x_{s+1} + \cdots + c_{1n}x_n + d_1 \\ \vdots \\ x_s = c_{s,s+1}x_{s+1} + \cdots + c_{sn}x_n + d_s \end{cases}$$

Это выражение называется общим решением системы. Подставляя вместо свободных неизвестных конкретное число из $\mathbb{R}$, получаем значение для главных.

$\Longrightarrow$ получаем все решения СЛУ

Если СЛУ имеет более одного решения - такая СЛУ называется неопределенной.



Алгоритм. $AX = B \longmapsto (A|B) \sim (A_c|B_c) \longmapsto A_cX = B_c$

Определение. Матрица A имеет улучшенный ступенчатый вид, если выполнены следующие условия:

1. A - ступенчатого вида
2. Все лидеры равны 1
3. В каждом столбце, где есть лидер $\neq 0$, все элементы равны 0

Утверждение. Любую матрицу A можно привести к улучшенному ступенчатому виду с помощью элементарных преобразований.

Доказательство. Т.к. любую матрицу можно привести к ступенчатому виду $\Longrightarrow$ будем считать, что A - ступенчатая.
Рассмотрим последний лидер a_{sk_s}. Если $a_{sk_s} \neq 1$, то s-ю строку делим на a_{sk_s} и получаем, что $\widetilde{a_{sk_s}} = 1$.
Далее из всех строк вычитаем первую, умноженную на $a_{ik_s} \Longrightarrow \widetilde{a_{ik_s}} = 0$ и т.д. □

Определение. СЛУ $AX = B$ называется однородной, если $B = 0$, т.е. все свободные члены нулевые.

Утверждение. Однородная система всегда совместна.

Доказательство. $AX = 0$ всегда имеет решение $x_1 = 0, ..., x_n = 0$ (тривиальное решение) □

Следствие. Однородная СЛУ, в которой число уравнений $<$ числа неизвестных, имеет нетривиальное решение.

Доказательство. (в обозначениях из метода Гаусса)
Т.к. система совместна (т.к. $B = 0$), то $s = \widetilde{s}$
С другой стороны $s = \overline{s} \leq$ число исходных уравнений $<$ n $\Longrightarrow s = \widetilde{s} < n \Longrightarrow$ СЛУ неопределена $\Longrightarrow \exists$ более одного решения $\Longrightarrow \exists$ нетривиальное решение. □

2 Векторные пространства

2.1 Аксиомы элементов векторного пространства

Мы рассматриваем векторные пространства над полем $\mathbb{R}$.

Определение. Векторным пространством над $\mathbb{R}$ называют множество элементов V, на котором введены операции сложения и умножения на числа из $\mathbb{R}$:

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

Удовлетворяет следующим свойствам:

1. $x + y = y + x$ (коммутативность)
2. $(x + y) + z = x + (y + z)$ (ассоциативность)
3. $\exists\, 0 \in V : \forall x \in V : x + 0 = 0 + x = x$ (нейтральный элемент относительно сложения)
4. $\forall x \in V : \exists\, x' : x + x' = 0$ (противоположный элемент)
5. $\forall \lambda \in \mathbb{R}, \forall x, y \in V : \lambda(x + y) = \lambda x + \lambda y$ (дистрибутивность умножения относительно сложения)
6. $\forall \lambda, \mu \in \mathbb{R}, \forall x \in V : (\lambda + \mu)x = \lambda x + \mu x$ (дистрибутивность сложения относительно умножения)
7. $\forall \lambda, \mu \in \mathbb{R}, \forall x \in V : \lambda(\mu x) = (\lambda\mu)x$ (ассоциативность умножения)
8. $\forall x \in V : 1 \cdot x = x$ (нейтральный элемент относительно умножения)

Определение. Любой элемент векторного пространства называется вектором.

Примеры векторных пространств:

1. V^2 - Геометрические векторы на плоскости.
2. V^3 - Геометрические векторы в пространстве.
3. $\mathbb{R}^n = \{(a_1, ..., a_n) \mid a_i \in \mathbb{R}\}$ - арифметические векторы.

   "+": $(a_1, ..., a_n) + (b_1, ..., b_n) = (a_1 + b_1, ..., a_n + b_n)$
   "×": $(a_1, ..., a_n) \times \lambda = (a_1\lambda, ..., a_n\lambda)$

Упражнение. Проверьте, что $\mathbb{R}^n$ (арифметическое пространство строк) с этими операциями является векторным пространством.

2.2 Следствия

1. Нулевой вектор единственный.

   Доказательство. Пусть существуют два $\overline{0}_1, \overline{0}_2 \in V$, тогда:

   $$\overline{0}_2 = \overline{0}_1 + \overline{0}_2 = \overline{0}_2 + \overline{0}_1 = \overline{0}_1$$

   □

2. $\forall x \in V$ противоположный вектор единственный

   Доказательство. Пусть существуют два x_1, x_2 - различные элементы, являющиеся противоположными к вектору x, тогда:

   $$\overline{0} + x_2 = (x_1 + x) + x_2 = x_1 + (x + x_2) = x_1 + \overline{0}$$

   □

3. $\forall \lambda \in \mathbb{R} : \lambda \cdot \overline{0} = \overline{0}$

   Доказательство.

   $$\lambda \cdot \overline{0} = \lambda \cdot (\overline{0} + \overline{0}) = \lambda \cdot \overline{0} + \lambda \cdot \overline{0}$$

   Прибавим к обеим частям уравнения $\lambda \cdot \overline{0} = \lambda \cdot \overline{0} + \lambda \cdot \overline{0}$ противоположный к $\lambda \cdot \overline{0}$, тогда:

   $$\lambda \cdot \overline{0} + (-\lambda \cdot \overline{0}) = \lambda \cdot \overline{0} + \lambda \cdot \overline{0} + (-\lambda \cdot \overline{0})$$
   $$\overline{0} = \lambda \cdot \overline{0}$$

   □

4. $\lambda \cdot (-x) = -\lambda \cdot x$
5. $\lambda \cdot (x - y) = \lambda x - \lambda y$
6. $(-1) \cdot x = -x$
7. $(\lambda - \mu) \cdot x = \lambda x - \mu x$

2.3 Векторные подпространства

Определение. Подмножество $U \subseteq V$ называется векторным подпространством, если:

1. $x, y \in U \Longrightarrow x + y \in U$
2. $\forall \lambda \in \mathbb{R}, \forall x \in U \Longrightarrow \lambda \cdot x \in U$
3. $U \neq \varnothing$

Замечание. 3 условие заменить на условие: $0 \in U$

$\Longleftarrow$ очевидно.

$\Longrightarrow$ если $U \neq \varnothing$, то $\exists\, x \in U \Longrightarrow$ по 2. : $(-1) \cdot x \in U \Longrightarrow -x \in U \Longrightarrow$
$x + (-x) \in U \Longrightarrow 0 \in U$

Утверждение. Любое векторное подпространство векторного пространства V само является векторным пространством относительно операций векторного пространства V.

Доказательство. Надо проверить определение. 1 и 2 свойство из операций векторного пространства означают, что в U заданы операции сложения и умножения на вещественное число. Проверка аксиом векторного пространства: 1,2,5,6,7,8 - выполнены для всех векторов из V, а значит и для всех векторов из U.
3,4 доказательство как в замечании:

$$\forall x \in U,\ \exists\, (-x) = (-1) \cdot x \in U,\ \overline{0} \in U,\ \text{т.к. } U \neq \varnothing$$

□

Примеры.

1. V^3, U - множество всех векторов из V^3, параллельных фиксированной плоскости.
2. $\mathbb{R}^n, U = \{(a_1, ..., a_n) \mid a_{2i} = 0\}$ - векторное подпространство
   $\widetilde{U} = \{(a_1, ..., a_n) \mid a_{2i} = 1\}$ - не векторное подпространство, т.к. множество не замкнуто относительно сложения и умножения.
3. В любом векторном простанстве V есть такие подпространства, состоящие только из нулевого вектора. (тривиальное или несобственное подпространство) (остальные называются собственными)

2.4 Линейная зависимость системы векторов

V - векторное пространство над полем $\mathbb{R}$

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

$$\lambda_1 x_1 + \cdots + \lambda_n x_n$$

Говорят, что вектора $w \in V$ линейно выражаются через $(v_1, ..., v_n)$,
если $\exists\, \lambda_1, ..., \lambda_n \in \mathbb{R} : w = \lambda_1 x_1 + \cdots + \lambda_n x_n$

Определение. Линейная комбинация $\lambda_1 x_1 + \cdots + \lambda_n x_n$ называется тривиальной, если $\lambda_1 = 0, ..., \lambda_n = 0$. Иначе - нетривиальной.

Определение. Система векторов $v_1, ..., v_n$ называется линейно зависимой (ЛЗ), если $\exists$ нетривиальная линейная комбинация равная 0, (т.е. $\exists\, \lambda_1, ..., \lambda_n \in \mathbb{R}$ не все равные 0) такая, что $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$. Иначе система называется линейно независимой (ЛНЗ), т.е. из любого такого равенства $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$
$\Longrightarrow (\lambda_1, ..., \lambda_n) = 0$.

Примеры. $V^2:\ v_1 = i + j, v_2 = 2i, v_3 = 3i$ - линейно зависимая система, т.к.

$$1 \cdot (i + j) + (-\frac{1}{2}) \cdot (2i) + (-\frac{1}{3}) \cdot (3i) = 0$$

$$1 \cdot v_1 + (-\frac{1}{2}) \cdot v_2 + (-\frac{1}{3}) \cdot v_3 = 0$$

Свойства.

1. Система из одного вектора V_1 ЛЗ $\Longleftrightarrow V_1 = 0$
2. Система из 2-х векторов v_1и v_2 ЛЗ $\Longleftrightarrow$ они пропорциональные, т.е. $v_1 = \lambda v_2,\ v_2 = \mu v_1$.

Пример. $\mathbb{R}^n$
Система $\underbrace{(1, 0, 0, ..., 0)}_{e_1}, \underbrace{(0, 1, 0, ..., 0)}_{e_2}, ..., \underbrace{(0, 0, 0, ..., 1)}_{e_n}$ линейно независимая
$\lambda_1 e_1 + \cdots + \lambda_n e_n = (0, ..., 0) \Longleftrightarrow (\lambda_1, ..., \lambda_n) = 0 \Longleftrightarrow$ ЛНЗ

Лемма 1. (Критерий линейной зависимости)
Система векторов $v_1, ..., v_n \in V,\ n > 1$ - линейно зависима $\Longleftrightarrow$ хотя бы один вектор линейно выражается через оставшиеся.

Доказательство.

$\Longrightarrow$ По определению ЛЗ $\exists\, \lambda_1, ..., \lambda_n \in \mathbb{R}$ не все нулевые: $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$. Без ограничения общности можем считать, что $\lambda_1 \neq 0$, тогда $v_1 = \frac{1}{\lambda_1}(-\lambda_2 v_2 - \cdots - \lambda_n v_n)$

$\Longleftarrow$ Пусть один из этих векторов выражается через оставшиеся. Без ограничения общности можем считать, что v_1 выражается через оставшиеся
$v_1 = \mu_2 v_2 + \cdots + \mu_n v_n$
$1 \cdot v_1 - \mu v_2 - \cdots - \mu_n v_n = 0$ - нетривиальная линейная комбинация,
т.к. μ_1(коэф. перед v_1) $\neq 0 \Longrightarrow v_1, ..., v_n$ - линейно зависимы.

□

Замечание. В лемме 1 нельзя «хотя бы один» заменить на «любой»!
Пусть $v_1 \neq 0, v_2 = 0$ и v_1, v_2 - ЛЗ, т.к. $0 \cdot v_1 + 1 \cdot v_2 = 0$

Лемма 2. Пусть $v_1, ..., v_n \in V$ - ЛНЗ, тогда $w \in V$ линейно выражается через $v_1, ..., v_n \Longleftrightarrow (w, v_1, ..., v_n)$ - ЛЗ.

Доказательство.

$\Longrightarrow$ $\exists\, \mu_1, ..., \mu_n \in \mathbb{R} : w = \mu_1 v_1 + \cdots + \mu_n v_n \Longrightarrow$ по критерию ЛЗ система $\{w, v_1, ..., v_n\}$ - ЛЗ.

$\Longleftarrow$ Пусть система ЛЗ $\Longrightarrow \exists\, \lambda_0, ..., \lambda_n \in \mathbb{R}$ - не все нули, так что $\lambda_0 w + \lambda_1 v_1 + \cdots + \lambda_n v_n = 0$, тогда:

1. $\lambda_0 = 0$, то $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ - нетривиальная линейная комбинация
2. $\lambda_0 \neq 0 \Longrightarrow w = (-\frac{\lambda_1}{\lambda_0})v_1 + \cdots + (-\frac{\lambda_n}{\lambda_0})v_n$

□

Лемма 3. Если $v_1, ..., v_k \in V$ - ЛНЗ и вектор $w \in V$ линейно выражается через $v_1, ..., v_k \Longleftrightarrow$ это выражение единственное.

Доказательство.

$\Longleftarrow$ Пусть выражается единственно. Допустим, $v_1, .., v_k$ - ЛЗ $\Longrightarrow \exists\{\lambda_1, .., \lambda_k\}$ не все нулевые, т.ч. $\lambda_1 v_1 + \cdots + \lambda_k v_k = 0$
Тогда если $w = \mu_1 v_1 + \cdots + \mu_k v_k$, то $w + 0 = (\mu_1 + \lambda_1)v_1 + \cdots + (\mu_k + \lambda_k)v_k$ другое разложение, противоречие.

$\Longrightarrow$ Пусть $v_1, .., v_k$ - ЛНЗ. Допустим, что существует два разложения:

$$w = \mu_1 v_1 + \cdots + \mu_k v_k$$

$$w = \widetilde{\mu_1} v_1 + \cdots + \widetilde{\mu_k} v_k$$

$$\mu_1 v_1 + \cdots + \mu_k v_k = \widetilde{\mu_1} v_1 + \cdots + \widetilde{\mu_k} v_k$$

$$v_1(\mu_1 - \widetilde{\mu_1}) + \cdots + v_n(\mu_n - \widetilde{\mu_n}) = 0$$

Т.к. $v_1, .., v_k$ - ЛНЗ $\Longrightarrow (\mu_i - \widetilde{\mu_i}) = 0 \implies \mu_i = \widetilde{\mu_i} \ \ \forall i = \overline{1, k}$

□

Лемма 4.

1. Если какая-то подсистема векторов ЛЗ, то вся система ЛЗ.
2. Если система векторов ЛНЗ, то любая подсистема ЛНЗ.

Доказательство.

1. Пусть подсистема $v_1, .., v_k$ системы $v_1, .., v_k, ..., v_m$ - ЛЗ $\Longrightarrow \exists \lambda_1, ..., \lambda_k$ не все равные нулю, т.ч. $\lambda_1 v_1 + \cdots + \lambda_k v_k = 0$ Положим $\lambda_{k+1} = 0, ..., \lambda_m = 0$ Тогда $\lambda_1 v_1, .., \lambda_k v_k, ..., \lambda_m v_m = 0$ - нетривиальная ЛК $\Longrightarrow \{v_1, ..., v_k, v_{k+1}, ..., v_m\}$ - ЛЗ.
2. Следует из 1.

□

Лемма 5. (ОЛЛЗ)
Пусть $v_1, ..., v_k \in V, \ w_1, ..., w_m \in V$, причем каждый w_i линейно выражается через $v_1, ..., v_k$, тогда если $m > k$, то $\{w_1, ..., w_m\}$ - ЛЗ.

Доказательство. Пусть

$$\begin{cases} w_1 = c_{11} v_1 + \cdots + c_{1k} v_k \\ w_2 = c_{21} v_1 + \cdots + c_{2k} v_k \\ \vdots \\ w_m = c_{m1} v_1 + \cdots + c_{mk} v_k \end{cases} \quad \text{где } c_{ij} \in \mathbb{R}$$

Докажем, что $\exists$ нетривиальная ЛК $w_1, ..., w_m = 0$
Для произвольных $\lambda_1, ..., \lambda_m$ рассмотрим выражение:

$$\lambda_1 w_1 + \cdots + \lambda_m w_m =$$
$$= \lambda_1(c_{11}v_1 + \cdots + c_{1k}v_k) + \cdots + \lambda_m(c_{m1}v_1 + \cdots + c_{mk}v_k) =$$
$$= (\lambda_1 c_{11} + \cdots + \lambda_m c_{m1})v_1 + \cdots + (\lambda_1 c_{1k} + \cdots + \lambda_m c_{mk})v_k$$

Рассмотрим СЛУ с неизвестными $\lambda_1, ..., \lambda_m$ из k уравнений:

$$\begin{cases} c_{11}\lambda_1 + \cdots + c_{m1}\lambda_m = 0 \\ \vdots \\ c_{1k}\lambda_1 + \cdots + c_{mk}\lambda_m = 0 \end{cases}$$

Т.к. $m > k$ и это ОСЛУ, в которой число уравнений $<$ числа неизвестных, то эта система имеет нетривиальное решение $\lambda_1, ..., \lambda_m$
$\Longrightarrow \lambda_1 w_1 + \cdots + \lambda_m w_m = 0$ - это нетривиальная ЛК
$\Longrightarrow w_1, ..., w_m$ - ЛЗ. □

2.5 Линейная оболочка множества S

V - векторное простанство над $\mathbb{R}$, $S \subseteq V$, $S \neq \varnothing$

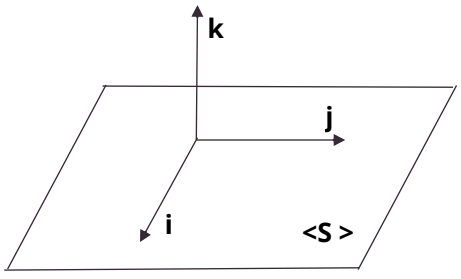
Утверждение. Множество всех ЛК $\lambda_1 s_1 + \cdots + \lambda_k s_k$, $\lambda_i \in \mathbb{R}$, $s_i \in S$ образует векторное подпространство в пространстве V.

Доказательство. Д/з. □

Определение. Такое векторное подпространство называется линейной оболочкой множества $S \subseteq V$.
Обозначается: $\langle S \rangle$.

Примеры.

1. $\mathbb{R}^3$, $S = \{(1,0,0),(0,1,0)\}$; $\quad \langle S \rangle = \{(\lambda, \mu, 0) \mid \lambda, \mu \in \mathbb{R}\}$
2. V^3, $S = \{i, j, i+j\}$



$\widetilde{s} = \{i + j\}$

Определение. Если $V = \langle S \rangle$, то S называется порождающим множеством векторного простанства V. Говорят, что векторное пространство V порождается множеством S.

Определение. Если $\exists$ конечное множество S, т.ч. $V = \langle S \rangle$, то V называется конечномерным (конечнопорожденным), иначе - бесконечномерным.

Пример. $\mathbb{R}^n = \langle (1, 0, ..., 0), ..., (0, ..., 0, 1) \rangle$

Лемма. (Переформулировка ОЛЛЗ) Пусть векторное пространство V пораждается k векторами. Тогда любые $m > k$ векторов из V - ЛЗ.

2.6 Базис

V- конечномерное векторное пространство над $\mathbb{R}$

Определение 1. Система векторов $\{e_1, ..., e_n\} \subseteq V$ называется базисом векторного пространства V, если:

1. $\{e_1, ..., e_n\}$ - ЛНЗ
2. $V = \langle e_1, ..., e_n \rangle$, т.е. $\forall x \in V$, $\exists\, x_1, ..., x_n \in \mathbb{R} : x = x_1 e_1 + \cdots + x_n e_n$

Эти числа $x_1, ..., x_n$ - называются координатами вектора x в базисе $\{e_1, ..., e_n\}$

Определение 2. Система векторов $\{e_1, ..., e_n\} \subseteq V$ называется базисом векторного простанства V, если любой вектор $x \in V$ выражается через $\{e_1, ..., e_n\}$ единственным образом.

Утверждение. (**Опр 1**) $\Longleftrightarrow$ (**Опр 2**)

Доказательство. По лемме (3). □

Теорема. Всякое конечномерное векторное пространство над $\mathbb{R}$ обладает базисом. Более того, из любого конечного порожденного множества можно выбрать базис.

Доказательство. Пусть S - какое-то порождающее множество векторного пространства V.
Если S - ЛНЗ, то S - базис
Если S - ЛЗ, то по критерию о ЛЗ один из векторов s_1 множества S линейно выражается через остальные.
Тогда $S_1 = S \setminus \{s_1\}$ - конечное порождащее множество. ч.т.д.
Т.к. S - конечное,то этот процесс прервется и мы получим ЛНЗ порожденную систему. □

Теорема. В любом базисе конечномерного векторного пространства V над $\mathbb{R}$ одно и тоже число векторов.

Доказательство. Пусть есть два базиса $\{e_1, ..., e_n\}$ и $\{f_1, ..., f_m\}$ векторного пространства V. Тогда каждый вектор f_i выражается через $e_1, ..., e_n$.
По ОЛЛЗ: $\{f_1, ..., f_m\}$ - ЛЗ $\Longrightarrow$ $\{f_1, ..., f_m\}$ - не базис $\Longrightarrow$ противоречие. □

Определение. Число векторов в базисе конечномерного векторного пространства V называется размерностью векторного простанства и обозначается: $\dim V$

Примеры.

1. $\dim V^2 = 2$
2. $\dim \mathbb{R}^n = n$

Замечание. Если $V = 0$, то $\dim V = 0$ (базис систоит из $\varnothing$)

Утверждение. Пусть V- векторное пространство над $\mathbb{R}$, $\dim V = n$, $S \subseteq V$
Любые $m > n$ векторов из S - ЛЗ. (по ОЛЛЗ)
$\Longrightarrow$ в S $\exists$ максимальная ЛНЗ подсистема (т.е. ничего нельзя добавить к этой подсистеме без нарушения ЛНЗ)

Лемма 6. Пусть V - n-мерное векторное пространство над $\mathbb{R}$, $S \subseteq V$. Тогда максимальная ЛНЗ система векторов из S образует базис в лин. оболочке $\langle S \rangle$

Доказательство. Пусть $\{s_1, ..., s_k\}$ максимальная (по включению) ЛНЗ система в $S \Longrightarrow \forall s \in S \setminus \{s_1, ..., s_k\} \Longrightarrow \{s, s_1, ..., s_k\} -$ ЛЗ.
По Лемме (2). $\Longrightarrow s = \lambda_1 s_1 + \cdots + \lambda_k s_k$
Докажем, что $\{s_1, ..., s_k\}$ - базис в $\langle S \rangle$.

1. ЛНЗ (очевидно)
2. $\forall x \in \langle S \rangle$: $x = x_1 s_1 + \cdots + x_k s_k$

По определению линейной оболочки x линейно выражается через вектора из S.
А каждый вектор из S линейно выражается через $\{s_1, ..., s_k\}$. □

Теорема. Пусть V конечномерное векторное пространство над $\mathbb{R}$, тогда:

1. Любая максимальная ЛНЗ система векторов из V - базис V.
2. Любую ЛНЗ систему векторов из V можно дополнить до базиса векторного пространства V.

Доказательство.

1. По лемме (6). $\langle S \rangle = V$
2. Пусть S - ЛНЗ система векторов из V

Если $V = \langle S \rangle$, тогда S - базис.
Если $V \neq \langle S \rangle$, то $\exists\ s_1 \in V \setminus \langle S \rangle$
$\Longrightarrow s_1$ линейно не выражается через $S \Longrightarrow$ (По лемме 2.) $S_1 = S \cup \{s_1\}$ - ЛНЗ.
$\Longrightarrow$ Если $V = \langle S_1 \rangle$, то S_1 базис, иначе $\exists s_2 \in V \setminus \langle S_1 \rangle$, и т.д.
Этот процесс прервется на конечном шаге, т.к. пространство V- конечное. (Если $\dim V \neq n$, то $\nexists$ ЛНЗ системы с числом векторов $> n$) $\square$

Следствие. Пусть V конечномерное векторное пространство над $\mathbb{R}$

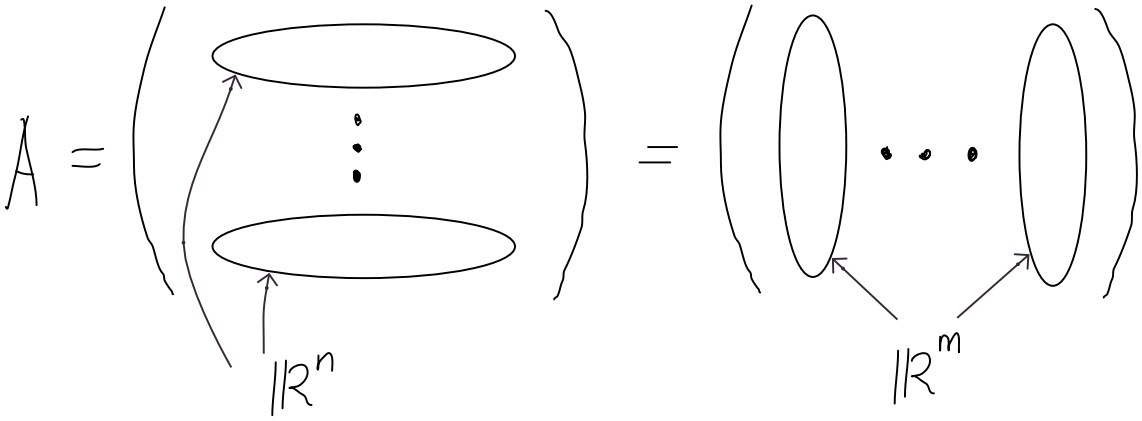
1. Любой ненулевой вектор можно дополнить до базиса.
2. Любые n ЛНЗ вектора в n-мерном пространстве V образуют базис.

3 Ранг

3.1 Ранг системы векторного простанства

Определение. Рангом системы векторов S, назовем $\dim\langle S\rangle$, т.е. число векторов в максимальной ЛНЗ системе из S.

A - матрица $m \times n$

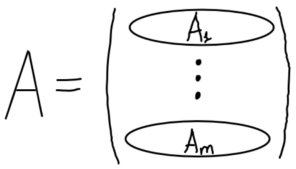


Определение. Рангом матрицы A называется ранг системы ее строк, т.е. максимальное число ЛНЗ строк матрицы.

3.2 Ранг матрицы

Определение. Ранг системы векторов $\{s_1, ..., s_n\}$ называется $\dim\langle s_1, ..., s_n\rangle$.

Определение. Рангом матрицы A размера $m \times n$ называется ранг системы её строк.



Определение. Две системы векторов $\{v_1, ..., v_n\}$, $\{w_1, ..., w_n\}$ называются эквивалентными, если каждый вектор v_i линейно выражается через $\{w_1, ..., w_n\}$, а w_i через $\{v_1, ..., v_n\}$.
Это условная эквивалентность: $\langle v_1, ..., v_n\rangle = \langle w_1, ..., w_n\rangle$

Утверждение. При элементарных преобразованиях над строками ранг матрицы A не изменяется.

Доказательство.

$$\langle A_1, ..., A_m \rangle = \langle \widetilde{A_1}, ..., \widetilde{A_m} \rangle$$

т.е. система строк A эквивалентна системе строк $\widetilde{A} \Longrightarrow rkA = rk\widetilde{A}$. □

Утверждение. При элементарных преобразованиях над столбцами, ранг матрицы A не изменяется.

Предложение 1. Ранг матрицы A равен числу ненулевых строк матрицы ступенчатого вида, к которому можно привести матрицу A с помощью элементарных преобразований строк.

Доказательство. $A \overset{\text{ЭП строк}}{\longrightarrow} A_{\text{ст}} \Longrightarrow rkA = rkA_{\text{ст}}$

$A_{\text{ст}} = \begin{pmatrix} a_{1i_1} & & * \\ & a_{2i_2} & \\ & & \ddots \\ 0 & & a_{si_s} \end{pmatrix}$

$a_{1i_1}, ..., a_{si_s}$ - лидеры строк в $A_{\text{ст}} \Longrightarrow a_{1i_1} \neq 0, ..., a_{si_s} \neq 0$

Очевидно, что $rkA_{\text{ст}} \leq s$. Достаточно доказать, что ненулевые строки ЛНЗ. Рассмотрим ЛК:

$\lambda_1(0, ..., 0, a_{1i_1}, *, ..., *) + \lambda_2(0, ..., 0, a_{2i_2}, *, ..., *) + \cdots + \lambda_s(0, ..., 0, a_{si_s}, *, ..., *) = (0, ..., 0)$

$(0, ..., 0, \lambda_1 a_{1i_1}, ..., \lambda_1 a_{1i_2} + \lambda_2 a_{2i_2}, ...) = (0, ..., 0) \Longrightarrow \lambda_1 \underbrace{a_{1i_1}}_{\text{лидер}} = 0 \Longrightarrow \lambda_1 = 0$

$\lambda_1 a_{i_2 1} + \lambda_2 \underbrace{a_{2i_2}}_{\text{лидер}} = 0 \Longrightarrow \lambda_2 = 0$ и т.д.

Получаем, что $\lambda_1 = 0, ..., \lambda_s = 0 \Longrightarrow$ это ЛК - ЛНЗ. □

Предложение 2. Ранг системы столбцов не изменяется при элементарных преобразованиях над строками.

Доказательство.

$$A \overset{\text{ЭП строк}}{\longmapsto} \widetilde{A}$$

Пусть $A = (a_{ij}) = (\underbrace{A_1, ..., A_n}_{\text{столбцы } A}), \ \widetilde{A} = (\widetilde{a_{ij}}) = (\underbrace{\widetilde{A_1}, ..., \widetilde{A_n}}_{\text{столбцы } \widetilde{A}})$.

Докажем, что если для некоторых чисел $\lambda_1, ..., \lambda_n \in \mathbb{R}$ выполнено:
$\lambda_1 A_1 + \cdots + \lambda_n A_n = 0$, то для этих же чисел $\lambda_1 \widetilde{A_1} + \cdots + \lambda_n \widetilde{A_n} = 0$ (Верно и обратное, т.к. ЭП обратимы, т.е. если для каких-то чисел $\lambda_i \in \mathbb{R} : \sum \lambda_i \widetilde{A_1} = 0$, то $\sum \lambda_i A_i = 0$).

Дано: $\lambda_1 A_1 + \cdots + \lambda_n A_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Longrightarrow \begin{cases} \lambda_1 a_{11} + \lambda_2 a_{12} + \cdots + \lambda_n a_{1n} = 0 \\ \vdots \\ \lambda_1 a_{m1} + \lambda_2 a_{m2} + \cdots + \lambda_n a_{mn} = 0 \end{cases} \Longrightarrow$

$\lambda_1, ..., \lambda_n -$ решение ОСЛУ $AX = 0$. Т.к. при ЭП над уравнениями множество решений не меняется, поэтому $\lambda_1, ..., \lambda_n$ - это решение ОСЛУ $\widetilde{A}X = 0 \Longrightarrow$ $\lambda_1 \widetilde{A_1} + \cdots + \lambda_n \widetilde{A_n} = 0$

Отсюда получаем, что если $A_{i_1}, ..., A_{i_s}$ - максимальная ЛНЗ система столбцов в A, то $\widetilde{A_{i_1}}, ..., \widetilde{A_{i_s}}$ - максимальная ЛНЗ система столбцов в $\widetilde{A} \Longrightarrow rk\{\widetilde{A_1}, ..., \widetilde{A_n}\} = rk\{A_1, ..., A_n\}$. □

Определение. Пусть $A = (a_{ij})$ - матрица $m \times n$, тогда $B = (b_{ij})$ матрица $n \times m$ называется транспонированной к матрице A, если $b_{ij} = a_{ji}$, где $i = \overline{1, m}; j = \overline{1, n}$
Обозначаем $B = A^T$

Пример.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$$

Следствие. Ранг системы строк матрицы A (=рангу матрицы A) не изменяется при элементарных преобразованиях над столбцами.

Доказательство. Предложение 2 применяем к A^T □

Теорема 1. Ранг системы строк матрицы A совпадает с рангом системы столбцов матрицы A.

Доказательство. Было доказано, что ранг системы строк (столбцов) матрицы не изменяется при ЭП над строками и над столбцами. Приведем матрицу A к ступенчатому виду с помощью ЭП над строками. $A_{\text{ст}}$ имеет вид:

$$\begin{pmatrix} a_{1i_1} & & & * \\ & a_{2i_2} & & \\ & & \ddots & \\ 0 & & & a_{si_s} \end{pmatrix}$$

$$a_{1i_1} \neq 0, ..., a_{si_s} \neq 0$$

Используем i_1-столбец, вычитая этот столбец из оставшихся с подходящими коэффициентами, получаем:

$$\begin{pmatrix} a_{1i_1} & 0 & 0 & \cdots & 0 \\ & a_{2i_2} & & * & \\ & & \ddots & & \\ 0 & & & a_{si_s} & \end{pmatrix}$$

Далее используем i_2-столбец, обнуляем все элементы правее $a_{i_2 2}$. В итоге получаем:

$$\begin{pmatrix} a_{1i_1} & & 0 \\ & \ddots & \\ 0 & & a_{si_s} \end{pmatrix}$$

Очевидно, что у такой матрицы ранг системы строк = рангу системы столбцов.

□

4 Возвращаемся к системе линейных уравнений

$$\begin{cases} a_{11}x_1 + ... + a_{1n}x_n = b_1 \\ a_{21}x_2 + ... + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + ... + a_{mn}x_n = b_m \end{cases} \qquad (AX = B)$$

Теорема. (Кронекера-Капелли)

1. (Критерий совместимости СЛУ)
   СЛУ $AX = B$ совместна $\Longleftrightarrow rk(A|B) = rkA$

2. (Критерий определенности СЛУ)
   Совместная СЛУ $AX = B$ - определена $\Longleftrightarrow rk(A|B) = rkA = n$

3. (Критерий существования нетривиального решения у однородной СЛУ)
   ОСЛУ $AX = 0$ имеет нетривиальное решение $\Longleftrightarrow rkA < n$

Однородная СЛУ:

$$\begin{cases} a_{11}x_1 + ... + a_{1n}x_n = 0 \\ a_{21}x_1 + ... + a_{2n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + ... + a_{mn}x_n = 0 \end{cases} \qquad (AX = 0)$$

Утверждение. ОСЛУ всегда совместна, т.к. есть тривиальное решение.

Свойства.

1. Если $X^0 = \begin{pmatrix} x_1^0 \\ \vdots \\ x_n^0 \end{pmatrix}$; $\quad \widetilde{X^0} = \begin{pmatrix} \widetilde{x_1^0} \\ \vdots \\ \widetilde{x_n^0} \end{pmatrix}$ - решение ОСЛУ,

   тогда $X^0 + \widetilde{X^0} = \begin{pmatrix} X_1^0 + \widetilde{X_1^0} \\ \vdots \\ X_n^0 + \widetilde{X_n^0} \end{pmatrix}$

2. Если $X^0 = \begin{pmatrix} x_1^0 \\ \vdots \\ x_n^0 \end{pmatrix}$ - решение ОСЛУ $AX = 0$, то $\lambda X^0 = \begin{pmatrix} \lambda x_1^0 \\ \vdots \\ \lambda x_n^0 \end{pmatrix}$ - решение.

Доказательство. Д/з □

Следствие. Множество всех решений ОСЛУ является векторным подпространством в $\mathbb{R}^n$. Будем говорить, что это пространство над ОСЛУ.

Замечание. Если $\exists$ нетривиальное решение ОСЛУ над $\mathbb{R}$, то $\exists$ бесконечно много решений.

Теорема 2. Пространство решений ОСЛУ $AX = 0$ имеет базис из $n - r$ векторов, где n - число неизвестных, а $r = rkA$.

4.1 Фундаментальная система решений

Определение. Любой базис пространства решений ОСЛУ называется Фундаментальной Системой Решений ОСЛУ (ФСР).

Доказательство. **(Теоремы 2.)**
Решение СЛУ методом Гаусса: приводим её к ступенчатому виду (число ступенек $r = rkA$), главные неизвестные выражаем через свободные.

$$\begin{cases} x_1 = c_{1,1}x_{r+1} + \cdots + c_{1,n-r}x_n \\ \vdots \\ x_r = c_{r,1}x_{r+1} + \cdots + c_{r,n-r}x_n \end{cases}$$

Определим $n-r$ частных решений, приравнивая одно из $x_1, ..., x_n$ к 1, а остальные к 0.

$$F_1 = \begin{pmatrix} c_{11} \\ \vdots \\ c_{r1} \\ \hline 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad F_2 = \begin{pmatrix} c_{12} \\ \vdots \\ c_{r2} \\ \hline 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, ..., \quad F_{n-r} = \begin{pmatrix} c_{1,n-r} \\ \vdots \\ c_{r,n-r} \\ \hline 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

Докажем, что $F_1, ..., F_{n-r}$ - базис пространства решений ОСЛУ

1. $F_1, ..., F_{n-r}$ - ЛНЗ?

   Рассмотрим ЛК $\lambda_1 F_1 + \cdots + \lambda_{n-r} F_{n-r} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$

$$\Longrightarrow \left(\begin{array}{c} * \\ \vdots \\ * \\ \hline \lambda_1 \\ \vdots \\ \lambda_{n-r} \end{array}\right) = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Longrightarrow \lambda_1 = 0, ..., \lambda_{n-r} = 0$$

2. Надо доказать, что любое решение выражено через $F_1, ..., F_{n-r}$

$$X^0 = \left(\begin{array}{c} c_{11} \\ \vdots \\ c_{r1} \\ \hline \mu_{r+1} \\ \vdots \\ \mu_n \end{array}\right) = \mu_{r+1}F_1 + \cdots + \mu_n F_{n-r}$$

□

Пример. Найти ФСР ОСЛУ

$$\begin{cases} x_1 + x_2 + 3x_3 + 5x_4 - x_5 = 0 \\ x_1 + 2x_2 + x_3 + x_4 + x_5 = 0 \end{cases}$$

$$\begin{pmatrix} 1 & 1 & 3 & 5 & -1 \\ 1 & 2 & 1 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 3 & 5 & -1 \\ 0 & 1 & -2 & -4 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 5 & 9 & -3 \\ 0 & 1 & -2 & -4 & 2 \end{pmatrix}$$

где x_1, x_2 - главные, x_3, x_4, x_5 - свободные

$$\begin{cases} x_1 = -5x_3 - 9x_4 + 3x_5 \\ x_2 = 2x_3 + 4x_4 - 2x_5 \end{cases} \quad x_3, x_4, x_5 \in \mathbb{R} \text{ - произвольные}$$

$$F_1 = \left(\begin{array}{c} -5 \\ 2 \\ \hline 1 \\ 0 \\ 0 \end{array}\right), \quad F_2 = \left(\begin{array}{c} -9 \\ 4 \\ \hline 0 \\ 1 \\ 0 \end{array}\right), \quad F_3 = \left(\begin{array}{c} 3 \\ -3 \\ \hline 0 \\ 0 \\ 1 \end{array}\right) \text{ - три частных решения ОСЛУ}$$

Проверим, что $\{F_1, F_2, F_3\}$- базис пространства решений ОСЛУ

$$\left(\begin{array}{c} * \\ * \\ \hline \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{array}\right) = \lambda_1 F_1 + \lambda_2 F_2 + \lambda_3 F_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Longrightarrow \lambda_{1,2,3} = 0 \Longrightarrow F_1, F_2, F_3 \text{ - ЛНЗ.}$$

Проверим, что $\{F_1, F_2, F_3\}$ порождает пространство решений. Возьмем произвольные числа μ_3, μ_4, μ_5 и приравняем $x_3 = \mu_3, x_4 = \mu_4, x_5 = \mu_5$

$$\left(\begin{array}{c} x_1 \\ x_2 \\ \hline x_3 \\ x_4 \\ x_5 \end{array}\right) = \left(\begin{array}{c} -5\mu_3 - 9\mu_4 + 3\mu_5 \\ 2\mu_3 + 4\mu_4 - 2\mu_5 \\ \hline \mu_3 \\ \mu_4 \\ \mu_5 \end{array}\right) = \mu_3 \left(\begin{array}{c} -5 \\ 2 \\ \hline 1 \\ 0 \\ 0 \end{array}\right) + \mu_4 \left(\begin{array}{c} -9 \\ 4 \\ \hline 0 \\ 1 \\ 0 \end{array}\right) + \mu_5 \left(\begin{array}{c} 3 \\ -2 \\ \hline 0 \\ 0 \\ 1 \end{array}\right)$$

Такой базис называется нормальной ФСР.

4.2 Неоднородная СЛУ

$$\begin{cases} a_{11}x_1 + ... + a_{1n}x_n = b_1 \\ a_{21}x_2 + ... + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + ... + a_{mn}x_n = b_m \end{cases} \qquad (AX = B)$$

Рассмотрим соответствующую (ассоциированную) к ней ОСЛУ

$$\begin{cases} a_{11}x_1 + ... + a_{1n}x_n = 0 \\ a_{21}x_2 + ... + a_{2n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + ... + a_{mn}x_n = 0 \end{cases} \qquad (AX = 0)$$

Теорема. Пусть СЛУ $AX = B$ - совместна. X_0 - произвольное частное решение. Тогда множество M всех решений неоднородной СЛУ: $AX = B$ равно сумме частного решения X_0 и множеству $M_{\text{одн}}$ всех решений соответствующей однородной СЛУ: $AX = 0$

$$M = X_0 + M_{\text{одн}} = \{X_0 + Y | Y \in M_{\text{одн}}\}$$

Доказательство. $X_0 + M_{\text{одн}} \subseteq M$
Рассмотрим произвольное решение ОСЛУ. $Y \in M_{\text{одн}}$

Пусть $X_0 = \begin{pmatrix} x_1^0 \\ \vdots \\ x_n^0 \end{pmatrix}$, $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$

Докажем, что $X_0 + Y = \begin{pmatrix} x_1^0 + y_1 \\ \vdots \\ x_n^0 + y_n \end{pmatrix}$ - решение СЛУ, т.е. $X_0 + Y \in M$

$$AX = B: \ a_{i1}x_1^0 + \cdots + a_{in}x_n^0 = b_i$$

$$AX = 0: \ a_{i1}y_1 + \cdots + a_{in}y_n = 0$$

где $i = \overline{1, m}$.

Проверим, что $X_0 + Y \in M$

$$a_{i1}(x_1^0 + y_1) + \cdots + a_{in}(x_n^0 + y_n) = b_i$$

$$\underbrace{(a_{i1}x_1^0 + \cdots + a_{in}x_n^0)}_{b_i \text{ (т.к. } X_0 \in M)} + \underbrace{(a_{i1}y_1 + \cdots + a_{in}y_n)}_{0 \text{ (т.к. } Y \in M_{\text{одн}})} = b_i$$

Обратное утверждение: $M \subseteq X_0 + M_{\text{одн}}$

Рассмотрим произвольное решение $Z = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$ - неоднородная СЛУ.

Докажем, что $Z - X_0 = \begin{pmatrix} z_1 - x_1^0 \\ \vdots \\ z_n - x_n^0 \end{pmatrix}$ - решение однородной СЛУ.

Проверяем

$$a_{i1}(z_1 - x_1^0) + \cdots + a_{in}(z_n - x_n^0) = 0$$

$$\underbrace{(a_{i1}z_1 + \cdots + a_{in}z_n)}_{b_i (\text{т.к. } Z \in M)} - \underbrace{(a_{i1}x_1^0 + \cdots + a_{in}x_n^0)}_{b_i (\text{т.к. } X_0 \in M)} = 0$$

□

Замечание.

Общее решение ОСЛУ имеет вид:

$$X = \mu_1 F_1 + \cdots + \mu_s F_s$$

где $F_1, ..., F_s$ - ФСР ОСЛУ, $s = n - rkA$

Общее решение неоднородной СЛУ:

$$X = X_0 + \mu_1 F_1 + \cdots + \mu_s F_s$$

X_0 - частное решение неоднородной СЛУ

5 Операции над матрицами

$Mat_{m\times n}(\mathbb{R})$ - множество всех матриц размера $m \times n$ с коэффициентами из $\mathbb{R}$
$A, B \in Mat_{m\times n}(\mathbb{R}),\ A = (a_{ij}),\ B = (b_{ij})$

Операции над матрицами:

1. Сложение матриц
   Суммой матриц A и B называется матрица $C = (c_{ij})$ размера $m \times n$, у которой $c_{ij} = a_{ij} + b_{ij}$. Обозначается: $C = A + B$

2. Умножение матриц на число $\lambda \in \mathbb{R}$
   Произведением матрицы $A = (a_{ij})$ на λ называется матрица $C = (c_{ij})$ размера $m \times n$, у которой $c_{ij} = \lambda a_{ij}$. Обозначается: $C = \lambda A$

   Утверждение. Множество $Mat_{m\times n}(\mathbb{R})$, относительно этих операций сложения и умножения на число, образует векторное пространство над $\mathbb{R}$.

   Доказательство. $A,\ B \in Mat_{m\times n}(\mathbb{R}) \Longrightarrow A + B,\ \lambda A \in Mat_{m\times n}(\mathbb{R})$
   Надо проверить 8 аксиом

   1) коммутативность
      $C = A + B \quad c_{ij} = a_{ij} + b_{ij}$
      $\widetilde{C} = B + A \quad \widetilde{c_{ij}} = b_{ij} + a_{ij}$
      т.к. сложение вещественных чисел из $\mathbb{R}$ - коммутативно, то $c_{ij} = \widetilde{c_{ij}} \Longrightarrow C = \widetilde{C}$
      $\Longrightarrow A + B = B + A$

      Упражнение. Аналогично доказать 2), 5)-8)

   3) $\exists\ 0 \in Mat_{m\times n}(\mathbb{R})\ \forall A \in Mat_{m\times n}(\mathbb{R}) : 0 + A = A$
      В качестве 0 берем нулевую матрицу размера $m \times n$
   4) $\forall A \in Mat_{m\times n}(\mathbb{R})\ \exists\ B \in Mat_{m\times n}(\mathbb{R}) : A + B = 0$
      В качестве B берем $b_{ij} = -a_{ij}$

   □

   Утверждение. $\dim M_{m\times n} = m \cdot n$

   Доказательство. Достаточно указать базис
   $\{E_{st}\},\ s = \overline{1, m},\ t = \overline{1, n}$
   $E_{st} = (a_{ij}),\ a_{ij} = \begin{cases} 1,\ i = s,\ j = t \\ 0, \text{ иначе} \end{cases}$

Упражнение. Проверить, что это базис.

□

Определение. Матрица E_{st} называется матричной единицей. Базис из всех матричных единиц называется стандартным базисом в пространстве $Mat_{m\times n}(\mathbb{R})$. $A = \sum a_{st}E_{st}$

3. Умножение матриц
   $A \in Mat_{m\times k}(\mathbb{R}),\ B \in Mat_{k\times n}(\mathbb{R})$
   Произведение матрицы A на матрицу B называется матрица C размера $m \times n$, у которой $c_{ij} = \sum\limits_{s=1}^{k} a_{is}b_{sj}$. Обозначаем $C = AB$.

   Свойство. Произведение матриц не коммутативно.

   Пример.

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\quad B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

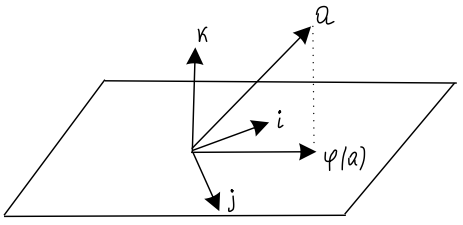
$$AB = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\quad BA = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Longrightarrow AB \neq BA$$

   Замечание.

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_n \end{cases} \Longleftrightarrow \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

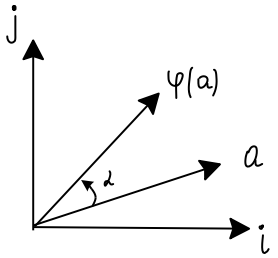
Примеры.

1. Проекция
   $\varphi : V^3 \to V^2, \varphi : x_1i + x_2j + x_3k \to x_1i + x_2j$



2. Поворот

   $\varphi : V^2 \to V^2$ Поворот на угол α вокруг точки O



6 Линейные отображения

6.1 Изоморфизм

V, W- векторные пространства над $\mathbb{R}$

Определение. Отображение $\varphi : V \to W$ называется изоморфизмом векторных пространств, если:

1. $\forall a, b \in V : \ \varphi(a + b) = \varphi(a) + \varphi(b)$
2. $\forall \lambda \in \mathbb{R} \ \forall a \in V : \ \varphi(\lambda a) = \lambda \varphi(a)$
3. φ является биекцией.

При этом V, W называются изоморфными.
Обозначается: $V \cong W$

Утверждение. Любое векторное пространство над $\mathbb{R}$ размерности n изоморфно $\mathbb{R}^n$.

Доказательство. Фиксируем базис $\{e_1, ..., e_n\}$ - в V.

1. $\forall x \in V$ однозначно раскладывается по базису $x = \sum\limits_{i=1}^{n} x_i e_i$. Зададим отображение $\varphi : V \to \mathbb{R}^n$ по правилу:

   $$\varphi : x = x_1 e_1 + \cdots + x_n e_n \to (x_1, ..., x_n)$$

   Т.к. координаты вектора определены однозначно, то φ инъективно, сюръективность очевидна $\Longrightarrow \varphi$ - биекция.

2. $\forall x, y \in V$

   $$x = \sum_{i=1}^{n} x_i e_i \quad y = \sum_{i=1}^{n} y_i e_i \quad x + y = \sum_{i=1}^{n} (x_i + y_i) e_i$$

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

3. $\forall \lambda \in \mathbb{R} \ \forall x \in V$

   $$\varphi(\lambda x) = \varphi(\sum_{i=1}^{n} \lambda x_i e_i) = (\lambda x_1, ..., \lambda x_n) = \lambda(x_1, ..., x_n) = \lambda \varphi(x)$$

□

Примеры.

1. $V^2 \cong \mathbb{R}^2$
   $V^3 \cong \mathbb{R}^3$

2. $M_{m\times n}(\mathbb{R}) \cong \mathbb{R}^{mn}$

Упражнение. $V \cong W \iff \dim V = \dim W$; $V, W-$ конечномерные пространства над $\mathbb{R}$.

6.2 Линейные отображения и матрицы

Определение. Отображение $\varphi : V \to W$ называется линейным, если

1. $\forall a, b \in V :\ \varphi(a+b) = \varphi(a) + \varphi(b)$

2. $\forall \lambda \in \mathbb{R}, \forall a \in V :\ \varphi(\lambda a) = \lambda\varphi(a)$

Утверждение. V, W- векторные пространства над $\mathbb{R}$.
Если $\{e_1, ..., e_n\}$ - базис V, $(w_1, ..., w_n)$ - набор векторов из W.
Тогда $\exists!$ линейное отображение $\varphi : V \to W$, которое $\varphi : e_i \to w_i\ \ \forall i = \overline{1, n}$.

Доказательство.

1. Пусть $\varphi : V \to W$ - линейное отображение такое, что
   $\varphi(e_i) = w_i\ \forall i = \overline{1, n}$. Тогда образ вектора x определяется однозначно по формуле:

   $$\varphi(x) = \varphi(x_1e_1 + \cdots + x_ne_n) = x_1\varphi(e_1) + \cdots + x_n\varphi(e_n) = x_1w_1 + \cdots + x_nw_n$$

   $\Longrightarrow$ линейное отображение определяется однозначно.

2. Докажем, что $\exists$ линейное отображение, которое переводит e_i в w_i. Отображение зададим формулой:

   $$\varphi : x = x_1e_1 + \cdots + x_ne_n \to x_1w_1 + \cdots + x_nw_n$$

   $$\varphi(a+b) = \varphi((a_1+b_1)e_1 + \cdots + (a_n+b_n)e_n) = (a_1+b_1)w_1 + \cdots + (a_n+b_n)w_n$$

   $$\varphi(a) + \varphi(b) = \varphi(a_1e_1 + \cdots a_ne_n) + \varphi(b_1e_1 + \cdots b_ne_n) =$$

   $$= a_1w_1 + \cdots + a_nw_n + b_1w_1 + \cdots + b_nw_n = w_1(a_1+b_1) + \cdots + w_n(a_n+b_n)$$

   $\Longrightarrow \varphi(a+b) = \varphi(a) + \varphi(b)$
   Проверить, что $\varphi(\lambda a) = \lambda\varphi(a)$ - ДЗ

□

Пусть $\varphi : V \to W$ - линейное отображение V- n-мерное, W − m-мерное пространство.
Фиксируем базис $\mathcal{E} = \{e_1, ..., e_n\}$ - базис в V; $\mathcal{F} = \{f_1, ..., f_m\}$ - базис в W

$$\varphi(e_1) = w_1 = a_{11}f_1 + \cdots + a_{m1}f_m$$

$$\vdots$$

$$\varphi(e_n) = w_n = a_{1n}f_1 + \cdots + a_{mn}f_m$$

Определение. Матрица A размера $m \times n$, составленная из столбцов координат образов векторов e_i в базисе $\mathcal{F}$, называется матрицей линейного отображения в базисах $\mathcal{E}$ и $\mathcal{F}$

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ \underbrace{a_{m1}}_{\varphi(e_1)} & \cdots & \underbrace{a_{mn}}_{\varphi(e_n)} \end{pmatrix}$$

Утверждение. Пусть $\mathcal{E} = \{e_1, ..., e_n\}$ - базис в V над $\mathbb{R}$; $\mathcal{F} = \{f_1, ..., f_m\}$ - базис в W над $\mathbb{R}$. Тогда:

- Каждому линейному отображению $\varphi : V \to W$ однозначно соответствует матрица размера $m \times n$ этого линейного отображения в базисах $\mathcal{E}$ и $\mathcal{F}$.
- Любой матрице A размера $m \times n$ однозначно соответствует линейное отображение $\varphi : V \to W$, для которого A - матрица этого линейного отображения в $\mathcal{E}, \mathcal{F}$.

6.3 Операции над линейными отображениями

Пусть V, W - векторные пространства над $\mathbb{R}$

1) Сложение линейных отображений.

$$\varphi_1 : V \to W \quad \varphi_2 : V \to W \text{ - два линейных отображения}$$

Зададим отображение по правилу

$$(\varphi_1 + \varphi_2)(x) = \varphi_1(x) + \varphi_2(x) \ \ \forall x \in V$$

Утверждение. Отображение $\varphi_1 + \varphi_2 : V \to W$ является линейным отображением.

Доказательство. $\forall a, b \in V$:

$$(\varphi_1 + \varphi_2)(a + b) = \varphi_1(a + b) + \varphi_2(a + b) =$$

$$= \varphi_1(a) + \varphi_1(b) + \varphi_2(a) + \varphi_2(b) = (\varphi_1 + \varphi_2)(a) + (\varphi_1 + \varphi_2)(b)$$

Аналогично для $(\varphi_1 + \varphi_2)(\lambda a) = \lambda(\varphi_1 + \varphi_2)(a)$ □

Фиксируем базисы $\mathcal{E} = \{e_1, ..., e_n\}$ - в V и $\mathcal{F} = \{f_1, ..., f_n\}$ - в W

A_1 - матрица линейного отображения φ_1 относительно $\mathcal{E}$ и $\mathcal{F}$.
A_2 - матрица линейного отображения φ_2 относительно $\mathcal{E}$ и $\mathcal{F}$.
B - матрица линейного отображения $\varphi_1 + \varphi_2$ относительно $\mathcal{E}$ и $\mathcal{F}$.

Утверждение. $B = A_1 + A_2$

Доказательство. Размеры совпадают

$$\varphi_1(e_i) = a_{1i}f_1 + \cdots + a_{mi}f_m$$

$$\varphi_2(e_i) = \widetilde{a_{1i}}f_1 + \cdots + \widetilde{a_{mi}}f_m$$

$$(\varphi_1 + \varphi_2)(e_i) = b_{1i}f_1 + \cdots + b_{mi}f_m$$

$$(\varphi_1+\varphi_2)(e_i) = \varphi_1(e_i)+\varphi_2(e_i) = (a_{1i}f_1+\cdots+a_{mi}f_m)+(\widetilde{a_{1i}}f_1+\cdots+\widetilde{a_{mi}}f_m) =$$

$$= (a_{1i} + \widetilde{a_{1i}})f_1 + \cdots + (a_{mi} + \widetilde{a_{mi}})f_m$$

Т.к. разложение по базису единственное, то

$$b_{1i} = a_{1i} + \widetilde{a_{1i}}, ..., b_{mi} = a_{mi} + \widetilde{a_{mi}} \Longrightarrow b_{ij} = a_{ij} + \widetilde{a_{ij}} \Longrightarrow B = A_1 + A_2$$

□

2) Умножение линейного отображение на число.
$\varphi : V \to W$ - линейное отображение, $\mu \in \mathbb{R}$ - произвольное число.
Зададим отображение по правилу: $(\mu\varphi)(x) = \mu\varphi(x) \quad \forall x \in V$

Утверждение. Отображение $\mu\varphi : V \to W$ является линейным (Упражнение)

Доказательство. Аналогично. □

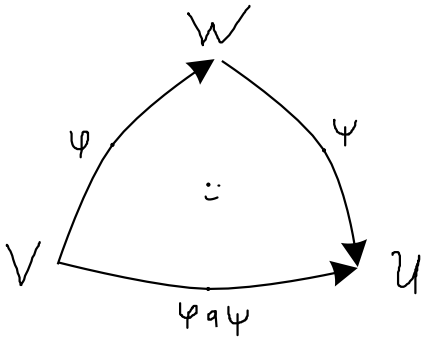
Пусть $\mathcal{E} = \{e_1, ..., e_n\}$ - базис в V и $\mathcal{F} = \{f_1, ..., f_n\}$ - базис в W.
A - матрица линейного отображения φ относительно $\mathcal{E}$ и $\mathcal{F}$.
B - матрица линейного отображения $\mu\varphi$ относительно $\mathcal{E}$ и $\mathcal{F}$.

Утверждение. $B = \mu A$

Доказательство. Видимо дз(□

3) Композиция (произведение) линейных отображений.
Пусть V, W, U - векторные простанства над $\mathbb{R}$

$$\varphi : V \to W \quad \psi : W \to U$$



Зададим отображение по правилу:

$$(\psi \circ \varphi)(x) = \psi(\varphi(x)) \ \ \forall x \in V$$

Утверждение. Отображение $\psi \circ \varphi : V \to U$ является линейным.

Доказательство. $\forall a, b \in V$

1. $(\psi \circ \varphi)(a + b) = \psi(\varphi(a + b)) = \psi(\varphi(a) + \varphi(b)) = \psi(\varphi(a)) + \psi(\varphi(b))$
2. Аналогично для $(\psi \circ \varphi)(\lambda a) = \lambda(\psi \circ \varphi)(a)$

□

Фиксируем базис: $\mathcal{E} = \{e_1, ..., e_n\}$ - базис в V
$\mathcal{F} = \{f_1, ..., f_m\}$ - базис в W
$\mathcal{G} = \{g_1, ..., g_k\}$ - базис в U

$\underset{m\times n}{A}$ - матрица линейного отображения φ относительно $\mathcal{E}, \mathcal{F}$.
$\underset{k\times m}{B}$ - матрица линейного отображения ψ относительно $\mathcal{F}, \mathcal{G}$.
$\underset{k\times n}{C}$ - матрица линейного отображения $\psi \circ \varphi$ относительно $\mathcal{E}, \mathcal{G}$.

Утверждение. $C = B \cdot A$

Доказательство.

$$\varphi(e_i) = \sum_{s=1}^{m} a_{si} f_s; \qquad \psi(f_s) = \sum_{t=1}^{k} b_{ts} g_t$$

По определению матрицы линейного отображения:

$$(\psi \circ \varphi)(e_i) = \sum_{l=1}^{k} c_{li} g_l \quad (*)$$

По определению композиции:

$$(\psi \circ \varphi)(e_i) = \psi(\varphi(e_i)) = \psi(\sum_{s=1}^{m} a_{si} f_s) = \sum_{s=1}^{m} a_{si} \psi(f_s) =$$

$$= \sum_{s=1}^{m} a_{si} (\sum_{t=1}^{k} b_{ts} g_t) = \sum_{t=1}^{k} (\sum_{s=1}^{m} b_{ts} a_{si}) g_t \quad (\star)$$

$\Longrightarrow (*) = (\star)$.

Т.к. координаты определены однозначно $\Rightarrow c_{it} = \sum\limits_{s=1}^{m} b_{ts} a_{si} \Rightarrow C = B \cdot C$ $\square$

6.4 Свойства операций над матрицами

Предположим, что все размеры матриц согласованы.

1. $M_{m \times n}(\mathbb{R})$ - векторное пространство над $\mathbb{R}$
2. Ассоциативность $A(BC) = (AB)C$

Доказательство. $\underset{m \times k}{A}, \underset{k \times n}{B}, \underset{n \times l}{C}$

Пусть $\underset{m \times l}{D} = A(BC)$, $\underset{m \times l}{\widetilde{D}} = (AB)C$.

Надо проверить, что $\forall i, j : [D]_{ij} = [\widetilde{D}]_{ij}$.

$$[D]_{ij} = [A(BC)]_{ij} = \sum_{s=1}^{k} [A]_{is} \cdot [BC]_{si} = \sum_{s=1}^{k} [A]_{is} (\sum_{t=1}^{n} [B]_{st} \cdot [C]_{ti}) =$$

$$= \sum_{s=1}^{k} \sum_{t=1}^{n} [A]_{ij} ([B]_{st} \cdot [C]_{ti})$$

$$[\widetilde{D}]_{ij} = [(AB)C]_{ij} = \sum_{t=1}^{n} [AB]_{it} [C]_{tj} = \sum_{t=1}^{n} (\sum_{s=1}^{k} [A]_{is} \cdot [B]_{st}) [C]_{tj} =$$

$$= \sum_{t=1}^{n} \sum_{s=1}^{k} ([A]_{is} \cdot [B]_{st}) \cdot [C]_{tj}$$

По свойствам операций над $\mathbb{R}$ результаты преобразований равны. $\square$

3. $A(B + C) = AB + AC$
4. $(B + C)A = BA + CA$
5. $\lambda(AB) = (\lambda A)B = A(\lambda B); \quad \forall \lambda \in \mathbb{R}$
6. $\forall A \in M_{m\times m}(\mathbb{R})$, $\exists$ единичная матрица $E \in M_{m\times m}(\mathbb{R}) : EA = A$
7. $\forall A \in M_{m\times n}(\mathbb{R}) : 0 \cdot A = 0$
8. Нет коммутативности: $AB \neq BA$ даже если размеры согласованы

Доказательство. Свойства 3. - 7. упражнение) $\square$

6.5 Свойства операции транспонирования

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

Доказательство. 4. $\underset{m\times k}{A}, \underset{k\times n}{B} \Longrightarrow \underset{n\times k}{B^T}, \underset{k\times m}{A^T}$ (размеры совпадают)
Проверим равенство $D = (AB)^T$ и $\widetilde{D} = B^T A^T$.

$$[D]_{ij} = [(AB)^T]_{ij} = [(AB)]_{ji} = \sum_{s=1}^{k} [A]_{js}[B]_{si}$$

$$[\widetilde{D}]_{ij} = B^T A^T = \sum_{s=1}^{k} [B]_{is}[A]_{sj} = \sum_{s=1}^{k} [A]_{js}[B]_{si}$$

$\square$

6.6 О ранге и операциях над матрицами

Теорема.

1. $rkA^T = rkA$
2. $rk(\lambda A) = \begin{cases} rkA, \text{ если } \lambda \neq 0 \\ 0, \text{ если } \lambda = 0 \end{cases}$
3. $rk(A+B) \leq rkA + rkB$
4. $rk(AB) \leq \min\{rkA, rkB\}$

Доказательство.

1. Следует из того, что ранг системы строк = рангу системы столбцов, и из определения ранга матрицы.
2. Очевидно.
3. Пусть $\overline{a_1}, ..., \overline{a_m}$ - строки матрицы A. $\overline{b_1}, .., \overline{b_m}$ - строки матрицы B.
   $\overline{a_1} + \overline{b_1}, ..., \overline{a_m} + \overline{b_m}$ - строки матрицы $A + B$.

   $$rkA = \dim\langle\overline{a_1}, ..., \overline{a_m}\rangle, \ rkB = \dim\langle\overline{b_1}, ..., \overline{b_m}\rangle$$

   $$rk(A+B) = \dim\langle\overline{a_1} + \overline{b_1}, ..., \overline{a_m} + \overline{b_m}\rangle$$

   Заметим, что $(\langle\overline{a_1} + \overline{b_1}, ..., \overline{a_m} + \overline{b_m}\rangle) \subseteq (\langle\overline{a_1}, ..., \overline{a_m}, \overline{b_1}, ..., \overline{b_m}\rangle)$

   Лемма. Пусть V векторное пространсво над $\mathbb{R}$ $\dim V = n$
   U - произвольное подпространство в V. Тогда $\dim U \leq n$
   Более того, если $U \neq V$, то $\dim U < n$.

   Доказательство. Пусть $\{e_1, ..., e_m\}$ - базис $U \subseteq V$, т.е. $\dim U = m$
   ЛНЗ систему $\{e_1, ..., e_m\}$ можно дополнить до базиса в $V \Longrightarrow m \leq n$
   Если $m = n$, то $\{e_1, ..., e_m\}$ - базис $V \Longrightarrow V = U$ □

   Применяем лемму и получаем, что

   $$\dim\langle\overline{a_1} + \overline{b_1}, ..., \overline{a_m} + \overline{b_m}\rangle \leq \dim\langle\overline{a_1}, ..., \overline{a_m}, \overline{b_1}, ..., \overline{b_m}\rangle$$

   Т.к. объединение базисов линейной оболочки $\overline{a_1}, ..., \overline{a_m}$ и $\overline{b_1}, .., \overline{b_m}$ является конечной порождающей системой линейной оболочки $\langle\overline{a_1}, ..., \overline{a_m}, \overline{b_1}, ..., \overline{b_m}\rangle$, а из любой конечной порождающей системы можно выбрать базис, значит:

   $$\dim\langle\overline{a_1} + \overline{b_1}, ..., \overline{a_m} + \overline{b_m}\rangle \leq \dim\langle\overline{a_1}, ..., \overline{a_m}\rangle + \dim\langle\overline{b_1}, ..., \overline{b_m}\rangle$$

   $$\Longrightarrow rk(A+B) \leq rkA + rkB$$

4. Докажем, что $rkAB \leq rkA$. Пусть $C = AB$, $\underset{m\times k}{A}, \underset{k\times n}{B}$

$A_1, ..., A_n$ - столбцы матрицы A

$B_1, ..., B_n$ - столбцы матрицы B

$C_1, ..., C_n$ - столбцы матрицы C

$$C_1 = AB_1 = A_1b_{11} + \cdots + A_kb_{k1}$$

$$C_2 = AB_2 = A_1b_{12} + \cdots + A_kb_{k2}$$

$$\vdots$$

$$C_n = AB_n = A_1b_{1n} + \cdots + A_kb_{kn}$$

$\Longrightarrow \langle C_1, ..., C_n\rangle \subseteq \langle A_1, ..., A_k\rangle \Longrightarrow \dim\langle C_1, ..., C_n\rangle \leq \dim\langle A_1, ..., A_k\rangle \Longrightarrow rkC \leq rkA$.

Докажем, что $rkAB \leq rkB$.

$$rk(AB) = rk(AB)^T = rk(B^TA^T) \leq rkB^T = rkB$$

□

7 Перестановки

Определение. Упорядоченная последовательность $(k_1, ..., k_n)$ чисел $1, 2, ..., n$, расположенных в некотором порядке, называется перестановкой из n элементов.

Пример. $(3, 1, 2)$ перестановка из 3-х элементов.

Определение. Перестановка $(1, 2, ..., n)$ называется тривиальной.

Определение. Говорят, что пара элементов k_i и k_j образуют инверсию, если:

$$i < j \Longrightarrow k_i > k_j$$

Определение. Перестановка называется четной (нечетной), если число инверсий в ней четное (нечетное).
Знак переставки $\rightarrow \operatorname{sgn}(k_1, ..., k_n) = (-1)^s$, где s - число инверсий в перестановке.

Определение. Перемена двух элементов в перестановке называется транспозицией этих элементов.

Утверждение. При транспозиции любых двух элементов четность меняется на противоположную.

Доказательство.

1. Транспозиция двух соседних элементов.
   При этом изменится расположение только этих элементов относительно других $\Longrightarrow$ количество инверсий изменился на $1 \Longrightarrow$ четность поменяется.

2. Общий случай:
   $$(..., k_i, ..., k_j, ...) \rightarrow (..., k_j, ..., k_i, ...)$$
   Пусть между k_i и k_j (s) элементов.
   Перемену k_i и k_j произведем за $2s + 1$ транспозицию соседних элементов.
   Сначала k_i переставим последовательно с каждым из элементов, стоящих между k_i и k_j (это s транспозиций), потом k_i переставим с k_j, затем k_j поставим на i позицию (это еще s транспозиций).
   Т.к. транспозиция соседних элементов меняет четность, то за $2s+1$ транспозицию четность изменится.

□

Следствие. Пусть $n > 1$. Тогда число четных перестановок из n элементов равно числу нечетных.

Доказательство. Перечислим все четные перестановки и в каждой поменяем местами первые 2 элемента. При этом получим различные нечетные перестановки $\Longrightarrow$ число четных перестановок $\leq$ числа нечетных. Аналогично в обратную сторону.
$\Longrightarrow$ число четных $=$ число нечетных. $\square$

Утверждение. Число перестановок из n элементов равно $n!$

Доказательство. $(k_1, ..., k_n)$ для k_1 вариантов - n
Пусть выбрали $k_1 \Longrightarrow$ для k_2 вариантов - $n-1$ и т.д. Получаем всего вариантов: $n \cdot (n-1) \cdot ... \cdot 1 = n!$ $\square$

8 Определители n-го порядка

Определение. Определителем квадратной матрицы $\underset{n\times n}{A} = (a_{ij})$ порядка n называется число, которое вычисляется по формуле:

$$|A| = \det A = \sum_{(k_1,\ldots,k_n)} \operatorname{sgn}(k_1,\ldots,k_n) a_{1k_1} a_{2k_2} \ldots a_{nk_n}$$

Где $\sum\limits_{(k_1,\ldots,k_n)}$ - сумма по всем перестановкам из n элементов. Эта формула называется формулой полного разложения или полного развертывания определителя.

Пример.

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \operatorname{sgn}(1,2) a_{11}a_{22} + \operatorname{sgn}(2,1) a_{12}a_{21} = a_{11}a_{22} - a_{12}a_{21}$$

$$\underset{n\times n}{A} = \begin{pmatrix} \overline{a_1} \\ \overline{a_2} \\ \vdots \\ \overline{a_n} \end{pmatrix}$$

Пусть $\overline{a_1}, \overline{a_2}, \ldots \overline{a_n}$ - строки матрицы A. Тогда определитель можно рассматривать как функцию от строк $\det A = \det(\overline{a_1}, \overline{a_2}, \ldots \overline{a_n})$

Определение. Функция $f(v_1, \ldots, v_n)$, которая векторам $v_1, \ldots, v_n$ в вектроном простанстве V над $\mathbb{R}$ ставит в соответствие число из $\mathbb{R}$, то есть:

$$f : V \times \cdots \times V \to \mathbb{R}$$

называется полилинейной, если она линейна по каждому аргументу, т.е. для каждого $i = \overline{1, n}$ выполнено:

1. $f(v_1, \ldots, v_i + \widetilde{v_i}, \ldots, v_n) = f(v_1, \ldots, v_i, \ldots, v_n) + f(v_1, \ldots, \widetilde{v_i}, \ldots, v_n)$, $\forall v_i, \widetilde{v_i} \in V$.
2. $f(v_1, \ldots, \lambda v_i, \ldots, v_n) = \lambda f(v_1, \ldots, v_i, \ldots, v_n),\ \forall \lambda \in \mathbb{R},\ \forall v_i \in V$.

Определение. Полилинейная функция $f : V \times \cdots \times V \to \mathbb{R}$ называется кососимметричной, если при перестановке любых двух аргументов значение функции умножается на (-1). Кососимметричная функция с двумя одинаковыми аргументами равна нулю.

Пример. Если f - кососимметричная функция и $v_1 = v_2$, то
$f(v_1, v_2, v_3, \ldots, v_n) = -f(v_2, v_1, v_3, \ldots, v_n) = a \Longrightarrow a = -a \Longrightarrow a = 0$.

8.1 Свойства определителей

Теорема 1. Определитель n-го порядка является кососимметричной полилинейной функцией от строк матрицы.

Доказательство.

$$A = \begin{pmatrix} \overline{a_1} \\ \overline{a_2} \\ \vdots \\ \overline{a_n} \end{pmatrix} = (a_{ij}),\ \overline{a_i} = (a_{i1}, \dots, a_{in})$$

$$\det A = \det(\overline{a_1}, \dots \overline{a_n}) = \sum_{(k_1, \dots k_n)} \operatorname{sgn}(k_1, \dots k_n) a_{1k_1} \dots a_{nk_n}$$

Докажем, что $\det A$ линеен по i-му аргументу.

$$\det A = \sum_{k=1}^{n} a_{ik} u_k$$

где u_k - число, не зависящее от элементов строки $\overline{a_i}$

1. $\det(\overline{a_1}, \dots, \overline{a_i} + \overline{a_i}', \dots, \overline{a_n}) = \sum_{k=1}^{n} (a_{ik} + a'_{ik}) u_k = \sum_{k=1}^{n} a_{ik} u_k + \sum_{k=1}^{n} a'_{ik} u_k =$
$$= \det(\overline{a_1}, \dots, \overline{a_i}, \dots, \overline{a_n}) + \det(\overline{a_1}, \dots, \overline{a_i}', \dots, \overline{a_n})$$

2. $\det(\overline{a_1}, \dots, \lambda\overline{a_i}, \dots, \overline{a_n}) = \sum_{k=1}^{n} (\lambda a_{ik}) u_k = \lambda \sum_{k=1}^{n} a_{ik} u_k = \lambda \det(\overline{a_1}, \dots, \overline{a_i}, \dots, \overline{a_n})$

Теперь докажем кососимметричность:

$$\det(\overline{a_1}, \dots, \underset{(a_i)}{\overline{a_j}}, \dots, \underset{(a_j)}{\overline{a_i}}, \dots, \overline{a_n}) =$$
$$= \sum_{(k_1 \dots k_i \dots k_j \dots k_n)} \operatorname{sgn}(k_1, \dots k_n) a_{1k_1} \dots a_{jk_i} \dots a_{ik_j} \dots a_{nk_n} =$$
$$= \sum_{(k_1 \dots k_i \dots k_j \dots k_n)} \operatorname{sgn}(k_1, \dots k_n) a_{1k_1} \dots a_{ik_j} \dots a_{jk_i} \dots a_{nk_n} =$$
$$= - \sum_{(k_1 \dots k_i \dots k_j \dots k_n)} \operatorname{sgn}(k_1, \dots k_n) a_{1k_1} \dots a_{ik_i} \dots a_{jk_j} \dots a_{nk_n} =$$
$$= - \det(\overline{a_1}, \dots, \overline{a_i}, \dots, \overline{a_j}, \dots, \overline{a_n})$$

□

Теорема 2. Пусть $f(A) = f(\overline{a_1}, \ldots, \overline{a_n})$ - функция от строк, $A \in M_n(\mathbb{R})$ такие, что:

1. $f(E) = 1$
2. f - Полилинейная
3. f - Кососимметричная

тогда $f(A) = \det A$.

Доказательство. $e_1 = (1, 0, ..., 0), ..., e_n = (0, ..., 0, 1)$ - строки единичной матрицы $E = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \Longrightarrow \{e_1, ..., e_n\}$ - базис в векторном пространстве $\mathbb{R}^n$

$$\Longrightarrow \overline{a_i} = (a_{i1}, ..., a_{in}) = a_{i1}e_1 + \cdots + a_{in}e_n$$

$$\Longrightarrow f(A) = f(\overline{a_1}, ..., \overline{a_n}) = f(\sum_{k_1=1}^{n} a_{1k_1}e_{k_1}, ..., \sum_{k_n=1}^{n} a_{nk_n}e_{k_n}) =$$

$$= \sum_{k_1=1}^{n} ... \sum_{k_n=1}^{n} a_{1k_1} \cdot ... \cdot a_{nk_n} \cdot f(e_{k_1}, ..., e_{k_n}) =$$

$$= \sum_{(k_1,...,k_n)} f(e_{k_1}, ..., e_{k_n}) \cdot a_{1k_1} \cdot ... \cdot a_{nk_n}$$

Осталось доказать, что $f(e_{k_1}, ..., e_{k_n}) = \operatorname{sgn}(k_1, ..., k_n)$.
Т.к. $f(E) = 1$, то $f(A) = f(e_1, e_2, ..., e_n) = \operatorname{sgn}(1, 2, ..., n)(*)$
Меняя любые два аргумента местами, f меняет знак, т.к. f кососимметрична. С другой стороны, меняя два любые числа перестановки местами, знак перестановки sgn тоже меняет знак.
Любую перестановку можно получить из тривиальной за конечное число транспозиций.
Т.к. $(*)$ верно, то, делая последовательно транспозицию в перестановке, и такую же перемену аргументов у функции f, получим $f(e_{k_1}, ..., e_{k_n}) = \operatorname{sgn}(k_1, ..., k_n)$. □

Следствие.

1. Если в квадратной матрице A одна из строк равна линейной комбинации остальных, то $detA = 0$

2. Если к строке квадратной матрицы A применить ЭП1 (т.е. к строке прибавить другую, умноженную на число), то определитель не изменится.

Доказательство.

2) $det(\overline{a_1}, ..., \overline{a_i} + \lambda\overline{a_j}, ..., \overline{a_n}) =$

$$= det(\overline{a_1}, ..., \overline{a_i}, ..., \overline{a_j}, ..., \overline{a_n}) + \lambda det(\overline{a_1}, ..., \overline{a_j}, ..., \overline{a_j}, ..., \overline{a_n}) =$$

$$= det(\overline{a_1}, ..., \overline{a_i}, ..., \overline{a_j}, ..., \overline{a_n})$$

□

Определение. Квадратная матрица $A = (a_{ij})$ называется верхнетреугольной (нижнетреугольной) матрицей, если $a_{ij} = 0$ при $i > j$.

Пример. $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 2 \\ 0 & 0 & 0 \end{pmatrix}$

Можно проследить, как влияют ЭП на определитель:

- ЭП1: $\overline{a_i} \to \overline{a_i} + \lambda\overline{a_j}$ — det не изменится.
- ЭП2: $\overline{a_i} \leftrightarrow \overline{a_j}$ — det умножается на -1.
- ЭП3: $\overline{a_i} \to \mu\overline{a_i}, \mu \neq 0$ — det умножится на μ.

Утверждение. Определитель верхнетреугольной матрицы равен произведению диагональных элементов.

Доказательство. $\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ & & \ddots & \\ 0 & 0 & \cdots & a_{nn} \end{vmatrix} = a_{11} \cdot a_{22} \cdot ... \cdot a_{nn}$

Рассмотрим любую не тождественную перестановку $(k_1, ..., k_n)$, где $k_i \neq i$. Тогда найдется такой множитель $(i > j)$ $a_{ij} = 0 \Longrightarrow$ это слагаемое обнулится. $\Longrightarrow$ Во всей сумме останется только тождественная перестановка. □

Теорема 3. Определитель при транспонировании не изменяется: $detA = detA^T$

Доказательство. Пусть $B = A^T,\ a = (a_{ij}),\ B = (b_{ij})$
$detA = \sum\limits_{(l_1,...,l_n)} \text{sgn}(l_1,...,l_n)a_{1l_1},...,a_{nl_n}$

$$detA^T = detB = \sum_{(k_1,...,k_n)} \text{sgn}(k_1,...,k_n)b_{1k_1},...,b_{nk_n} =$$
$$= \sum_{(k_1,...,k_n)} \text{sgn}(k_1,...,k_n)a_{k_1 1},...,a_{k_n n} =$$
$$= \sum_{(k_1,...,k_n)} \text{sgn}(k_1,...,k_n)\text{sgn}(1,2,...,n)a_{k_1 1},...,a_{k_n n} = (*)$$

Переставим a_{ij}, переупорядочив номера строк, т.е. первые индексы по возрастанию последовательно, меняя два множителя местами:

$$a_{k_1 1},...,\underbrace{a_{k_i i},...,a_{k_j j}}_{\text{меняем}},...,a_{k_n n}$$

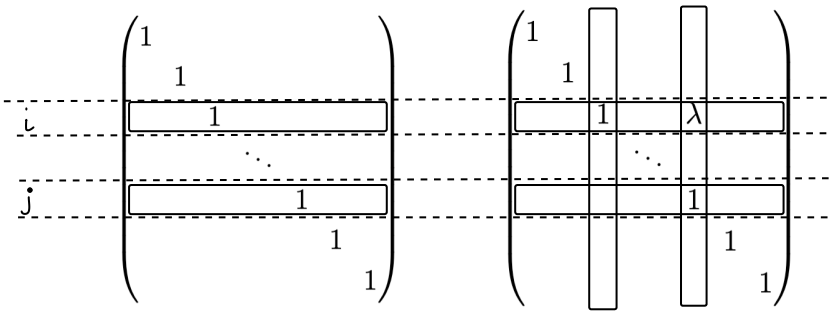
При этой перемене двух множителей местами меняются местами и первые индексы, и вторые. При этом:

$$\text{sgn}(k_1,...,k_i,...,k_j,...,k_n)\cdot\text{sgn}(1,...,i,...,j,...,n) =$$
$$= (-1)^2\text{sgn}(k_1,...,k_j,...,k_i,...,k_n)\cdot\text{sgn}(1,...,j,...,i,...,n)$$
$$(*) = \sum_{(l_1,...,l_n)} \text{sgn}(1,2,...,n)\text{sgn}(l_1,...,l_n)a_{1l_1},...,a_{nl_n} = detA \qquad \square$$

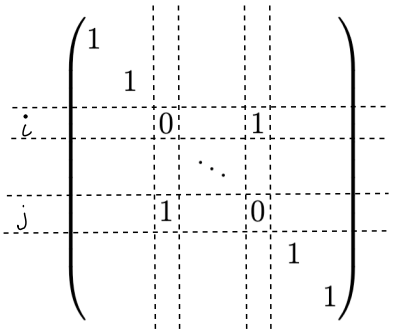
Следствие. Определитель матрицы есть кососимметричная и полилинейная функция столбцов матрицы.
Все свойства определителя, которые верны для строк матрицы, верны и для столбцов.

8.2 Элементарные матрицы

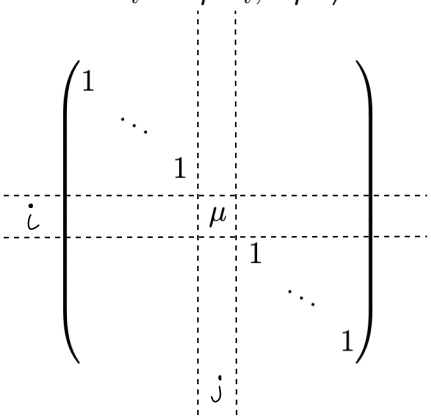
Определение. Матрица T , полученная из единичной матрицы E, с помощью одного элементарного преобразования над строками или столбцами, называется элементарной матрицей.
ЭП1: $\overline{a_i} \to \overline{a_i} + \lambda\overline{a_j},\quad i \neq j$



ЭП2: $\overline{a_i} \leftrightarrow \overline{a_j}, \quad i \neq j$



ЭП3: $\overline{a_i} \leftrightarrow \mu\overline{a_i}, \quad \mu \neq 0$



Лемма 1.

1.1 Любые ЭП над строками матрицы A равносильны умножению матрицы A слева на элементарную матрицу, т.е.
$A \rightsquigarrow \widetilde{A} \Longleftrightarrow \widetilde{A} = T \cdot A$, где T - элементарная матрица, такая что $E \rightsquigarrow T$

1.2 Любые ЭП над столбцами матрицы A равносильны умножению матрицы A справа на элементарную матрицу.

Доказательство. Непосредственная проверка □

Лемма 2. Пусть A - квадратная матрица порядка n, тогда:

1. Если $detA \neq 0$, то с помощью ЭП над строками A можно привести к E.
2. Если $detA = 0$, то с помощью ЭП над строками в A можно получить нулевую строку

Доказательство. Методом Гаусса любую матрицу можно привести к ступенчатому виду. Ступенчатый вид для квадратной матрицы является верхнетреугольной, т.е.:

$$A \rightsquigarrow \widetilde{A} = \begin{pmatrix} \widetilde{a_{11}} & & * \\ & \ddots & \\ 0 & & \widetilde{a_{nn}} \end{pmatrix}$$

$\Longrightarrow detA = \xi \cdot det\widetilde{A}$, где $\xi \neq 0$, $det\widetilde{A} = \widetilde{a_{11}} \cdot ... \cdot \widetilde{a_{nn}}$
Итак,

$$detA = 0 \Longleftrightarrow det\widetilde{A} = 0 \Longleftrightarrow \widetilde{a_{11}} \cdot ... \cdot \widetilde{a_{nn}} = 0$$

1. Если $detA \neq 0$, то $a_{11} \neq 0, ..., a_{nn} \neq 0$ - лидеры матрицы A
   $\Longrightarrow \widetilde{A}$ приводится к улучшенному ступенчатому виду обратным ходом Гаусса и этот улучшенный ступенчатый вид совпадает с E

2. Если $detA = 0$, то $a_{11} \cdot ... \cdot a_{nn} = 0 \Longrightarrow \exists k : a_{kk} = 0$. По определению ступенчатого вида $\forall i > k : \widetilde{a_{ii}} = 0 \Longrightarrow \widetilde{a_{nn}} = 0 \Longrightarrow$ последняя строка в $\widetilde{A}$ нулевая.

□

Теорема 4. Пусть A, B - квадратные матрицы порядка n, тогда:

$$detAB = detA \cdot detB$$

Доказательство. Из ассоциативности умножения $T(AB) = (TA)B$, где T элементарная матрица, получаем, что элементраное преобразование над строками матрицы A соответствует элементарному преобразованию строк матрицы AB.

1 случай. $detA = 0$ (по лемме (1), пункт 2)$\Longrightarrow A \rightsquigarrow \widetilde{A}$(с нулевой строкой)
$\Longrightarrow \widetilde{A} = \cdot(T_1 \cdot ... \cdot T_k) \cdot A$, где T_i - матрицы элементарных преобразований.
$\Longrightarrow (T_1 \cdot ... \cdot T_k)(AB) = ((T_1 \cdot ... \cdot T_k)A)B = \widetilde{A}B \Longrightarrow detAB = 0$, т.к. $AB \rightsquigarrow \widetilde{A}B$

2 случай. $detA \neq 0$ (по лемме (1), пункт 1) $\Longrightarrow A \rightsquigarrow E \Longrightarrow E = (T_1 \cdot ... \cdot T_k)A$, где T_i - матрицы элементарных преобразований.
$(T_1 \cdot ... \cdot T_k)(AB) = ((T_1 \cdot ... \cdot T_k)A)B = EB = B$
$\Longrightarrow detAB = c \cdot det((T_1 \cdot ... \cdot T_k)AB) = c \cdot detB$
Рассмотрим отношение:

$$\frac{detAB}{detA} = (*)$$

Произведем над матрицей A ЭП, которые приведут матрицу $A \rightsquigarrow E$, одновременно производим такие же ЭП над AB.

$$(*) = \frac{detEB}{detE} = detB$$

□

Теорема 5. (Об определителе с углом нулей)
Пусть A - квадратная матрица порядка k
B - квадратная матрица порядка m
C - матрица размера $k \times m$.
Тогда:

$$det \left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array}\right) (*) = detA \cdot detB$$

Доказательство.

1 случай. $detB = 0$

(По лемме (2), пункт 2) $B \rightsquigarrow \widetilde{B}$ Производя точно такие же ЭП над последними m строками матрицы $(*)$, получаем нулевую строку

$$\Longrightarrow det \left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array}\right) = detA \cdot detB = 0$$

2 случай. $detA = 0$ Аналогично как в 1 случае, только ЭП над столбцами.

3 случай. $detA \neq 0, detB \neq 0$

Рассмотрим отношение:

$$\frac{det \left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array}\right)}{detA \cdot detB}$$

(По лемме (2), пункт 1) $A \rightsquigarrow E$, $B \rightsquigarrow E$

Преобразуем матрицу A с помощью ЭП над столбцами, которые приводят $A \rightsquigarrow E$, преобразуем B с помощью ЭП над строками, которые приводят $B \rightsquigarrow E$. Одновременно преобразуем матрицу $(*)$ с помощью таких же ЭП над строками и столбцами, отношение при этом не изменится.

Тогда:

$$\frac{det \left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array}\right)}{detA \cdot detB} = \frac{det \left(\begin{array}{c|c} E & C \\ \hline 0 & E \end{array}\right)}{detE \cdot detE} = 1$$

□

8.3 Разложение определителя по строке

A - матрица размера $m \times n$.

$i_1, ..., i_k$ - номера некоторого разложения строк в A.

$j_1, ..., j_t$ - номера некоторого разложения столбцов в A.

Определение. Матрица, состоящая из элементов матрицы A, стоящих на пересечении строк с номерами $i_1, ..., i_k$ и столбцов с номерами $j_1, ..., j_t$, называется подматрицей матрицы A

Обозначение: $A^{\begin{matrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_t \end{matrix}}$

Определение. Минором $k-$ого порядка матрицы A называется определитель квадратной подматрицы порядка k.

Пример.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & \boxed{6} & 7 & \boxed{8} \\ 9 & \boxed{7} & 8 & \boxed{7} \end{pmatrix} \Longrightarrow \text{Минор} = \begin{vmatrix} 6 & 8 \\ 7 & 7 \end{vmatrix}$$

Пусть A - квадратная матрица порядка n

Определение. Минор порядка $(n-1)$ квадратной матрицы A, порядка n, полученный вычеркиванием $i-$ой строки и $j-$ого столбца, называется дополнительным минором к элементу a_{ij}.
Обозначается: M_{ij}

Пример.

$$\begin{pmatrix} 1 & 2 & 3 \\ \boxed{4} & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \Longrightarrow M_{12} = \begin{vmatrix} 2 & 3 \\ 8 & 9 \end{vmatrix} = -6$$

Определение. Алгебраическое дополнение к элементу a_{ij} - это число:

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

Пример. (к прошлому примеру) $A_{21} = (-1)^{2+1}(-6) = 6$

Лемма. Матрица $\overline{A}$, полученная из A заменой $i-$ой строки на $(0, ..., 0, a_{ij}, 0, ..., 0)$:

$$det\overline{A} = det \begin{pmatrix} & & \vdots & & \\ 0 & \cdots & a_{ij} & \cdots & 0 \\ & & \vdots & & \end{pmatrix} = a_{ij} \cdot A_{ij}$$

Доказательство.

$$\begin{vmatrix} a_{11} & ... & ... & ... & a_{1n} \\ \vdots & & & & \vdots \\ 0 & ... & a_{ij} & ... & 0 \\ \vdots & & & & \vdots \\ a_{n1} & ... & ... & ... & a_{nn} \end{vmatrix} = (-1)^{i-1} \cdot (-1)^{j-1} \cdot \left|\begin{array}{c|c} a_{ij} & 0 \\ \hline * & B \end{array}\right| =$$

$$= (-1)^{i+j} \cdot a_{ij} \cdot detB = (-1)^{i+j} \cdot a_{ij} \cdot M_{ij} = a_{ij} \cdot A_{ij}$$

где B - подматрица A, из которой вычеркнули $i-$ую строку и $j-$ый столбец. $\square$

Теорема 6.

1. $detA = \sum\limits_{j=1}^{n} a_{ij}A_{ij}$ - формула разложения по i-ой строке.

2. $detA = \sum\limits_{i=1}^{n} a_{ij}A_{ij}$ - формула разложения по j-ому столбцу.

Доказательство.

$$detA = \begin{vmatrix} a_{11} & ... & ... & ... & a_{1n} \\ \vdots & & & & \vdots \\ a_{i1} & ... & ... & ... & a_{in} \\ \vdots & & & & \vdots \\ a_{n1} & ... & ... & ... & a_{nn} \end{vmatrix} \overset{\text{В силу линейности}}{=}$$

$$= \begin{vmatrix} a_{11} & ... & ... & ... & a_{1n} \\ \vdots & & & & \vdots \\ a_{i1} & 0 & ... & ... & 0 \\ \vdots & & & & \vdots \\ a_{n1} & ... & ... & ... & a_{nn} \end{vmatrix} + ... + \begin{vmatrix} a_{11} & ... & ... & ... & a_{1n} \\ \vdots & & & & \vdots \\ 0 & ... & ... & 0 & a_{in} \\ \vdots & & & & \vdots \\ a_{n1} & ... & ... & ... & a_{nn} \end{vmatrix} =$$

$$= a_{i1}A_{i1} + ... + a_{in}A_{in} = \sum_{j=1}^{n} a_{ij}A_{ij}$$

□

8.4 Определитель Вандермонда

Определение. $V(x_1, ..., x_n)$ - определитель Вандермонда.

$$V(x_1, ..., x_n) = \begin{vmatrix} 1 & 1 & 1 & ... & 1 \\ x_1 & x_2 & x_3 & ... & x_n \\ x_1^2 & x_2^2 & x_3^2 & ... & x_n^2 \\ \vdots & \vdots & \vdots & ... & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & ... & x_n^{n-1} \end{vmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i)$$

Вычисление индукции по n

База: $n = 2 : \begin{vmatrix} 1 & 1 \\ x_1 & x_2 \end{vmatrix} = x_2 - x_1$

Пусть верно для $(n-1)$, тогда вычислим для n:

$$V(x_1,...,x_n) \overset{(1)}{=}$$

$$\overset{(1)}{=} \begin{vmatrix} 1 & 1 & 1 & ... & 1 \\ 0 & x_2-x_1 & x_3-x_1 & ... & x_n-x_1 \\ 0 & x_2^2-x_1x_2 & x_3^2-x_1x_3 & ... & x_n^2-x_1x_n \\ \vdots & \vdots & \vdots & ... & \vdots \\ 0 & x_2^{n-1}-x_1x_2^{n-2} & x_3^{n-1}-x_1x_3^{n-2} & ... & x_n^{n-1}-x_1x_n^{n-2} \end{vmatrix} \overset{(2)}{=}$$

$$\overset{(2)}{=} \begin{vmatrix} x_2-x_1 & x_3-x_1 & ... & x_n-x_1 \\ x_2^2-x_1x_2 & x_3^2-x_1x_3 & ... & x_n^2-x_1x_n \\ \vdots & \vdots & ... & \vdots \\ x_2^{n-1}-x_1x_2^{n-2} & x_3^{n-1}-x_1x_3^{n-2} & ... & x_n^{n-1}-x_1x_n^{n-2} \end{vmatrix} \overset{(3)}{=}$$

$$\overset{(3)}{=} \begin{vmatrix} x_2-x_1 & x_3-x_1 & ... & x_n-x_1 \\ x_2(x_2-x_1) & x_3(x_3-x_1) & ... & x_n(x_n-x_1) \\ \vdots & \vdots & ... & \vdots \\ x_2^{n-2}(x_2-x_1) & x_3^{n-2}(x_3-x_1) & ... & x_n^{n-2}(x_n-x_1) \end{vmatrix} =$$

$$= \prod_{j=2}^{n}(x_j-x_1) \begin{vmatrix} 1 & 1 & ... & 1 \\ x_2 & x_3 & ... & x_n \\ \vdots & \vdots & ... & \vdots \\ x_2^{n-2} & x_3^{n-2} & ... & x_n^{n-2} \end{vmatrix} =$$

$$= \prod_{j=2}^{n}(x_j-x_1) \prod_{2\le i<j\le n}(x_j-x_i) = \prod_{1\le i<j\le n}(x_j-x_i)$$

(1) Из каждой строки, начиная с последней, вычитаем предыдущую, умноженную на x_1

(2) По теореме об определителе с углом нулей

(3) Выносим (x_j-x_1)

Следствие. (О фальшивом разложении определителя)
Пусть $A=(a_{ij})$ - квадратная матрица порядка n, тогда:

$$\sum_{j=1}^{n} a_{ij}A_{kj} = 0 \text{ (при } i \neq k)(*)$$

$$\sum_{i=1}^{n} a_{ij}A_{ik} = 0 \text{ (при } j \neq k)$$

$(*)$ - Т.е. алгебраическое дополнение берем из другой строки

Доказательство. Для сторок (для столбцов аналогично)

$$A = \begin{pmatrix} \overline{a_1} \\ \overline{a_2} \\ \vdots \\ \overline{a_n} \end{pmatrix}$$

Рассмотрим матрицу B, где вместо k-ой строки стоит i-ая.

$$detB = \begin{vmatrix} \overline{a_1} \\ \vdots \\ \overline{a_i} \\ \vdots \\ \overline{a_i} \\ \vdots \\ \overline{a_n} \end{vmatrix} = 0 \text{ (т.к совпадающие строки)}$$

С другой стороны, разложим $detB$ по k-ой строке:

$$B = (b_{ij}),\ detB = \sum_{j=1}^{n} b_{kj}B_{kj} = \sum_{j=1}^{n} a_{ij}A_{kj}$$

□

8.5 О ранге

Определение. Квадратная матрица A порядка n называется невырожденной, если $rkA = n$ (т.е. её строки ЛНЗ, как и все столбцы)

Теорема 7. Квадратная матрица A является невырожденной $\iff detA \neq 0$

Доказательство. Пусть $A = (a_{ij})$ - квадратная матрица порядка n
Надо доказать, что $rkA = n \iff detA \neq 0$

$\Longleftarrow$ $detA \neq 0 \Longrightarrow$ (по лемме (2), пункт 1) $A \sim E \Longrightarrow rkA = rkE = n$

$\Longrightarrow$ $rk = n$. Допустим, что $detA = 0 \Longrightarrow$ (по лемме (2), пункт 2) $A \sim \widetilde{A}$, где $\widetilde{A}$ - матрица с нулевой строкой $\Longrightarrow rkA = rk\widetilde{A} < n$. Противоречие $\Longrightarrow detA \neq 0$

□

Следствие.

- Все строки квадратной матрицы A ЛНЗ $\Longleftrightarrow detA \neq 0$
- Все столбцы квадратной матрицы A ЛНЗ $\Longleftrightarrow detA \neq 0$

Теорема. (О ранге матрицы)
Ранг матрицы A совпадает с максимальным порядком отличного от нуля минора.

Доказательство. Пусть $rkA = r$

- Докажем, что все миноры порядка s, где $s > r$ равны нулю.
  Рассмотрим произвольный минор M порядка s:

$$M = det\ A\begin{matrix} i_1 & \cdots & i_s \\ j_1 & \cdots & j_s \end{matrix}$$

  т.к. $s > r$, то строки матрицы A с номерами $i_1, ..., i_s$ ЛЗ $\Longrightarrow$ строки, образующие минор, ЛЗ $\Longrightarrow M = 0$

- Докажем, что $\exists$ хотя бы один ненулевой минор $\widetilde{M}$ порядка r.
  Т.к. $rkA = r$, то $\exists$ r ЛНЗ строк $\Longrightarrow rkB = r$ (где B - матрица с r ЛНЗ строк и все столбцы) $\Longrightarrow$ в B $\exists$ r ЛНЗ столбцов. Сформируем матрицу C из этих столбцов $\Longrightarrow detC \neq 0$
  $det\ C$ - это и есть искомый минор $\widetilde{M}$

□

Определение. Пусть $M = det\ A\begin{matrix} i_1 & \cdots & i_s \\ j_1 & \cdots & j_s \end{matrix}$ - минор порядка s
$i \notin \{i_1, .., i_s\},\ j \notin \{j_1, .., j_s\}$

$\widetilde{M} = det\ A\begin{matrix} i_1 & \cdots & i_s\ i \\ j_1 & \cdots & j_s\ j \end{matrix}$ - минор порядка $s + 1$
$\widetilde{M}$ - окаймляющий минор минора M.

Пример.

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 1 & 3 & 5 \\ 1 & -1 & 0 & 7 \end{pmatrix}$$

$$M = det\ A\begin{matrix} 1 & 3 \\ 2 & 4 \end{matrix} = \begin{vmatrix} 2 & 4 \\ 1 & 5 \end{vmatrix} = 6$$

$$\widetilde{M} = det\ A \begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{matrix} = \begin{vmatrix} 2 & 3 & 4 \\ 6 & 7 & 8 \\ 1 & 3 & 5 \end{vmatrix} = 0$$

Метод окаймляющих миноров:

$\exists\ M_1 \neq 0?$

да ↙ ↘ нет

$\exists\ M_2 \neq 0?$ $\quad rkA = 0$

да ↙ ↘ нет

$\exists\ M_3 \neq 0?$ $\quad rkA = 1$

да ↙ ↘ нет

... $\quad$ ...

Утверждение. Пусть $A = (a_{ij})$ - матрица размера $m \times n$, $\exists$ минор M порядка r, отличный от нуля, и все миноры, окаймляющие его, равны нулю.
Тогда $rkA = r$.

Доказательство. Пусть $M = det\ A \begin{matrix} i_1 & \cdots & i_r \\ j_1 & \cdots & j_r \end{matrix}$. Т.к. $M \neq 0$, то строки матрицы A с номерами $i_1, ..., i_r$ ЛНЗ $\Longrightarrow rkA \geq r$
Предположим, что $rkA \geq r+1$. Рассмотрим строки $\overline{a_{i_1}}, ..., \overline{a_{i_r}}$, которые формируют минор M. Они ЛНЗ.
Т.к. $rkA \geq r+1$, то $\exists\ i \notin \{i_1, ..., i_r\} : \overline{a_i}$ не выражается линейно через $\overline{a_{i_1}}, ..., \overline{a_{i_r}} \Longrightarrow \overline{a_{i_1}}, ..., \overline{a_{i_r}}, \overline{a_i}$ - ЛНЗ.
Образуем из этих строк матрицу $B \Longrightarrow rkB = r+1 \Longrightarrow \exists\ r+1$ ЛНЗ столбец.
Столбцы с номерами $j_1, ..., j_r$ ЛНЗ, т.к. $M \neq 0$
Т.к. $rkB = r+1$, то $\exists\ j \notin \{j_1, ..., j_r\}$: столбец с номером j не выражается через столбцы с номерами $j_1, ..., j_r$
Расмотрим подматрицу C матрицы B, составленную из столбцов с номерами $j_1, ..., j_r, j \Longrightarrow C-$ квадратная матрица порядка $r+1$ из ЛНЗ столбцов $\Longrightarrow det\ C \neq 0$
$\Longrightarrow$ т.к. $det\ C$ является окаймляющим минором минора M, получаем противоречие условию $\Longrightarrow rkA = r$. $\square$

8.6 Правила Крамера СЛУ

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_n \end{cases}$$ Матричная форма $AX = B$

СЛУ называется квадратной, если $m = n$

Пусть СЛУ $AX = B$ - квадратная.

Обозначение: $\triangle = detA = det(A_1, ..., A_n)$

$\triangle_i = det(A_1, ..., B, ...A_n)$

Теорема. Пусть $AX = B$ - квадратная СЛУ с невырожденной A
Тогда СЛУ имеет единственное решение и это решение можно найти по формуле:

$$x_1 = \frac{\triangle_1}{\triangle}, ..., x_n = \frac{\triangle_n}{\triangle}$$

Доказательство. Т.к. A - невырожденная, то $detA \neq 0 \Longrightarrow A \rightsquigarrow E$
Будем решать СЛУ методом Гаусса:

$$(A|B) = (E|\widetilde{B}) \Longrightarrow \begin{cases} x_1 = \widetilde{b_1} \\ \vdots \\ x_n = \widetilde{b_n} \end{cases}$$

$$\frac{\triangle_i}{\triangle} = \frac{det(A_1, ..., B, ..., A_n)}{det(A_1, ..., A_i, ...A_n)} = \frac{det(E_1, ..., \widetilde{B}, ..., E_n)}{det(E_1, ..., E_i, ...E_n)} = \frac{\widetilde{b_i}}{1} = \widetilde{b_i}$$

□

8.7 Обратная матрица

Пусть A - квадратная матрица порядка n

Определение. Матрица B - называется обратной матрицей к A, если:

$$\begin{cases} A \cdot B = E \\ B \cdot A = E \end{cases}$$

Обозначается A^{-1}

Утверждение. Если квадратная матрица A имеет обратную матрицу, то она одна.

Доказательство. Пусть $\exists$ две обратной матрицы B_1, B_2 , тогда:

$$B_1(AB_2) = (B_1A)B_2$$

$$B_1E = EB_2$$

$$B_1 = B_2$$

□

Свойства.

1. Если матрица A имеет обратную, то A^{-1} тоже имеет обратную, причем $(A^{-1})^{-1} = A$
2. Если матрица A имеет обратную, $\lambda \neq 0$, то λA, тоже имеет обратную, причем $(\lambda A)^{-1} = \lambda^{-1}A^{-1}$
3. Если матрица A имеет обратную, то A^T тоже имеет обратную, причем $(A^T)^{-1} = (A^{-1})^T$
4. Если матрицы A, B квадратные порядка n и каждая имеет обратную, то AB тоже имеет обратную, причем $(AB)^{-1} = B^{-1}A^{-1}$

Доказательство. Докажем, что $B^{-1}A^{-1}$ удовлетворяет определению обратной матрицы для AB

$$(A \cdot B)(B^{-1} \cdot A^{-1}) = A(BB^{-1})A^{-1} = AEA^{-1} = AA^{-1} = E$$

$$(B^{-1} \cdot A^{-1})(A \cdot B) = B^{-1}(A^{-1}A)B = B^{-1}EB = B^{-1}B = E$$

$$\Longrightarrow (A \cdot B)(B^{-1} \cdot A^{-1}) = (B^{-1} \cdot A^{-1})(A \cdot B) = E$$

□

Замечание. A, B, имеют обратные $\not\Rightarrow A + B$, имеет обратную.

Пример. A и $-A$

Утверждение. Любая элементарная матрица T имеет обратную, причем она соответствует обратному преобразованию.

Доказательство. Непосредственная проверка. □

Теорема. (Критерий существования обратной матрицы)
Квадратная матрица A имеет обратную $\Longleftrightarrow$ она невырожденная.

Доказательство. Пусть A - квадратная, порядка n
Надо доказать, что $\exists A^{-1} \iff rkA = n \iff detA \neq 0$

$\Longrightarrow$ Пусть $\exists\ A^{-1}$. По определению $AA^{-1} = E$
Вычислим определитель обеих частей равенства:

$$detA \cdot detA^{-1} = det(AA^{-1}) = detE = 1 \Longrightarrow detA \neq 0$$

$\Longleftarrow$ Пусть A - невырожденная, $detA \neq 0 \Longrightarrow A \rightsquigarrow E \Longrightarrow \exists$ набор элементарных матриц
$T_1, ..., T_k : (T_1 \cdot ... \cdot T_k)A = E \ \ (*)$
По утверждению $\forall i = \overline{1,k} \ \ T_i$ имеет обратную.
По свойству (4) : $T_1 \cdot ... \cdot T_k$ имеет обратную.
Умножим $(*)$ на обратную к $(T_1 \cdot ... \cdot T_k) : (T_1 \cdot ... \cdot T_k)^{-1} \cdot (T_1 \cdot ... \cdot T_k) \cdot A = (T_1 \cdot ... \cdot T_k)^{-1}E \Longrightarrow A = (T_1 \cdot ... \cdot T_k)^{-1}$
По свойству (1) $\exists\ ((T_1 \cdot ... \cdot T_k)^{-1})^{-1} = (T_1 \cdot ... \cdot T_k) \Rightarrow \exists A^{-1} = (T_1 \cdot ... \cdot T_k)$

□

Из доказательства имеем:

1. $A^{-1} = T_1 \cdot ... \cdot T_k = (T_1 \cdot ... \cdot T_k)E$
2. $(T_1 \cdot ... \cdot T_k)A = E$

Т.е. A^{-1} получена из E с помощью ЭП над строками, которые приводят A к E. Чтобы производить такие же ЭП над строками матрицы E, как над строками A, преобразования делают над расширенной матрицей:

$$(A|E) \rightsquigarrow ((T_1 \cdot ... \cdot T_k)A(T_1 \cdot ... \cdot T_k)E) = (E|A^{-1})$$

Это метод нахождения обратной матрицы.

Теорема. (о явном выражении элементов обратной матрицы)
Пусть $A = (a_{ij})$ - квадратная невырожденная матрица порядка n, тогда $\exists$ обратная матрица к A и её элементы могут найдены по формуле:

$$b_{ij} = \frac{1}{detA} \cdot A_{ji}$$

где $A^{-1} = (b_{ij}),\ A_{ji}$ - алгебраическое дополнение.

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}; \quad A^{-1} = \frac{1}{detA} \begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & & \vdots \\ A_{n1} & \cdots & A_{nn} \end{pmatrix}$$

Доказательство. Т.к. A - невырожденная, то $\exists\ A^{-1}$ по предыдущей теореме. Обратная матрица к A (назовем её X) удовлетворяет уравнению: $AX = E$
Пусть $X = (X_1, ..., X_n),\ E = (E_1, ..., E_n)$, где X_i, E_i - стобцы соответствующих матриц, тогда $AX = E$ эквивалентно системе:

$$\begin{cases} AX_1 = E_1 \\ AX_2 = E_2 \\ \vdots \\ AX_n = E_n \end{cases}$$

$\forall k = \overline{1, n}$ расмотрим соответствующую СЛУ: $AX_k = E_k$. Она квадратная с невырожденной матрицей коэффициентов $\Longrightarrow$ Решение единственное и может быть найдено по формулам Крамера:

$$X_k = \begin{pmatrix} X_{1,k} \\ \vdots \\ X_{n,k} \end{pmatrix}, \quad \text{где } \forall i = \overline{1, n};\ X_{i,k} = \frac{\triangle_i}{\triangle} = \frac{\triangle_i}{detA}$$

$$\triangle_i = det(A_1, ..., \underset{i-\text{ое место}}{E_k}, ..., A_n) = A_{ki} \Longrightarrow X_{i,k} = \frac{A_{ki}}{detA}$$

□

9 Алебраические структуры

A, B -множества.
Декартово произведение: $A \times B = \{(a, b) \mid a \in A, b \in B\}$

Определение. Бинарной операцией на множестве A называется отображение:

$$\rho : A \times A \to A$$

Обозначается:

1. $\rho(a_1, a_2) = a_3$
2. $a_1 \ \rho \ a_2 = a_3$
3. $a_1 * a_2 = a_3$
4. $(A, *)-$ на A задана бинарная операция $*$

Определение. $(A, *)$ - говорят, что на A определена алгебраическая структура. $(A, *)$ называется алгебраической системой.

Определение. Бинарная операция $(*)$ на A называется коммутативной, если $\forall a, b \in A : a * b = b * a$

Определение. Бинарная операция $(*)$ на A называется ассоциативной, если $\forall a, b, c \in A : a * (b * c) = (a * b) * c$

Примеры.

1. $(\mathbb{Z}, +)$ ассоциативна и коммутативна.
2. $(\mathbb{Z}, -)$ НЕ ассоциативна и НЕ коммутативна.
3. $(M_{m\times n}, +)$ ассоциативна и коммутативна.
4. $(M_{m\times n}, \cdot)$ ассоциативна и НЕ коммутативна.

Определение. Элемент $e \in A$ называется нейтральным элементом относительно бинарной операции $(*)$, если $\forall a \in A : a * e = e * a = a$

Примеры.

1. $(\mathbb{Z}, +)$: $e = 0$
2. $(\mathbb{Z}, \cdot)$: $e = 1$

3. $(\mathbb{Z}, -)$: $e = 0$

4. $(\mathbb{N}, +)$: $\nexists\, e$

Утверждение. Если нейтральный элемент существует, то он единственный.

Доказательство. (От противного) Допустим, что $\exists\, e_1, e_2 \in A$ - нейтральные

$$e_1 \neq e_2 \Longrightarrow \underbrace{e_1}_{\text{нейтральный}} * e_2 = e_2; \quad e_1 * \underbrace{e_2}_{\text{нейтральный}} = e_1 \Longrightarrow e_1 = e_2$$

□

Определение. Группоид - это множество A, на котором введена бинарная операция $(*)$.
Обозначается: $(A, *)$

Определение. Полугруппа - группоид с ассоциативной бинарной операцией.

Определение. Моноид - полугруппа, в которой $\exists$ нейтральный элемент.
Обозначение: $(A, *, e)$

Утверждение. Если элемент a моноида A имеет обратный, то этот обратный единственный.

Доказательство. Допустим $\exists\, b_1, b_2$ - обратные к a элементы: $b_1 \neq b_2$
В силу ассоциативности:

$$b_1 * (a * b_2) = (b_1 * a) * b_2$$

$$b_1 * e = e * b_2$$

$$b_1 = b_2$$

□

Примеры.

1. $(M_{n\times m}(\mathbb{R}), \cdot, E)$ моноид, $\exists\, A^{-1} \Longleftrightarrow detA \neq 0$

2. $(\mathbb{Z}, \cdot, 1)$ моноид, 1 и -1 обратимы

3. $(\mathbb{R}, \cdot, 1)$ моноид, $\forall a \neq 0 : \exists\, a^{-1}$

Свойства.

1) Если элемент a имеет обратный b , то элемент b имеет обратный и этот обратный равен a

2) Если a_1 имеет обратный b_1, a_2 имеет обратный b_2, то: $(a_1 * a_2)^{-1} = b_2 * b_1$

Определение. Группа - моноид, в котором каждый элемент имеет обратный.

Определение. Группоид (полугруппа, моноид, группа) называется коммутативным, если бинарная операция коммутативна.

Определение. Абелева группа - коммутативная группа.

Примеры.

1. $(\mathbb{Z}, +, 0)$ - группа (абелева)
2. $(\mathbb{Z}, \cdot, 1)$ - НЕ группа (коммутативный моноид)
3. $(\mathbb{R}, \cdot, 1)$ - НЕ группа
4. $(\mathbb{R}/\{0\}, \cdot, 1)$ - группа (абелева)
5. $(M_{m\times n}(\mathbb{R}), \cdot, E)$ - НЕ группа
6. $(GL_n, \cdot, E)$ - группа
   (GL_n - множество невырожденных матриц порядка n с коэф. из $\mathbb{R}$)

Определение. Множество A, на котором задана бинарная операция $(*)$, называется группой, если:

1. $\forall a, b, c \in A: \ a * (b * c) = (a * b) * c$ (ассоциаивность)
2. $\exists\ e \in A : \forall a \in A: \ a * e = e * a = a$ (нейтральный элемент)
3. $\forall a \in A\ \exists\ b \in A: \ a * b = b * a = e$ (обратный элемент)

Терминология		
	Аддитивность	Мультипликативность
$*$	$+$, сложение	$\cdot$, умножение
e	0, нулевой элемент	e, единичный элемент
обратный к a	$-a$, противоположный	a^{-1}, обратный

9.1 Изоморфизм группы

Пусть $(G_1, *, e_1)$, $(G_2, \circ, e_2)$ - группы

Определение. Группы G_1, G_2 называются изоморфными, если $\exists$ отображение $\varphi : G_1 \to G_2$:

1. $\varphi-$ биекция.
2. $\forall a, b \in G_1 : \ \varphi(a * b) = \varphi(a) \circ \varphi(b)$

Обозначение: $G_1 \cong G_2$
При этом отображение называется изоморфизмом групп.

Пример. $(\mathbb{R}, +, 0)$, $(\mathbb{R}^+, \cdot, 1)$
$\varphi : \mathbb{R} \to \mathbb{R}^+$

$$\begin{cases} \varphi(x) = e^x - \text{биекция} \\ \varphi(a+b) = e^{a+b} = e^a \cdot e^b = \varphi(a) \cdot \varphi(b) \end{cases} \Longrightarrow \mathbb{R} \cong \mathbb{R}^+$$

Свойства.

1. $\varphi(e_1) = e_2$
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$

Доказательство.

1) $\forall a \in G_1$:

$$a * e_1 = a$$
$$\varphi(a * e_1) = \varphi(a)$$
$$\varphi(a) \circ \varphi(e_1) = \varphi(a)$$

Т.к. G_2 - группа, то $\exists \ \varphi(a)^{-1}$. Умножение на $\varphi(a)^{-1}$ слева:

$$\varphi(a)^{-1} \circ (\varphi(a) \circ \varphi(e_1)) = \varphi(a)^{-1} \circ \varphi(a) = e_2$$

2)

$$a^{-1} * a = e_1$$
$$\varphi(a^{-1} * a) = \varphi(e_1) = e_2$$
$$\varphi(a^{-1}) \circ \varphi(a) = e_2$$

$\Longrightarrow$ обратный к $\varphi(a)$ является $\varphi(a)^{-1}$
Аналогично $\varphi(a) \circ \varphi(a^{-1}) = e_2$

□

9.2 Группа подстановок

Определение. Подстановкой степени n называется биективным отображением σ множества $\{1, ..., n\}$ в себя.

$$\{1, ..., n\} \to \{1, ..., n\} - \text{биекция}$$

Подстановку можно написать в виде таблицы:

$$\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}$$

В верхней строке расположены числа от 1 до n в некотором порядке. В нижней строке расположены их образы, т.е. $j_k = \sigma(i_k)$

Пример. $n = 3$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Если поменять столбцы местами, отображение не изменится.
Если в верхней строке числа упорядочить по возрастанию, то такая запись будет называться стандартной.

Определение. Подстановка id степени n называется тождественной, если:

$$\forall k \in \{1, ..., n\} : \mathrm{id}(k) = k$$

т.е.

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

Обозначение: $\Omega = \{1, ..., n\}$ (множество, являющееся отрезком натурального ряда)

Определение. Произведение подстановок π и τ степени n - это их композиция $\pi \circ \tau$, т.е.

$$(\pi \circ \tau)(k) = \pi(\tau(k))$$

Утверждение. (1) Произведение подстановок степени n - снова подстановка длины n.

Утверждение. (2) Множество S_n всех подстановок степени n, относительно этого произведения (композиции), является группой.

Доказательство. По утверждению (1) произведение - это бинарное отношение:

1) ассоциаивность верна.

2) id - нейтральный элемент.

3) $\forall \sigma \in S_n \; \exists \; \sigma^{-1} \in S_n$, т.к. $\sigma : \Omega \overset{\text{биекция}}{\longrightarrow} \Omega$

□

Определение. Группа S_n называется симметрической группой степени n (группой всех подстановок степени n).

Утверждение. $|S_n| = n!$

Утверждение. Группа S_n - НЕ коммутативна.

Пример.

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

$$\neq$$

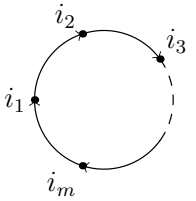
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Определение. Циклом длины k называется подстановка, в которой $\forall i \in \{1, ..., n\} \setminus \{i_1, ..., i_k\}$, где $\sigma(i) = i$, при этом:

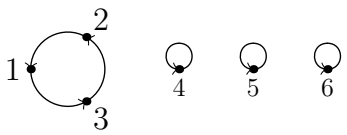
$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, .., \sigma(i_k) = i_1$$

Обозначение: $(i_1, ..., i_k)$

Представление в виде графа:



Пример. $n = 6, \quad \sigma = (1, 3, 2)$



Замечание. Заметим, что $(i_1, i_2, ..., i_k) = (i_k, i_1, ..., i_{k-1}) = (i_2, i_3, .., i_1) = ...$

Определение. Циклы $(i_1, ..., i_k)$ и $(j_1, ..., j_k)$ называются независимыми, если:

$$\{i_1, ..., i_k\} \cap \{j_1, ..., j_k\} = \varnothing$$

Пример. $(1, 2, 3), \; (4, 5)$

Утверждение. Независимые циклы коммутируют.

Пример. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 4 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 4 & 5 \end{pmatrix} \begin{pmatrix} 6 \end{pmatrix}$

Теорема 1. Любая подстановка $\sigma \in S_n,\ \sigma \neq \mathrm{id}$ раскладывается в произведение независимых циклов длины ≥ 2, причем это разложение единственно с точностью до перестановки множителей.

Доказательство.

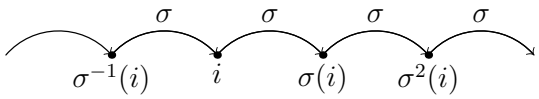
$\exists$: Рассмотрим степени подстановки σ.
По определению: $\sigma^0 = \mathrm{id}$;

$$\sigma^m := \sigma \cdot ... \cdot \sigma, \text{ при } m > 0;$$
$$\sigma^m := \sigma^{-1} \cdot ... \cdot \sigma^{-1}, \text{ при } m < 0$$

Отметим, что:

1. Степень подстановки σ^m - это подстановка $\forall m \in \mathbb{Z}$
2. $\sigma^{m_1} \cdot \sigma^{m_2} = \sigma^{m_1+m_2}$
3. $(\sigma^{m_1})^{m_2} = \sigma^{m_1 \cdot m_2}$

Рассмотрим произвольный $i \in \{1, ..., n\}$



Определение. Множество $\mathrm{Orb}(i) = \{\sigma^m(i) \mid m \in \mathbb{Z}\}$ называется орбитой числа i.

$\mathrm{Orb}(i) \subseteq \{1, ..., n\} \Longrightarrow \exists\ m_1, m_2 \in \mathbb{Z} : \sigma^{m_1}(i) = \sigma^{m_2}(i) = j$
Допустим, что $m_1 > m_2$, тогда $\sigma^{m_1-m_2}(i) = \sigma^{-m_2}(\sigma^{m_1}(i)) = \sigma^{-m_2}(j) = i$
$\Longrightarrow$ (т.к. $m_1 - m_2 \in \mathbb{N}$) $\exists$ такое наименьшее $k \in \mathbb{N}\ :\ \sigma^k(i) = i$

$$\mathrm{Orb}(i) = \{i, \sigma(i), ..., \sigma^{k-1}(i)\}$$

Свойства.

1. Различные орбиты не пересекаются.

   Доказательство. Пусть $l \in \mathrm{Orb}(i) \cap \mathrm{Orb}(j) \Longrightarrow \exists\ m_1, m_2 \in \mathbb{N}^0 :$
   $\sigma^{m_1}(i) = l = \sigma^{m_2}(j) \Longrightarrow \sigma^{m_1-m_2}(i) = \sigma^{-m_2}(\sigma^{m_1}(i)) = \sigma^{-m_2}(l) = j \Longrightarrow$
   $\forall p \in \mathbb{Z} :\ \sigma^p(j) = \sigma^p(\sigma^{m_1-m_2}(i)) = \sigma^{m_1-m_2+p}(i) \Longrightarrow \mathrm{Orb}(j) \subseteq \mathrm{Orb}(i)$
   Аналогично $\mathrm{Orb}(i) \subseteq \mathrm{Orb}(j) \Longrightarrow \mathrm{Orb}(i) = \mathrm{Orb}(j)$ $\square$

2. $\{1, ..., n\} = \text{Orb}(i_1) \cup ... \cup \text{Orb}(i_s)$

Доказательство. Т.к. $\forall i \in \{1, ..., n\} : \ i \in \text{Orb}(i)$ □

Продолжаем доказательство теоремы. Рассмотрим разложение $\{1, ..., n\}$ как объединение Orb, где k_i - количество элементов в Orb:

$$\{1, ..., n\} = \underbrace{\text{Orb}(i_1)}_{k_1} \sqcup ... \sqcup \underbrace{\text{Orb}(i_t)}_{k_t} \sqcup \underbrace{\text{Orb}(i_{t+1})}_{k_{t+1}} \sqcup ... \sqcup \underbrace{\text{Orb}(i_s)}_{k_s}$$

Если $\sigma \neq \text{id}$, то $k_1 > 1, ..., k_t > 1, k_{t+1} = 1, ..., k_s = 1 \Longrightarrow$
$\sigma = (i_1 \ \sigma(i_1) \ ... \ \sigma^{k_1-1}(i_1)) \ ... \ (i_t \ \sigma(i_t) \ ... \ \sigma^{k_t-1}(i_t))$. $\exists$ доказано.

! : (От противного)
Допустим,

$$\sigma = \pi_1 \cdot ... \cdot \pi_\nu$$

$$\sigma = \tau_1 \cdot ... \cdot \tau_\mu$$

Различные разложения на независимые циклы длины ≥ 2
Т.к. $\sigma \neq id$, то $\exists \ j : \sigma(j) \neq j \Longrightarrow$ с точностью до нумерации:

$$\pi_1(j) \neq j, \ \tau_1(j) \neq j$$

$$\begin{matrix} \sigma(j) = \pi_1(j) \\ \sigma(j) = \tau_1(j) \end{matrix} \Longrightarrow \forall m \in \mathbb{N}^0 : \quad \begin{matrix} \sigma^m(j) = \pi_1^m(j) \\ \sigma^m(j) = \tau_1^m(j) \end{matrix}$$

Т.к. цикл полностью определяется степенями σ, то $\pi_1 = \tau_1 \Longrightarrow \pi_2...\pi_\nu = \tau_2...\tau_\mu$. Далее индукция по ν и $\mu \Longrightarrow$ Противоречие $\Longrightarrow$ Разложение σ единственно.

□

Определение. Цикл длины 2 называется транспозицией.

Теорема. Любая подстановка $\sigma \in S_n$ раскладывается в произведение транспозиций.

Доказательство. Если $\sigma = \text{id}$, то $\sigma = (12)(12)$
Если $\sigma \neq \text{id}$, то по Теореме (1) σ раскладывается в произведение независимых циклов длины ≥ 2
Поэтому достаточно разложить на транспозиции каждый такой цикл.

$$k > 1 \quad (1, 2, ..., k) = (1, k)(1, k-1)...(1, 3)(1, 2)$$

□

9.3 Четность подстановки

$$\sigma \in S_n; \quad \sigma = \begin{pmatrix} i_1 & \cdots & i_n \\ j_1 & \cdots & j_n \end{pmatrix}$$

Определение. Знаком подстановки σ называется функция:

$$\operatorname{sgn}(\sigma) := \operatorname{sgn}(i_1, ..., i_n) \cdot \operatorname{sgn}(j_1, ..., j_n)$$

Утверждение. Знак подстановки не зависит от способа записи подстановки в виде таблицы.

Доказательство. Если $\begin{pmatrix} i_1 & \cdots & i_n \\ j_1 & \cdots & j_n \end{pmatrix}$ и $\begin{pmatrix} m_1 & \cdots & m_n \\ k_1 & \cdots & k_n \end{pmatrix}$ - две записи одной и той же подстановки σ, то от $\begin{pmatrix} i_1 & \cdots & i_n \\ j_1 & \cdots & j_n \end{pmatrix}$ к $\begin{pmatrix} m_1 & \cdots & m_n \\ k_1 & \cdots & k_n \end{pmatrix}$ можно перейти за конечное число перемен столбцов местами. Каждая перемена столбцов местами производит транспозицию в верхней и в нижней строке $\Longrightarrow$ знак меняется и там, и там $\Longrightarrow$ знак произведения не изменяется. $\square$

$$\text{В стандартной записи } \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \Longrightarrow \operatorname{sgn}(\sigma) = \operatorname{sgn}(i_1, i_2, ..., i_n)$$

Определение. Подстановка σ называется четной (нечетной), если:

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

Свойства.

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

   Доказательство. $\sigma = \begin{pmatrix} i_1 & \cdots & i_n \\ j_1 & \cdots & j_n \end{pmatrix} \Longrightarrow \sigma^{-1} = \begin{pmatrix} j_1 & \cdots & j_n \\ i_1 & \cdots & i_n \end{pmatrix}$ $\square$

2. $\operatorname{sgn}(\sigma \cdot \tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau) \ \ (\sigma, \tau \in S_n)$

   Доказательство.

   $$\sigma = \begin{pmatrix} i_1 & \cdots & i_n \\ j_1 & \cdots & j_n \end{pmatrix}, \tau = \begin{pmatrix} k_1 & \cdots & k_n \\ i_1 & \cdots & i_n \end{pmatrix}$$

   $\Longrightarrow \sigma \cdot \tau = \begin{pmatrix} k_1 & \cdots & k_n \\ j_1 & \cdots & j_n \end{pmatrix} \Longrightarrow \operatorname{sgn}(\sigma \cdot \tau) = \operatorname{sgn}(k_1, ..., k_n) \cdot \operatorname{sgn}(j_1, ..., j_n) =$
   $\operatorname{sgn}(k_1, ..., k_n) \cdot \underbrace{\operatorname{sgn}(i_1, ..., i_n) \cdot \operatorname{sgn}(i_1, ..., i_n)}_{1} \cdot \operatorname{sgn}(j_1, ..., j_n) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$ $\square$

Утверждение.

1. если τ - транспозиция, то $\operatorname{sgn}(\tau) = -1$
2. если σ - цикл длины k, то $\operatorname{sgn}(\sigma) = (-1)^{k-1}$
3. если $\sigma = \tau_1 \cdot ... \cdot \tau_l$, где τ_i - транспозиции, то $\operatorname{sgn}(\sigma) = (-1)^l$

Доказательство.

1)
$$\tau = \begin{pmatrix} 1 & \cdots & i & \cdots & j & \cdots n \\ 1 & \cdots & j & \cdots & i & \cdots n \end{pmatrix}$$
$$\Longrightarrow \operatorname{sgn}(\tau) = \operatorname{sgn}(1, ..., j, ..., i, ..., n) = -\operatorname{sgn}(1, ..., i, ..., j, ..., n) = -1$$

3) следует из Свойства (2) и Утверждения (1):
$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1) \cdot \operatorname{sgn}(\tau_2) \cdot ... \cdot \operatorname{sgn}(\tau_l) = \underbrace{(-1) \cdot (-1) \cdot ... \cdot (-1)}_{l} = (-1)^l$$

2) $\sigma = (i_1, ..., i_k) = (i_1, i_k)(i_1, i_{k-1})...(i_1, i_2) =$ (по Утверждения (3)) $= (-1)^{k-1}$

□

Пример.
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 4 & 5 \end{pmatrix} = (-1)^2 \cdot \text{ (нечет) } =$$
$$= \text{ (чет) } \cdot \text{ (нечет) } = \text{ (нечет)}$$

9.4 Подгруппа

$(A, *)$ - множество с бинарной операцией. $B \subseteq A$

Определение. Говорят, что B замкнуто относительно бинарной операции $*$, если:
$$\forall b_1, b_2 \in B : \ b_1 * b_2 \in B$$

В этом случае B превращается в алгебраическую структуру.

Пример. $\mathbb{N}$ (коммутативная полугруппа) $\subset \mathbb{Z}$ (с $+$ абелева группа)

Определение. Множество H называется подгруппой группы G, если:

1. $\forall h_1, h_2 \in H \Longrightarrow h_1 \cdot h_2 \in H$

2. $e \in H$

3. $\forall h \in H \Longrightarrow h^{-1} \in H$

Обозначается: $H \leq G$

Утверждение. Любая подгруппа группы G сама является группой, относительно той же операции.

Замечание. В определении подгруппы (2.) $\longleftrightarrow$ "$H \neq \varnothing$"

Примеры.

1) $\mathbb{N} \leq \mathbb{Z}$

2) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$

3) $m\mathbb{Z} \leq \mathbb{Z},\ m \in \mathbb{N}$

4) A_n - все четные подстановки
$A_n \leq S_n$. (для нечетных неверно)

9.5 Кольца и поля

Определение. Множество K, на котором введены 2 бинарные операции:
" $+$ " - сложение, " $\cdot$ " - умножение, называется кольцом, если выполнены следующие аксиомы:

1. $(K, +)$ - абелева группа

2. $\forall a, b, c \in K:\ a(b + c) = ab + ac$ и $(a + b)c = ac + bc$

Обозначается: $(K, +, \cdot)$

Примеры.

1. $(\mathbb{Z}, +, \cdot)$

2. $(M_n(\mathbb{R}), +, \cdot)$

Определение. Кольцо называется ассоциативным, если умножение ассоциативно.

Определение. Кольцо называется коммутативным, если умножение коммутативное.

Определение. Кольцо называется кольцом с единицей, если существует нейтральный элемент по умножению:

$$\exists\, e \in K :\ \forall a \in K :\ e \cdot a = a \cdot e = a$$

Утверждение. Если в K есть единица, то она единственная.

Примеры.

1. $(\mathbb{Z}, +, \cdot)$ - коммутативное, ассоциативное кольцо с 1
2. $(M_n(\mathbb{R}), +, \cdot)$ - НЕ коммутативное, ассоциативное кольцо с 1
3. $(V^3, +, \times)$, ($\times$ - векторное произведение) - НЕ коммутативное, НЕ ассоциативное кольцо без 1
4. $(2\mathbb{Z}, +, \cdot)$ - коммутативное, ассоциативное кольцо без 1

Следствия. (простейшие)

1. - 0 - единственный
   - $\forall a \in K$ - противоположный единственный
   - $\forall a, b \in K\ \exists!\ x \in K :\ a + x = b \Longrightarrow x = b + (-a)$; ($x$!, т.к. $(-a)$!)
     Обозначается: $x = b - a$
2. $\forall a \in K :\ a \cdot 0 = 0 \cdot a = 0$
3. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
4. $\forall a, b, c \in K :\ a(b - c) = ab - ac,\ (b - c)a = ba - ca$
5. Если K - кольцо с 1, то $a(-e) = (-e)a = -a$

Замечание. Пусть K - кольцо с единицей (e), тогда если $e = 0 \Longrightarrow K = \{0\}$

Доказательство. $\forall a \in K :\ 0 = 0 \cdot a = e \cdot a \Longrightarrow a = 0$ □

Пусть K - кольцо с единицей

Определение. Элемент $a \in K$ называется обратимым, если:

$$\exists\, b \in K : ab = ba = 1$$

При этом элемент b должен быть обратным к a

Утверждение. Пусть K - ассоциативное кольцо с 1, тогда если элемент $a \in K$ имеет обратный, то он единственный.

Примеры.

1. $(\mathbb{Z}, +, \cdot)$: $1, -1$ - обратимые, других нет.
2. $(\mathbb{R}, +, \cdot)$: $\forall a \in \mathbb{R},\ a \neq 0$ - обратим.
   Обозначается: K - ассоциативное кольцо с 1

K^* - множество элементов кольца K, имеющих обратный.

Утверждение. K^* - группа относительно умножения.

Пример. $\mathbb{Z}^* = \{1, -1\}$

Определение. Поле K - коммутативное, ассоциативное кольцо с $1 \neq 0$, в котором любой ненулевой элемент обратим.

Замечание. $0 = e \iff K = \{0\}$ - не поле.

Примеры.

1. $(\mathbb{R}, +, \cdot)$ - поле
2. $(\mathbb{Q}, +, \cdot)$ - поле
3. $(\mathbb{Z}, +, \cdot)$ - НЕ поле

Пример. $\mathbb{Z}_n$ - коммутативное, ассоциативное кольцо с 1

Утверждение. $k \in \mathbb{Z}_n$ - обратим $\iff (k, n) = 1$

Теорема. $\mathbb{Z}_n$ - поле $\iff n-$ простое

Доказательство.

$\Longrightarrow$ Пусть $\mathbb{Z}_n$ - поле, тогда $\forall k \in \mathbb{Z}_n$ имеет обратный $m:\ km = 1$.
Предположим, что n - не простое, тогда $n = st$, где $1 < s, t < n$
$\Longrightarrow s, t \neq 0$, но $st = n = 0$ (в $\mathbb{Z}_n$) $\Longrightarrow s$ и t - делители нуля - противоречие (в поле нет делителей нуля, это доказывается чуть ниже).

$\Longleftarrow$ n - простое, то $\forall k \neq 0 \in \mathbb{Z}_n:\ n \neq k \Longrightarrow (n, k) = 1$
$\Longrightarrow k$ - обратим (остальные аксиомы поля проверяются непостредственно).

□

Определение. Говорят, что кольцо K не имеет делителей нуля, если из равенства $a \cdot b = 0 \Longrightarrow a = 0$ или $b = 0$.
Если же для ненулевого элемента $a \in K$ найдется ненулевой элемент $b \in K$: $a \cdot b = 0$, то a, b называются делителями нуля.

Примеры.

1. $\mathbb{Z}$: без делителя нуля
2. $\mathbb{Z}_6$: $2 \cdot 3 = 0 \Longrightarrow$ есть делители нуля.
3. $M_2(\mathbb{R})$: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Утверждение. Если в кольце K нет делителя нуля, то возможно сокращение, если $a \cdot c = b \cdot c$, и $c \neq 0$, то $a = b$

Доказательство. $a \cdot c = b \cdot c \Longrightarrow a \cdot c - b \cdot c = 0 \Longrightarrow (a - b) \cdot c = 0$
т.к. нет делителя нуля $\Longrightarrow$ либо $c = 0$, либо $a - b = 0$, но $c \neq 0 \Longrightarrow a = b$ □

Утверждение. В поле нет делителя нуля.

Доказательство. Предположим, что: $\begin{cases} a \cdot b = 0 \\ a \neq 0 \\ b \neq 0 \end{cases}$ т.к. $a \neq 0$, в поле $\exists\ a^{-1}$

Умножим $a \cdot b = 0$ на a^{-1}

$$\begin{cases} a^{-1}(a \cdot b) = a^{-1} \cdot 0 = 0 \\ a^{-1}(a \cdot b) = (a^{-1} \cdot a)b = 1 \cdot b = b \end{cases} \Longrightarrow b = 0$$ □

Утверждение. Пусть K - коммутативное, ассоциативное кольцо с 1, тогда:

$$x - \text{обратим} \Longleftrightarrow x - \text{не делитель нуля}$$

Доказательство. Упражнение □

9.6 Изоморфные кольца и поля

Определение. Кольца K и $\widetilde{K}$ называются изоморфными, если: $\exists\, \varphi :\ K \to \widetilde{K}$:

1. φ - биекция
2. $\forall a, b \in K :\ \varphi(a + b) = \varphi(a) + \varphi(b)$

3. $\forall a, b \in K: \ \varphi(ab) = \varphi(a) \cdot \varphi(b)$

Обозначается: $K \cong \widetilde{K}, \ \varphi -$ изоморфизм колец

Следствия.

1. $\varphi(0) = \widetilde{0}$
2. $\varphi(-a) = -\varphi(a)$
3. Если K - ассоциативное кольцо с 1, то $\varphi(e) = e$,
   а если $a \in K$ обратим, то $\varphi(a^{-1}) = \varphi(a)^{-1}$

Определение. Поля P и $\widetilde{P}$ изоморфны, если они изоморфны как кольца.

Определение. Подмножество L кольца K называется подкольцом, если:

1. L - подгруппа адитивной группы кольца K, т.е.
   - $\forall a, b \subset L: \ a + b \in L$
   - $0 \in L$
   - $\forall a \in L : (-a) \in L$
2. $\forall a, b \in L: \ a \cdot b \in L$

Утверждение. Любое подкольцо кольца K само является кольцом относительно тех же операций.

Определение. Подмножество L поля K называется подполем, если:

1. L - подкольцо кольца K
2. $e \in L$
3. $\forall a \in L, \ a \neq 0 \Longrightarrow a^{-1} \in L$

Утверждение. Любое подмножество поля K само является полем относительно тех же операций.

Примеры.

1. $\mathbb{Q} \subseteq \mathbb{R}$ - подполе
2. $\mathbb{Z} \subseteq \mathbb{R}$ - подкольцо
3. $2\mathbb{Z} \subseteq \mathbb{Z}$ - подкольцо

Упражнение. В $\mathbb{Q}$ нет подполей, отличных от самого $\mathbb{Q}$.

9.7 Характеристика поля

Определение. Говорят, что поле P имеет характеристику n, если n - наименьшее натуральное число, такое, что $\underbrace{1+1+...+1}_{n} = 0$.

Если такого числа нет, то говорят, что поле имеет характеристику 0.
Обозначается: $\mathrm{char}P = n$

Примеры.

1. $\mathrm{char}\mathbb{Z}_3 = 3$ $(1+1+1=0)$
2. $\mathrm{char}\mathbb{R} = 0$

Замечание. Если $n \neq 0,\ \mathrm{char}P = n$, то $\forall a \in P$:

$$\underbrace{a+a+...+a}_{n} = \underbrace{a\cdot 1 + a\cdot 1 + ... + a\cdot 1}_{n} = a\cdot(\underbrace{1+1+...+1}_{n}) = a\cdot 0 = 0$$

Утверждение. Если P - поле характеристики $n,\ n \neq 0$, то $n -$ простое.

Доказательство. Докажем, $n = m\cdot k,\ 1 < m,\ k < n$:

$$\underbrace{1+1+...+1}_{n} = (\underbrace{1+1+...+1}_{m})(\underbrace{1+1+...+1}_{k}) \Longrightarrow m\cdot k = 0$$

В поле нет делителей нуля $\Longrightarrow \underbrace{1+1+...+1}_{m} = 0$. Противоречие. □

Замечание. Теория решения СЛУ (метод Гаусса, правила Крамера, ...), теория определителей, утверждения о векторных пространсвах (в частности о матрицах), которые мы рассматривали раннее, переносятся с $\mathbb{R}$ на произвольные поля.
Исключение - поле характеристики 2: в определении кососимметричной и полилинейной функции надо требовать, чтобы при 2 совпадающих аргументах $f(...,v,...,v,...) = 0$. Отсюда получаем, что $f(...,v,...,w,...) = -f(...,w,...,v,...)$ (при $\mathrm{char}P = 2$ получаем: $1 = -1$)

9.8 Поле комплексных чисел

Определение. Поле комплексных чисел $\mathbb{C}$ - это поле, в котором выполнены следующие условия:

1. Поле $\mathbb{R}$ содержится в $\mathbb{C}$ в качестве подполя.

2. В $\mathbb{C}$ $\exists$ элемент $i:\ i^2 = -1$

3. $\mathbb{C}$ - наименьшее поле, удовлетворяющее условиям 1. и 2.
   Т.е. $\forall F \subseteq \mathbb{C}:\ \mathbb{R} \subseteq F,\ i \in F \Longrightarrow F = \mathbb{C}$

Теорема. Поле $\mathbb{C}$ комплексных чисел существует, причем оно единсвенно с точностью до изоморфизма, оставляющего все вещественные числа на месте. Кроме того, $\forall z \in \mathbb{C}$ представляется единсвенным образом в виде: $z = a + bi$, где $a, b \in \mathbb{R}$.

Доказательство.

1.) Предположим, что поле комплексных чисел $\mathbb{C}$ существует, и докажем его единственность.
Для этого исследуем $\mathbb{C}$
Рассмотрим в $\mathbb{C}$ подмножество F:

$$F = \{a + bi \mid a, b \in \mathbb{R}\} \subseteq \mathbb{C}$$

Докажем, что F - подполе:

1) $(a + bi) + (\widetilde{a} + \widetilde{b}i) = (a + \widetilde{a}) + (b + \widetilde{b})i \in F$
2) $0 = 0 + 0i \in F$
3) $-(a + bi) = (-a) + (-b)i \in F$
4) $(a + bi)(\widetilde{a} + \widetilde{b}i) = (a\widetilde{a} - b\widetilde{b}) + (a\widetilde{b} + \widetilde{a}b)i \in F$
5) $e = 1 + 0i \in F$
6) $\forall (a + bi) \in F\ \exists\ (a + bi)^{-1} = \frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = (\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i) \in F$

$\Longrightarrow F$ - подполе поля $\mathbb{C}$
$\mathbb{R} \subseteq F$, т.к. $\forall a \in \mathbb{R}\ \exists\ (a + 0 \cdot i) \in F$ и $\exists\ i = (0 + 1 \cdot i) \in F$
По третьей аксиоме из определения поле $\mathbb{C}:\ F = \mathbb{C}$
Мы доказали, что если поле комплексных чисел существует, то любой элемент в нем представляется в виде $z = a + bi$, где $a, b \in \mathbb{R}$.
Проверим, что это представление единственное.
От противного:

$$a + bi = \widetilde{a} + \widetilde{b}i, \quad a, \widetilde{a}, b, \widetilde{b} \in \mathbb{R}$$

$$(a - \widetilde{a}) = (\widetilde{b} - b)i$$

$$(a - \widetilde{a})^2 = -1 \cdot (\widetilde{b} - b)^2 \Longrightarrow$$

$$\Longrightarrow \begin{cases} (a-\widetilde{a})^2 \geq 0 \\ -(\widetilde{b}-b)^2 \leq 0 \end{cases} \Longrightarrow \begin{cases} (a-\widetilde{a})^2 = 0 \\ (\widetilde{b}-b)^2 = 0 \end{cases} \Longrightarrow \begin{cases} a = \widetilde{a} \\ b = \widetilde{b} \end{cases}$$

Предположим, что $\exists$ еще одно поле комплексных чисел $\mathbb{C}$.
Т.к. рассуждения выше верны и для $\widetilde{\mathbb{C}}$, то $\forall \widetilde{z} \in \widetilde{\mathbb{C}}$ представляетя единственным образом в виде:

$$\widetilde{z} = a + b\widetilde{i}, \text{ где } a, b \in \mathbb{R}, \ (\widetilde{i})^2 = -1$$

Рассмотрим отображение:

$$\varphi : \mathbb{C} \to \widetilde{\mathbb{C}}$$
$$\varphi : a + bi \to a + b\widetilde{i}$$

Это отображение - изоморфизм полей, сохраняющий вещественные числа на месте.

2.) Докажем существование поля помплексных чисел.
Построим поле, удовлетворяющее определению:

$$\Gamma = \{(a, b) \mid a, b \in \mathbb{R}\}$$

Введем операции:

- $(a, b) + (\widetilde{a}, \widetilde{b}) = (a + \widetilde{a}, \ b + \widetilde{b})$
- $(a, b) \cdot (\widetilde{a}, \widetilde{b}) = (a\widetilde{a} - b\widetilde{b}, \ a\widetilde{b} + \widetilde{a}b)$

1. Относительно $(+)$ и $(\cdot)$ выполнены коммутативность, ассоциативность, дистрибутивность (непосредственная проверка).
2. $(0, 0)$ - ноль
3. $(-a, -b)$ - противоположный к (a, b)
4. $(1, 0)$ - единица
5. $\forall (a, b) \neq (0, 0) \ \exists$ обратный $: (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$

$\Longrightarrow \Gamma$ - поле.
Рассмотрим подмножество $\mathsf{L} \subseteq \Gamma$:

$$\mathsf{L} = \{(a, 0) \mid a \in \mathbb{R}\}$$

Такое поле изоморфно $\mathbb{R}$:

$$\begin{cases} \varphi : \mathbb{R} \to L \ : \ a \to (a, 0) - \text{биекция} \\ \varphi(a_1 + a_2) = (a_1 + a_2, 0) = (a_1, 0) + (a_2, 0) = \varphi(a_1) + \varphi(a_2) \\ \varphi(a_1 \cdot a_2) = (a_1 \cdot a_2, 0) = (a_1, 0) \cdot (a_2, 0) = \varphi(a_1) \cdot \varphi(a_2) \end{cases}$$

$\circ$ $-1 \longleftrightarrow (-1,0) = (0,1)(0,1)$

$\circ$ $i = (0,1) \in \Gamma$

$\circ$ $\forall (a,b) \in \Gamma : (a,0)(1,0) + (b,0)(0,1) = (a,b)$, т.е. $\forall z \in \Gamma$:

$$z = a \cdot 1 + b \cdot i$$

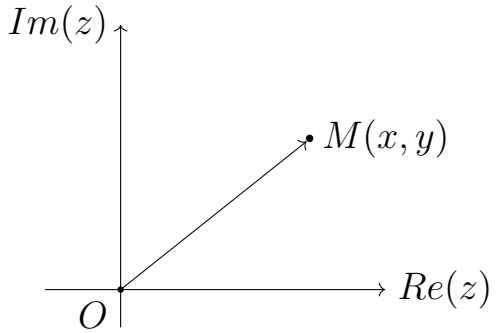
$$\Longrightarrow \forall\ \Gamma \subseteq F : \begin{cases} \mathbb{R} \subseteq F \\ i \in F \end{cases} \Longrightarrow \Gamma = F$$

□

Замечание. Запись $z = a + bi$ называется алгебраической записью комплексного числа.

- $Re(z) = x$ - вещественная часть комплексного числа.
- $Im(z) = y$ - мнимая часть комплексного числа.
- i - мнимая единица.

На декартовой плоскоси:



$$z = x + iy \longleftrightarrow \text{точка } M(x,y) \longleftrightarrow \text{вектор } \overrightarrow{OM}$$

Определение. Число $\overline{z} = x - iy$ называется комплексно-сопряженным к $z = x + iy$.

Утверждение. Отображеие $\varphi : z \to \overline{z}$ является изоморфизмом поля $\mathbb{C}$ в себя (т.е. является автоморфизмом).

Доказательство.

1) биекция очевидна

2) $\overline{z_1 + z_2} = (x_1 + x_2) - (y_1 + y_2)i = \overline{z_1} + \overline{z_2}$

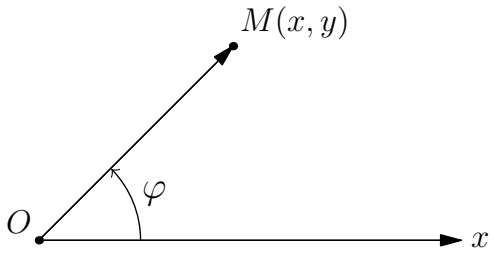
3) $\overline{z_1 z_2} = (x_1 x_2 - y_1 y_2) + (x_1 y_2 + x_2 y_1)i = \overline{z_1} \cdot \overline{z_2}$

□

Свойства.

1. $\overline{\overline{z}} = z$
2. $z \cdot \overline{z} = x^2 + y^2 \in \mathbb{R}$
3. $z + \overline{z} = 2x \in \mathbb{R}$
4. $\forall z = x + iy,\ z \neq 0,\ \exists\ z^{-1} = \frac{1}{z} = \ \frac{\overline{z}}{z \cdot \overline{z}} = \frac{x - iy}{x^2 + y^2}$

Определение. Тригонометрическая форма (полярная система координат на плоскости)
Точка $M(x, y) \longleftrightarrow (\rho, \varphi)$



$$\rho = |\overrightarrow{OM}|; \quad \varphi = \angle(Ox, \overrightarrow{OM})$$

$$\begin{cases} x = \rho \cos(\varphi) \\ y = \rho \sin(\varphi) \end{cases}$$

$$z = \rho(\cos(\varphi) + i \sin(\varphi)); \quad \rho = |z| = \sqrt{x^2 + y^2}$$

• φ называется аргументом комплексного числа z, определяется с точностью до $2\pi k,\ k \in \mathbb{Z}$.

$$Arg(z) = \varphi + 2\pi k, k \in \mathbb{Z}$$

$$0 \leq Arg(z) \leq 2\pi - \text{главный аргумент}$$

$$Arg(z) = \begin{cases} arctg(\frac{y}{x}), & x > 0 \\ arctg(\frac{y}{x} + \pi), & x < 0 \end{cases}$$

Если $z = 0$, то аргумент не определяется (либо угол любой, либо $|z| = 0$)

$$z_1 = z_2 \Longleftrightarrow \begin{cases} |z_1| = |z_2| \\ \varphi_1 = \varphi_2 + 2\pi k,\ k \in \mathbb{Z} \end{cases}$$

Утверждение. (Формула Муавра)
Пусть $z_1 = \rho_1(\cos(\varphi_1) + i\sin(\varphi_1)), \quad z_2 = \rho_2(\cos(\varphi_2) + i\sin(\varphi_2))$
Тогда:

1. $z_1 \cdot z_2 = (\rho_1 \cdot \rho_2)(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2))$
2. если $z_2 \neq 0$, то $\frac{z_1}{z_2} = \frac{\rho_1}{\rho_2}(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2))$

Доказательство.

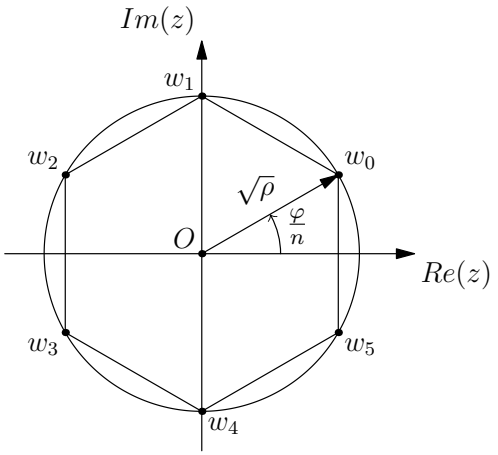
1. $z_1 \cdot z_2 = \rho_1(\cos(\varphi_1) + i\sin(\varphi_1)) \cdot \rho_2(\cos(\varphi_2) + i\sin(\varphi_2)) =$
$= (\rho_1 \cdot \rho_2)(\cos(\varphi_1)\cos(\varphi_2) - \sin(\varphi_1)\sin(\varphi_2) +$
$+ \cos(\varphi_1)\sin(\varphi_2)i + \cos(\varphi_2)\sin(\varphi_1)i) =$
$= (\rho_1 \cdot \rho_2)(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2))$
2. Аналогично

□

Определение. Число $w \in \mathbb{C}$ называется корнем n-ой степени из $z \in \mathbb{C}$, где $n \in \mathbb{N}$, если $w^n = z$.

Утверждение. Пусть $z = \rho(\cos(\varphi) + i\sin(\varphi)),\ z \neq 0,\ n \in \mathbb{N}$
Тогда $\exists$ ровно n корней n-ой степени из $z \in \mathbb{C}$: $w_0, w_1, ..., w_{n-1}$, причем:

$$w_l = \sqrt[n]{\rho} \cdot (\cos(\frac{\varphi + 2\pi l}{n}) + i\sin(\frac{\varphi + 2\pi l}{n}))$$



$w_0, w_1, ..., w_{n-1}$ - лежат в верщинах правильного n - угольника, вписанного в окружность.

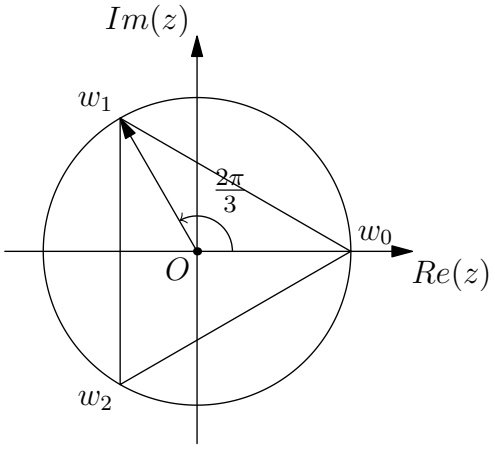
Доказательство. Рассмотрим $w = r(\cos(\psi) + i\sin(\psi))$

$$z = \rho(\cos(\varphi) + i\sin(\varphi)) = r^n(\cos(n\psi) + i\sin(n\psi)) = w^n$$

$$\Longrightarrow \begin{cases} r^n = \rho \\ n\varphi = \varphi + 2\pi k, k \in \mathbb{Z} \end{cases} \Longrightarrow w = \sqrt[n]{\rho} \cdot (\cos(\tfrac{\varphi+2\pi k}{n}) + i\sin(\tfrac{\varphi+2\pi k}{n})),\ k \in \mathbb{Z}$$

при $k = \{0, 1, ..., k-1\}$ - w принимает все различные значения. □

Пример. $z = 1,\ n = 3,\ \sqrt[3]{1}$



10 Алгебра над полем

Пусть F - поле

Определение. Алгеброй над полем F называется множество A с операциями сложения, умножения и умножения на элементы поля, удовлетворяющие следующим аксиомам:

1. $(A, +, \cdot)$ - кольцо
2. $(A, +, \lambda\cdot)$ - векторное пространство над полем F
3. $\forall a, b \in A, \lambda \in F: \quad \lambda(a \cdot b) = (\lambda a)b = a(\lambda b)$

Обозначается: $(A, +, \cdot, \lambda\cdot), \quad \lambda \in F$

Определение. Алгебра над полем называется коммутативной (ассоциативной, с единицей и т.д.), если алгебра, как кольцо, имеет соответствующее свойство.

Определение. Размерность алгебры - размерность алгебры, как векторного пространства над полем.

Примеры.

1. $M_n(F)-$ алгебра матриц с коэффициентами из F (это НЕ коммутативная, ассоциативная с единицей алгебра над F)
2. $(V^3, +, \times, \lambda\cdot)$ - векторное произведение (НЕ коммутативна, НЕ ассоциативная без единицы алгебра над $\mathbb{R}$, размерности 3)
3. L - подполе поля $F \Longrightarrow F$ можно рассматривать, как алгебру над L

   Пример. $\mathbb{C}$ - алгебра над $\mathbb{R}$ размерности 2 (Базис: $\{1, i\}$)

Пусть A - алгебра над полем F, $\{e_1, ..., e_n\}$ - базис алгебры A, как векторного пространства, тогда

$$\forall a, b \in A : a = \sum_{j=1}^{n} a_j e_j, \ b = \sum_{j=1}^{n} a_j e_j$$

$$\Longrightarrow a \cdot b = (\sum_{j=1}^{n} a_j e_j)(\sum_{j=1}^{n} a_j e_j) = \sum_{j,k=1}^{n} a_j b_k (e_j e_k)$$

Для умножения произвольных элементов достаточно знать таблицу умножения базисных элементов $(e_j \cdot e_k)$

Утверждение. Для проверки коммутативности $(\cdot)$ в алгебре (ассоциативности и т.д.) достаточно проверить на базисных векторах.

Доказательство. Очевидно $\square$

Примеры.

1. $\mathbb{C}$ - алгебра над $\mathbb{R}$ с базисом $\{1, i\}$

	1	i
1	1	i
i	i	-1

2. $(V^3, +, \times, \lambda\cdot)$; V^3 с базисом $\{i, j, k\}$

x	i	j	k
i	0	k	j
j	-k	0	i
k	-j	-i	0

3. $M_n(F)$

Замечание. Пусть V - векторное пространство над полем F. Хотим превратить V в алгебру над полем F.
Пусть e_{jk} - произвольные векторы из V, $j, k = \overline{1, n}$
Положим $e_j \cdot e_k = e_{jk} \Longrightarrow$

$$\forall a, b \in V : \ a \cdot b = \sum_{j,k=1}^{n} a_j b_k e_{jk}$$

Это произведение превращает V в алгебру над полем F.

Пример. Алгебра кватернионов $\mathbb{H}$
$\mathbb{H}$ - 4-х - мерное векторное пространство над $\mathbb{R}$ с базисом $\{1, i, j, k\}$ и таблицей умножения:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	i	-1

$\Longrightarrow$ ассоциативная, НЕ коммутативная алгебра, в которой каждый не нулевой элемент обратим (тело).

Определение. Подмножество B алгебры A назвается подалгеброй A, если B - подпространство A, как кольца, и подпространства A, как пространства.

Утверждение. Любоя подалгебра сама является алгеброй относильно тех же оперций и тем же полем.

Определение. Алгебра A и $\widetilde{A}$ над одним и тем же полем назваются изоморфные, если они изоморфны.

10.1 Алгебра многочленов над полем

F - поле

Определение. Бесконечная последовательность $(a_0, a_1, a_2, ...)$, где $a_i \in \mathbb{R}$, называется финитной, если только конечное число a_i отлично от нуля.

$$F^\infty = \{(a_0, a_1, a_2, ...) \mid a_i \in \mathbb{R}\}$$

Утверждение. Множество F^∞ относительно операции сложения:

$$(a_0, a_1, a_2, ...) + (b_0, b_1, b_2, ...) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, ...)$$

и умножения на элементы $\lambda \in F$:

$$(a_0, a_1, a_2, ...) \cdot \lambda = (\lambda a_0, \lambda a_1, \lambda a_2, ...)$$

F^∞ - бесконечномерное векторное пространство.

Утверждение. F^∞ - счетномерно с базисом:

$$(e_0, e_1, e_2, ...) = (\ (1, 0, 0, ...),\ (0, 1, 0, ...),\ (0, 0, 1, ...), ...\ )$$

Зададим умножение $e_k \cdot e_l = e_{k+l} \Longrightarrow F^\infty$ превращается в алгебру над полем F

Замечание. Так как $e_k \cdot e_l = e_{k+l}$ и в $\mathbb{Z}$ сложение коммутативно и ассоциативно, то F^∞ - ассоциативная, коммутативная алгебра над F с единицей: $e_0 = (1, 0, 0, ...)$

Определение. Такая алгебра называется алгеброй многочленов над полем F. Обозначается: $F[x]$

Получаем привычный вид многочлена: $\forall a \in F:\ a \cdot e_0$ отожествим с элементом a, а вектор e_1 обозначим через x:

$$e_k = \underbrace{e_1 \cdot e_1 \cdot ... \cdot e_1}_{k} = x^k$$

Рассмотрим произвольный $(a_0, a_1, a_2, ...) \in F^\infty$. Так как она финитная, то:

$$(a_0, a_1, ..., a_n, 0, 0, ...) = a_0e_0 + a_1e_1 + ... + a_ne_n = a_0 + a_1x + ... + a_nx^n$$

a_i называется коэффициентом многочлена.

Определение. Если $f = a_0 + a_1x + ... + a_nx^n$, где $a_n \neq 0$, $a_k = 0$, $\forall k > n$, то a_n называется старшим членом, а число $\deg f = n$ называется степенью многочлена.

Замечание. $\deg 0 = -\infty$ (или неопределена)
$f \neq 0$, $\deg f \in \mathbb{N} \cup \{0\}$

Свойства.

1. $\deg(f + g) \leq \max\{\deg f, \deg g\}$
2. $\deg(fg) = \deg f + \deg g$

Доказательство.

1. Упражнение
2. $$f = a_0 + a_1x + ... + a_nx^n,\ a_n,\ \deg f = n$$
$$g = b_0 + b_1x + ... + b_mx^m,\ b_m,\ \deg f = m$$
$$fg = a_0b_0 + ... + a_nb_mx^{n+m}$$
$a_n, b_m \neq 0$, т.к. в поле нет делителей нуля $\Longrightarrow a_nb_m$ - старший член
$$\Longrightarrow \deg fg = \deg f + \deg g$$

□

Следствие.

1. в $F[x]$ нет делителей нуля.
2. Обратные в $F[x]$ - это многочлены нулевой степени и только они, т.е. это все ненулевые константы.

10.1.1 Деление с остатком

Теорема. Пусть F - поле, $f, g \in F[x],\ g \neq 0$. Тогда $\exists!\ q, r\colon\ f = g \cdot q + r$, причем либо $r = 0$, либо $\deg r < \deg g$

Доказательство. Пусть $f, g \neq 0$

$$f = a_0 + a_1 x + ... + a_n x^n,\ a_n \neq 0,\ \deg f = n$$

$$g = b_0 + b_1 x + ... + b_m x^m,\ b_m \neq 0,\ \deg f = m$$

Докажем существование:

1. $n < m \Longrightarrow f = 0 \cdot g + f\ (q = 0, f = r)$
2. $n \geq m \Longrightarrow f_1 = f - \frac{a_n}{b_m} \cdot g \cdot x^{n-m}$
   Если $\deg f_1 < \deg g \Longrightarrow r = f_1,\ q = \frac{a_n}{b_m} \cdot x^{n-m}$
   Иначе продолжаем процесс с f_1 (заметим, что $\deg f_1 < \deg f$): находим f_2 и т.д. Процесс закончится на конечном шаге.

Докажем единственность:
Допустим, $f = g \cdot q_1 + r_1$ и $f = g \cdot q_2 + r_2$

$$\Longrightarrow r_1 - r_2 = g(q_2 - q_1) \Longrightarrow \deg(r_1 - r_2) = \deg g + \deg(q_2 - q_1)$$

$$\deg(r_1 - r_2) \geq \deg g$$

. С другой стороны

$$\deg(r_1 - r_2) < \max\{\deg r_1, \deg r_2\} < \deg g$$

- получаем противоречие. □

10.1.2 Мгогочлены как функции

F - поле, $f = a_n x^n + a_{n-1} x^{n-1} + ... + a_0$

Определение. Значение многочлена f в точке c называет число, равное:

$$f(c) = a_n c^n + a_{n-1} c^{n-1} + ... + a_0$$

Таким образом, множество f задает отображение $F \to F$

$$c \to f(c) \Longrightarrow f \text{ задает функцию}$$

Замечание. Разные многочлены могут задавать одну функцию.

Пример. $F = \mathbb{Z}_2,\ f_1 = x^2,\ f_2 = x$ - разные многочлены, но они задают одну и ту же функцию:

$$f_1(0) = 0,\ f_1(1) = 1,\ f_2(0) = 0,\ f_2(1) = 1$$

Теорема. Пусть F - бесконечное поле. Тогда разные многочлены задают разные функции.

Доказательство. Допустим, $f, g \in F[x],\ f \neq g,\ \forall c \in F,\ f(c) = g(c)$
Введем $h = f - g \in F[x],\ h \neq 0,\ \forall c \in F,\ h(c) = 0$
Т.к. поле F - бесконечное, то $\exists\ c_0, c_1, ..., c_n \in F$ - различные числа, такие что:

$$\begin{cases} h(c_0) = 0 \\ h(c_1) = 0 \\ \vdots \\ h(c_n) = 0 \end{cases} \Longrightarrow \begin{cases} a_0 + a_1c_0 + ... + a_{n-1}c_0^{n-1} + a_nc_0^n = 0 \\ a_0 + a_1c_1 + ... + a_{n-1}c_1^{n-1} + a_nc_1^n = 0 \\ \vdots \\ a_0 + a_1c_n + ... + a_{n-1}c_n^{n-1} + a_nc_n^n = 0 \end{cases}$$

- квадратная однородная СЛУ относительно неизвестных $a_0, a_1, ..., a_n$ с матрицей коэффициентов A :

$$A = \begin{pmatrix} 1 & c_0 & \cdots & c_0^n \\ 1 & c_1 & \cdots & c_1^n \\ \vdots & \vdots & & \vdots \\ 1 & c_n & \cdots & c_n^n \end{pmatrix},\quad \det A = \underbrace{V(c_0, c_1, ..., c_n)}_{\text{Опр. Вандермонда}} \neq 0$$

$\Longrightarrow$ по правилу Крамера СЛУ имеет единственное решение и оно тривиальное
$\Longrightarrow \forall i \in \{0, 1, ..., n\} : a_i = 0 \Longrightarrow n = 0$ противоречие. □

Теорема. (Безу) Пусть F - поле, $f \in F[x], c \in F$.
Тогда остаток при делении f на $(x - c)$ равен значению многочлена в точке c.

Доказательство. Пусть $f(x) = (x - c)g(x) + r(x)\ (*)$

$$\deg r(x) < \deg(x - c) = 1 \Longrightarrow r(x) - const$$

$\Longrightarrow$ Либо $r(x) = 0$, либо $r(x) = r \in F$
Подставим в $(*)$ $x = c$:

$$f(c) = (c - c) \cdot q(c) + r(c) = r$$

□

10.1.3 Корни многочленов

Определение. Элемент $c \in F$ - корень многочлена $f \in F[x]$, если $f(c) = 0$. Из теоремы Безу получаем утверждение:

Утверждение. $c \in F$ - корень многочлена $f \in F[x] \iff (x - c) \mid f$.

Определение. Если c - корень многочлена f и $(x - c)^2 \nmid f$, то корень c - называется простым, иначе - кратным.

Определение. Если c - корень и $(x - c)^k \mid f,\ (x - c)^{k+1} \nmid f$, то c - корень кратности $k\ \ (k \in \mathbb{N})$.

Утверждение. c - корень многочлена f кратности $k \iff \begin{cases} f = (x - c)^k \cdot g \\ g(c) \neq 0 \end{cases}$

Следствие. Пусть $f \in F[x],\ f \neq 0,\ \deg f = n,\ k$ - число всех корней многочлена f с учетом кратности.
Тогда $k \leq n$, причем если $k = n \iff f$ раскладывается на линейные многочлены.

Доказательство. Если c_1 - корень, то $f = (x - c_1)g_1$
Если c_2 - корень, то $f = (x - c_1)(x - c_2)g_2$ и т.д.

$$\Longrightarrow f = (x - c_1)(x - c_2)...(x - c_k)g$$

где g не имеет корней. То есть $c_1, ..., c_k$ - корни многочлена f, при этом среди них могут быть одинаковые.

$$\Longrightarrow f = (x - \widetilde{c_1})^{k_1}(x - \widetilde{c_2})^{k_2}...(x - \widetilde{c_s})^{k_s}g$$

где $\widetilde{c_1}, ..., \widetilde{c_s}$ - все различные корни.
Т.к.

$$f = (x - \widetilde{c_l})h$$

где $h(\widetilde{c_l}) \neq 0 \Longrightarrow \widetilde{c_l}$ - корень кратности k_l

$$\Longrightarrow \deg f = k_1 + ... + k_s + \deg g \Longrightarrow k = k_1 + ... + k_s \leq n$$

При этом:

$$k = n \iff \deg g = 0 \iff f = \prod_{l=1}^{s}(x - \widetilde{c_l})^{k_l}$$

□

Определение. Формальной производной многочлена

$$f = a_n x^n + a_{n-1} x^{n-1} + ... + a_0$$

называется многочлен:

$$f' = a_n n x^{n-1} + a_{n-1}(n-1) x^{n-2} + ... + a_1$$

Утверждение.

1. $(f+g)' = f' + g'$
2. $(\alpha f)' = \alpha f'$
3. $(fg)' = f'g + fg'$

Утверждение. Пусть $\mathrm{char} F = 0,\ c \in F,\ f \in F[x],$ тогда:

$$f(x) = f(c) + \frac{f'(c)}{1!}(x-c) + \frac{f^{(2)}(c)}{2!}(x-c)^2 + ... + \frac{f^{(n)}(c)}{n!}(x-c)^n$$

Доказательство. $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0$.
Подставим $x = y + c$:

$$f = b_n y^n + b_{n-1} y^{n-1} + ... + b_0$$

Подставим $y = x - c$:

$$f = b_n (x-c)^n + b_{n-1}(x-c)^{n-1} + ... + b_0$$

$\Longrightarrow f^{(k)}(c) = k! \cdot b_k$ □

Следствие. Пусть $\mathrm{char} F = 0,\ f \in F[x],\ c \in F$

Тогда c - корень многочлена f кратности $k \Longleftrightarrow \begin{cases} f(c) = 0 \\ f'(c) = 0 \\ \vdots \\ f^{(k-1)}(c) = 0 \\ f^{(k)}(c) \neq 0 \end{cases}$

10.2 Основная теорема алгебры

Теорема. Любой многочлен над полем комплексных числел положительной степени имеет хотя бы один корень.

Утверждение.

Свойства. $\forall z_1, z_2 \in \mathbb{C}$

1. $|z_1 + z_2| \leq |z_1| + |z_2| \quad (\star)$
2. $||z_1| - |z_2|| \leq |z_1 - z_2| \quad (*)$

Доказательство. Из свойств векторов ($z = x + iy$ - вектор, $\sqrt{x^2 + y^2}$ - длина вектора) □

Определение. Последовательность $\{z_k\}_{k=1}^{\infty} \subseteq \mathbb{C}$ называется сходящейся к $z_0 \in \mathbb{C}$, если $|z_k - z_0| \to 0, \ k \to \infty$
Обозначается: $z_k \to z_0$ при $k \to \infty$

Лемма 1. Пусть $z_k = x_k + iy_k, \ z_0 = x_0 + iy_0$, тогда:

$$z_k \to z_0 \Longleftrightarrow \begin{cases} x_k \to x_0 \\ y_k \to y_0 \end{cases}$$

Доказательство.

$$|z_k - z_0| = |(x_k - x_0) + (y_k - y_0)i| = \sqrt{(x_k - x_0)^2 + (y_k - y_0)^2}$$

□

Лемма 2. Если $z_k \to z_0$, то $|z_k| \to |z_0|$

Доказательство.

$$z_k \to z_0 \Longrightarrow |z_k - z_0| \to 0 \Longrightarrow ||z_k| - |z_0|| \to 0 \underset{(*)}{\Longrightarrow} |z_k| - |z_0| \to 0$$

□

Лемма 3. Если $z_k \to z_0, \ w_k \to w_0$, то:

1. $z_k + w_k \to z_0 + w_0$
2. $z_k \cdot w_k \to z_0 \cdot w_o$

Доказательство.

1. $|z_k + w_k - z_0 - w_0| \underset{(\star)}{\leq} |z_k - z_0| + |w_k - w_0| \to 0$

2.

$$|z_k w_k - z_0 w_0| = |z_k w_k - z_k w_0 + z_k w_0 - z_0 w_0| =$$
$$= |z_k(w_k - w_0) + w_0(z_k - z_0)| \underset{(\star)}{\leq} |z_k(w_k - w_0)| + |w_0(z_k - z_0)| =$$
$$= |z_k||(w_k - w_0)| + |w_0||(z_k - z_0)| \to 0$$

□

Следствие. Если $f \in \mathbb{C}[z],\ \deg f > 0,\ z_0 \in \mathbb{C},\ z_k \to z_0$, тогда:

$$f(z_k) \to f(z_0)$$

Лемма 4. (О возрастании модуля |f(z)|)
Пусть $f \in \mathbb{C}[z],\ \deg f > 0$, тогда если $|z_k| \to \infty$, то:

$$|f(z_k)| \to \infty$$

Доказательство. $f(z) = a_n x^n + ... + a_1 x + a_0 \in \mathbb{C}[z] \neq 0$

$$|f(z_k)| = |a_n z_k^n + a_{n-1} z_k^{n-1} ... + a_1 z_k + a_0| =$$
$$= |z_k^n \cdot (a_n + \frac{a_{n-1}}{z_k} + ... + \frac{a_1}{z_k^{n-1}} + \frac{a_0}{z_k^n})| =$$
$$= |z_k^n| \cdot |(a_n - (-\frac{a_{n-1}}{z_k} - ... - \frac{a_1}{z_k^{n-1}} - \frac{a_0}{z_k^n}))| \underset{(*)}{\geq}$$
$$\underset{(*)}{\geq} |z_k|^n \cdot ||a_n| - \frac{|a_{n-1|}}{|z_k|} - ... - \frac{|a_{1|}}{|z_k|^{n-1}} - \frac{|a_{0|}}{|z_k|^n}| \to \infty$$

□

Лемма 5. (Лемма Даламбера)
Пусть $f \in \mathbb{C}[z],\ \deg f > 0,\ f(z_0) \neq 0$, тогда $\exists\ z \in \mathbb{C}$ сколько угодно близкое к z_0 такое, что:

$$|f(z)| < |f(z_0)|$$

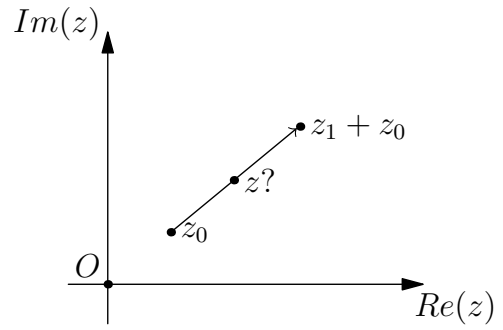
Доказательство. Разложим f по степеням $(z - z_0)$:

$$f(z) = f(z_0) + b_s(z - z_0)^s + ... + b_n(z - z_0)^n, \quad \text{где } b_s \neq 0$$

Так как $f(z_0) \neq 0$, то можно поделить на него:

$$\frac{f(z)}{f(z_0)} = 1 + c_s(z - z_0)^s + ... + c_n(z - z_0)^n,\ c_i = \frac{b_i}{f(z_0)} \neq 0$$

Найдем $z_1 \in \mathbb{C}:\ c_s z_1^s = -1$



Рассмотрим $z = z_0 + tz_1$, где $t \in (0, 1)$

Подставим:

$$\frac{f(z)}{f(z_0)} = 1 - t^s + t^{s+1}g(t), \text{ где } g(t) \in \mathbb{C}, \ \deg g \leq n - (s+1)$$

$$|g(t)| = |\alpha_0 + \alpha_1 t + ... + \alpha_{n-(s+1)}t^{n-(s+1)}|$$

Обозначим $C = \max\{|\alpha_i|\}$, тогда $|g(t)| \leq C(n-s)$

$$|\frac{f(z)}{f(z_0)}| = |1 - t^s + t^{s+1}g(t)| \leq |1 - t^s| + t^{s+1}|g(t)| \leq$$

$$\leq 1 - t^s + t^{s+1}C(n-s) = 1 - t^s(1 - tC(n-s)) \underbrace{<}_{\text{хотим}} 1$$

$$1 - tC(n-c) > 0 \Longleftrightarrow t < \frac{1}{C(n-s)}$$

Выбираем такое $t \in (0, 1)$ и получаем:

$$1 - t^s(1 - tC(n-s)) < 1$$

Если $C = 0$, то верно и очевидно. □

Теорема. (Основная теорема алгебры)

$$\forall f \in \mathbb{C}[z], \ \deg f > 0 \Longrightarrow \exists \ z_0 \in \mathbb{C} : \ f(z_0) = 0$$

Доказательство. Рассмотрим $M = \underbrace{\inf}_{z} |f(z)|$

1 шаг. Хотим доказать, что inf достигается, т.е. $\exists \ z_0 \in \mathbb{C} : \ |f(z_0)| = M$
По определению inf $\exists$ последовательность $\{z_k\} : \ |f(z_k)| \to M$

1 случай. $\{z_k\}$ - не ограничена, т.е. $\exists\{z_{k_i}\} \subseteq \{z_k\} : \ |z_{k_i}| \to \infty$.
По лемме (4): $|f(z_{k_i})| \to \infty$ - противоречие.

2 случай. $\{z_k\}$ - ограничена $\Longrightarrow \exists\ C > 0 :\ |z_k| < C \Longrightarrow$

$$z_k = x_k + iy_k < C \Longrightarrow \begin{cases} |x_k| < |z_k| < C \\ |y_k| < |z_k| < C \end{cases}$$

Так как $\{x_k\}, \{y_k\}$ - ограничены, то по теореме Больцано-Вейштрасса:

$$\exists\ \{x_{k_i}\} \subseteq \{x_k\} :\ \{x_{k_i}\} \to x_0$$

$$\exists\ \{y_{k_{i_l}}\} \subseteq \{y_{k_i}\} :\ \{y_{k_{i_l}}\} \to y_0$$

Значит по Лемме (1):

$$\{z_{k_{i_l}}\} \to x_0 + y_0 i = z_0 \Longrightarrow |f(\{z_{k_{i_l}}\})| \to |f(z_0)| = M$$

2 шаг. Допустим, что $M > 0 \Longrightarrow$ по Лемме Даламбера:

$$\exists\ \widetilde{z} \in \mathbb{C} :\ |f(\widetilde{z})| < M = f(z_0) - \text{противоречие, т.к. } M \text{ это } \inf$$

$$\Longrightarrow M = 0 \Longrightarrow f(z_0) = 0$$

□

Следствие 1. Любой многочлен над $\mathbb{C}$ положительной степени раскладывается на линейные множители.

Следствие 2. Любой многочлен над $\mathbb{C}$ степени n имеет n корней с учетом кратности.

Теорема. (О мнимых корнях многочлена с вещественными коэффициентами)
Пусть $f \in \mathbb{R}[x],\ c$ - корень, $\ c \in \mathbb{C} \setminus \mathbb{R}$ и пусть этот корень имеет кратность k, тогда $\overline{c}$ - тоже корень многочлена f кратности k.

Доказательство. $f(x) = a_n x^n + ... + a_1 x + a_0,\ a_i \in \mathbb{R},\ c$ - корень $\Longrightarrow f(c) = 0$

$$f(\overline{c}) = a_n \overline{c}^n + ... + a_1 \overline{c} + a_0 = \overline{a_n c^n + ... + a_1 c + a_0} = \overline{f(c)} = \overline{0} = 0$$

Кратность одинаковая, т.к. $f^{(s)}(c) = 0 \Longleftrightarrow f^{(s)}(\overline{c}) = 0$ □

Теорема. Любой многочлен над $\mathbb{R}$ положительной степени раскладывается на линейные множители и квадратные множители с отрицательным дискриминантом.

Доказательство. $f \in \mathbb{R}[x] \subseteq \mathbb{C}[x] \Longrightarrow$ (по следствию 1 и ОТА)
$\alpha_1, ..., \alpha_s \in \mathbb{R}$ - все корни кратности $k_1, .., k_s$
$c_1, ..., c_t \in \mathbb{C} \setminus \mathbb{R}$ - мнимые корни кратности $m_1, ..., m_t$
$\overline{c_1}, ..., \overline{c_t}$ - тоже мнимые корни, той же кратности $(c_1 \to \overline{c_1})$
$\Longrightarrow \alpha_1, .., \alpha_s, c_1, ..., c_t, \overline{c_1}, ..., \overline{c_t}$ - все корни многочлена

$$f(x) = a_n \prod_{j=1}^{s} (x - \alpha_j)^{k_j} \cdot \prod_{\nu=1}^{t} (x - c_\nu)^{m_\nu} (x - \overline{c_\nu})^{m_\nu} = (*)$$

Если $c = a + bi \in \mathbb{C} \setminus \mathbb{R}$, то:

$$(x - c)(x - \overline{c}) = x^2 - (c + \overline{c})x + c\overline{c}$$

$$c + \overline{c} = 2a, \quad c\overline{c} = a^2 + b^2$$

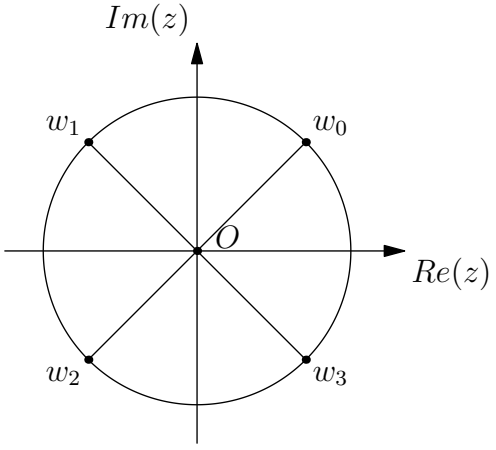
$\Longrightarrow$ уравнение с отрицательным дискриминантом

$$(*) = a_n \prod_{j} (x - \alpha_j)_j^k \cdot \prod_{\nu} (\underbrace{x^2 + \beta_\nu x + \gamma_\nu}_{D<0})^{m_\nu}$$

□

Пример. $x^4 + 1 = 0, \ x^4 = -1, \ w_k = \cos(\frac{\pi + 2\pi k}{4}) + i \sin(\frac{\pi + 2\pi k}{4})$

$$x^4 + 1 = (x - w_0)(x - \overline{w_0})(x - w_1)(x - \overline{w_1}) =$$
$$= (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$$



10.3 Неприводимые многочлены

F - поле

Определение. Многочлен $f \in F[x], \ \deg f > 0$ называется неприводимым над полем F, если f нельзя разложить в произведение многочленов gh,
где $gh \in F[x], \ \deg g < \deg f, \ \deg h < \deg f$.

Утверждение. Любой многочлен 1-ой степени является неприводимым над F.

Пример. $x^2+1 \in \mathbb{C}[x]$ - приводимый

$$x^2+1=(x+i)(x-i)$$

$x^2+1 \in \mathbb{R}[x]$ - неприводимый

Утверждение. (1) Неприводимые многочлены над $\mathbb{C}$ - это линейные многочлены и только они.

Утверждение. (2) Неприводимые многочлены над $\mathbb{R}$ - это все линейные многочлены и все квадратные многочлены с отрицательным дискриминантом и только такие.

Замечание. Над любым полем $\exists$ бесконечное число непропорциональных неприводимых многочленов.

10.4 Многочлены от нескольких переменных

F - поле, $n \in \mathbb{N}$ - фиксированная.
Рассмотрим бесконечномерную алгебру над полем F с базисом
$\{e_{k_1},...,e_{k_n} \mid k_i \in \mathbb{N} \cup \{0\}\}$ и умножением:

$$e_{k_1},...,e_{k_n} \cdot \ e_{m_1},...,e_{m_n} = e_{k_1+m_1},...,e_{k_n+m_n} \ (*)$$

Такая алгебра называется алгеброй множеств от n переменных над полем F.
Обозначается: $F[x_1,...,x_n]$
Из правила $(*) \Longrightarrow$ что алгебра коммутативна, ассоциативна, с единицей: $e_{0,...,0}$
Отождествляем: $\alpha \in F \longleftrightarrow \alpha \cdot e_{0,...,0}$

$$\begin{cases} e_{1,0,...,0} = x_1 \\ e_{0,1,...,0} = x_2 \\ \vdots \\ e_{0,0,...,1} = x_n \end{cases} \Longrightarrow (\text{из } *) \ \ e_{k_1,...,k_n} = x_1^{k_1} \cdot ... \cdot x_n^{k_n} \Longrightarrow$$

$\Longrightarrow$ произвольный элемент из алгебры (по определению базиса) раскладывается, как

$$f = \sum \alpha_{k_1,...,k_n} \cdot e_{k_1,...,k_n} = \sum \alpha_{k_1,...,k_n} \cdot x_1^{k_1} \cdot ... \cdot x_n^{k_n}$$

$$f := f(x_1,...,x_n)$$

- многочлен над полем F.

Пример.

$$f = x_1^5 x_2^7 x_3 - 5x_2^4 x_3 x_4 + 6x_2 x_3 + 7$$

Любой многочлен $f \in F[x_1, ..., x_n]$ можно предствить в виде:

$$(**)\ f = \sum_{k=0}^{s} f_k(x_2, ..., x_n) x_1^k \Longrightarrow$$

$\Longrightarrow$ кольцо $F[x_1, ..., x_n]$ можно рассматривать, как кольцо многочленов от x_1 с коэффициентами из кольца $F[x_2, ..., x_n]$.
Как и для $n = 1$, многочлен $f \in F[x_1, ..., x_n]$ задает функцию из $F^n = F \times ... \times F$.

Теорема. Если поле F - бесконечно, то разные многочлены из $F[x_1, ..., x_n]$ задает разные функции.

Доказательство. Идея: индукция по n. База: $n = 1$ - было доказано.
$n - 1 \to n$. Нужно рассмотреть разложение многочленов в виде $(**)$
Доказательство д/з ($\square$

10.5 Лексикографический порядок на одночленах

$\alpha x_1^{k_1} \cdot ... \cdot x_n^{k_n}$ - одночлен, $\alpha \in F$.

Определение. Порядок $\alpha x_1^{k_1} \cdot ... \cdot x_n^{k_n} \succ \beta x_1^{m_1} \cdot ... \cdot x_n^{m_n}$ $(\alpha, \beta \neq 0)$, называется лексикографическим, если:

$$\exists\ s = \overline{0, n-1} : k_1 = m_1\ , ...,\ k_s = m_s,\ k_{s+1} > m_{s+1}$$

Пример.

$$3x_1^{30} x_2^7 \succ 5x_1^{10} x_2^{150}$$

Свойства.
Если $u,\ v,\ w,\ u_1,\ u_2,\ v_1,\ v_2$ - ненулевые одночлены, то:

1. $u \succ v,\ v \succ w \Longrightarrow u \succ w$ - транзитивность
2. $u \succ v \Longrightarrow uw \succ vw$
3. $u_1 \succ v_1,\ u_2 \succ v_2 \Longrightarrow u_1 u_2 \succ v_1 v_2$

Утверждение. Любой многочлен $f \in F[x_1, ..., x_n]$ однозначно раскладывается в сумму различных одночленов.

Определение. Среди этих одночленов $\exists$ одночлен, который старше остальных. Он называется сташим и обозначается: $LT(f)$

Пример.

$$f = x_1^2x_2 + 7x_1^3x_2x_3 - 9x_1x_2^5x_6, \quad LT(f) = 7x_1^3x_2x_3$$

Лемма. (О старшем члене произведения)
Пусть $f, g \in F[x_1, ..., x_n],\ f, g \neq 0$, тогда:

$$LT(fg) = LT(f) \cdot LT(g)$$

Доказательство.

$$\begin{matrix} f = u_0 + ... + u_s \\ g = v_0 + ... + v_t \end{matrix}, \quad \text{где } u_i, v_i - \text{одночлены}$$

$$LT(f) = u_s,\ LT(g) = v_t$$

$$fg = \sum u_iv_i; \quad u_sv_t \succ u_iv_j, \text{ при } i + j < s + t \Longrightarrow LT(fg) = u_sv_t$$

(Здесь учитывается, что F - поле, а в поле нет делителей нуля) □

Следствие. В $F[x_1, ..., x_n]$ нет делителей нуля.

Определение. Степень одночлена $\alpha x_1^{k_1} \cdot ... \cdot x_n^{k_n},\ \alpha \neq 0$ - это сумма: $k_1 + ... + k_n$

Определение. Степень многочлена $f \in F[x_1, ..., x_n]$ - это максимум степеней его одночленов.
Обозначается: $\deg f$
По определению считаем, что $\deg 0 = -\infty$

Определение. Многочлен $f \in [x_1, ..., x_n]$ называется однородным, если все его одночлены имеют одну и ту же степень.

Утверждение. Любой многочлен $f \in F[x_1, ..., x_n]$ однозначно раскладывается в виде $f = f_0 + ... + f_s$, где f_i - однородный многочлен степени i.

Пример.

$$f = \underbrace{x_1^3x_2 + 2x_1^2x_2^2 + 5x_1x_2x_3^2}_{f_4} + \underbrace{7x_1^2x_3 - 8x_1x_2x_3}_{f_3} + \underbrace{9x_1x_2}_{f_2}$$

$$\deg f = 4$$

f_i - называются однородными компонентами.

Свойства.

1. $\deg(f + g) \leq max\{\deg f, \deg g\}$

2. $\deg(fg) = \deg f + \deg g$

Доказательство.

1. - д/з

2.
$$\begin{matrix} f = f_0 + ... + f_s \\ g = g_0 + ... + g_t \end{matrix} \neq 0 \ - \text{различные однородные компоненты}$$
$$\deg f = \deg f_s,\ \deg g = \deg g_t$$
$$fg = \sum f_i g_i,\ \deg(f_s g_t) > \deg(f_i g_i),\ \text{где } s+t > i+j \Longrightarrow$$
$$\Longrightarrow \deg(fg) = \deg(f_s g_t) = s+t$$

□

10.6 Симметрические многочлены

Определение. Многочлен $f \in F[x_1, ..., x_n]$ назвается симметрическим, если:

$$\forall \sigma \in S_n :\ f(x_1, ..., x_n) = f(x_{\sigma(1)}, ..., x_{\sigma(n)})$$

Пример.

$$f(x_1, x_2) = 2x_1^3 x_2 + 2x_1 x_2^3 - 7x_1 x_2^2 - 7x_1^2 x_2$$

Утверждение. Если f - симметрический и f раскладывается на однородные компоненты, то f_i - симметрический $\forall i$:

$$f = f_0 + ... + f_s,\ \text{где } f_i - \text{ однородные}$$

Утверждение. Множество всех симметрических многочленов от n переменных над F образует подалгебру в алгебре $F[x_1, ..., x_n]$.

Доказательство. f, g - симметрические $\Longrightarrow f+g,\ fg,\ \alpha f$ - симметрические. (непосредственная проверка) □

10.6.1 Элементарные симметрические многочлены от n переменных

Определение.

$$\sigma_1 = \sigma_1(x_1, ..., x_n) = \sum_{i=1}^{n} x_i$$

$$\sigma_2 = \sigma_2(x_1, ..., x_n) = \sum_{1 \leq i_1 < i_2 \leq n} x_{i_1} x_{i_2}$$

$$\vdots$$

$$\sigma_k = \sigma_k(x_1, ..., x_n) = \sum_{1 \le i_1 < i_2 < ... < i_k \le n} x_{i_1} x_{i_2} \cdot ... \cdot x_{i_k}$$

$$\vdots$$

$$\sigma_n = \sigma_n(x_1, ..., x_n) = x_1 x_2 \cdot ... \cdot x_n$$

Теорема 2. (Основная теорема о симметрических многочленах)
Любой симметрический многочлен $f \in F[x_1, ..., x_n]$ однозначно раскладывается в виде многочлена от элементарных симметрических:

$$\exists!\ g \in F[y_1, ..., y_n] : g(\sigma_1, ..., \sigma_n) = f$$

Пример.

$$f(x_1, x_2) = x_1^2 + x_2^2 = x_1^2 + x_2^2 + 2x_1x_2 - x_1x_2 = (x_1 + x_2)^2 - 2x_1x_2 = \sigma_1^2 - 2\sigma_2$$

$$g(y_1, y_2) = y_1^2 - 2y_2$$

Определение. Одночлен $\alpha x_1^{k_1} \cdot ... \cdot x_n^{k_n}$ называется монотонным, если:

$$k_1 \ge k_2 \ge ... \ge k_n$$

Пример. $f(x_1, x_2, x_3) = x_1^5 x_2^3 x_3$ - монотонный
$g(x_1, x_2, x_3) = x_1^6 x_2^7 x_3$ - не монотонный.

Лемма 1. (О старшем члене симметрического многочлена)
Если $f \in F[x_1, ..., x_n]$ - симметрический, то $LT(f)$ - монотонный.

Доказательство. (От противного)
Пусть $LT(f) = \alpha x_1^{k_1} \cdot ... \cdot x_n^{k_n}$ - не монотонный $\Longrightarrow \exists\ i = \overline{1, n-1} :\ k_i < k_{i+1}$
Т.к. f - симметрический, то $\sigma \in S_n :\ \sigma = (i, i+1)$ - транспозиция $\Longrightarrow$ среди одночленов многочлена f должен $\exists\ u = x_1^{k_1} \cdot ... \cdot x_i^{k_{i+1}} x_{i+1}^{k_i} \cdot ... \cdot x_n^{k_n}$
Но $u \succ LT(f)$ - противоречие определению LT $\square$

Лемма 2. Пусть f - симметрический. $LT(f) = \alpha x_1^{k_1} \cdot ... \cdot x_n^{k_n}$, тогда:

$$\exists\ e_1, ..., e_n :\ LT(\alpha\sigma_1^{e_1}, ..., \sigma_n^{e_n}) = \alpha x_1^{k_1} \cdot ... \cdot x_n^{k_n}$$

Доказательство.

$$LT(\alpha\sigma_1^{e_1}, ..., \sigma_n^{e_n}) = \alpha LT(\sigma_1^{e_1}) LT(\sigma_2^{e_2}) \cdot ... \cdot LT(\sigma_n^{e_n}) =$$
$$= \alpha x_1^{e_1} (x_1x_2)^{e_2} \cdot ... \cdot (x_1 \cdot ... \cdot x_k)^{e_k} \cdot ... \cdot (x_1x_2 \cdot ... \cdot x_n)^{e_n} =$$
$$= \alpha x_1^{e_1 + ... + e_n} x_2^{e_2 + ... + e_n} \cdot ... \cdot x_n^{e_n} = \alpha x_1^{k_1} \cdot ... \cdot x_n^{k_n} \Longrightarrow$$

$$\Longrightarrow \text{СЛУ: } \begin{cases} e_1 + e_2 + ... + e_{n-1} + e_n = k_1 \\ e_2 + ... + e_{n-1} + e_n = k_2 \\ \ddots \\ e_{n-1} + e_n = k_{n-1} \\ e_n = k_n \end{cases} \iff \begin{cases} e_1 = k_1 - k_2 \\ e_2 = k_2 - k_3 \\ \vdots \\ e_{n-1} = k_{n-1} - k_n \\ e_n = k_n \end{cases}$$

Т.к. f - симметрический, то $k_1 \geq k_2 \geq ... \geq k_n$ по Лемме (1) $\Longrightarrow \forall i: \ e_i \geq 0$ $\square$

Доказательство. (Основной теоремы о симметрических многочленах)

$\exists:$ Если $f = 0$, то $g = 0$
Если $f \neq 0$, то $LT(f) = \alpha x_1^{k_1} \cdot ... \cdot x_n^{k_n}$
По Лемме (2):

$$\exists\ e_1, ..., e_n \geq 0: \ LT(\alpha\sigma_1^{e_1}, ..., \sigma_n^{e_n}) = \alpha x_1^{k_1} \cdot ... \cdot x_n^{k_n}$$

$$f_1 = f - \alpha\sigma_1^{e_1}, ..., \sigma_n^{e_n}$$

$f_1 = 0: \ f = \alpha\sigma_1^{e_1}, ..., \sigma_n^{e_n} \Longrightarrow g = \alpha y_1^{e_1}, ..., y_n^{e_n}$

$f_1 \neq 0: \ LT(f) \succ LT(f_1)$, f_1 - симметрический.
Повторяем процесс для $f_1 \Longrightarrow f_1, f_2, f_3, ...$ - симметрические и
$LT(f) \succ LT(f_1) \succ LT(f_2) \succ LT(f_3) \succ ...$
Т.к. каждый $LT(f_i)$ - монотонный, то этот процесс прервется на конечном шаге.

$\underline{!}:$ (Докажем от противного)
Допустим у нас $\exists$ 2 различных многочлена: $g, \widetilde{g} \in F[y_1, ..., y_n]: \ g \neq \widetilde{g}$

$$g(\sigma_1, ..., \sigma_n) = \widetilde{g}(\sigma_1, ..., \sigma_n)$$

Рассмотрим $h = g - \widetilde{g}, \ h \neq 0, \ h(\sigma_1, ..., \sigma_n) = 0$

$$h(y_1, ..., y_n) = \sum \beta_{e_1,...,e_n} \cdot y_1^{e_1} \cdot ... \cdot y_n^{e_n}$$

По лемме (2):

$$(e_1, ..., e_n) \neq (\widetilde{e_1}, ..., \widetilde{e_n}) \implies LT(\sigma_1^{e_1}, ..., \sigma_n^{e_n}) \neq LT(\sigma_1^{\widetilde{e}_1}, ..., \sigma_n^{\widetilde{e}_n})$$

$$h(\sigma_1, ..., \sigma_n) = \sum \beta_{e_1,...,e_n} \cdot \sigma_1^{e_1} \cdot ... \cdot \sigma_n^{e_n} \ (**)$$

Среди всех $LT(\sigma_1^{e_1}, ..., \sigma_n^{e_n})$ есть тот, который старше остальных. В $(**)$ при приведении подобных этот старший член не сможет сократиться $\Longrightarrow$ $h(\sigma_1^{e_1}, ..., \sigma_n^{e_n}) \neq 0$ - противоречие.

$\square$

10.7 Формулы Виета

F - поле, $f \in F[x]$, $\deg f = n > 0$

$$f(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n$$

Пусть $c_1, ..., c_n \in F$ - все корни многочлена f с учетом кратности, тогда:

$$f(x) = a_0(x - c_1)(x - c_2)...(x - c_n) =$$
$$= a_0x^n - a_0(c_1 + ... + c_n)x^{n-1} + a_0(\sum_{i<j} c_ic_j)x^{n-2} -$$
$$- a_0(\sum_{i<j<k} c_ic_jc_k)x^{n-3} + ... + (-1)^nc_1...c_n$$

$$a_k = (-1)^k a_0\sigma_k(c_1, ..., c_k),\ k = \overline{1, n}$$
$$\Longrightarrow \sigma_k(c_1, ..., c_k) = (-1)^k\frac{a_k}{a_0}\ \textbf{– Формулы Виета}$$

11 Теория делимости в Евклидовых кольцах

Определение. Коммутативное, ассоциативное кольцо с единицей, в котором нет делителя нуля, называется целостным.

Примеры.

1. $\mathbb{Z}$
2. $F[x]$, где F - поле
3. $K[x]$, где K - целостное кольцо

Определение. Пусть K - целостное кольцо, тогда говорят, что b делит a, где $a, b \in K$, если $\exists\ c \in K :\ a = bc$.
Обозначается: $b|a$

Определение. Элементы a и b называются ассоциированными, если $a|b$ и $b|a$.
Обозначается: $a \sim b$

Утверждение. $a \sim b \iff a = bc$, где c обратим в K, a и b не нулевые.

Доказательство.

$\Longrightarrow$: $\begin{cases} a|b \\ b|a \end{cases} \implies \begin{cases} b = ac_1 \\ a = bc_2 \end{cases} \implies a = ac_1c_2 \implies c_1c_2 = 1 \implies c_2$ обратим.

$\Longleftarrow$: $a = bc \implies b|a$, с другой стороны, $b = ac^{-1} \implies a|b \implies a \sim b$

□

Примеры.

1. $\mathbb{Z} :\ a \sim b \iff a = \pm b$
2. $F[x]$, где F - поле: $f \sim g \iff f = cg$, где $c \in F \setminus \{0\}$

Определение. Целостное кольцо K, которое не является полем, называется евклидовым, если введена функция:

$$N :\ K \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

такая, что:

1. $N(ab) \geq N(b)$ $(\forall a, b \in K \setminus \{0\})$

2. $\forall a, b \in K,\ b \neq 0\ \exists\ q, r \in K:\ a = bq + r$, где $r = 0$ или $N(r) < N(b)$ (т.е. возможно деление с остатком)

При этом N называют нормой.

Примеры.

1. $\mathbb{Z}:\ N(a) = |a|$

2. $F[x]$, где F - поле: $N(f) = \deg f$

Упражнение. $z[i] = \{a + bi \mid a, b \in \mathbb{Z}\},\ N(a + bi) = a^2 + b^2 \Longrightarrow$ $z[i]$ с такой нормой - евклидово кольцо.

Утверждение. $N(ab) = N(a) \Longleftrightarrow b$ обратим

Доказательство.

1) Пусть b обратим

$$N(ab) \geq N(a) \text{ и } N(a) = N((ab)b^{-1}) \geq N(ab) \Longrightarrow N(ab) = N(a)$$

2) Пусть b необратим
Поделим a на ab с остатком:

$$a = abq + r$$

Если $r = 0$, то $a = abq \Longrightarrow bq = 1 \Longrightarrow b$ обратим - противоречие.
Иначе $N(r) < N(ab)$
С другой сторон:

$$r = a - abq = a(1 - bq) \Longrightarrow N(r) = N(a(1 - bq)) \geq N(a) \Longrightarrow N(r) \geq N(a)$$

$$\begin{cases} N(r) < N(ab) \\ N(r) \geq N(a) \end{cases} \Longrightarrow N(ab) > N(a) - \text{ противоречие}$$

□

Определение. Наибольшим общим делителем элементов $a, b \in K$ называется элемент $d \in K$ такой, что:

1) $d|a,\ d|b$

2) Если $d_1|a$ и $d_1|b$, то $d_1|d$

Обозначается: НОД(a, b)

Замечание.

1. НОД$(a, 0) = a$
2. НОД может не существовать

Лемма. Если $\exists$ НОД(a, b), то он определяется однозначно с точностью до ассоциированности.

Доказательство. d_1, d_2 - это НОД(a, b), по свойству 2):

$$d_1|d_2, \quad d_2|d_1 \Longrightarrow d_1 = d_2$$

□

Теорема. Пусть K - евклидово кольцо. Тогда $\forall a, b \in K \ \exists$ НОД$(a, b) = d$, причем НОД$(a, b) = au + bv$ для некоторых $u, v \in K$.

Доказательство.

1. $b = 0$: НОД$(a, b) = a = a \cdot 1 + b \cdot v$
2. $b|a$: НОД$(a, b) = b = a \cdot 0 + b \cdot 1$
3. $b \neq 0, \ b \nmid a$: Делим:

   0) $a = bq_1 + r_1$, где $N(r_1) < N(b)$

   1) $b = r_1q_2 + r_2$, где $N(r_2) < N(r_1)$

   2) $r_1 = r_2q_3 + r_3$, где $N(r_3) < N(r_2)$

   $\vdots$

   k) $r_{k-1} = r_kq_{k+1} + r_{k+1}$, где $N(r_{k+1}) < N(r_k)$

   k+1) $r_k = r_{k+1}q_{k+2}$

   Докажем, что $r_{k+1} =$ НОД(a, b) :

$$r_{k+1}|a, \ r_{k+1}|b \ ?$$

из k+1) $r_{k+1}|r_k$

из k) $r_{k+1}|r_{k-1}$

$\vdots$

из 2) $r_{k+1}|r_1$

из 1) $r_{k+1}|b$

из 0) $r_{k+1}|a$

Что бы доказать 2-е условие, докажем, что $r_{k+1} = au + bv$
Сверху вниз $\forall s: \ r_s = au_s + bv_s$

0) $r_1 = a - bq_1 = au_1 + bv_1 \Longrightarrow u_1 = 1, \ v_1 = -q_1$

1) $r_2 = b - r_1q_2 = b - (a - bq_1)q_2 = au_2 + bv_2$

$\vdots$

Далее по индукции. Получаем:

$$r_s = r_{s-2} - r_{s-1}q_s = (au_{s-2} + bv_{s-2}) - (au_{s-1} + bv_{s-1})q_s = au_s + bv_s$$

Так как $r_{k+1} = au + bv$, то если $d_0|a, \ d_0|b \Longrightarrow d_0|(au + bv) \Longrightarrow d_0|r_{k+1}$
$\Longrightarrow$ НОД$(a, b) = r_{k+1}$

□

Определение. Процедура находа НОД(a, b) в доказательстве теоремы называется алгоритмом Евклида.

Пусть K - евклидово колько

Определение. Элементы K называются взаимопростыми, если НОД$(a, b) = 1$

Следствие. Пусть K - евклидово колько, $a, b \in K$ - взаимопростые, тогда:

$$\exists \ u, v \in K: \ au + bv = 1$$

11.1 Разложение на простые элементы

Пусть K - евклидово колько

Пример. $\forall a \in K: \ a = (ac)c^{-1}$, где c - обратим.

Определение. Элемент $p \in K$ называется простым, если он:

1) $p \neq 0$
2) p не является обратимым
3) Равенство $p = ab$, где $a, b \in K$ возможно только при a - обратим или b - обратим

Примеры.

1. В $\mathbb{Z}$ простые элементы - это $\pm p$, где p - простое число

2. В $F[x]$, где F - поле, простые элементы - это неприводимые многочлены

Замечание. Простые элементы - это ненулевые, необратимые элементы, которые имеют в точности два неассоциированных друг с другом элемента.

Лемма 1. (Важная Лемма)
Пусть K - евклидово колько, $p \in K$ - простой элемент, тогда:

$$p|ab,\ \text{НОД}(a,p) = 1 \implies p|b$$

Доказательство. $\text{НОД}(a,p) = 1 \implies \exists\ u, v \in K$:

$$au + pv = 1 \mid \cdot b \implies \underbrace{bau}_{\vdots\ p} + \underbrace{bpv}_{\vdots\ p} = b \implies p|b$$

□

Следствие. Пусть K - евклидово колько, $p \in K$ - простой элемент.
Если $a_i \in K :\ p|(a_1 \cdot ... \cdot a_s)$, тогда:

$$\exists\ i = \overline{1,s} :\ p|a_i$$

Доказательство. Индукция по s. База $s = 2 :\ p|(a_1 \cdot a_2)$
Если $p \nmid a$, то $\text{НОД}(a_1, p) = 1 \implies p|a_2$ (по важной Лемме)
Переход: $p|a_1 \cdot (a_2 \cdot ... \cdot a_n)$
Если $p \nmid a_1$, то $\text{НОД}(a_1, p) = 1 \underbrace{\implies}_{\text{по Лемме}} p|(a_2 \cdot ... \cdot a_n) \underbrace{\implies}_{\text{по Инд.}} \exists\ i = \overline{2,n} :\ p|a_i$ □

Теорема. Пусть K - евклидово кольцо, $a \neq 0 \in K$ - произвольный, необратимый элемент. Тогда a можно разложить:

$$a = p_1^{k_1} \cdot ... \cdot p_n^{k_s}$$

Причем это разложение единственное с точностью до домножения на обратимый и перестановки множителей.

Доказательство.

$\exists$: От противного:
Среди всех ненулевых и необратимых элементов кольца K найдем такие, которые не допускают такое разложения, возьмем наименьший по норме - обозначим его a.

1 случай: a - простой элемент $\Longrightarrow a$ - это и есть разложение на простые

2 случай: a - не простой $\Longrightarrow \exists\ b, c \in K$ - ненулевые, обратимые: $a = bc$

$$N(a) > N(b) \text{ и } N(a) > N(c)$$

$\Longrightarrow$ т.к. a - наименьший по норме, который не допускает это разложение на простые, то

$$b = p_1 \cdot ... \cdot p_t, \quad c = q_1 \cdot ... \cdot q_s$$

Где $p_i,\ q_i$ - простые числа $\Longrightarrow a = p_1 \cdot ... \cdot p_t \cdot q_1 \cdot ... \cdot q_s$ - противоречие

! : От противного:
$a = p_1 \cdot ... \cdot p_s = q_1 \cdot ... \cdot q_s$, где p_i, a_i - простые числа. Индукция по s:

$$\Longrightarrow p_1 | (q_1 \cdot ... \cdot q_s)$$

$\Longrightarrow$ т.к. p_1 - простое, то следовательно:

$$\exists\ i = \overline{1, t}:\ p_1 | q_i \Longrightarrow p_1 \sim q_i$$

Можем считать, что $i = 1,\ q_1 = c_1 p_1,\ c_1$ - обратим
Сокращаем на p_1 : $\quad p_2 \cdot ... \cdot p_s = c q_2 \cdot ... \cdot q_m$
Далее индукция по s: $\Longrightarrow s = t,\ p_i \sim q_i$ (при подходящей перестановке)

□

Следствие 1. Основная теорема арифметики.

Следствие 2. Пусть F - поле, $\ f \in F[x],\ \deg f \geq 1$
Тогда f раскладывается на простые неприводимые многочлены над F и это разложение единственно с точностью до перестановки множителей и умножения на ненулевые константы из F.

Следствие 3. Пусть K - евклидово кольцо, $a \in K,\ \ a = p_1^{k_1} \cdot ... \cdot p_s^{k_s}$, где p_i - простые элементы K и $p_i \not\sim p_j$ при $i \neq j$
Пусть $d \in K,\ d|a$. Тогда $d = c p_1^{l_1} \cdot ... \cdot p_s^{l_s}$, где $0 \leq l_i \leq k_i,\ \ c$ - обратимый элемент в K

Доказательство. Т.к. $d|a$, то $a = db$. По теореме разложим d и b на простые (если они необратимы, иначе очев) и сравниваем в $a = db$ правую и левую часть. В силу единсвенности разложения на простые получаем следствие. □

11.2 Поле отношений целостного кольца

K - целостное кольцо

Рассмотрим множество пар:

$$M = \{(a, b) \mid a, b \in K,\ b \neq 0\}$$

Введем отношение эквиватентности:

$$(a, b) \sim (c, d) \Longleftrightarrow ad = bc$$

Утверждение.

$$\forall c \in K,\ c \neq 0 \Longrightarrow (a, b) \sim (ac, bc)$$

Класс эквивалентности пары (a, b) - это:

$$\{(c, d) \in M \mid (c, d) \sim (a, b)\}$$

Класс называется дробью и обозначается: $\frac{a}{b}$

Множество всех таких классов эквивалентности обозначается: $\mathbb{Q}(K)$

Операции на $\mathbb{Q}(K)$:

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_1},\quad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 b_1}{a_1 b_1}$$

Утверждение. Операции корректны, т.е. не зависят от предствитлей.

Доказательство.

$(+)$:

$$\frac{a_1}{b_1} = \frac{\widetilde{a_1}}{\widetilde{b_1}};\ \frac{a_2}{b_2} = \frac{\widetilde{a_2}}{\widetilde{b_2}} \Longrightarrow \frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{\widetilde{a_1}}{\widetilde{b_1}} + \frac{\widetilde{a_2}}{\widetilde{b_2}}$$

Дано: $a_1\widetilde{b_1} = \widetilde{a_1}b_1,\ a_2\widetilde{b_2} = \widetilde{a_2}b_2$

$$\frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \stackrel{?}{=} \frac{\widetilde{a_1}\widetilde{b_2} + \widetilde{a_2}\widetilde{b_1}}{\widetilde{b_1}\widetilde{b_2}}$$

$$(a_1 b_2 + a_2 b_1)\widetilde{b_1}\widetilde{b_2} \stackrel{?}{=} (\widetilde{a_1}\widetilde{b_2} + \widetilde{a_2}\widetilde{b_1})b_1 b_2$$

$a_1 b_2 \widetilde{b_1}\widetilde{b_2} + a_2 b_1 \widetilde{b_1}\widetilde{b_2} = \widetilde{a_1}\widetilde{b_2} b_1 b_2 + \widetilde{a_2}\widetilde{b_1} b_1 b_2$ - это верно

$(\cdot)$: Д/з

□

Утверждение. $Q(K)$ относительно операций $(+)$ и $(\cdot)$ - это поле.

Доказательство. При сложении можем считать, что знаменатель больше, т.е.:
$\frac{a_1}{b} + \frac{a_2}{b} = \frac{a_1+a_2}{b} \Longrightarrow$ коммутативное по сложению, ассоциативное по сложению, $\frac{0}{1}$ - нулевой элемент, $\forall \frac{a}{b}\ \exists\ -\frac{a}{b} = \frac{-a}{b}$
$\Longrightarrow$ это абелева группа по сложению
Непосредственно проверяется дистрибутивность, коммутативность и ассоциативность умножения, $\frac{1}{1}$ - единица (нейтральный по умножению),
$\forall \frac{a}{b} \in Q(K), \frac{a}{b} \neq 0 \Longrightarrow a \neq 0$, $\exists \frac{b}{a} \in Q(K)$ - обратный к $\frac{a}{b} \Longrightarrow Q(K)$ - поле. $\square$

Определение. Такое поле называется полем отношений целостного кольца K (полем частных, полем дробей).
Рассмотрим множество:

$$\{\ \frac{a}{1} \mid a \in K\ \} \text{ в } Q(K)$$

Оно образует подкольцо в $Q(K)$, которое изоморфно кольцу K:

$$\frac{a}{1} - \text{ отождествлен с } a \in K$$

Пример. $Q(\mathbb{Z}) = \mathbb{Q}$

Определение. Пусть K - евклидово кольцо
$a, b \in K,\ b \neq 0,\ a = a_1 d,\ b = b_1 d$, где $d = \text{НОД}(a, b) \Longrightarrow$

$$\frac{a}{b} = \frac{a_1}{b_1},\ \text{где НОД}(a_1, b_1) = 1$$

Такие дроби называются несократимыми.

Утверждение. Пусть K - евклидово кольцо, тогда несократимая дробь $\frac{a}{b} \in Q(K)$ определена однозначно с точностью до умножения числителя и знаменателя на обратимый элемент, т.е.:

$$\frac{a}{b} = \underbrace{\frac{ca}{cb}}_{\text{несокр}},\ \text{где } c \text{ - обратимый элемент кольца } K$$

Доказательство.

$$\frac{a}{b} = \frac{\widetilde{a}}{\widetilde{b}} \Longrightarrow \begin{cases} a\widetilde{b} = b\widetilde{a} \\ \text{НОД}(a, b) = 1 \\ \text{НОД}(\widetilde{a}, \widetilde{b}) = 1 \end{cases} \Longrightarrow \begin{cases} a \mid b\widetilde{a} \\ \text{НОД}(a, b) = 1 \end{cases} \underbrace{\Longrightarrow}_{\text{По важной лемме}} a \mid \widetilde{a}$$

аналогично $\widetilde{a} \mid a \Longrightarrow a \sim \widetilde{a}$, т.е. $\widetilde{a} = ca$, c - обратим

$$\begin{cases} a\widetilde{b} = b\widetilde{a} \\ \widetilde{a} = ca \end{cases} \Longrightarrow a\widetilde{b} = cab \Longrightarrow \widetilde{b} = cb$$

$\square$

11.3 Поле рациональных дробей

F - поле, $K = F[x]$

Определение. Поле отношения кольца $K = F[x]$ называется полем рациональных дробей.
Обозначается: $F(x)$
Элементы этого поля: $\frac{f(x)}{g(x)}$, где $f, g \in F[x],\ g \neq 0$ называются рациональными дробями.

Определение. Дробь $\frac{f}{g} \in F(x)$ называется правильной, если $\deg f < \deg g$. Это определение не зависит от представителей.

Утверждение 1. Сумма и произведение правильных дробей - правильная дробь.

Утверждение 2. Произвольная рациональная дробь $\frac{f}{g} \in F(x)$ единственным образом представима в виде суммы многочлена и правильной дроби.

Доказательство.

$\exists$: Поделим f на g с остатком: $f = qg + r$, где $\left[\begin{array}{l} r = 0 \\ \deg r < \deg g \end{array}\right.$, тогда:

$$\frac{f}{g} = q + \frac{r}{g}$$

$!$: Пусть $\frac{f}{g} = q + \frac{r}{g} = \widetilde{q} + \frac{\widetilde{r}}{\widetilde{g}}$, тогда:

$$q - \widetilde{q} = \frac{\widetilde{r}}{\widetilde{g}} - \frac{r}{g} \implies q = \widetilde{q},\ \frac{\widetilde{r}}{\widetilde{g}} = \frac{r}{g}$$

□

Утверждение 3. Любая правильная дробь $\frac{f}{g} \in F(x)$ раскладывается в сумму правильных дробей со знаменателями: $g_1, g_2, ..., g_s$, где $g = g_1 \cdot g_2 \cdot ... \cdot g_s$ и НОД$(g_i, g_j) = 1$, при $i \neq j$:

$$\frac{f}{g} = \underbrace{\frac{r_1}{g_1} + ... + \frac{r_s}{g_s}}_{\text{правильные}}$$

Доказательство. Индукция по s:
$s = 2,\ g = g_1 g_2,\ $ НОД$(g_1, g_2) = 1 \Longrightarrow \exists\, u, v \in F[x] :\ ug_1 + vg_2 = 1$, тогда:

$$\frac{f}{g} = \frac{f \cdot 1}{g_1 g_2} = \frac{f(ug_1 + vg_2)}{g_1 g_2} = \frac{fu}{g_2} + \frac{fv}{g_1} = q_1 + \frac{r_1}{g_1} + q_2 + \frac{r_2}{g_2}$$

По утверждению (1): $q_1 + q_2$ - правильная дробь. многочлен, который является правильной дробью - нулевой многочлен $\Longrightarrow q_1 + q_2 = 0 \Longrightarrow$

$$\frac{f}{g} = \frac{r_1}{g_1} + \frac{r_2}{g_2}$$

Переход: $s-1 \ \rightarrow \ s : \frac{f}{g_1(g_2 \cdot \ldots \cdot g_s)} = \frac{r_1}{g_1} + \frac{r_2}{g_2 \cdot \ldots \cdot g_s} \underbrace{=}_{\text{По предп. индукции}} \frac{r_1}{g_1} + \frac{r_2}{g_2} + \ldots + \frac{r_s}{g_s}$ $\square$

Определение. Рациональная дробь $\frac{f}{g} \in F(x)$ называется простейшей,если:

1) $\frac{f}{g} \neq 0$

2) $g = p^s$, где p - неприводимый множитель над F, $s \in \mathbb{N}$

3) $\deg f < \deg p$

Примеры.

1. $\forall$ поля F: $\frac{\alpha}{(x-c)^k}$, где $\alpha, c \in F$, $\alpha \neq 0$, $k \in \mathbb{N}$ является простейшей всегда.
2. Если $F = \mathbb{C}$, то простейщий другого вида нет.
3. $F = \mathbb{R}$: $\frac{\alpha}{(x-c)^k}$, $\frac{\beta x+\gamma}{(x^2+ax+b)^k}$, где $\alpha, \beta, \gamma, a, b, c \in \mathbb{R}$, $\alpha, \beta \neq 0$, $\beta^2+\gamma^2 \neq 0$, $k \in \mathbb{N}$ и у $(x^2 + ax + b)$ отрицательный дискриминан.

Теорема. Любая правильная дробь $\frac{f}{g} \in F(x)$ раскладывается в сумму простейших.
Более того, если $g = p_1^{s_1} \cdot \ldots \cdot p_k^{s_k}$, где p_i - неприводимый над F и $\forall i \neq j$: $p_i \not\sim p_j$, тогда $\frac{f}{g}$ раскладывается в сумму простейших со знаменателями:

$$p_1, \ p_1^2, \ \ldots, \ p_1^{s_1}, \ \ldots, \ p_k^1, \ p_k^2, \ \ldots, \ p_k^{s_k}$$

и это разложение единственно.

Доказательство.

$\exists$: $g = p_1^{s_1} \cdot \ldots \cdot p_k^{s_k}$. По утверждению (3) $\frac{f}{g} = \frac{r_1}{g_1^{s_1}} + \ldots + \frac{r_k}{g_k^{s_k}}$
Достаточно рассмотреть правильную дробь вида $\frac{r}{p^s}$.
Индукция по s:
Поделим r на p с остатком:

$$r = pg + \widetilde{r}, \quad \text{где} \left[\begin{array}{l} \widetilde{r} = 0 \\ \deg \widetilde{r} < \deg p \end{array} \right.$$

$$\Longrightarrow \frac{r}{p^s} = \frac{pq + \widetilde{r}}{p^s} = \frac{q}{p^{s-1}} + \frac{\widetilde{r}}{p^s}$$

где $\frac{\widetilde{r}}{p^s}$ - либо 0, либо простейшая.

Повторяем процесс для $\frac{q}{p^{s-1}}$

$\underline{!}$: (От противного)

$$\frac{f}{g} = \sum_{i=1}^{s} \left(\frac{r_{i_1}}{p_i} + \frac{r_{i_2}}{p_i^2} + ... + \frac{r_{i_s}}{p_i^{s_i}}\right) = \sum_{i=1}^{s} \left(\frac{\widetilde{r}_{i_1}}{p_i} + \frac{\widetilde{r}_{i_2}}{p_i^2} + ... + \frac{\widetilde{r}_{i_s}}{p_i^{s_i}}\right)$$

$$\Longrightarrow \sum_{i=1}^{s} \left(\frac{\widetilde{\widetilde{r}}_{i_1}}{p_i} + \frac{\widetilde{\widetilde{r}}_{i_2}}{p_i^2} + ... + \frac{\widetilde{\widetilde{r}}_{i_s}}{p_i^{s_i}}\right) = 0, \quad \text{где } \widetilde{\widetilde{r}}_{i_j} = r_{i_j} - \widetilde{r}_{i_j}$$

Допустим, что $\exists\ \widetilde{\widetilde{r}}_{i_j} \neq 0$

Рассмотрим $\widetilde{\widetilde{r}}_{i_t}$, где t - максимальный с таким условием (самый правый) и без ограничение общности считаем, что $i = 1$.

Приводим к общему знаменателю и приравниваем числители:

$$\widetilde{\widetilde{r}}_{1_t} p_2^{s_2} \cdot ... \cdot p_k^{s_k} + p_1 h(x) = 0$$

$h(x)$ - собрали все кратные p_1 в числителе

$$p_1 \not\sim p_i \ (i \neq 1) \Longrightarrow p_1 \mid \widetilde{\widetilde{r}}_{1_t} \Longrightarrow \widetilde{\widetilde{r}}_{1_t} = 0$$

т.к. иначе $\deg \widetilde{\widetilde{r}}_{1_t} < \deg p_1$ по определению простейших.

□

Теорема. (Декарта)

Пусть $f(x) \in \mathbb{R}[x],\ \deg f \geq 1$

$f(x) = a_n x^n + ... + a_1 x + a_0$, где $a_i \in \mathbb{R}$.

$L(f)$ - число перемен знака в последовательности $a_n, a_{n-1}, ..., a_1, a_0$

$N(f)$ - число положительных вещественных корней многочлена f

Тогда число $N(f) \leq L(f)$. При этом $N(f) = L(f) \Longleftrightarrow$ нет мнимых корней.

Удалю Копатыча, когда сдам досрок, а пока он посидит тут, на удачу: