Лекция #1
Матрицы и системы линейных алгебраических уравнений (СЛАУ)

Матрицей называют совокупность элементов, расположенных в виде таблицы из m строк и n столбцов.
Обозначение:

$$A = \begin{pmatrix} a_{11} & . & . & a_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & . & . & a_{mn} \end{pmatrix}$$

a_{ij} – элемент матрицы
$[A]_{ij} = a_{ij}$
Числа m и n называют **размерами** матрицы. *(другие названия: тип, порядок)*
Множество всех матриц размера $m \times n$ обозначаем $M_{mn}(\mathbb{R})$

Частные случаи:
1. $m = n$ — квадратные матрицы
2. $n = 1$ (т.е. $m \times 1$) — m-мерный столбец
3. $m = 1$ (т.е. $1 \times n$) — n-мерная строка
4. $\forall i, j.\ [A]_{ij} = 0$ —нулевая матрица

Операции над матрицами:
Две матрицы A и B называются **равными**, если они одинакового размера и соответствующие элементы равны, т.е. $a_{ij} = b_{ij}$

Матрица C называется **суммой** матриц A и B, если все три матрицы одинаковых размеров и $[C]_{ij} = [A]_{ij} + [B]_{ij}$, $(i = 1..m\ , j = 1..n)$
Обозначение: $\boldsymbol{C = A + B}$

Свойства сложения матриц:
1. Коммутативность: $\boldsymbol{A + B = B + A}$
2. Ассоциативность: $\boldsymbol{(A + B) + C = A + (B + C)}$
3. $\exists$ нейтральный элемент по сложению матриц $\theta \in M_{mn}(\mathbb{R})$:
   $\forall$ матрицы $A \in M_{mn}(\mathbb{R})$: $\boldsymbol{A + \theta = A = \theta + A}$
   θ - Нулевая матрица.
4. $\forall$ матрицы $A \in M_{mn}(\mathbb{R})$ $\exists$ единственное $B \in M_{mn}(\mathbb{R})$: $\boldsymbol{A + B = \theta}$,
   т.е. $\forall$ матрицы $\exists$ обратная по сложению – *противоположная матрица*.
   Обозначение: **-A** (т.е. $b_{ij} = -a_{ij}$)

Разностью матриц A и B называется сумма A и -B

Транспонированием матрицы называется операция, переводящая все строки матрицы в столбцы с сохранением порядка.
Обозначение: A^T
Матрица типа $m \times n$ при транспонировании переходит в матрицу типа $n \times m$.
$[A]_{ij} = [A^T]_{ji}$

Пример:

$$(1 \quad 2 \quad 3)^T_{1\times3} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}_{3\times1}$$

Умножение матриц:

Рассмотрим матрицу А типа $m \times n$ с элементами a_{ij} $(i = 1..m, j = 1..n)$ и матрицу B типа $n \times p$ с элементами b_{ke} $(k = 1..n, e = 1..p)$

Произведением А и В называют матрицу С типа $m \times p$ с элементами $c_{ij} = \sum_{r=1}^{n} a_{ir} b_{rj}$

$$\begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ a_{i1} & \cdot & \cdot & a_{ip} \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} \cdot \begin{pmatrix} \cdot & \cdot & b_{1j} & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & b_{pj} & \cdot \end{pmatrix} = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & c_{ij} & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

Умножение матриц **не коммутативно:**
В общем случае $A \cdot B \neq B \cdot A$

Свойства умножения:

1. Ассоциативность: $(A \cdot B) \cdot C = A \cdot (B \cdot C)$

   Док-во:

   Пусть А, В, С — матрицы типов $m \times n$, $n \times k$, $k \times e$

   $(A \cdot B) \cdot C = A \cdot (B \cdot C)$

   $$[(A \cdot B) \cdot C]_{ij} = \sum_{r=1}^{k} [AB]_{ir} \cdot [C]_{rj} = \sum_{r=1}^{k} (\sum_{s=1}^{n} [A]_{is} \cdot [B]_{sr}) \cdot [C]_{rj} =$$
   $$= \sum_{r=1}^{k} \sum_{s=1}^{n} [A]_{is} \cdot [B]_{sr} \cdot [C]_{rj} = \sum_{s=1}^{n} [A]_{is} \cdot (\sum_{r=1}^{k} [B]_{sr} \cdot [C]_{rj}) =$$
   $$= \sum_{s=1}^{n} [A]_{is} \cdot ([BC]_{sj}) = [A \cdot (B \cdot C)]_{ij}$$

2. Дистрибутивность относительно сложения: $(A + B) \cdot C = A \cdot C + B \cdot C$
3. $\exists$ нейтральный элемент $E \in M_n(\mathbb{R})$: $A \cdot E = A = E \cdot A$

   Док-во:

   $A \cdot E = A = E \cdot A$

   $$[A \cdot E]_{ij} = \sum_{r=1}^{n} [A]_{ir} \cdot [E]_{rj} = [A]_{ij} \cdot [E]_{jj} = [A]_{ij}$$

4. $\forall$ матрицы $A \in M_{mn}(\mathbb{R})$: $A \cdot \theta = \theta$
5. $(A \cdot B)^T = B^T \cdot A^T$

   Док-во:

   $(A \cdot B)^T = B^T \cdot A^T$

   $$[(A \cdot B)^T]_{ij} = [A \cdot B]_{ji} = \sum_{r=1}^{n} [A]_{jr} \cdot [B]_{ri} = \sum_{r=1}^{n} [A^T]_{rj} \cdot [B^T]_{ir} = \sum_{r=1}^{n} [B^T]_{ir} \cdot [A^T]_{rj} = [B^T \cdot A^T]_{ij}$$

Лекция #2
<u>Элементарные преобразования. Метод Гаусса.</u>

Элементарными преобразованиями строк матрицы называют следующие операции:

1. Умножение *(i)*-ой строки матрицы $(\lambda) \neq 0$
   $(i) \longmapsto \lambda(i)$
2. Перестановка двух строк местами
   $(i) \leftrightarrow (j)$
3. Добавление к *(i)*-й строке матрицы ее *(k)*-й строки с коэффициаентом
   $(i) \to (i) + \lambda(k)$

<u>Матрица имеет:</u>
Ступенчатый вид, если номера первых *ненулевых* элементов всех строк (такие элементы называются ведущими) возрастают, а нулевые строки стоят *внизу*

Канонический вид, если матрица имеет *ступенчатый* вид, все ведущие элементы равны 1 и в любом столбце с ведущим элементом выше и ниже его стоят только нули

<u>Теорема О методе Гаусса:</u>
Любую конечную матрицу A можно привести элементарными преобразованиями к ступенчатому (каноническому) виду

<u>Док-во:</u>
Предъявим алгоритм.
Движемся из левого верхнего угла матрицы
Элемент в левом верхнем углу - ткущий

1. Если текущий элемент $= 0$, переходим к шагу *(2)*
   Если он $\neq 0$, то текущий элемент объявляется ведущим.
   Теперь прибавляем ведущую к остальным так, чтобы все элементы, расположенные ниже и выше обратились в 0.
   Если ведущий элемент $[A]_{ij}$, то для (k)-ой строки $(k \neq i)$ берём число:
   $\lambda = -[A]_{ki}/[A]_{ij}$ Делим ведущую строку на $[A]_{ij}$
   Выбираем новый текущий элемент, смещаясь в матрице на 1 столбец вправо на 1 строку вниз и переходим к следующему шагу, повторяя *(1)*.
   Если это невозможно, то STOP.

2. Если текущий элемент $= 0$, то просматриваем все элементы под ним.
   Если среди них нет $\neq 0$, то переходим к *(3)*.
   Если в k-ой строке есть элемент $\neq 0$, то меняем местами текущую строку и k-ую и переходим к *(1)*

3. Если текущий элемент и все под ним $= 0$, то меняем текущий столбец, смещаясь на 1 вправо и переходим к *(1)*, если это невозможно, то STOP

Так как матрица конечна, а за 1 итерацию алгоритма положение текущего элемента смещается вправо на 1 столбец, то процесс преобразований закончится не более, чем за *n* шагов.

Зам. Каждое элементарное преобразование имеет обратное элементарное преобразование

Зам. Каждое элементарное преобразование строк матрицы A можно трактовать как умножение A слева на матрицу специального вида. Эта матрица получается, если сделать такие же преобразования с единичной матрицей соответствующего размера

Лекция #3
Система линейных алгебраических уравнений

СЛАУ называется:

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m \end{cases}$$

↑ *(3.1) Координатная форма записи СЛАУ*

$A = \begin{pmatrix} a_{11} & \cdot & \cdot & a_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & \cdot & \cdot & a_{mn} \end{pmatrix}$ — Матрица системы; $\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ — столбец правых частей

$A \cdot x = b$, где

↑ *Матричная форма записи СЛАУ*

$$\begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} \cdot x_1 + \ldots + \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix} \cdot x_n = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \quad \leftrightarrow \quad x_1 \cdot A_1 + \ldots + x_n \cdot A_N = b$$

↑ *(3.2) Векторная форма записи СЛАУ*

СЛАУ называется **совместной**, если у нее существует хотя бы одно решение
Если $b = 0$, то СЛАУ называется **однородной**

Метод Гаусса для СЛАУ

$(A\,|\,b) \rightsquigarrow$

$$\rightsquigarrow \begin{array}{cc} & \overbrace{\qquad\qquad\quad}^{r} \\ r\left\{\begin{array}{c} \\ \\ \\ \end{array}\right. & \left(\begin{array}{cccc|ccc|c} 1 & \cdot & \cdot & 0 & \widetilde{a}_{1\,r+1} & \cdot & \widetilde{a}_{1n} & \widetilde{b}_1 \\ \vdots & \ddots & & \vdots & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & 1 & \widetilde{a}_{r\,r+1} & \cdot & \widetilde{a}_{rn} & \widetilde{b}_r \\ \hline 0 & \cdot & \cdot & 0 & 0 & \cdot & 0 & \widetilde{b}_{r+1} \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \end{array}\right) \end{array}$$

Если $\widetilde{b}_{r+1} \neq 0$, то СЛАУ **несовместна**

Если $\widetilde{b}_{r+1} = 0$, то перепишем СЛАУ:

$$\begin{cases} x_1 + \sum_{j\,=\,1+r}^{n} \widetilde{a}_{1j}x_j = \widetilde{b}_1 \\ \vdots \\ x_r + \sum_{j\,=\,1+r}^{n} \widetilde{a}_{rj}x_j = \widetilde{b}_r \end{cases}$$

$$\begin{cases} x_1 = \widetilde{b}_1 - \sum_{j\,=\,1+r}^{n} \widetilde{a}_{1j}x_j \\ \vdots \\ x_r = \widetilde{b}_r - \sum_{j\,=\,1+r}^{n} \widetilde{a}_{rj}x_j \end{cases} \qquad \textbf{(3.2)}$$

Переменные $x_1, \,..\,, x_r$ называются **главными**, они единственным образом вычисляются по формуле *3.2* при любом заданном наборе $x_{r+1}, \,..\,, x_n$ (**свободных** переменных)

Произвольный набор $X = (x_1, \,..\,, x_n)^T$, удовлетворяющий исходной СЛАУ, вычисляется в виде:

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_r \\ x_{r+1} \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \widetilde{b}_1 - \sum_{j\,=\,1+r}^{n} \widetilde{a}_{1j}x_j \\ \vdots \\ \widetilde{b}_r - \sum_{j\,=\,1+r}^{n} \widetilde{a}_{rj}x_j \\ x_{r+1} \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \widetilde{b}_1 \\ \vdots \\ \widetilde{b}_r \\ 0 \\ \vdots \\ 0 \end{pmatrix} + x_{r+1} \begin{pmatrix} \phi_{11} \\ \vdots \\ \phi_{r1} \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \,..\, + x_n \begin{pmatrix} \phi_{1\;n-r} \\ \vdots \\ \phi_{r\;n-r} \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

где $\begin{pmatrix} \widetilde{b}_1 & .. & \widetilde{b}_r & 0 & .. & 0 \end{pmatrix}^T$ — частные решения СЛАУ

<u>Определители</u>

Любое расположение чисел $1, \, \dots, \, n$ в определенном порядке называют **перестановкой** $\alpha = (\alpha_1, \dots, \alpha_n)$

Пример:
$\alpha = (3, \, 1, \, 2, \, 4)$

α_i и α_j образуют **инверсию**, если $\alpha_j > \alpha_i$ и $i > j$
Знак перестановки $\operatorname{sgn} \alpha = (-1)^n$, *где n — количество инверсий*

Транспозиция — преобразование, при котором α меняются α_i и α_j **,** $i \neq j$, а остальные не меняются
Зам. Любая транспозиция меняет четность

Подстановка — биекция множества $1, \,..\,, n$ в себя

$$\sigma = \begin{pmatrix} 1 & . & . & n \\ \sigma(1) & . & . & \sigma(n) \end{pmatrix}$$

Биекция — взаимно однозначное отображение

$f : X \to Y$

1. Сюръекция: $\forall y \in Y \; \exists x \in X : y = f(x)$
2. Инъекция: $\forall x_1, x_2 \in X, x_1 \neq x_2 : f(x_1) \neq f(x_2)$

Зам. На множестве всех постановок для n можно ввести операцию умножения композицию $|S_n| = n!$

Определителем порядка n, соответствующим квадратной матрице *A*, называют сумму из $n!$ слагаемых:

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot a_{1\;\sigma(1)} \cdot \ldots \cdot a_{n\;\sigma(n)}$$

Лекция #4

<u>Свойства определителей</u>

Зам. Все свойства для строк справедливы для столбцов

1. $\det A^T = \det A$
2. Определитель *линеен* по столбцам, то есть
   A. $\det(A_1, .., A_{i-1}, A_i' + A_i'', .., A_n) = \det(A_1, .., A_{i-1}, A_i', .., A_n) + \det(A_1, .., A_{i-1}, A_i'', .., A_n)$
   B. $\det(A_1, .., \alpha A_i, .., A_n) = \alpha \cdot \det(A_1, .., A_i, .., A_n)$
3. При перестановке строк определитель *меняет* знак
   Т.е. Определитель — *кососимметрическая функция*

   <u>*Док-во:*</u>
   Если произведение $a_{1\alpha_1}, a_{2\alpha_2}, \ .. \ , a_{i\alpha_i}, \ .. \ , a_{j\alpha_j}, \ .. \ , \ a_{n\alpha_n}$ участвует в первом определителе, то он участвует и во втором

$$\Delta_1 = \begin{vmatrix} \alpha_{11} & . & . & \alpha_{1m} \\ . & . & . & . \\ \alpha_{i1} & . & . & \alpha_{im} \\ . & . & . & . \\ \alpha_{j1} & . & . & \alpha_{jm} \\ . & . & . & . \\ \alpha_{n1} & . & . & \alpha_{nm} \end{vmatrix}, \Delta_2 = \begin{vmatrix} \alpha_{11} & . & . & \alpha_{1m} \\ . & . & . & . \\ \alpha_{j1} & . & . & \alpha_{jm} \\ . & . & . & . \\ \alpha_{i1} & . & . & \alpha_{im} \\ . & . & . & . \\ \alpha_{n1} & . & . & \alpha_{nm} \end{vmatrix}$$

   Т.е. Если сомножители стояли в разных строках и разных стольбцах в Δ_1, то они обладают этим же свойством в Δ_2
   Знак в Δ_1 определяется:
   $\sigma = \begin{pmatrix} 1 & . & i & . & j & . & n \\ \alpha_1 & . & \alpha_i & . & \alpha_j & . & \alpha_n \end{pmatrix}$

   А в Δ_2:

   $\tau = \begin{pmatrix} 1 & . & j & . & i & . & n \\ \alpha_1 & . & \alpha_j & . & \alpha_i & . & \alpha_n \end{pmatrix}$
   $\Rightarrow \operatorname{sgn} \sigma = -\operatorname{sgn} \tau$
   #

4. $\det A = 0$, если
   A. В матрице есть *нулевая* строка
   B. В матрице есть две *одинаковые* строки
5. $\det A = 0$, если одна из строк является *линейной комбинацией* остальных строк

   <u>*Док-во:*</u>
   $\det(A_1, .., \sum_{i=1 \ i\neq j}^{n} \alpha_i A_i, .., A_n) = \sum_{i=1 \ i\neq j}^{n} \alpha_i \cdot \det(A_1, .., A_i, .., A_n) = 0$
   (по свойству 4б)

6. Определитель не меняется, если к любой строке прибавить *линейную комбинацию* остальных

   <u>*Док-во:*</u>
   $\det(A_1, .., A_{j-1}, A_j + \sum_{i=1 \ i\neq j}^{n} \alpha_i A_i \ , \ A_{j+1}, .. , \ A_n) = \det(A_1, .., A_{j-1}, A_j, \ A_{j+1}, .. , \ A_n) +$

   $+ \det(A_1, .., A_{j-1}, \sum_{i=1 \ i\neq j}^{n} \alpha_i A_i \ , \ A_{j+1}, .. , \ A_n) = \det A$
   #

7. $\det E_n = 1$
   Если f — линейная функция столбцов матрицы, то свойства *(3)* и *(4B)* эквивалентны

   Док-во:
   $f(A_1, A_2)$ — функция от столбов и она обладает свойствами *(4B)* и *(2)*
   $0 = f(A_1 + A_2, A_1 + A_2) = f(A_1, A_1 + A_2) + f(A_2, A_1 + A_2) =$
   $= f(A_1, A_1) + f(A_1, A_2) + f(A_2, A_1) + f(A_2, A_2) = f(A_1, A_2) + f(A_2, A_1)$
   $\Rightarrow f(A_1, A_2) = -f(A_2, A_1)$
   #

Утв. Любая функция, удовлетворяющая свойствам *(2), (4B), (7)* является определителем. То есть любая *полилинейная кососимметрическая функция* от столбцов матрицы, равная 1 для E, является **определителем**

Док-во:
Пусть f — такая функция, $n = 2$

$$f\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = f\left(a_{11}\begin{pmatrix}1\\0\end{pmatrix} + a_{21}\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}a_{12}\\a_{22}\end{pmatrix}\right) = a_{11}\cdot f\begin{pmatrix} 1 & a_{12} \\ 0 & a_{22} \end{pmatrix} + a_{21}\cdot f\begin{pmatrix} 0 & a_{12} \\ 1 & a_{22} \end{pmatrix} =$$

$$= a_{11}\cdot f\left(\begin{pmatrix}1\\0\end{pmatrix}, a_{12}\begin{pmatrix}1\\0\end{pmatrix} + a_{22}\begin{pmatrix}0\\1\end{pmatrix}\right) + a_{21}\cdot f\left(\begin{pmatrix}0\\1\end{pmatrix}, a_{12}\begin{pmatrix}1\\0\end{pmatrix} + a_{22}\begin{pmatrix}0\\1\end{pmatrix}\right) =$$

$$= a_{11}a_{12}\cdot f\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + a_{11}a_{22}\cdot f\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + a_{21}a_{12}\cdot f\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + a_{21}a_{22}\cdot f\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} =$$

$$= a_{11}a_{22}\cdot f\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + a_{11}a_{22}\cdot f\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = (a_{11}a_{22} - a_{11}a_{22})\cdot f(E_2) = \det A$$

#

В матрице A_n вычеркнем i-ю строку и j-й столбец. Определитель получившейся матрицы называется **дополнительным минором** элемента a_{ij}

Обозначение: M_{ij}

Алгебраическим дополнением элемента a_{ij} называется число $A_{ij} = (-1)^{i+j}M_{ij}$

8. Разложения определителя по строке или столбцу:
   $\det A = \sum_{j=1}^{n} a_{ij}A_{ij} = \sum_{i=1}^{n} a_{ij}A_{ij}$ — теорема Лапласа
9. Фальшивое разложение
   $$\sum_{j=1}^{n} a_{ij}A_{kj} = 0$$
   $$\sum_{i=1}^{n} a_{ij}A_{ik} = 0$$

10. $\begin{vmatrix} a_{11} & a_{12} & . & a_{1n} \\ 0 & a_{22} & . & . \\ . & . & . & . \\ 0 & . & . & a_{nn} \end{vmatrix} = a_{11}\cdot a_{22}\cdot \ldots \cdot a_{nn}$

11. $\det\left(\begin{array}{c|c} A & * \\ \hline 0 & B \end{array}\right) = [\text{A и B — квадратные}] = \det A \cdot \det B$

12. $\forall\ A, B \in M_n(\mathbb{R}) : \det(A \cdot B) = \det A \cdot \det B$

Док-во:

Рассмотрим $f(B) = \det(A \cdot B)$

Покажем, что $f(B)$ выполняются свойства *(2)* и *(4B)*, то есть она *линейна* и *кососимметрична.*

1. Если столбцы i и j одинаковы в матрице B, то и в матрице $A \cdot B$ они тоже одинаковы $\rightarrow$ выполняется свойство *(4B)*
2. Если в матрице B i-ый столбец имеет вид $\lambda a + b$, то в $A \cdot B$ он имеет вид $\lambda Aa + Ab$ $\rightarrow$ выполняется свойство (2)

$\Rightarrow\ f(B) = \det B \cdot f(E_n)$, но $f(E_n) = \det(A \cdot E) = \det\ A \Rightarrow f(B) = \det B \cdot \det A$

#

Лекция #5

<u>Правило Крамера</u>

Утв. Пусть $Ax = b$ — совместная СЛАУ с квадратной матрицей
Тогда $x_i = \det(A_1, \ldots, A_{i-1}, b, A_{i+1}, \ldots A_n)$

Зам. Если $\det A \neq 0 \Rightarrow x = \dfrac{\Delta_i}{\det A}$ — Формулы Крамера

<u>Док-во:</u>

$Ax = b \Leftrightarrow x_1A_1 + \ldots + x_nA_n = b$, где A_k — столбец матрицы A

$$\Delta_i = \det(A_1, \ldots, A_{i-1}, b, A_{i+1}, \ldots A_n) = \det(A_1, \ldots, A_{i-1}, \sum_{j=1}^{n} x_jA_j, A_{i+1}, \ldots A_n) =$$

$$= \sum_{j=1}^{n} x_j \cdot \det(A_1, \ldots, A_{i-1}, A_j, A_{i+1}, \ldots A_n) = x_i \cdot \det A$$

#

Зам. Пусть $a_1 = \begin{pmatrix} a_{11} \\ a_{12} \end{pmatrix}, a_2 = \begin{pmatrix} a_{21} \\ a_{22} \end{pmatrix}$ — в прямоугольной декартовой системе координат (ПДСК)

Площадь параллелограмма на a_1, a_2

$$S = \left| \det \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix} \right|$$

<u>Обратная матрица</u>

Обратной матрицей к матрице $A \in M_n(\mathbb{R})$ называется матрица A_n^{-1}, такая что: $AA^{-1} = A^{-1}A = E$

Зам. Обратная матрица существует не всегда (например, для нулевой не существует)

Теор. **<u>Критерий существования обратной матрицы</u>**

Для $A \in M_n(\mathbb{R})\, \exists A^{-1} \Leftrightarrow \det A \neq 0$ (то есть A является невырожденной)

<u>Док-во:</u>

«→» Необходимость:

Дано: $\exists A^{-1}$

Доказать: $\det A \neq 0$

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

$\det(A \cdot A^{-1}) = \det A \cdot \det A^{-1} = 1$

$\Rightarrow \det A \neq 0$

«←» Достаточночность:

Дано: $\det A \neq 0$

Доказать: $\exists A^{-1}$

$A^{-1} = \dfrac{1}{detA} \cdot \widetilde{A}$, где $\widetilde{A}$ — союзная матрица

$\widetilde{A} = \begin{pmatrix} A_{11} & . & . & A_{1n} \\ \vdots & & & \vdots \\ A_{n1} & . & . & A_{nn} \end{pmatrix}^T$, где A_{ij} — алгебраическое дополнение к a_{ij}

$$A\frac{1}{\det A}\widetilde{A} = \frac{1}{\det A}\begin{pmatrix} a_{11} & . & . & a_{1n} \\ \vdots & & & \vdots \\ a_{n1} & . & . & a_{nn} \end{pmatrix}\begin{pmatrix} A_{11} & . & . & A_{1n} \\ \vdots & & & \vdots \\ A_{n1} & . & . & A_{nn} \end{pmatrix}^T = \begin{pmatrix} \det A & . & . & 0 \\ . & \det A & & . \\ . & . & . & . \\ 0 & . & . & \det A \end{pmatrix}\frac{1}{\det A} = E_n$$

#

Зам. $\det A^{-1} = \dfrac{1}{\det A}$, если A^{-1} существует

Зам. Если обратная матрица существует, то она единственна.

Док-во:
Пусть B и B' — обратные к A, тогда
$B = BE = B(AB') = (BA)B' = EB' = B'$
#

Зам. $(AB)^{-1} = B^{-1}A^{-1}$, если все матрицы существуют

Док-во:
$(AB)(A^{-1}B^{-1}) = A(BB^{-1})A^{-1} = AEA^{-1} = AA^{-1} = E$
$(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}EB = B^{-1}B = E$
$\Rightarrow (AB)^{-1} = B^{-1}A^{-1}$
#

Зам. $(A^T)^{-1} = (A^{-1})^T$

Решение простейших матричных уравнений

1. $A \cdot X = B$, где A — квадратная невырожденная матрица
   $A^{-1}A \cdot X = A^{-1}B \to X = A^{-1}B$
2. $X \cdot A = B$
   $X \cdot A^{-1}A = BA^{-1} \to X = BA^{-1}$

Зам. $(x \cdot A)^T = B^T$

Вычисление обратной матрицы с помощью элементарных преобразований:
$Ax = b \Rightarrow (A\,|\,b) \rightsquigarrow (E\,|\,x)$
$A \Rightarrow (A\,|\,E) \rightsquigarrow (E\,|\,A^{-1})$

Ранг матрицы

Минором порядка k в матрице $A_{m\times n}$ называется *определитель* матрицы, составленной из элементов, стоящих на пересечении *фиксированных* k строк и k столбцов.
Обозначение: $M^{j_1..j_k}_{i_1..i_k}$

Рангом матрицы $A_{m\times n}$ называется *порядок* наибольшего *отличного от нуля* минора.
Обозначение: $\mathrm{Rg}\,A$

Зам. Определение означает, что в матрице существует минор порядка $r = \mathrm{Rg}\,A$, отличный от нуля, а все миноры больших порядков либо равны 0, либо не существуют.

Лекция #6

Линейная зависимость

Линейной комбинацией строк (столбцов) $a_1, .., a_k$ *одинаковой длины* называют выражение вида $\lambda_1 a_1 + .. + \lambda_k a_k$, где $\lambda_1, .., \lambda_k$ — некоторые числа

Строки $a_1, .., a_k$ называются **линейно-зависимыми** (л.з.), если существуют числа $\lambda_1, .., \lambda_k$, *не все равные нулю*, такие что: $\lambda_1 a_1 + .. + \lambda_k a_k = 0$, то есть существует *нетривиальная* линейная комбинация, равная нулю

Строки $a_1, .., a_k$ называются **линейно-независимыми** (л.н.з.), если из равенства $\lambda_1 a_1 + .. + \lambda_k a_k = 0$ следует, что все $\lambda_i = 0,\ i = \overline{1,k}$

Критерий линейной зависимости

Строки $a_1, .., a_k$ являются л.з. $\Leftrightarrow$ существует одна строка, которая является *линейной комбинацией* остальных

Док-во:

«→» *Необходимость:*

Дано: $a_1, .., a_k$ — *л.з.*

Док-ть: хотя бы одна из них является л.к. остальных

Существуют числа $\alpha_1, .., \alpha_k$ не все равные нулю, такие что $\alpha_1 a_1 + .. + \alpha_k a_k = 0$

Пусть $\alpha_1 \neq 0$, тогда $a_1 = -\dfrac{\alpha_2}{\alpha_1} a_2 + .. + \dfrac{\alpha_k}{\alpha_1} a_k = 0$

— это и есть линейная комбинация остальных

«←» *Достаточность:*

Дано: одна из строк — л.к. остальных

Док-ть: $a_1, .., a_k$ — *л.з.*

Пусть $a_1 = \beta_2 a_2 + .. + \beta_k a_k$, тогда

$1 \cdot a_1 - \beta_2 a_2 - .. - \beta_k a_k = 0$ — это нетривиальная л.к., так как $1 \neq 0$

#

Любой отличный от нуля минор, порядок которого равен рангу матрицы, называют **базисным минором** матрицы.

Строки (столбцы), попавшие в базисный минор, называются **базисными**.

Свойства ранга

1. $\operatorname{Rg} A^T = \operatorname{Rg} A$
2. Элементарные преобразования строк не меняют ранга.

Док-во:

Покажем, что $\operatorname{Rg} A^T \geqslant \operatorname{Rg} A$

Если это верно, то $\operatorname{Rg} A \leqslant \operatorname{Rg} A^T \leqslant \operatorname{Rg} (A^T)^T = \operatorname{Rg} A \Rightarrow \operatorname{Rg} A = \operatorname{Rg} A^T$

Пусть $\operatorname{Rg} A = r \Rightarrow \exists$ минор $M^{j_1,\dots,j_r}_{i_1,\dots,i_r} \neq 0$

В матрице A^T есть минор $N^{i_1,\dots,i_r}_{j_1,\dots,j_r} \neq 0$, получающийся из M транспонированием

$\Rightarrow N \neq 0 \Rightarrow \operatorname{Rg} A^T \geqslant r = \operatorname{Rg} A$

Теорема о базисном миноре

1. Базисные строки (столбцы), соответствующие любому базисному минору *л.н.з.*
2. Строки (столбцы) матрицы A, не входящие в базисный минор M, являются *линейными комбинациями базисных.*

Док-во:

1. Предположим, что они л.з.
   По критериям линейной зависимости найдется строка, которая является линейной комбинацией остальных
   $\Rightarrow$ по *(5)* свойству определителя $M = 0$ — противоречие
2. Будем считать, что базисный минор M расположен в левом верхнем углу

$$A = \left(\begin{array}{cccc|ccc} & & & & a_{1\,r+1} & \cdot & a_{1n} \\ r\Big\{ & \multicolumn{3}{c|}{\overbrace{\qquad M \qquad}^{r}} & \vdots & & \vdots \\ & & & & a_{r\,r+1} & \cdot & a_{rn} \\ \hline a_{r+1\,1} & \cdot & \cdot & \cdot & \cdot & \cdot & a_{r+1\,n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{m1} & \cdot & \cdot & \cdot & \cdot & \cdot & a_{mn} \end{array}\right)$$

Возьмем и покажем, что существует $\lambda_1, \ .., \lambda_k$ такие что:
$A_k = \lambda_1 A_1 + .. + \lambda_r A_r$, где $A_1, .., A_r$ — базисные строки

Составим определитель:

$$\Delta = \begin{vmatrix} a_{11} & \cdot & \cdot & a_{1r} & a_{1j} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{r1} & \cdot & \cdot & a_{rr} & a_{rj} \\ a_{k1} & \cdot & \cdot & a_{kr} & a_{kj} \end{vmatrix}$$

Столбец j выбираем произвольно.

Покажем, что $\Delta = 0$:
Если $j \leqslant r$, то в Δ есть два одинаковых столбца $\Rightarrow$ по *(4B)* $\Delta = 0$
Если $j > r$, то Δ — это минор порядка $r + 1$ в исходной матрице А $\Rightarrow \Delta = 0$

Разложим Δ по последнему столбцу:
$a_{1j}B_1 + .. + a_{rj}B_r + a_{kj}B_k = 0$,
где B_i — алгебраические дополнения в Δ для элементов последнего столбца.
$B_k = M \neq 0$, так как это базисный минор
$a_{kj} = -\dfrac{B_1}{M}a_{1j} - .. - \dfrac{B_r}{M}a_{rj} = \lambda_1 a_{1j} + .. + \lambda_r a_{rj}$, где $j = 1..n$ и $k = r + 1..m$

$(a_{k1} \cdot\cdot \quad a_{kn}) = \lambda_1 (a_{11} \cdot\cdot \quad a_{1n}) + .. + \lambda_r (a_{r1} \cdot\cdot \quad a_{rn})$, где $(a_{k1} \cdot\cdot \quad a_{kn})$ — k-тая строка

— это и есть нужное равенство для строк
#

<u>Следствие 1.</u>
<u>Теорема о ранге матрицы</u>
Ранг матрицы равен *максимальному* числу ее л.н.з. сток (столбцов)

<u>Док-во:</u>
Пусть $\operatorname{Rg} A = r$, а максимальное число л.н.з. строк — k
Покажем, что $k = r$
1. Так как в А есть r л.н.з. строк (по т. О базисном миноре все базисные строки л.н.з.) $\Rightarrow k \geqslant r$
2. Вычеркнем в A все строки, кроме k л.н.з.
   Получим матрицу A_1, в ней k строк.

   При этом $\operatorname{Rg} A_1 = k$, так как если бы $\operatorname{Rg} A_1$ был бы < k, то среди строк как минимум одна выражалась бы через другие по т. О базисном миноре и они были бы л.з. по критерию линейной зависимости.

   В матрице A_1 возьмем базисный минор порядка k
   Базисный минор A_1 имеет порядок k и является отличным от нуля минором в исходной матрице А $\Rightarrow \operatorname{Rg} A = r \geqslant k \Rightarrow k = r$

#

<u>Следствие 2.</u>
Теор. <u>Критерий невырожденности квадратной матрицы</u>
Рассмотрим матрицу $A_n \in M_n(\mathbb{R})$
Следующие условия эквивалентны:
1. $\det A \neq 0$
2. $\operatorname{Rg} A = n$
3. Все строки A л.н.з.

<u>Док-во:</u>
$(1 \to 2)$
Если $\det A \neq 0$, то в матрице есть минор порядка n, $\neq 0 \Rightarrow$ по определению $\operatorname{Rg} A = n$
$(2 \to 3)$
Пусть $\operatorname{Rg} A = n \Rightarrow$ все строки базисные $\rightarrow$ по теореме они все л.н.з.
$(3 \to 1)$
Пусть все строки л.н.з.
Предположим, что $\det A = 0 \Rightarrow \operatorname{Rg} A < n \Rightarrow$ по крайней мере одна строка линейно выражается через другие $\Rightarrow$ по критерию линейной зависимости они линейно зависимы — противоречие
#

Вычисление ранга матрицы

Минор N называется **окаймляющим** для минора M матрицы A, если N получается добавлением к M одной новой строки и одного нового столбца из матрицы A.

Утв.

1. Пусть в матрице $A \in M_{mn}(\mathbb{R})$ существует минор порядка r, отличный от нуля
2. Все миноры, его окаймляющие, равны нулю $\Rightarrow \operatorname{Rg} A = r$

Док-во:

Пусть M (базисный минор) расположен в левом верхнем углу матрицы
Тогда по т. О базисном миноре строки, не вошедшие в базисный минор, линейно выражаются через базисные:

$A_{r+1} = \lambda_1 A_1 + .. + \lambda_r A_r$
...
$A_m = \alpha_1 A_1 + .. + \alpha_r A_r$

Сделаем следующие элементарные преобразования:
(обнулим все строки, кроме базисных)

$A_{r+1} - \lambda_1 A_1 - .. - \lambda_r A_r \rightsquigarrow A_{r+1}$
...
$A_m - \alpha_1 A_1 - .. - \alpha_r A_r \rightsquigarrow A_m$

Получится матрица:

$$A_1 = \left(\begin{array}{cccc|ccc} & & & & a_{1\ r+1} & \cdot & a_{1n} \\ & M & & & \vdots & & \vdots \\ & & & & a_{r\ r+1} & \cdot & a_{rn} \\ \hline 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \end{array}\right)$$

Так как ранг не меняется при элементарных преобразованиях $\operatorname{Rg} A = \operatorname{Rg} A_1$
А $\operatorname{Rg} A_1 = r$, так как в A_1 все миноры порядка $r+1$ равны нулю (они содержат нулевую строку)
#

Свойства решений СЛАУ:

1. Пусть $x^1, .., x^s$ — решения однородной СЛАУ $Ax = 0$
   Тогда для любых $\lambda_1, .., \lambda_s$:
   $\lambda_1 x^1 + .. + \lambda_s x^s$ тоже является решением однородной СЛАУ $Ax = 0$

   Док-во:
   $A(\lambda_1 x^1 + .. + \lambda_s x^s) = \lambda_1\ A\ x^1 + .. + \lambda_s\ A\ x^s = 0 + .. + 0 = 0$
   #

2. Пусть x^1 — решение СЛАУ $Ax = b$, а x^2 — решение СЛАУ $Ax = 0$ (с той же матрицей)
   Тогда $x^1 + x^2$ — решения СЛАУ $Ax = b$

   Док-во:
   $A(x^1 + x^2) = Ax^1 + Ax^2 = b + 0 = b$
   #

3. Если x^1 и x^2 — решения неоднородной СЛАУ $Ax = b$, то $x^1 - x^2$ — решения однородной СЛАУ $Ax = 0$

   Док-во:
   $A(x^1 - x^2) = Ax^1 - Ax^2 = b - b = 0$
   #

Критерий совместности СЛАУ

Рассмотрим неоднородную СЛАУ $Ax = b$, где $A \in M_{mn}(\mathbb{R})$
Матрицу $(A\,|\,b)_{m\ n+1}$ называют **расширенной** матрицей системы

Теорема Кронекера-Капелли

СЛАУ $Ax = b$ совместна $\Leftrightarrow \operatorname{Rg} A = \operatorname{Rg}(A\,|\,b)$

Док-во:

«→» *Необходимость:*

Дано: $\exists$ *решение СЛАУ*
Док-ть: $\operatorname{Rg} A = \operatorname{Rg}(A\,|\,b)$
Если СЛАУ совместна, то существует решение x^0

То есть $\exists\ x^0 = \begin{pmatrix} x_1^0 \\ \vdots \\ x_n^0 \end{pmatrix}$ такое, что $x_1^0 A_1 + .. + x_n^0 A_n = b$, где A_j — столбцы м-цы A

$\Rightarrow \operatorname{Rg}(A\,|\,b)$ совпадает с $\operatorname{Rg} A$
Т.к. ранг равен максимальному числу л.н.з. столбцов, а для столбца b нашлось выражение через столбцы матрицы A

«←» *Достаточность:*

Дано: $\operatorname{Rg} A = \operatorname{Rg}(A\,|\,b)$
Док-ть: СЛАУ $Ax = b$ *совместна*
Пусть M — базисный минор матрицы A
Пусть он расположен в левом верхнем углу матрицы A
Тогда он является базисным минором для $(A\,|\,b)$, так как $Rg\ A = Rg\ (A\,|\,b)$
Тогда по т. О базисном миноре столбец b линейно выражается через столбцы

$A_1, .., A_r$: $b = \lambda_1 A_1 + .. + \lambda_r A_r$

Тогда $x^0 = \begin{pmatrix} \lambda_1 \\ \cdot \\ \lambda_r \\ 0 \\ \cdot \\ 0 \end{pmatrix}$ является решением СЛАУ $Ax = b$

#

Однородные СЛАУ

Рассмотрим СЛАУ $Ax = 0$, где $A \in M_{mn}(\mathbb{R})$
Любые

1. $k = n - r$ строк ($r = \operatorname{Rg} A$, n — число неизвестных)
2. л.н.з.
3. решений однородной СЛАУ

называются **фундаментальной системой решений** (ФСР) однородной СЛАУ

<u>Теорема о существовании ФСР</u>

Рассмотрим СЛАУ $Ax = 0$

У нее всегда существует $k = n - r$ л.н.з. решений ($r = \operatorname{Rg} A$, n — число неизвестных)

<u>Док-во:</u>

Будем предполагать, что базисный минор расположен в левом верхнем углу

Сделаем элементарные преобразования:

(обнулим все строки, кроме базисных)

$A_{r+1} - \lambda_1 A_1 - .. - \lambda_r A_r \rightsquigarrow A_{r+1}$

...

$A_m - \alpha_1 A_1 - .. - \alpha_r A_r \rightsquigarrow A_m$

Тогда получим систему:

$$(*)\begin{cases} a_{11}x_1 + \ldots + a_{1r}x_r = -a_{1\ r+1}x_{r+1} - \ldots - a_{1n}x_n \\ \vdots \\ a_{r1}x_1 + \ldots + a_{rr}x_r = -a_{r\ r+1}x_{r+1} - \ldots - a_{rn}x_n \end{cases}$$

Здесь:

$x_1, .., x_r$ — базисные (главные) переменные

$x_{r+1}, .., x_n$ — свободные переменные

Придадим свободным переменным следующие наборы значений:

1-й набор	2-й набор	.	k-й набор
$x_{r+1} = 1$	$x_{r+1} = 0$	.	$x_{r+1} = 0$
$x_{r+2} = 0$	$x_{r+2} = 1$	.	$x_{r+2} = 0$
...	...	.	...
$x_{n-1} = 0$	$x_{n-1} = 0$	.	$x_{n-1} = 0$
$x_n = 0$	$x_n = 0$	.	$x_n = 1$

Для каждого набора решим СЛАУ (*)

Она всегда имеет $\exists!$ решение, так как ее определитель — это базисный минор $M \neq 0 \to \exists!$ решение по правилу Крамера

Получим следующие решения:

Для 1-го набора: $\begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = \begin{pmatrix} \phi_{11} \\ \vdots \\ \phi_{1r} \end{pmatrix}$, для 2-го: $\begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = \begin{pmatrix} \phi_{21} \\ \vdots \\ \phi_{2r} \end{pmatrix}$, ... , для k-го: $\begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = \begin{pmatrix} \phi_{k1} \\ \vdots \\ \phi_{kr} \end{pmatrix}$

$$\text{Тогда столбцы: } \Phi_1 = \begin{pmatrix} \phi_{11} \\ \vdots \\ \phi_{1r} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \end{matrix}}\right\} r \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} n-r \end{matrix}, .., \Phi_k = \begin{pmatrix} \phi_{k1} \\ \vdots \\ \phi_{kr} \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

$\Phi_1, .., \Phi_k$ — решения исходной однородной СЛАУ

Покажем, что они л.н.з.

Рассмотрим равенство:

$$\alpha_1 \begin{pmatrix} \phi_{11} \\ \vdots \\ \phi_{1r} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \,..\, + \alpha_k \begin{pmatrix} \phi_{k1} \\ \vdots \\ \phi_{kr} \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} * \\ \vdots \\ * \\ \alpha_1 \\ \vdots \\ \alpha_k \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} * \\ \vdots \\ * \end{matrix}}\right\} r \\ \left.\vphantom{\begin{matrix} \alpha_1 \\ \vdots \\ \alpha_k \end{matrix}}\right\} n-r \end{matrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$\Rightarrow \alpha_1 = \,..\, = \alpha_k = 0$, то есть $\Phi_1, \,..\,, \Phi_k$ л.н.з. по определению $\Rightarrow$ они образуют ФСР
#

Зам. ФСР, построенная в ходе доказательства, называется нормальной, так как в каждом столбце одна свободная переменная равна 1, а остальные равны 0

Следствие
Критерий существования ненулевых решений однородной квадратной СЛАУ
Однородная квадратная СЛАУ $Ax = 0$ имеет решение $\neq 0 \;\Leftrightarrow \det A = 0$

Лекция #7

Утв. Рассмотрим $A \in M_n(\mathbb{R})$. Однородная СЛАУ $Ax = 0$ имеет решения $x \neq 0 \Leftrightarrow \det A = 0$

Док-во:

«→» *Необходимость:*

Дано: СЛАУ $Ax = 0$ имеет решения $x \neq 0$

Док-ть: $\det A = 0$

Предположим, что $\det A \neq 0$, тогда по формулам Крамера $\exists!$ решение $x_i = \dfrac{\Delta_i}{\det A}$,

где $\Delta_i = 0 \to x_i = 0$ — противоречие

«←» *Достаточность:*

Дано: $\det A = 0$

Док-ть: $\exists\ x \neq 0$

$Ax = 0$ $\qquad \det A = 0 \Rightarrow \operatorname{Rg} A < n \Rightarrow k = n - \operatorname{Rg} A > 0$

Тогда по т. О существовании ФСР найдется k л.н.з. решений.

Они являются ненулевым

#

<u>Теорема о структуре общего решения однородной СЛАУ</u>

Пусть $\Phi_1, \ldots, \Phi_k$ — ФСР однородной СЛАУ $Ax = 0$. Тогда любое решение этой СЛАУ можно представить в виде $x = c_1\Phi_1 + \ldots + c_k\Phi_k$, где c_i — коэффициенты

Док-во:

Пусть $x^0 = \begin{pmatrix} x_1^0 \\ \vdots \\ x_n^0 \end{pmatrix}$ — произвольное решение однородной СЛАУ.

Предположим, что базисный минор расположен в левом верхнем углу матрицы A

Тогда можно выразить базисные переменные $(x_1 \ \cdots \ x_r)$ через свободные $(x_{r+1} \ \cdots \ x_n)$

(7.1) $\begin{cases} x_1 = -\alpha_{1\ r+1}x_{r+1} + \ldots + \alpha_{1n}x_n \\ \vdots \\ x_r = \alpha_{r\ r+1}x_{r+1} + \ldots + \alpha_{rn}x_n \end{cases}$, где α_{ij} — некоторые числа

Составим матрицу:

$$D = \begin{pmatrix} x_1^0 & \phi_{11} & . & \phi_{k1} \\ . & . & . & . \\ x_r^0 & \phi_{1r} & . & \phi_{kr} \\ x_{r+1}^0 & \phi_{1\ r+1} & . & \phi_{k\ r+1} \\ . & . & . & . \\ x_n^0 & \phi_{1n} & . & \phi_{kn} \end{pmatrix}$$ — это записанные друг за другом столбцы $x^0, \Phi_1, \ldots, \Phi_k$

Покажем, что $\operatorname{Rg} D = k$

1. $\operatorname{Rg} D \geqslant k$, т.к. $\Phi_1, \ldots, \Phi_k$ — л.н.з. , а по определению $\operatorname{Rg} D \geqslant k$
2. $\operatorname{Rg} D \leqslant k$, т.к. $x^0, \Phi_1, \ldots, \Phi_k$ — решения СЛАУ $Ax = 0$
   Тогда для них выполнимо **(7.1)**
   $$\begin{cases} x_1^0 = -\alpha_{1\ r+1} \cdot x_{r+1}^0 + \ldots + \alpha_{1n} \cdot x_n^0 \\ \phi_{11} = \alpha_{1\ r+1} \cdot \phi_{1\ r+1} + \ldots + \alpha_{1n} \cdot \phi_{1n} \\ \vdots \\ \phi_{k1} = \alpha_{1\ r+1} \cdot \phi_{k\ r+1} + \ldots + \alpha_{1n} \cdot \phi_{kn} \end{cases}$$
   То есть первая строка d_1 матрицы D — линейная комбинация строк $d_{r+1} \, .. \, d_n$:
   $d_1 = \alpha_{1\ r+1} \cdot d_{r+1} + \ .. \ + \alpha_{1n} \cdot d_n$

   Аналогично со всеми строками до r-той:
   $d_r = \alpha_{r\ r+1} \cdot d_{r+1} + \ .. \ + \alpha_{rn} \cdot d_n$

   Сделаем элементарные преобразования:
   $d_1 - \alpha_{1\ r+1} \cdot d_{r+1} - .. - \alpha_{1n} \cdot d_n \rightsquigarrow d1$
   ...
   $d_r - \alpha_{r\ r+1} \cdot d_{r+1} - .. - \alpha_{rn} \cdot d_n \rightsquigarrow dr$

   Тогда $D \rightsquigarrow D_1$:

   $$D_1 = \begin{pmatrix} 0 & . & . & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & . & . & 0 \\ x_{r+1}^0 & \phi_{1\ r+1} & . & \phi_{k\ r+1} \\ \cdot & \cdot & \cdot & \cdot \\ x_n^0 & \phi_{1n} & . & \phi_{kn} \end{pmatrix}$$

   $\Rightarrow \operatorname{Rg} D_1 \leqslant k$, а при элементарных преобразованиях ранг не меняется $\Rightarrow \operatorname{Rg} D \leqslant k$
   $\Rightarrow \operatorname{Rg} D = k$

$\Rightarrow$ Столбцы $\Phi_1, \ldots, \Phi_k$ — базисные (они л. н. з.)
$\Rightarrow x^0$ — линейная комбинация $\Phi_1, \ldots, \Phi_k$ (по т. О базисном миноре)
$\Rightarrow \exists \ c_1, \ldots, c_k : \ x^0 = c_1\Phi_1 + \ .. + \ c_k\Phi_k$
#

<u>Теорема о структуре общего решения неоднородной СЛАУ</u>
Рассмотрим СЛАУ $Ax = b, \ A \in M_{mn}(\mathbb{R})$
Пусть известно частное решение $\widetilde{x}$ СЛАУ $Ax = b$
Тогда любое решение этой СЛАУ может быть представлено в виде
$x = \widetilde{x} + c_1\Phi_1 + \ .. \ + c_k\Phi_k$,где $\Phi_1, \ldots, \Phi_k$ — ФСР соответствующей однородной СЛАУ $Ax = 0$, а $c_1, \ldots, c_k$ — некоторые числа

<u>Док-во:</u>
Пусть x^0 — произвольное решение СЛАУ $Ax = b$
Тогда $(x^0 - \widetilde{x})$ — решение однородной СЛАУ $Ax = 0$ (по свойству решений)
$\Rightarrow$ По т. О структуре решений однородной СЛАУ
$\exists \ c_1, \ldots, c_k : \ x^0 - \widetilde{x} = c_1\Phi_1 + \ .. + \ c_k\Phi_k$
$\Rightarrow x^0 = \widetilde{x} + c_1\Phi_1 + \ .. + \ c_k\Phi_k$
#

Зам. Решения СЛАУ $Ax = b$ всегда представляемо в виде
$X_{\text{общ неод}} = X_{\text{частн неод}} + X_{\text{общ од}}$

Лекция #8
Комплексные числа

$\mathbb{N}$ — Натуральные числа

$\mathbb{Z}$ — Целые числа

$\mathbb{Q}$ — Рациональные числа

$\mathbb{R}$ — Вещественные числа

$\mathbb{C}$ — Комлексные числа

Множество пар вещественных чисел с двумя операциями:
1. $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2,\ y_1 + y_2)$ — *сложение*
2. $(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2,\ x_1y_2 + x_2y_1)$ — *умножение*
Называется **комплексами числами** и обозначается C

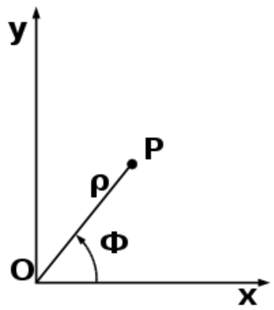
Мнимая единица:
$i^2 = (0,1)(0,1) = (-1,0) = -1$

Любое число может быть представлено в виде:
$z = (x, y) = (x,0)(1,0) + (y,0)(0,1) = x \cdot 1 + i \cdot y$

Тут $x = Re\ z$ — вещественная часть, $y = Im\ z$ — мнимая часть

Свойства операций:
$\forall a, b, c \in \mathbb{C}$
1. $a + b = b + a$
2. $(a + b) + c = a + (b + c)$
3. $\exists 0 = (0,0) : a + 0 = a$
4. $\forall a \exists (-a) : a + (-a) = 0$
5. $a \cdot b = b \cdot a$
6. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
7. $\exists 1 = (1,0) : a \cdot 1 = a$
8. $\forall a \neq 0\ \exists\ a^{-1} : a \cdot a^{-1} = 1$
9. $(a + b) \cdot c = a \cdot c + b \cdot c$
$\Rightarrow \mathbb{C}$ — поле (а его элементы могут называться числами)

Полярная система координат:
$z(r, \phi)$ — полярные координаты



$x = r \cdot \cos\phi \ \rightarrow r = \sqrt{x^2 + y^2}$

$z = x + i \cdot y = r \cdot \cos\phi + i \cdot r \cdot \sin\phi = r \cdot (\cos\phi + i \cdot \sin\phi)$
(алгебраическая и тригонометрическая формы записи)

$r = |z|$ — **модуль** комплексного числа
$\phi = Arg\ z = \{arg\ z + 2\pi k, k \in Z\}$ — **аргумент** комплексного числа

Главное значение аргумента $arg\ z$:

1. $arg\ z \in [0,\ 2\pi)$
2. $arg\ z \in (-\pi,\ \pi]$

Утв. $z_1 \cdot z_2 = r_1 \cdot r_2 \cdot (\cos(\phi_1 + \phi_2) + i \cdot \sin(\phi_1 + \phi_2))$

<u>*Док-во:*</u>
$z_1 \cdot z_2 = r_1 \cdot r_2 \cdot (\cos\phi_1 + i \cdot \sin\phi_1) \cdot (\cos\phi_2 + i \cdot \sin\phi_2) =$
$= r_1 \cdot r_2 \cdot (\cos\phi_1 \cos\phi_2 - \sin\phi_1 \sin\phi_2 + i(\cos\phi_1 \sin\phi_2 + \cos\phi_2 \sin\phi_1)) =$
$= r_1 \cdot r_2 \cdot (\cos(\phi_1 + \phi_2) + i \cdot \sin(\phi_1 + \phi_2))$
#

<u>Комплексное сопряжение</u>

$z = a + ib$
$\overline{z} = a - ib$

$z \cdot \overline{z} = (a + ib)(a - ib) = a^2 + b^2 = |z|^2 \in \mathbb{R}$

1. $\dfrac{z_1}{z_2} \cdot \dfrac{\overline{z}_2}{\overline{z}_2} = \dfrac{z_1\ \overline{z}_2}{|z_2|^2}$, $z_2 \neq 0$
2. $\dfrac{z_1}{z_2} = \dfrac{r_1(\cos\phi_1 + i\sin\phi_1)}{r_2(\cos\phi_2 + i\sin\phi_2)} = \dfrac{r_1}{r_2}(\cos(\phi_1 - \phi_2) + i\sin(\phi_1 - \phi_2))$, $r_2 \neq 0$

Утв. Формула Муавра
$z^n = r^n \cdot (\cos(n\phi) + i \cdot \sin(n\phi))$

<u>*Док-во:*</u>
При $n = 2$:
$z^2 = r^2 \cdot (\cos(2\phi) + i \cdot \sin(2\phi))$ — база индукции
Пусть утверждение верно для всех $n \leqslant k$
Покажем, что из этого следует, что оно верно для всех $n = k + 1$:
$z^{k+1} = r^k \cdot r \cdot (\cos(k\phi) + i \cdot \sin(k\phi))(\cos\phi + i \cdot \sin\phi) = r^{k+1} \cdot (\cos(k\phi + \phi) + i \cdot \sin(k\phi + \phi))$
По определению математической индукции утверждение верно для $\forall n \in \mathbb{N}$
#

<u>Извлечение комплексного корня</u>

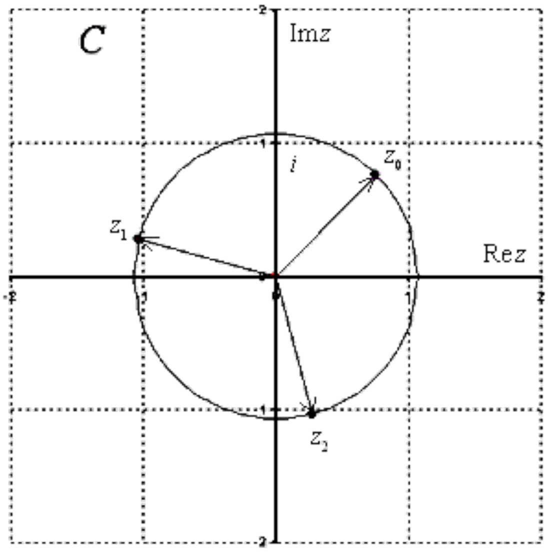
Дано число $\omega = \rho(\cos\psi + i\sin\psi)$ и число $n \in \mathbb{N}$
Нужно найти корень n-ой степени из ω, то есть $\sqrt[n]{\omega}$, то есть нужно найти все z : $z^n = \omega$
Пусть $z = r \cdot (\cos\phi + i \cdot \sin\phi)$,
тогда по формуле Муавра: $z^n = r^n \cdot (\cos(n\phi) + i \cdot \sin(n\phi)) = \omega$

$$\Rightarrow \begin{cases} \rho = r^n \\ \psi + 2\pi k = \phi n \end{cases}, k \in \mathbb{Z}$$

$$\Rightarrow \begin{cases} r = \sqrt[n]{\rho} \\ \phi = \frac{\psi + 2\pi k}{n} \end{cases}, k \in \mathbb{Z}$$

Достаточно взять $k = 0,1, \dots, n-1$

$\sqrt[n]{\omega} = \{ \sqrt[n]{\rho} \cdot (\cos \frac{\psi + 2nk}{n} + i \cdot \sin \frac{\psi + 2nk}{n}) \}$



Утв. Формула Эйлера

$e^{i\phi} = \cos \phi + i \sin \phi$

$e^{-i\phi} = \cos \phi - i \sin \phi$

$\cos \phi = \dfrac{e^{i\phi} + e^{-i\phi}}{2}$

$\sin \phi = \dfrac{e^{i\phi} - e^{-i\phi}}{2i}$

Основная теорема алгебры

$\forall$ многочлена $a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0 = 0$, где $a_i \in C,\ a_n \neq 0,\ n \in \mathbb{N}$

$\exists$ корень $z_0 \in \mathbb{C}$

Следствие

У многочлена $P_n(z)$ степени $n \in \mathbb{N}$ есть ровно n корней с учетом кратности

Зам. Говорят, что поле $\mathbb{C}$ алгебраически замкнуто

Лекция # 9
Разложение многочленов на неприводимые множители

Разложение многочлена $f(x) = g(x)h(x)$ называется **нетривиальным**, если $\begin{cases} \deg g < \deg f \\ \deg h < \deg f \end{cases}$

Многочлен называется **приводимым**, если существует *нетривиальное* разложение $f = gh$, и **неприводимым**, если такого не существует

Теорема Безу
Остаток от деления $f(x)$ на $x - a$ равен $f(a)$

Док-во:
Разделим $f(x)$ на $x - a$
$f(x) = (x - a)Q(x) + R(x)$, где $R(x)$ — остаток
$\deg R(x) < \deg(x - a) = 1 \to \deg R(x) = 0 \to \deg R(x)$ — const
$f(a) = (a - a)Q(a) + \text{const} \to R(x) = f(a)$
#

I. Комплексный многочлен степени n над полем $\mathbb{C}$

Раскладываются в произведение:
$P_n(z) = a_n(z - z_1) \cdot \ldots \cdot (z - z_n)$, где $a_n, z_i \in \mathbb{C}$
$P_n(z) = a_n(z - z_1)^{\alpha_1} \cdot \ldots \cdot (z - z_k)^{\alpha_k}$, где $z_1, \ldots, z_k$ различны, $\alpha_1 + \ldots + \alpha_k = n$
Это следствие из основной теоремы алгебры и теоремы Безу

II. Многочлены с действительными коэффициентами

Утв. 1
Если $z_0 \in \mathbb{C}$ является корнем кратности k многочлена $f(x)$ с действительными коэффициентами, то и $\bar{z}_0$ является корнем $f(x)$ кратности k
$\triangleright$ z_0 является корнем $P(z_0) = 0$
$P_n(z) = a_n z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0$, где $a_i \in \mathbb{R}$
$\overline{a_n z_0^n + a_{n-1}z_0^{n-1} + \ldots + a_1 z_0 + a_0} = \overline{0} = 0$
$\overline{a_n}(\overline{z_0})^n + \overline{a_{n-1}}(\overline{z_0})^{n-1} + \ldots + \overline{a_1}\,\overline{z_0} + \overline{a_0} = 0$
$a_n(\overline{z_0})^n + a_{n-1}(\overline{z_0})^{n-1} + \ldots + a_1\overline{z_0} + a_0 = 0$
То есть, $\overline{z_0}$ является корнем $\triangleleft$

Утв. 2
$(x - z_0)(x - \overline{z_0}) = x^2 - 2\mathrm{Re}\, z_0\ x + |z_0|^2$
$\triangleright$ $(x - (a + ib))(x - (a - ib)) = x^2 - x(a - ib) - x(a + ib) + (a + ib)(a - ib) =$
$= x^2 - 2ax + a^2 + b^2 = x^2 - 2\mathrm{Re}\, z_0 x + |z_0|^2$

Зам. Над $\mathbb{R}$ неприводимы все многочлены первой степени и все многочлены второй степени с $D < 0$, а остальные приводимы

Следствие
Каноническое разложение $f(x)$ с вещественными коэффициентами имеет вид
$f(x) = a_n(x - c_1)^{k_1} \ldots (x - c_s)^{k_s}(x^2 + p_1 x + q_1)^{L_1} \ldots (x^2 + p_t x + q_t)^{L_t}$

<u>Теорема Виета</u>

Пусть $c_1, \ldots, c_n$ — корни многочлена степени n
$P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, тогда

$$a_{n-1} = -(c_1 + \ldots + c_n)$$
$$a_{n-2} = c_1c_2 + c_1c_3 + \ldots + c_1c_n + c_2c_3 + \ldots + c_{n-1}c_n$$
$$a_{n-3} = -(c_1c_2c_3 + c_1c_2c_4 + \ldots + c_{n-2}c_{n-1}c_n)$$
$$\ldots$$
$$a_1 = (-1)^{n-1}(c_1c_2\ldots c_{n-1} + c_2c_3\ldots c_n)$$
$$a_0 = (-1)^n c_1\ldots c_n$$

<u>Док-во:</u>
Запишем многочлен в виде
$P_n(x) = 1(x - c_1)\ldots(x - c_n)$
и раскроем скобки
Это следствие основной теоремы алгебры
#

Правильной называется дробь вида $\dfrac{f(x)}{g(x)}$, где $f,\ g$ — многочлены, $\deg f < \deg g$

Простейшей называется дробь вида $\dfrac{f(x)}{(p(x))^k}$, где $p(x)$ — неприводимый многочлен, $\deg f < \deg p$

<u>Теорема</u>

$\forall$ правильная дробь разлагается в сумму простейших

Лекция #10

Элементы общей алгебры

Множество - это любая совокупность объектов

Обозначения:

$S \cap T$ — пересечение множеств

$S \cup T$ — объединение множеств

$S \setminus T$ — разность множеств

$S \times T = \{(x, y) | x \in S, y \in T\}$ — декартово произведение множеств

$f : X \to Y$ — отображение одного множества в другое

$Im\ f = \{f(x) | x \in X\}$, $f(x) \subseteq Y$ — образ отображения

$f^{-1}(y) = \{x \in X | f(x) = y\}$ — полный прообраз отображения

Отображение $f : X \to Y$ называется

1. **Сюръективным**, если $\mathrm{Im} f = Y$
2. **Инъективным**, если $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$
3. **Биективным**, если оно сюръективно и инъективно

Произведение двух отображение называется их **композицией**

$f \circ g : U \to W$ — композиция f и g, если

$f : V \to W$

$g : U \to V$

$(f \circ g)(u) = f(g(u))$

Зам. Композиция отображений, вообще говоря, *некоммутативна*

Зам. Композиция *ассоциативна*

$h : U \to V$

$g : V \to W$

$f : W \to T$

$f(gh) = (fg)h$

Лекция #11

Бинарные отношения

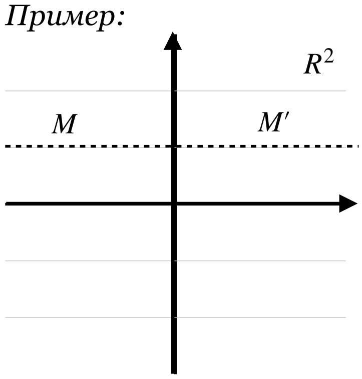
$\forall$ множеств X и Y всякое подмножество $\omega \in X \times Y$ называется **бинарным отношением** между X и Y (или на X, если $X = Y$)
Зам. Часто вметсто $(x, y) \in \omega$ пишут $x\omega y$

Бинарное отношение $\sim$ называется **отношением эквивалентности**, если
$\forall x, x', x'' \in X$ выполняются условия:

1. $x \sim x$ — рефлексивность
2. $x \sim x' \Rightarrow x' \sim x$ — симметричность
3. $x \sim x', x' \sim x'' \Rightarrow x \sim x''$ — транзитивность

Подмножество $\overline{x} = \{x' \in X \,|\, x' \sim x\} \subseteq X$ называется **классом эквивалентности**, содержащим x

Пример:



$M \sim M'$, если они лежат на одной горизонтальной прямой

Зам. Множество классов эквивалентности по отношению $\sim$ является разбиением множества X, то есть $X = \bigcup\limits_{x \in X} \overline{x}$ и $\overline{x'} \cap \overline{x''} = \emptyset$ (смежные кассы совпадают или не пересекаются)
Зам. Если существует разбиение $\pi(X)$ множества x на непересекающиеся подмножества C_x, то C_x будут **классами эквивалентности** по некоторому отношению эквивалентности $\sim$

<u>*Док-во:*</u>
Пусть $x \sim x' \Leftrightarrow$ они лежат в одном подмножестве
Это рефлексивно, симметрично и транзитивно
#

Разбиение, отвечающее отношению эквивалентности, обозначается $x/\sim$ и называется **фактормножеством** x относительно $\sim$

Отображение $p : x \to \overline{x} = p(x)$ называется **канонической проекцией** x на фактормножество $x/\sim$

Бинарные операции

Бинарной операцией на множестве X называется отображение $\tau : X \times X \to X$

Множество X с заданной на нем *бинарной операцией* называется **группоидом (магмой)**

Пример:

$X = V_3$ — множество векторов в трехмерном пространстве
$\tau = [\ ,\ ]$ — векторное произведение

Операция $\circ$ называется **ассоциативной** на множестве X, если
$\forall a, b, c \in X : (a \circ b) \circ c = a \circ (b \circ c)$

Множество X с заданной на нем *ассоциативной* бинарной операцией называется **полугруппой**

Пример:

$X = \mathbb{N} \setminus \{1\}$ — натуральные числа, кроме 1

τ — умножение целых чисел

Элемент $e \in X$ называется **нейтральным** элементом, если $\forall x \in X : x \circ e = e \circ x = x$

Полугруппа, в которой есть *нейтральный элемент*, называется **моноидом**

Пример:

$(\mathbb{N}, \cdot)$ — натуральные числа с операцией умножения

Элемент a моноида $(M, \circ)$ называется **обратимым**, если $\exists b \in M : a \circ b = b \circ a = e$ (тогда b тоже обратим)

Моноид G, все элементы которого *обратимы*, называется **группой**
Эквивалентно:
Множество G с заданной на нем бинарной операцией называется **группой,** если:
1. $\forall x, y, z \in G : (x \circ y) \circ z = x \circ (y \circ z)$ — операция *ассоциативна*
2. $\exists e \in G \, \forall x \in G : x \circ e = e \circ x = x$ — есть *нейтральный элемент*
3. $\forall x \in G \, \exists \, x^{-1} \in G : x \circ x^{-1} = x^{-1} \circ x = e$ — все элементы *обратимы*

Примеры:

$GL_n(\mathbb{R})$ — общая линейная группа *(множество всех невырожденных матриц порядка n с операцией матричного умножения)*

S_n — симметрическая группа *(множество всех подстановок длины n с операцией композиции)*

Бинарная операция называется **коммутативной**, если $\forall a, b \in X : a \circ b = b \circ a$

Группа называется **абелевой**, если ее бинарная операция *коммутативна*

Пример:

$X = V_3$ — множество векторов в трехмерном пространстве

τ — сложение векторов

Подмножество $H \subseteq G$ называется **подгруппой** в G, если:
1. $e \in H$ — есть *нейтральный элемент*
2. $\forall h_1, h_2 \in H : h_1 \circ h_2 \in H$ — замкнутость относительно умножения
3. $\forall h \in H \to h^{-1} \in H$ — замкнутость относительно обратимости

То есть H сама является группой относительно той же операции
Пример:

$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \,|\, \det A = 1\}$ — специальная линейная группа *(множество всех матриц порядка n, определитель которых равен 1, с операцией матричного умножения)*

Зам. $SL_n(\mathbb{R}) \subset GL_n(\mathbb{R})$

Лекция #12

Циклические группы

Если $\forall$ элемент $g \in G$ имеет вид $g = a^n$ (мультипликативная запись), где $a \in G$, то G называется **циклической группой**

Обозначение: $G = \langle a \rangle$

Пример:
$(\mathbb{N}, +) = \langle 1 \rangle$

Говорят, что число a является **порождающим элементом**

Зам. $\forall$ элемента $b \in G$ множество $\langle b \rangle = \{b^n, n \in \mathbb{Z}\}$ является циклической подгруппой

Пример:
Группа — $(\mathbb{Z}, +)$
Подгруппа — $\{n \cdot 1 \,|\, n \in \mathbb{Z}\}$

Пусть q — *наименьшее натуральное* число, для которого $a^q = e$
Тогда a — элемент **конечного порядка**
Если такого q не существует, то говорят, что a имеет **бесконечный порядок**
Обозначение: $\operatorname{ord} a$

Порядок группы — это количество элементов в ней
Обозначение: $|G|$

Пример:
$|\mathbb{Z}| = \infty$

Утв. Порядок элемента равен порядку циклической группы, которую он порождает:
$\operatorname{ord}(a) = |\langle a \rangle|$

Таблица Кэли — это матрица вида:

	g_1	g_2	g_3	…
g_1	g_1g_1	g_1g_2	g_1g_3	.
g_2	g_2g_1	g_2g_2	g_2g_3	.
g_3	g_3g_1	g_3g_2	g_3g_3	.
…	.	.	.	.

Зам. Если таблица Кэли для группы *симметрична,* то группа *абелева*

Пусть даны две группы $(G_1, \circ)$ и $(G_2, *)$
Тогда отображение $f : G_1 \to G_2$ называется **гомоморфизмом** (морфизмом), если
$\forall a, b \in G_1 : f(a \circ b) = f(a) * f(b)$

Зам. Говорят, что f «уважает» умножение

Пример:
$G_1 = (\mathbb{R}_+, \cdot),\ G_2 = (\mathbb{R}_+, +)$
$f = \ln(x)$
$\forall a, b \in \mathbb{R}_+$ выполнено: $\ln(a \cdot b) = \ln(a) + \ln(b)$

Свойства гомоморфизма:

1. Нейтральный элемент переходит в нейтральный элемент
   Док-во:
   $f(e_1) * f(a) = f(e_1 \circ a) = f(a)$
   $f(a) * f(e_1) = f(a \circ e_1) = f(a)$
   $\Rightarrow f(e_1) = e_2$
   #

2. $f(a^{-1}) = (f(a))^{-1}$
   Док-во:
   $f(a) * f(a^{-1}) = f(a \circ a^{-1}) = f(e_1) = e_2$
   $f(a^{-1}) * f(a) = f(a^{-1} \circ a) = f(e_1) = e_2$
   $\Rightarrow (f(a))^{-1} = f(a^{-1})$
   #

Инъективный гомоморфизм называется **мономорфизмом**
Сюръективный гомоморфизм называется **эпиморфизмом**
Биективный гомоморфизм называется **изоморфизмом**

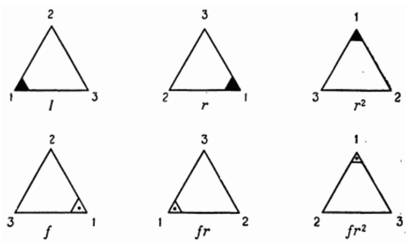
Свойство изоморфизма:

Обратное отображение $f^{-1} : G_2 \to G_1$ тоже является изоморфизмом
$f^{-1}(f(a) * f(b)) = f^{-1}(f(a \circ b)) = a \circ b$ и f^{-1} тоже биекция

Примеры групп:

1. **Группа Диэдра** — группа симметрий правильного n-угольника
   Обозначение: $D_n = \{r, s \mid r^n = 1,\ s^2 = 1,\ s^{-1}rs = r^{-1}\}$
   Операция: композиция
   $|D_n| = 2n$

   Пример:
   $D_3 \simeq S_3$
   $S_3 = \{id, (123), (132), (12), (23), (13)\}$
   D_3
   $\phi_0 \to id \qquad \psi_1 \to (23)$
   $\phi_1 \to (123) \qquad \psi_2 \to (13)$
   $\phi_2 \to (132) \qquad \psi_3 \to (12)$



2. **Группа кватернионов** Q_8
   $Q_8 = \{\pm 1, \pm i, \pm j \pm k \mid (-1)^2 = 1,\ i^2 = j^2 = k^2 - 1,\ ijk = -1\}$

	1	**-1**	***i***	***-i***	***j***	***-j***	***k***	***-k***
1	1	-1	*i*	-*i*	*j*	-*j*	*k*	-*k*
-1	-1	1	-*i*	*i*	-*j*	*j*	-*k*	*k*
i	*i*	-*i*	-1	1	*k*	-*k*	-*j*	*j*
-i	-*i*	*i*	1	-1	-*k*	*k*	*j*	-*j*
j	*j*	-*j*	-*k*	*k*	-1	1	*i*	-*i*
-j	-*j*	*j*	*k*	-*k*	1	-1	-*i*	*i*
k	*k*	-*k*	*j*	-*j*	-*i*	*i*	-1	1
-k	-*k*	*k*	-*j*	*j*	*i*	-*i*	1	-1

Лекция #13

Утв. Пусть G — группа и $g \in G$, тогда $\operatorname{ord}(g) = |\langle g \rangle|$

Док-во:

Если g имеет бесконечный порядок, то все элементы всегда $g^n, n \in \mathbb{Z}$
Они различны, тк если $g^k = g^s, k > s$, то $g^{k-s} = e,\ \operatorname{ord}(g) < \infty$
А их бесконечное число $\Rightarrow \operatorname{ord}(g) = |\langle g \rangle|$
Если $\operatorname{ord}(g) = m < \infty \Rightarrow$ из минимальности m следует, что $g_0 = e,\ g = g^1, g^2, .., g^{m-1}$,
где все различны, так как если $g^k = g^s \Rightarrow g^{k-s} = e$
$\forall n \in \mathbb{Z} : n = mq + r$ — разделим n на m с остатком
$0 \leqslant r < m$
$g^n = g^{mq+r} = (g^m)^q g^r = eg^r = g^r$
$|\langle g \rangle| = m = \operatorname{ord}(g)$
#

3. **Знакопеременная группа** A_n
   Множество всех четных подстановок
   $|A_n| = \dfrac{n!}{2}$

$f : G_1 \to G_2$
Ядром гомоморфизма называется множество $\operatorname{Ker} f$
$\operatorname{Ker} f = \{g \in G_1 | f(g) = e_2\}$

Утв. $\operatorname{Ker} f$, где f — гомоморфизм из группы G_1 в группу G_2 всегда является подгруппой в G_1

Док-во:

1. $e_1 \in \operatorname{Ker} f$, тк по первому свойству гомоморфизма $f(e_1) = e_2$
2. $\forall g_1, g_2 \in \operatorname{Ker} f \Rightarrow g_1 \cdot g_2 \in \operatorname{Ker} f$
   $f(g_1 \cdot g_2) = f(g_1) \circ f(g_2) = e_2 \circ e_2 = e_2$
   $\Rightarrow g_1 \cdot g_2 \in \operatorname{Ker} f$
3. $\forall g \in \operatorname{Ker} f \Rightarrow g^{-1} \in \operatorname{Ker} f$
   $f(g^{-1}) = (f(g))^{-1} = e_2^{-1} = e_2$
   $\Rightarrow g^{-1} \in \operatorname{Ker} f$

#

Пример:
$\det : GL_n(\mathbb{R}) \to \mathbb{R}$, тогда $\operatorname{Ker}\ \det = SL_n(\mathbb{R})$

Утв. $\forall$ подгруппа $b\ (\mathbb{Z}, +)$ имеет вид $k\mathbb{Z} = \{kz | z \in \mathbb{Z}\}$ для некоторого $k \in \mathbb{N} \cup \{0\}$

Док-во:

Если $H = \{0\}$, то берем $k = 0$
Если $H \neq \emptyset$, то берем $k = \min(H \cap \mathbb{N})$
Докажем, что $H = k\mathbb{Z}$
Очевидно, что $k\mathbb{Z} \subseteq H$
Возьмем произвольный $a \in H$
Разделим a на k с остатком r: $a = kq + r$
$0 \leqslant r < k$
$r = a - kq \in H$ и $r \in \mathbb{N} \cup \{0\}$
$\Rightarrow r = 0$ (это следует из минимальности k)
То есть $a = kq,\ q \in \mathbb{Z}$
То есть $H \subseteq k\mathbb{Z} \Rightarrow H = k\mathbb{Z}$
#

Утв. Все циклические подгруппы одного порядка *изоморфны*

<u>*Док-во:*</u>
Если группа бесконечна, то изоморфизм: $f : \langle g \rangle \to (\mathbb{Z}, +)$
Полагая, что $g^n \mapsto n$
Это биекция и это гомоморфизм
$f(g^m \cdot g^n) = f(g^m) + f(g^n) = n + m$
Если $G = \{e, g, g^2, \ldots, g^{m-1}\}$ и $G' = \{e', g', (g')^2, \ldots, (g')^{m-1}\}$,
то $f : g^k \mapsto (g')^k$
#

Пусть G — группа и $H \subseteq G$ подгруппа и $g \in G$
Тогда **левым смежным классом** элемента g по подгруппе H называется множество $gH = \{gh \mid h \in H\}$

<u>**Лемма 1**</u>
$\forall g_1, g_2 \in G$ либо $g_1H = g_2H$, либо $g_1H \cap g_2H = \varnothing$

<u>*Док-во:*</u>
Если $g_1H \cap g_2H \neq \varnothing$, то $\exists h_1, h_2 \in H : g_1h_1 = g_2h_2 \Rightarrow g_1 = g_2h_2h_1^{-1} \Rightarrow g_1H = g_2h_2h_1^{-1}H \subseteq g_2H$
Аналогично $g_2H \subseteq g_1H \Rightarrow g_1H = g_2H$
#

<u>**Лемма 2**</u>
$\forall g \in G : |gH| = |H|$

<u>*Док-во:*</u>
$|gH| \leqslant |H|$, т.к. $gH = \{gh \mid h \in H\}$
Если $gh_1 = gh_2 \Rightarrow h_1 = h_2$, т.к. $\exists g^{-1}$
Склеиваний не происходит $\Rightarrow |gH| = |H|$
#

Индексом подгруппы H в группе G называется число *левых смежных классов* в G по H
Обозначение: $[G : H]$

<u>Теорема Лагранжа</u>
Пусть G — конечная группа и H — ее подгруппа
Тогда $|G| = |H| \cdot [G : H]$

<u>*Док-во:*</u>
$\forall$ элемент группы G лежит в своем левом смежном классе по H и смежные классы не пересекаются (Лемма 1)
В $\forall$ смежном классе $|H|$ элементов (Лемма 2)
#

<u>**Следствие 1**</u>
Пусть G — конечная группа и $g \in G$
Тогда $\operatorname{ord}(g)$ делит $|G|$

<u>*Док-во:*</u>
Рассмотрим $\langle g \rangle = H$
Тогда по теореме Лагранжа $|G| = |\langle g \rangle| \cdot [G : \langle g \rangle]$
$\Rightarrow \operatorname{ord}(g)$ делит $|G|$
#

H называется **собственной подгруппой** в группе G, если $H \neq G$ и $H \neq \{e\}$

Классы смежности группы $\mathbb{Z}$ по подгруппе $n\mathbb{Z}$ называют вычетами по модулю n

Следствие 2
$\forall g \in G$, где G — конечная группа, верно $g^{|G|} = e$

Док-во:
По следствию 1 $|G| = ord(g) \cdot s$, где $s \in \mathbb{N}$
Тогда $g^{|G|} = g^{ord(g) \cdot s} = (g^{ord(g)})^s = e^s = e$
#

Следствие 3
Малая теорема Ферма
Пусть $\overline{a}$ — ненулевой вычет по модулю p
Тогда $\overline{a}^{p-1} = \overline{1}$

Док-во:
Это следствие 2, примененное к группе $\mathbb{Z}_p^* = (\mathbb{Z}_p \backslash \{0\}, \cdot)$
p — простое число
$\overline{1}$ — нейтральный элемент в $\mathbb{Z}_p^*$
$|\mathbb{Z}_p^*| = p - 1$
#

Лекция #14

Зам. Точно так же можно было рассмотреть и правые смежные классы $Hg = \{h \cdot g | h \in H\}$

Зам. Количество правых и левых смежных классов совпадает и $= \dfrac{|G|}{|H|}$

Зам. Не все делители порядка группы G являются порядками подгрупп G

Пример:
$|A_4| = \dfrac{4!}{2} = 12$, в A_4 нет подгруппы порядка 6

Прямым произведением групп $(G_1, \circ)$ и $(G_2, \star)$ является упорядоченное множество пар $G_1 \times G_2$ (декартово произведение) с операцией *покоординатного* умножения то есть $(g1,g2) \cdot (g_1', g_2') = (g_1 \circ g_1', g_2 \star g_2')$

Пример:
$\mathbb{Z}_2 \times \mathbb{Z}_2 = G$
$|G| = 4$

Зам. Все с точностью до изоморфизма группы порядка 8: $\mathbb{Z}_8,\ D_4,\ Q_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

<u>Теорема Кэли</u>

Любая конечная группа порядка n изоморфна подгруппе группы S_n

<u>*Док-во:*</u>
$\forall a \in G$ рассмотрим отображение $L_a : G \to G$,
заданное формулой $L_a(g) = a \cdot g$
Пусть $g_1 = e, g_2, g_3, \ldots, g_n$ — элементы группы
Тогда $a, a \cdot g_2, a \cdot g_3, \ldots, a \cdot g_n$ — тоже элементы, но в другом порядке
Т.к. $a \cdot g_i = g_j$
$\exists a^{-1} \Rightarrow a^{-1}ag_i = a^{-1}ag_j \Rightarrow eg_i = eg_j \Rightarrow g_i = g_j$
$\Rightarrow$ нет склеиваний
$\Rightarrow L_a$ — биективное разложение G в себя
Обратим внимание на то, что $L_e, L_{g_2}, \ldots, L_{g_n}$
Если нейтральный элемент L_e , то $(L_a)^{-1} = L_{a^{-1}}$
Из ассоциативности в G следует $L_{ab}(g) = (ab)g = a(bg) = L_a(L_b(g))$
Множество $L_e, L_{g_2}, \ldots, L_{g_n}$ отображает подгруппу H в группу $S(G)$ всех биективных отображений G в себя, то есть S_n
Изоморфизм: $a \mapsto L_a \in H \subseteq S_n$, это биекция и гомоморфизм
#

<u>Применение циклической группы к криптографии</u>

Задача дискретного логарифмирования
Пусть G — конечная группа и $g \in G$, причем $\operatorname{ord}(g)$ достаточно большой
Задача: для данного элемента $h \in \langle g \rangle$ найти $k : h = g^k$
Дискретное логарифмирование трудоемко, а возведение в степень — нет

Лекция #15

<u>Система Diffe-Hellman обмена ключами</u>

Всем участниками известна конечная группа G и элемент $g \in G$ достаточно большого порядка

Участник Алиса фиксирует *натуральное число* a (оно секретное) и сообщает всем g^a

У Боба есть секретное значение b и он всем сообщает g^b

<u>Как создать общий для Алисы и Боба секретный ключ?</u>

Алиса возводит g^b в степень a, а Боб возводит g^a в степень b

Тогда в результате элемент g^{ab} есть только у Алисы и Боба и они могут использовать его в качестве секретного ключа

<u>Криптосистема Elgamal</u>

Снова всем участниками известна конечная группа G и элемент $g \in G$

Участник Алиса фиксирует *натуральное число* a (оно секретное) и сообщает всем g^a

Если Боб хочет конфидециально передать Алисе элемент $M \in G$, то он выбирает *некоторое натуральное* k и сообщает всем следующую пару значений: $(g^k,\ M \cdot (g^a)^k)$

<u>По этим данным восстановить M может только Алиса, и она это делает так:</u>

$M \cdot g^{ak} \cdot (g^k)^{|G|-a} = M \cdot g^{ak-ak} \cdot g^{|G|k} = M \cdot e \cdot (g^{|G|})^k = M \cdot e = M$

Зам. Говорят, что элементы $a_1, \,..\,, a_n \in G$ порождают подгруппу H, если H — это множество произведений степеней $a_1, \,..\,, a_n$ и обратных к ним

Примеры:

$\forall$ циклическая группа порождается одним элементом $\langle a \rangle$

$D_n = \langle r, s \rangle$

Подгруппа H группы G называется **нормальной подгруппой**, есть $\forall g \in G: \ gH = Hg$ совпадают

Зам. Это эквивалентно тому, что $\forall g \in G: \ H = g^{-1}Hg$, то есть H нормальна $\Leftrightarrow$ она инвариантна относительно сопряжений

Пусть H — нормальная подгруппа, тогда *фактормножество* G/H — множество левых смежных классов по H — с операцией умножения:

$$(g_1H) \cdot (g_2H) = (g_1 \cdot g_2)H$$

называется **факторгруппой** группы G по подгруппе H

Зам. Операция ассоциативна (следует из ассоциативности в G), обладает нейтральным элементом $eH = H$ и $\forall g \in G$ и соответствующего смежного класса $gH \ \exists g^{-1}H$ — обратный элемент $\Rightarrow G/H$ является группой

Зам. Нормальность нужна для корректности определения операции умножения, то есть результат не зависит от выбора представителя смежного класса:

$g_1h_1 \cdot H$ и $g_2h_2 \cdot H$

или $g_1 \cdot H$ и $g_2 \cdot H$

$\Rightarrow g_1h_1g_2h_2H = g_1g_2g_2^{-1}h_1g_2h_2H$

$h_1, h_2 \in H \Rightarrow g_2^{-1}h_1g_2 \in H \Rightarrow g_2^{-1}h_1g_2h_2 \in H$

$\Rightarrow g_1g_2h_3H$ — тот же смежный класс, что и g_1g_2H

Зам. $\forall$ подгруппа $\forall$ абелевой группы является нормальной

Зам. $H = \langle (12) \rangle$ в S_3 не является нормальной

Отображение $\varepsilon : G \to G/H$, сопоставляющее каждому элементу $g \in G$ его *класс смежности* gH, то есть $\varepsilon : g \mapsto gH$ называется **естественным гомоморфизмом**

<u>Теорема о гомоморфизме</u>

Пусть $f : G \to F$ — гомоморфизм группы G и F
Тогда группа

$$\mathrm{Im} f = \{a \in F \mid \exists g \in G : f(g) = a\}$$

изоморфна факторгруппе $G/\mathrm{Ker} f$
То есть

$$G/\mathrm{Ker} f \cong \mathrm{Im} f$$

<u>Док-во:</u>
Рассмотрим отображение $\tau : G/\mathrm{Ker} f \to \mathrm{Im} f \subseteq F$
Заданное формулой $\tau(g\mathrm{Ker} f) = f(g)$
Докажем, что это изоморфизм
Проверим корректность определения, то есть проверим, что результат не зависит от выбора представителя в смежном классе

$$\forall h_1, h_2 \in \mathrm{Ker} f = H$$
$$f(gh_1) = f(g) \cdot f(h_1) = f(g) \cdot e_F = f(g)$$
$$f(gh_2) = f(g) \cdot f(h_2) = f(g) \cdot e_F = f(g)$$

Проверим, что τ — гомоморфизм:

$$\tau((g_1\mathrm{Ker} f) \cdot (g_2\mathrm{Ker} f)) = \tau((g_1 \cdot g_2)\mathrm{Ker} f)) =$$
$$= f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2) = \tau(g_1\mathrm{Ker} f) \cdot \tau(g_2\mathrm{Ker} f)$$

τ является биекцией:

τ сюръективно по своему определению и инъективно в силу того, что $f(g) = e_f \Leftrightarrow g \in \mathrm{Ker} f$, то есть нейтральному элементу, так как ядро тривиально, то $e\mathrm{Ker} f$ в факторгруппе

$\to \tau$ — биекция $\to \tau$ — изоморфизм
#

Зам.

$$\begin{tikzcd}
G \arrow[r, "\varepsilon"] \arrow[dr, "f"'] & G/H \arrow[d, "\tau"] \\
 & \mathrm{Im} f \subseteq F
\end{tikzcd}$$

$f = \tau \circ \varepsilon$
Здесь f — данный гомоморфизм
G и F — данные группы
$H = \mathrm{Ker} f \subseteq G$
ε — естественный гомомофризм

Лекция #16

Пусть f — гомоморфизм, тогда f инъективен $\Leftrightarrow$ $\mathrm{Ker} f$ — тривиальное

<u>*Док-во:*</u>

«→» *Необходимость:*

Дано: f *инъективен*

Док-ть: $\mathrm{Ker} f = \{e_1\}$

$\forall x_1 \neq x_2 :\ f(x_1) \neq f(x_2)$

$\forall x \in G$ и $x \neq e_1 :\ f(x) \neq f(e_1) = e_2$

$\Rightarrow x \neq e_1$ не лежит в ядре $\Rightarrow \mathrm{Ker} f = \{e_1\}$

«←» *Достаточность:*

Дано: $\mathrm{Ker} f = \{e_1\}$

Док-ть: f *— гомоморфизм и он инъективен*

Предположим, что $\exists x_1 \neq x_2 :\ f(x_1) = f(x_2)$

Умножим справа на $(f(x_2))^{-1} :\ f(x_1)(f(x_2))^{-1} = e_2$

$f(x_1) \cdot f(x_2^{-1}) = e_2 \Rightarrow\ f(x_1 \cdot x_2^{-1}) = e_2$

$\Rightarrow x_1 \cdot x_2^{-1} \in \mathrm{Ker} f \Rightarrow x_1 \cdot x_2^{-1} = e_1$

Умножим на x_2 справа $\Rightarrow x_1 = x_2$ — противоречие

#

Примеры:

1. $\mathbb{Z}/k\mathbb{Z} \simeq \mathbb{Z}_k$
   Гомоморфизм сопоставляет целому числу n остаток от деления n на k
2. $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$
   Гомоморфизм — определитель матрицы

Утв. <u>Критерий нормальности</u>

Пусть $H \subseteq G$, тогда три условия эквивалентны:

1. H — нормальная подгруппа
2. $gHg^{-1} \subseteq H\ \forall g \in G$
3. $gHg^{-1} = H\ \forall g \in G$

<u>*Док-во:*</u>

(1) → (2)

Пусть $g \in G$ и $h \in H$.

Из определения нормальности: $gh = h'g$ для. Некоторого $h' \in H$

$\Rightarrow ghg^{-1} = h' \in H \Rightarrow gHg^{-1} \subseteq H$

(2) → (3)

Остается проверить, что $H \subseteq gHg^{-1}$

Для $h \in H :\ h = (gg^{-1})h(gg^{-1}) = g(g^{-1}hg)g^{-1} \in gHg^{-1}$

$\Rightarrow H \subseteq gHg^{-1} \Rightarrow H = gHg^{-1}$ — инвариантность относительно сопряжений

(3) → (1)

$\forall g \in G :\ gH = gH(g^{-1}g) = (gHg^{-1})g = Hg$

Это определение нормальности

#

Утв. **<u>Критерий нормальности с использованием понятия ядра</u>**
Пусть $H \subseteq G$, тогда H нормальна $\Leftrightarrow \exists f$ — гомоморфизм и $\operatorname{Ker} f = H$

<u>Док-во:</u>

«→» *Необходимость:*

Дано: H нормальна
Док-ть: $\exists f : \operatorname{Ker} f = H$
Возьмем естественный гомоморфизм $\varepsilon : G \to G/H$
$\varepsilon(g) = gH \ \forall g \in G$
$\operatorname{Ker} \varepsilon = H$

«←» *Достаточность*

Дано: f — гомоморфизм и $\operatorname{Ker} f = H$
Док-ть: H нормальна
Пусть $f : G \to F$ и $z \in Ker\ f$
Докажем, что $\forall x \in G : x^{-1}zx \in \operatorname{Ker} f$
Тогда по пункту (2) критерия нормальности $\operatorname{Ker} f$ будет нормальным
$f(x^{-1}zx) = f(x^{-1}) \cdot f(z) \cdot f(x) = f(x^{-1}) \cdot f(x) = f(x^{-1}x) = f(e_G) = e_F$
$\forall x \in G$ и $\forall z \in \operatorname{Ker} f : x^{-1}zx \in \operatorname{Ker} f$
$\Rightarrow \operatorname{Ker} f$ — нормальна

#

<u>RSA (Rivest, Shamir, Adleman)</u>

— криптографический алгоритм с открытым ключом
Используется TLS/SSL
Схема:

I. **<u>Создание отрытых ключей</u>**
$\phi(n)$ — функция Эйлера — количество натуральных чисел, меньших n и взаимно простых с n
1. Выбирается два достаточно больших простых числа p и q (лучше > 2048 бит каждое)
2. Вычисляется модуль $n = pq$
3. Вычисляется $\phi(n) = (p-1)(q-1)$
4. Выбирается натуральное число $e : \ 1 < e < \phi(n)$, взаимно простое с $\phi(n)$
   e — открытая экспонента
5. Вычисляется d — обратное к e по модулю $\phi(n)$,
   то есть решение $x \cdot e = 1 \bmod \phi(n)$
   d — секретная экспонента
6. Пара (e, n) публикуется в виде открытого ключа RSA
7. Пара (d, n) держится в секрете

II. **<u>Шифрование и дешифрование</u>**
1. <u>Шифрование</u>
   Берем открытый ключ e и сообщение M
   $C = M^e \bmod n$
2. <u>Дешифровка</u>
   $M = C^d \bmod n = M^{ed} \bmod n = M \bmod n$

Пусть G — группа, тогда ее **центром** называется множество
$Z(G) = \{a \in G \,|\, ab = ba \,\forall b \in G\}$
т.е. Элементы $Z(G)$ коммутируют со всеми элементами G

Зам. G абелева $\Leftrightarrow Z(G) = G$

Утв. $Z(G) \forall G$ — нормальная подгруппа
Зам. H — подгруппа $\Leftrightarrow \forall a, b \in H : ab^{-1} \in H$

Док-во:
1. Докажем, что $Z(G)$ является подгруппой
Возьмем $a, b \in Z(G)$
Докажем, что $ab^{-1} \in Z(G)$, то есть $\forall g \in G: \ \ gab^{-1} = ab^{-1}g$
$ab^{-1}g = ab^{-1}(g^{-1})^{-1} = a(g^{-1}b)^{-1} = a(bg^{-1})^{-1} =$
$= a(g^{-1})^{-1}b^{-1} = agb^{-1} = gab^{-1}$
$\Rightarrow Z(G)$ — подгруппа
2. Докажем, что $Z(G)$ — нормальная подгруппа
Пусть $a \in Z(G)$ и $g \in G$
$\forall b \in G: \ \ g^{-1}ag \in Z(G)$, т.е $g^{-1}agb = bg^{-1}ag$

$\forall g \in G : gZ(G) = Z(G)g$
т.к. Элементы $Z(G)$ коммутируют со всеми элементами группы
#

Лекция #17

Автоморфизм — это изоморфизм группы G в себя

Зам. Множество всех *автоморфизмов* является *группой* относительно операции композиции отображений
Обозначение: $\mathrm{Aut}\,(G)$

Внутрненними автоморфизмами называют отображения $I_a : g \mapsto aga^{-1}$

Зам. Множество всех *внутренних автоморфизмов* является группой относительно операции композиции отображений
Обозначение: $\mathrm{Inn}\,(G)$

Зам. Это подгруппа $\mathrm{Aut}\,(G)$, т.к:
$\exists$ нейтральный элемент $I_e : g \mapsto ege^{-1} = g$ — тождественное отображение
Композиция ассоциативна
$\forall I_a \exists (I_a)^{-1} = I_{a^{-1}}$

Зам. Если G — абелева, то $\mathrm{Inn}\,(G) = id$

Утв. $\forall G : G/Z(G) \simeq \mathrm{Inn}\,(G)$

<u>*Док-во:*</u>
Применим теорему о гомоморфизме
Рассмотрим отображение $f : G \to \mathrm{Aut}\,(G)$, заданное формулой $f : g \mapsto ghg^{-1}$,
где $ghg^{-1} = \phi_g(h)$ — это элемент $\mathrm{Aut}(G)$, $h \in G$
Тогда $\mathrm{Im} f = \mathrm{Inn}\,(G)$ по определению $\mathrm{Inn}\,(G)$
$\mathrm{Ker} f = Z(G)$, т.к. $ghg^{-1} = h \Leftrightarrow gh = hg \in Z(G)$
Теорема о гомоморфизме:
$G/\mathrm{Ker} f \simeq \mathrm{Im} f$, а в нашем случае: $G/Z(G) \simeq \mathrm{Inn}\,(G)$
#

<u>Кольца</u>

Пусть $K \neq \varnothing$ — множество, на котором заданы две бинарные операции: *«сложение» и «умножение»* такие, что:
1. $(K, +)$ — абелева группа
2. $(K, \cdot)$ — полугруппа
3. Умножение дистрибутивно относительно сложения:
   $\forall a, b, c \in K$
   $a(b + c) = ab + ac$
   $(b + c)a = ba + ca$

Тогда $(K, +, \cdot)$ называется **кольцом**

Зам. $(K, +)$ — аддитивная группа кольцо
$(K, \cdot)$ — мультипликативная полугруппа кольца

Если $(K, \cdot)$, то $(K, +, \cdot)$ — **кольцо с единицей**

Подмножество $L \subseteq K$ называется **подкольцом**, если $\forall x, y \in L$
1. $x - y \in L$
   Это xy^{-1} в аддитивной записи, то есть $(L, +)$ является подгруппой в группе $(K, +)$
2. $xy \in L$, то есть L замкнуто относительно умножения

Зам. Подмножество L является подкольцом, если оно является кольцом относительно операций $(K, +, \cdot)$

Примеры:
1. $(\mathbb{Z}, +, \cdot)$ — кольцо целых чисел
   Это коммутативное кольцо с «1»
2. Другие числовые кольца: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
   Коммутативные кольца с «1»
3. $(M_n(\mathbb{R}), +, \cdot)$ — полное матричное кольцо
   не коммутативное кольцо с «1»
4. $\mathbb{Z}_m$ — кольцо вычетов по модулю m
   $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$

Фиксируем $m \in \mathbb{N}, m > 1$
Рассмотрим остаток от деления произвольного $n \in \mathbb{Z}$ на m
Все целые числа можно разбить на смежные классы по подгруппе $m\mathbb{Z}$,
то есть $\mathbb{Z} = \{0\}_m \cup \{1\}_m \cup \ldots \cup \{m-1\}_m$, где $\{r\}_m = r + m\mathbb{Z} = \{r + mk \mid k \in \mathbb{Z}\}$
На множестве смежных классов $\mathbb{Z}/m\mathbb{Z}$ введены две операции:
1. $\{k\}_m + \{l\}_m = \{k + l\}_m$
2. $\{k\}_m \cdot \{l\}_m = \{kl\}_m$

$(\mathbb{Z}_m, +, \cdot)$ — коммутативное кольцо с единицей $(1 + m\mathbb{Z} = \{1\}_m)$

Пример:
$\mathbb{Z}_4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Если $ab = 0$ при $a \neq 0$ и $b \neq 0$ в кольце K, то a называется **левым**, а b — **правым делителями нуля**

Коммутативное кольцо с «1» $(\neq 0)$ и без делителей нуля называется **целостным кольцом** (областью целостности)

Утв. Нетривиальное коммутативное кольцо с «1» является целостным $\leftrightarrow$ в нем выполняется *«закон сокращения»*: $\forall a, b, c$ из $ab = ac$ при $a \neq 0$ следует, что $b = c$

<u>*Док-во:*</u>

«$\rightarrow$»*Необходимость*

Пусть K — область целостности

$ab = ac, a \neq 0$

$ab - ac = 0$

$a(b - c) = 0$

$\Rightarrow b - c = 0$, так как $a \neq 0$

«$\leftarrow$» *Достаточность*

Есть закон сокращения из $ab = 0 = a \cdot 0$

$\begin{cases} a = 0 \\ a \neq 0,\ b \neq 0 \end{cases}$ — нет делителей нуля

$\Rightarrow$ кольцо целостное

#

Пусть K — коммутативное кольцо с «1», тогда $K[x]$ — **кольцо многочленов** от переменной x с коэффициентами из K

Пример:

$\mathbb{R}[x]$ — многочлены от x с вещественными коэффициентами

Лекция #18

В кольце многочленов $K[x]$ можно находить *НОД* с помощью **алгоритма Евклида**

Дано: $a, b \in K[x]$, $\deg a \geqslant \deg b$
$a = q_1 b + r_1, \ \deg r_1 < \deg b$
$b = q_2 r_1 + r_2, \ \deg r_2 < \deg r_1$
$r_1 = q_3 r_2 + r_3$
$r_{k-2} = q_k r_{k-1} + r_k$
$r_{k-1} = q_{k+1} r_k$
$r_{k+1} = 0$
У нас есть убывающая последовательность неотрицательных целых чисел
$\Rightarrow$ она обрывается, а это возможно, только за счет обращения в ноль остатка
Тогда *НОД*$(a, b) = r_k$

Утв. В кольцах многочленов $K[x]\ \forall a, b \in K[x]$: НОД$(a, b) = au + bv$, где $u, v \in K[x]$

Подмножество I кольца K называется **двусторонним идеалом**, если

1. $(I, +)$ является *подгруппой в аддитивной группе* кольца K
2. $\forall a \in I$ и $\forall k \in K : ak$ и $ka \in I$
   При умножении на элемент из идеала получается элемент из идеала

Пример:

1. $m\mathbb{Z} \subset \mathbb{Z}$
   $(m\mathbb{Z}, +)$ — подгруппа в $\mathbb{Z}$
   $mb \in I$ и $\forall k \in \mathbb{Z} \Rightarrow mbk = bkm \in m\mathbb{Z}$
2. $\langle x^2 + 1 \rangle = \{(x^2+1)f(x) \,|\, f(x) \in \mathbb{R}[x]\}$

Зам. Идеал I *всегда* является *нормальной подгруппой в аддитивной группе* кольца, так как по определению является подгруппой в абелевой группе

Так как I — нормальная подгруппа в $(K, +)$, можно рассматривать факторгруппу $(K/I, +)$
Введем на ней умножение $(a + I)(b + I) = ab + I$, тк $aI = Ib = I$

Множество K/I — *множество смежных классов* — с двумя операциями *(«+» и «·»)* называется **факторкольцом** кольца K по идеалу I

Пример:
$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}m$

Поля

Элемент a в коммутативном кольце с «1» называется **обратимым**, если
$\exists a^{-1} \in K : aa^{-1} = a^{-1}a = 1$

Зам. Множество всех обратимых элементов кольца образует *группу по умножению*
Обозначение: K^* — мультипликативная группа кольца

Пример
$\mathbb{C}^*$, $\mathbb{R}^*$, $\mathbb{Z}_p^*$, p — простое

Идеал называется **главным**, если $\exists a \in K : I = aK$ (см. Примеры)

Пусть $(K_1, +, \cdot)$ и $(K_2, \oplus, \times)$ — кольца
Отображение $f : K_1 \to K_2$ называется **гомоморфизмом колец**, если

1. $\forall a, b \in K_1 : f(a + b) = f(a) \oplus f(b)$
2. $\forall a, b \in K_1 : f(a \cdot b) = f(a) \times f(b)$

Зам. Если a, b — взаимно простые многочлены, то $\exists u, v \in K[x] : au + bv = 1$
Это равенство может использоваться как определение взаимной простоты

Поле P — это коммутативное кольцо с «1» $\neq 0$, в котором *каждый ненулевой элемент обратим*

Примеры:
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ — числовые поля

Подмножество поля, которое само является полем относительно тех же операций, называется **подполем**

Пример:
$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ — цепочка подполей

Кольцо $\mathbb{Z}_m$ является полем $\Leftrightarrow m = p$

Поле, не обладающее никаким собственным (не совпадающем с полем и нетривиальным) подполем, называется **простым**

Пусть P — поле
Характеристикой поля называется наименьшее $p \in \mathbb{N}$: $1 + .. + 1 = 0$ (p раз)
Если такого p не существует, то характеристика равна 0
Обозначение: $char\ P$

Пример:
$char\, \mathbb{Q} = char\, \mathbb{R} = char\, \mathbb{C} = 0$
$char\, \mathbb{Z}_p = p$

Зам. $\forall$ поле характеристики 0 *бесконечно*

Утв. $char\ P = \begin{cases} 0 \\ p \text{ - простое} \end{cases}$

<u>*Док-во:*</u>
Пусть $p > 0 \rightarrow \mathrm{char}\ P \geqslant 2$, так как «1» $\neq 0$
Если $\mathrm{char}\ P = mk, m, k > 1$, то есть характеристика — составное число
$0 = 1 + .. + 1 = (1 + .. + 1)(1 + .. + 1)$
$0 = \mathrm{char}\ P = mk$
Скобки не равны 0, так как $\mathrm{char}\ P$ — минимальное натуральное число по определению
$\Rightarrow mk = 0$ — есть делители нуля
$\Rightarrow$ противоречие с определением поля
#

<u>**Теорема о гомоморфизме колец**</u>
Пусть $f : K_1 \rightarrow K_2$ — гомоморфизм колец
Тогда $K_1 / \mathrm{Ker} f \simeq \mathrm{Im} f$

Зам. $\mathrm{Ker} f$ — ядро гомоморфизма колец — *всегда является идеалом*

Лекция #19

Зам. Пересечение $\forall$ подполей данного поля является *снова полем*

В $\forall$ поле существует наименьшее по включению подполе, оно называется **простым подполем**

Утв. Пусть P — поле, P_0 — его простое подполе
Тогда
1. Если $char\ P = p > 0$, где p — простое, то $P_0 \simeq \mathbb{Z}_p$
2. Если $char\ P = 0$, то $P_0 \simeq \mathbb{Q}$

<u>*Док-во:*</u>
Рассмотрим $\langle 1 \rangle$ — циклическую подгруппу $(P, +)$ по сложению, порожденную нейтральным элементом
Заметим, что $\langle 1 \rangle$ является подкольцом P
Так как $\forall$ подполе P всегда содержит «1», то $\langle 1 \rangle \subseteq P_0$
1. Если $char\ P = p > 0$, где p — простое, то $\langle 1 \rangle \simeq \mathbb{Z}_p$
   А $\mathbb{Z}_p$ является полем $\Rightarrow P_0 \simeq \mathbb{Z}_p$
2. Если $char\ P = 0$, то $\langle 1 \rangle \simeq \mathbb{Z}$

Так как P_0 должен содержать $\langle 1 \rangle$ и все обратные элементы по умножению, то P_0 образуют дроби вида $\dfrac{a}{b}$, где $a, b \in \langle 1 \rangle$ и $b \neq 0$
Это множество изоморфно $\mathbb{Q}$
#

Если P_1 — подполе поля P_2 , то P_2 называется **расширением** P_1

Элемент $\alpha \in P_2$ называется **алгебраическим элементом** над полем P_1 $(P_1 \subseteq P_2)$, если $\exists f(x) \in P_1[x], f(x) \neq 0 : f(\alpha) = 0$
Если это не так, то α называется **транцендентным** над P_1

Примеры:
1. $\sqrt{2}$ является алгебраическим над $\mathbb{Q}$
   $f(x) = x^2 - 2 \in \mathbb{Q}[x]$
2. π является трансцендентным

Если $P_1 \subset P_2$ и $a \in P_2$, то говорят, что F — **подполе, полученное расширением** P_1 с помощью a, если это пересечение всех подполей, содержащих P_1 и a

Пример:
$P_1 = \mathbb{Q} \qquad P_2 = \mathbb{R}$
$a = \sqrt{2}$
$F = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

Минимальным многочленом для алгебраического элемента $\alpha \in P_2$ называется многочлен $f(x) \neq 0$ и $f(x) \in P_1[x]$ такой, что его степень минимальна среди многочленов, для которых выполняется $f(\alpha) = 0$ и старший коэффициент $= 1$

Пусть f — гомоморфизм колец, то есть $f : K_1 \to K_2$ и f «уважает» сложение и умножение
Тогда

$$\mathrm{Ker} f = \{r \in K \mid f(r) = 0\} \subseteq K_1$$
$$\mathrm{Im} f = \{f(r) \mid r \in K_1\} \subseteq K_2$$

<u>Лемма</u>

$\mathrm{Ker}\, f$ *всегда является идеалом* K_1

<u>Док-во:</u>

f — гомоморфизм групп $(K_1, +)$ и $(K_2, +)$, так как гомоморфизм колец всегда является гомоморфизмом аддитивных групп

$\Rightarrow \mathrm{Ker}\, f$ является подгруппой в абелевой группе $(K_1, +)$

Осталось доказать, что $\forall a \in \mathrm{Ker}\, f$ и $\forall r \in K_1$: $ar, ra \in \mathrm{Ker}\, f$

$f(a) = 0$ — по определению ядра гомоморфизма колец

$f(ar) = f(a) \cdot f(r) = 0 \Rightarrow ar \in \mathrm{Ker}\, f$

$f(ra) = f(r) \cdot f(a) = 0 \Rightarrow ra \in \mathrm{Ker}\, f$

$\Rightarrow \mathrm{Ker}\, f$ является идеалом K_1

#

Зам. $\mathrm{Im}\, f$ является подкольцом в K_2, так как это множество замкнуто относительно операций «+» и «·»:

$f(a) + f(b) = f(a + b) \in \mathrm{Im}\, f$

$f(a) \cdot f(b) = f(ab) \in \mathrm{Im}\, f$

<u>Теорема о гомоморфизме колец</u>

Пусть $f : K_1 \to K_2$ — гомоморфизм колец

Тогда $K_1 / \mathrm{Ker}\, f \simeq \mathrm{Im}\, f$

<u>Док-во:</u>

По лемме $\mathrm{Ker}\, f$ является идеалом I в K_1

$\forall$ идеал является нормальной подгруппой в $(K_1, +)$

Так как f — гомоморфизм групп $(K_1, +)$ и $(K_2, +)$, то справедлива *теорема о гомоморфизме групп*

Рассмотрим отображение из теоремы: $\tau(a + I) = f(a)$

В теореме доказано, что τ — изоморфизм групп по сложению

Осталось доказать, что τ — изоморфизм колец, то есть «уважает» умножение

Рассмотрим произведение двух элементов из K_1/I : $(a + I)(b + I)$

$\tau((a + I)(b + I)) = \tau(ab + I) = f(ab) = f(a) \cdot f(b) = \tau(a + I) \cdot \tau(b + I)$

$\Rightarrow \tau$ «уважает» умножение

$\Rightarrow \tau$ является гомоморфизмом не только групп, но и колец

$\Rightarrow \tau$ — изоморфизм колец

#

Лекция #20

Теор. <u>Китайская теорема об остатках</u>

Пусть $n_1, .., n_m$ — натуральные, попарно взаимно простые, тогда $\mathbb{Z}_{n_1} \times .. \times \mathbb{Z}_{n_m} \simeq \mathbb{Z}_n$,
где $n = n_1 \cdot ... \cdot n_m$

Утв. Кольцо $\mathbb{Z}_n$ является полем $\Leftrightarrow n = p$ — простому числу

<u>Док-во:</u>
$n = mk$ — составное, $m, k < n$, то $\overline{m} \neq \overline{0}$ и $\overline{k} \neq \overline{0}$ и $\overline{m}\overline{k} = \overline{mk} = \overline{n} = \overline{0}$
$\Rightarrow \overline{m}$ и $\overline{k}$ являются делителями нуля
$\Rightarrow$ это не поле
Покажем, что если $p = n$, то $\mathbb{Z}_p$ является полем
Оно, как и любое $\mathbb{Z}_n$, является коммутативным кольцом с «1»
Нам нужно показать, что для всех $\overline{a} \neq 0 \, \exists$ обратный по умножению
$a \in \{1,2,..,p-1\}$, то a взаимно просто с $p \Rightarrow \exists u, v \in \mathbb{Z}$:
$au + pv = 1 = $ НОД(a, p)
$\overline{a}\,\overline{u} = \overline{1} \mod p$
Это означает, что $\overline{u} = (\overline{a})^{-1}$ это и есть обратный
#

Утв. Факторкольцо $P[x]/\langle f(x) \rangle$ является полем $\Leftrightarrow$ многочлен $f(x)$ *неприводим* над полем P

<u>Док-во:</u>
Если многочлен $f(x)$ не является неприводимым, то $f(x) = f_1(x) \cdot f_2(x)$, где $\deg f_i < \deg f(x)$
Тогда $\overline{f_1}, \overline{f_2}$ отличны от $\overline{0}$, но $\overline{f_1} \cdot \overline{f_2} = \overline{f} = \overline{0}$
$\overline{f_1} = (f_1 + I)$
$\langle f(x) \rangle \Rightarrow$ в $P[x]/\langle f(x) \rangle$ есть делители нуля и оно не является полем
Покажем, что если $f(x)$ неприводим, то любой класс вычетов $\overline{a(x)} \neq \overline{0}$ обратим
$\mathbb{R}[x]/\langle x^2 + 1 \rangle \simeq \mathbb{C}$
$\deg(a + bx) < \deg(x^2 + 1)$
Представитель $\overline{a(x)}$ это многочлен $a(x)$ с $\deg a(x) < \deg f(x)$, так как f неприводим, то по алгоритму Евклида $\exists b(x), c(x) \in P[x]$
$a(x)b(x) + c(x)f(x) = 1 = $ НОД(a, f), где $c(x)f(x) \in I = \langle f(x) \rangle$
$\Rightarrow \overline{a}(x) \cdot \overline{b}(x) = \overline{1} \mod I \Rightarrow \overline{b}(x)$ является обратным по умножению
#

<u>Теорема (без доказательства)</u>
Пусть P — произвольное поле и $f(x) \in P[x]$, тогда *всегда существует расширение* этого поля $F (P \subseteq F)$, в котором $f(x)$ имеет корень

<u>Теорема (без доказательства)</u>
1. Число элементов конечнго поля *всегда* p^n, где p — простое, $n \in \mathbb{N}$
2. $\forall p$ — простое и $\forall n \in \mathbb{N} \exists!$ (с точностью до изоморфизма) поле из p^n элементов

Зам. $\forall$ подполе поля F_{p^n} изоморфно F_{p^m}, где m делит n

<u>Теорема (без доказательства)</u>
$\forall$ конечное поле F_{p^n} можно рассмотреть в виде факторгруппы $\mathbb{Z}_p[x]/\langle h(x) \rangle$, где $\langle h(x) \rangle$ — главный идеал, порожденный *неприводимым* многочленом степени $n - h(x)$

Пример:
F_4 можно реализовать как $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle \simeq F_4$, неприводимый над $\mathbb{Z}$
Смежные классы: $\overline{0}, \overline{1}, \overline{x}, \overline{x + 1}$

Линейная алгебра

Пусть V — произвольное множество, на котором заданы две операции:

1. Сложение, то есть $\forall x, y \in v \exists x + y \in V$
2. Умножение на число, то есть $\forall \alpha \in \mathbb{F} : \alpha x \in V$, где $\mathbb{F}$ — поле

Множество V называется **линейным (векторным) пространством** над полем $\mathbb{F}$, если выполняются следующие 8 свойств:

$\forall x, y, z \in V$ и $\forall \alpha, \beta \in \mathbb{F}$

1. $(x + y) + z = x + (y + z)$ — ассоциативность сложения
2. $\exists 0 \in V : \forall x \in Vx + 0 = 0 + x = x$ — нейтральный элемент по сложению
3. $\exists (-x) : x + (-x) = 0$ — элементы обратимы по сложению
4. $x + y = y + x$ — коммутативность сложения
5. $\exists 1 \in F : 1 \cdot x = x$ — нейтральный элемент по умножению
6. $(\alpha\beta)x = \alpha(\beta x)$ — ассоциативность умножения на число
7. $(\alpha + \beta)x = \alpha x + \beta x$ – дистрибутивность относительно умножения на вектор
8. $\alpha(x + y) = \alpha x + \alpha y$ — дистрибутивность относительно умножения на число

Вектор — это элемент векторного пространства

Примеры:

1. V_3 — геометрические векторы
2. $F^n = \{(x_1, . . , x_n) \,|\, x_i \in F\}$ — n-мерное арифметическое пространство
   Операции введены покоординатно
   $x + y = (x_1 + y_1, . . , x_n + y_n)$
   $\lambda x = (\lambda x_1, . . , \lambda x_n), \lambda \in F$
3. $F^\infty = \{(x_1, ...) \,|\, x_i \in F\}$
4. $C[a, b]$ — множество функций, непрерывных на отрезке $[a, b]$
   $\forall f_i(x) \in C[a, b]$
   $\Rightarrow f_1(x) + f_2(x) \in C[a, b]$
   $\forall \alpha \in \mathbb{R} : \alpha f(x) \in C[a, b]$
   $\Rightarrow C[a, b]$ является линейным пространством
   Примеры:
   $C[0,\pi]$, $\sin x$ и $\cos x$ является векторным пространством
   Аналогично можно ввести:
   $C^k[a, b]$ — это функции, имеющие непрерывную производную до k-того порядка включительно
   $C^\infty[a, b]$ — это множество гладких функций

Если K — кольцо, то $K(x) = \left\{ \frac{f_1(x)}{f_2(x)} \,\middle|\, f_i(x) \in K[x], f_2(x) \neq 0 \right\}$ называется **полем частных**

Лекция #21

Подмножество H линейного пространства называется **подпространством** в V, если оно *само является линейным пространством относительно операций* в V

Зам. Для проверки того, что подмножество H является подпространством, достаточно проверить, что $\forall x^1, x^2 \in H$ и $\forall \lambda \in \mathbb{F}$:

1. $x^1 + x^2 \in H$
2. $\lambda x^1 \in H$

Примеры:

1. $\forall$ прямая, проходящая через начало координат в V_3
2. Пусть дана ОСЛАУ $Ax = 0$ и число неизвестных $= n$
   Пусть L — множество решений этой СЛАУ
   По свойствам решений СЛАУ $x^1 + x^2$ является решением, если x^1, x^2 — решение,
   и λx^1 является решением, если x^1 — решение
   $\Rightarrow L$ является подпространством в $\mathbb{R}^n$

Базисом в линейном пространстве V называется упорядоченный набор $b_1, .., b_n$ такой, что:

1. $b_1, .., b_n$ — линейно независимы
2. $\forall x \in V$ выражается как линейная комбинация $b_1, .., b_n$,

   то есть $x = \alpha_1 b_1 + .. + \alpha_n b_n = \begin{pmatrix} b_1 & . & . & b_n \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$

Коэффициенты $\alpha_1, .., \alpha_n$ разложения вектора x по базису $\beta = b_1, .., b_n$ называются его **координатами** в базисе β

Утв. Если $b_1, .., b_n$ — базис в V, то коэффициенты $\alpha_1, .., \alpha_n$ $\forall x \in V$ *определены однозначно*

<u>*Док-во:*</u>

$x = \alpha_1 b_1 + .. + \alpha_n b_n = \alpha_1' b_1 + .. + \alpha_n' b_n$

$\Leftrightarrow$

$(\alpha_1 - \alpha_1')b_1 + .. + (\alpha_n - \alpha_n')b_n = 0$

Следовательно, так как $b_1, .., b_n$ — базис, то

$$\begin{cases} \alpha_1 = \alpha_1' \\ \vdots \\ \alpha_n = \alpha_n' \end{cases}$$

$\Rightarrow$ Коэффициенты определены однозначно

#

Зам. Сложению векторов соответствует сложение координат, а умножению вектора на число — умножение координат на число

Зам. Это означает, что $\forall$ конечномерное пространство изоморфно арифметическому пространству F^n

Изоморфизм:

Берем в V фиксированный базис $b_1, .., b_n$

$$x \mapsto \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in F^n$$

x — произвольный вектор

Максимальное количество линейно независимых векторов в данном линейном пространстве называют его **размерностью**
Обозначение: $\dim V$

Утв. Если в линейном пространстве V существует базис из n векторов, то $\dim V = n$

Примеры:
1. $\dim \mathbb{R}^n = n$
   $\mathbb{R}^n$ — арифметическое пространство
   Стандартный базис:
   $e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$
2. Пусть L — пространство решений ОСЛАУ $Ax = 0$ в $\mathbb{R}^n$
   По теореме о структуре общего решения ОСЛАУ $\forall x \in L$ можно представить в виде:
   $x = c_1\phi_1 + .. + c_{n-r}\phi_{n-r}$, где $r = \operatorname{Rg} A$, $\phi_1, .., \phi_{n-r}$ — это ФСР и векторы, ее образующие линейно независимы
   $\Rightarrow$ ФСР является базисом в пространстве решений ОСЛАУ
   $\dim L = n - r = n - \operatorname{Rg} A$
3. $P[a, b]$ — множество многочленов от x на отрезке $[a, b]$
   Это бесконечномерное линейное пространство, так как $\forall n \in \mathbb{N}$ многочлены $1, x, x^1, .., x^n$ линейно независимы
   $(\alpha_0 1 + \alpha_1 x + .. + \alpha_n x^n) \equiv 0$
   $\Rightarrow$ По основной теореме алгебры все $\alpha_i = 0$

<u>Переход к новому базису</u>
Пусть есть конеччномерное пространство V и в нем два базиса:
$A = (a_1, .., a_n)$ и $B = (b_1, .., b_n)$

Разложим векторы базиса B по базису A:
$b_1 = t_{11}a_1 + .. + t_{n1}a_n$
$\ldots$
$b_n = t_{1n}a_1 + .. + t_{nn}a_n$

Матрицей перехода от базиса A к базису B называется матрица $T_{A\to B} = \begin{pmatrix} t_{11} & \cdot & \cdot & t_{n1} \\ \vdots & & & \vdots \\ t_{1n} & \cdot & \cdot & t_{nn} \end{pmatrix}$,
то есть i-й столбец в этой матрице — это столбец координат вектора b_i в базисе A

Зам. Заметим, что определение матрицы перехода можно записать в матричной форме: $(b_1, .., b_n) = (a_1, .., a_n)T_{A\to B}$
$B = (b_1, .., b_n)$
$A = (a_1, .., a_n)$
— матрицы из векторов базиса
Определение матрицы перехода: $B = AT_{A\to B}$

Зам. Матрица перехода $T_{A\to B}$ всегда невырождена, так как векторы $b_1, .., b_n$ линейно независимы $\Rightarrow$ линейно независимы столбцы их координат $\Rightarrow \operatorname{Rg} T_{A\to B} = n \Rightarrow \det T_{A\to B} \neq 0$

Зам. Матрица перехода от B к A *равна обратной матрице перехода* от A к B, то есть $T_{B\to A} = T^{-1}_{A\to B}$
Домножим (1) справа на $T^{-1}_{A\to B}$: $bT^{-1}_{A\to B} = a \Rightarrow T_{B\to A} = T^{-1}_{A\to B}$

Утв. Пусть в линейном пространстве V даны два базиса: $A = (a_1, .., a_n)$ и $B = (b_1, .., b_n)$
Рассмотрим координаты относительно двух базисов

$x^a = \begin{pmatrix} x_1^a \\ \vdots \\ x_n^a \end{pmatrix}$ — столбец координат вектора x в базисе A

$x^b = \begin{pmatrix} x_1^b \\ \vdots \\ x_n^b \end{pmatrix}$ — столбец координат вектора x в базисе B

Тогда: $x^b = T_{A\to B}^{-1} x^a$

<u>Док-во:</u>
Докажем, что $x^a = T_{A\to B} x^b$

Запишем x в базисе A: $x = a x^a = (a_1 \quad .. \quad a_n) \begin{pmatrix} x_1^a \\ \vdots \\ x_n^a \end{pmatrix} = x_1^a a_a + .. + x_n^a a_n$

Аналогично: $x = b x^b$
$\Rightarrow a x^a = b x^b$
По определению матрицы перехода:
$b = a T_{A\to B}$
Подставим:
$a x^a = a T_{A\to B} x^b$
Так как разложение по базису единственно, то
$x^a = T_{A\to B} x^b \Rightarrow x^b = T_{A\to B}^{-1} x^a$
#

Лекция #22

Утв. Пусть $A = (a_1, .., a_n)$, $B = (b_1, .., b_n)$, $C = (c_1, .., c_n)$ — базисы в пространстве V. Тогда $T_{A\to C} = T_{A\to B} \cdot T_{B\to C}$

Док-во:
$c = bT_{B\to C}$
$b = aT_{A\to B}$
$c = aT_{A\to B}T_{B\to C} = aT_{A\to C}$
#

Подпространства

Пусть H_1, H_2 — подпространства в пространстве L
Тогда $H_1 \cap H_2$ является подпространством, а $H_1 \cup H_2$, вообще говоря, нет

Пример:
Пусть H_1 — ось абсцисс, H_2 — ось ординат, $V = \mathbb{R}^2$
$H_1 \cup H_2$ — не линейные пространства

Суммой подпространств H_1 и H_2 называется множество $H_1 + H_2 = \{x_1 + x_2 \,|\, x_i \in H_i\}$

Зам. Очевидно, что $H_1 + H_2$ является *подпространством*

Сумма подпространств называется **прямой**, если $H_1 \cap H_2 = \{0\}$
Обозначение: $H_1 \oplus H_2$

Утв. Сумма двух подпространств H_1 и H_2 *является прямой* $\Leftrightarrow \forall x \in H_1 + H_2$: представление x в виде $x = x_1 + x_2$, где $x_1 \in H_1, x_2 \in H_2$ *единственно*
Тогда x_1 называется проекцией x на H_1 вдоль H_2, а x_2 — на H_2 вдоль H_1

Док-во:
«→» Необходимость:
Пусть сумма прямая, то есть $H_1 \cap H_2 = \{0\}$
Предположим, что $x = x_1 + x_2$ и $x = y_1 + y_2$
То есть $x_1 - y_1 = y_2 - x_2$, где $x_1 - y_1 \in H_1, y_2 - x_2 \in H_2 \Rightarrow = 0$
$\Rightarrow \begin{cases} x_1 = y_1 \\ y_2 = x_2 \end{cases}$ — проекции определены однозначно

«←» Достаточночность:
Пусть представление $x = x_1 + x_2$ единственно
Предположим, что $\exists x \neq 0 : \ x \in H_1 \cap H_2$
Тогда $\forall \alpha \in \mathbb{F} : \alpha x \in H_1$ и $\alpha x \in H_2$
$\forall \beta \in H : \ (1 - \beta)x + \beta x$, где $(1 - \beta) \in H_1$ и $\beta \in H_2$
Нет однозначности $\Rightarrow$ противоречие
#

<u>Теорема</u>
Пусть H_1 и H_2 — подпространства в L
Тогда $\dim(H_1 + H_2) + \dim(H_1 \cap H_2) = \dim H_1 + \dim H_2$

<u>Следствие</u>
$\dim(H_1 \oplus H_2) = \dim H_1 + \dim H_2$

<u>Док-во:</u>
Пусть $\dim H_1 = n, \dim H_2 = m$
Рассмотрим $H_1 \cap H_2$
Если это $\neq \{0\}$, то рассмотрим базис в нем $e_1, .., e_r$, где $r = \dim(H_1 \cap H_2)$
Дополним этот базис до базисов в H_1 и H_2
(1) $e_1, .., e_r, v_1, .. v_{n-r}, w_1, .., w_{m-r}$
Весь набор (1) является базисом в $H_1 + H_2$
Найдем $\dim(H_1 + H_2)$, как количество элементов в базисе **(1)**:
$\dim(H_1 + H_2) = r + (n - r) + (m - r) = n + m - r = \dim H_1 + \dim H_2 - \dim(H_1 \cap H_2)$
#

Множество $L(a_1, .., a_k) = \{\lambda_1 a_1 + .. + \lambda_k a_k \,|\, \lambda_i \in F\}$, где $a_1, .., a_k$ — векторы из пространства L над F, называется **линейной оболочкой** векторов $a_1, .., a_k$

Зам. Очевидно, что $L(a_1, .., a_k)$ *всегда* является *линейным пространством*

Пример:
$L(j, k)$ в $\mathbb{R}^2$ с базисом i, j, k — это плоскость O_{yz}

Рангом системы векторов $a_1, .., a_k$ в линейном пространстве называется *размерность* линейной оболочки этих векторов $\dim L(a_1, .., a_k)$

Утв. *Ранг системы векторов* $a_1, .., a_k$ линейного пространства V *равен рангу матрицы*, составленной по строкам из координат векторов $a_1, .., a_k$ в некотором *фиксированном* базисе пространства V

<u>Билинейные формы</u>
Мы рассматриваем линейное пространство V над $\mathbb{R}$

Функцию $B : V \times V \to \mathbb{R}$, сопоставляющую паре векторов вещественное число, называют **билинейной формой**, если $\forall x, y, z \in V$ и $\forall \alpha, \beta \in \mathbb{R}$ выполнены свойства:
1. $B(\alpha x + \beta y, z) = \alpha B(x, z) + \beta B(y, z)$ — линейность по первому аргументу
2. $B(x, \alpha y + \beta z) = \alpha B(x, y) + \beta B(x, z)$— линейность по второму аргументу

Пример:
$\forall$ скалярное произведение является билинейной формой, обратное не справедливо

Рассмотрим базис в $V : e_1, \dots, e_n$

Разложим два вектора по базису:

$$x = \sum_{i=1}^{n} x_i e_i$$

$$y = \sum_{j=1}^{n} y_j e_j$$

$$B(x, y) = \begin{pmatrix} x = eX \\ y = eY \end{pmatrix} = B\Big(\sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} y_j e_j\Big) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j B(e_i, e_j)$$

$B(e_i, e_j)$ — это число $b_{ij} \in R$

Рассмотрим матрицу $(b_{ij}) = B$, где $i = \overline{1,n}$, $j = \overline{1,n}$

Она называется **матрицей билинейной формы**

Зам. Фиксируем базис в $V : e_1, \dots, e_n$

Пусть $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ — столбец координат вектора x, $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ — столбец координат вектора y в данном базисе

Тогда $B(x, y) = X^T_{1\times n} B_{n\times n} Y_{n\times 1}$

Пример:

В $V = \mathbb{R}^2$

$B(x, y) = 5x_1y_2$ — билинейная форма

$\begin{pmatrix} 0 & 5 \\ 0 & 0 \end{pmatrix}$ — матрица этой билинейной формы, так как

$(x_1 \quad x_2)\begin{pmatrix} 0 & 5 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 5x_1y_2$

Лемма

Если $\forall x, y \in R^n : \ x^T A y = x^T B y$, где A и B — квадратные матрицы порядка n, то $A = B$

Док-во:

Возьмем $x = e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, где 1 стоит на i-том месте, и аналогично $y = e_j$

Тогда: $a_{ij} = b_{ij}$

По определению матрицы равны

#

Лекция #23

Утв. Пусть U — матрица перехода от базиса e к базису e'.
Тогда $B' = U^T BU$, где B — матрица билинейной формы в базисе e, а B' — в базисе e'

Док-во:
$B(x, y) = (x')^T B'y'$
$x = Ux', y = Uy'$ — доказано ранее
$B(x, y) = (x)^T By = (Ux')^T BUy' = (x')^T U^T BUy'$
$\Rightarrow$ по лемме $B' = U^T BU$
#

Билинейная форма называется **симметрической**, если $B(x, y) = B(y, x) \forall x, y \in V$
Билинейная форма называется **кососимметрической**, если $B(x, y) = -B(y, x) \forall x, y \in V$

Зам. При фиксированном в V базисе существует взаимно однозначное соответствие между квадратными матрицами и билинейными формами: $B \Leftrightarrow x^T By = B(x, y)$, где $B \in M_n(\mathbb{R})$

Квадратичные формы

Однородный многочлен второй степени от n переменных, то есть

(1) $Q(x) = \sum_{i=1}^{n} a_{ii}x_i^2 + 2 \sum_{1 \leqslant i < j \leqslant n} a_{ij}x_i x_j$, где $a_{ij} \in \mathbb{R}$

называется **квадратичной формой**

Рассмотрим n-мерное пространство
Возьмем в нем базис
У произвольного вектора x есть набор координат: $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$
Тогда **(1)** задает $Q(x) : V \to R$ как функцию от вектора, она задается через координаты
$Q(x)$ всегда можно записать в виде $Q(x) = x^T Ax$, где A — симметрическая матрица
$[A]_{ij} = a_{ij}$ из (1)
Она называется **матрицей квадратичной формы**

Пример:
$Q(x)$ на $\mathbb{R}^3$:

$$Q(x) = x_1^2 + 8x_1x_2 = (x_1 \quad x_2 \quad x_3) \begin{pmatrix} 1 & 4 & 0 \\ 4 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

Зам. Если нам дана билинейная форма $B(x, y)$, то можно получить квадратичную форму, взяв $x = y$, то есть $Q(x) = B(x, x) = x^T Bx$

Зам. По квадратичной форме можно восстановить соответствующую симметрическую билинейную форму $B(x, y) = \frac{1}{2}(Q(x + y) - Q(x) - Q(y))$
Тогда говорят, что билинейная форма $B(x, y)$ получена *поляризацией из квадратичной формы* $Q(x)$

Утв. Пусть A — матрица квадратичной формы в базисе e, A' — матрица квадратичной формы в новом базисе e', S — матрица перехода от e к e', тогда $A' = S^T A S$

<u>*Док-во:*</u>
$x = Sx'$
$Q(x) = x^T A x = (Sx')^T A S x' = (x')^T S^T A S x' = (x')^T A' x'$
$\Rightarrow$ по лемме $A' = S^T A S$
#

Если $Q(x) = x^T A x$, то $\operatorname{Rg} A$ называется **рангом квадратичной формы**

<u>**Лемма**</u>
Пусть $A, U \in M_n(\mathbb{R})$, и $\det U \neq 0$
Тогда $\operatorname{Rg} AU = \operatorname{Rg} A = \operatorname{Rg} UA$, то есть при умножении на *невырожденную* матрицу ранг *не меняется*

<u>*Док-во:*</u>
$\operatorname{Rg} AU \leqslant \operatorname{Rg} A$, так как столбцы матрицы AU — это линейные комбинации столбцов матрицы A
А по теореме о ранге матрицы ранг равен максимальному количеству л.н.з. столбцов
$\operatorname{Rg} A = \operatorname{Rg} AUU^{-1} \leqslant \operatorname{Rg} AU$
$\Rightarrow \operatorname{Rg} A = \operatorname{Rg} AU$
#

Утв. <u>Об инвариантности ранга квадратичной формы</u>
Ранг матрицы квадратичной формы не зависит от выбора базиса

<u>*Док-во:*</u>
По ранее доказанному
$A' = U^T A U$, где U — матрица перехода $\Rightarrow$ U невырождена
$\operatorname{Rg} A' = \operatorname{Rg} (U^T A)U = \operatorname{Rg} U^T A = \operatorname{Rg} A$
#

Квадратичную форму $Q(x) = \alpha_1 x_1^2 + .. + \alpha_n x_n^2$, где $\alpha_i \in R, i = \overline{1,n}$, не имеющую попарные произведений, называют квадратичной формой **канонического вида**

Нормальным видом квадратичной формы называется канонический с условием
$\alpha_i \in \{-1,0,1\}$

Утв. Любую квадратичную форму можно привести к каноническому (нормальному) виду *методом Лагранжа*

Метод состоит в последовательном выделении полных квадратов, *не более одного на одну переменную*
Если на каком-то шаге переменных на квадрате не осталось, но при этом есть выражение вида cx_ix_j, то делают замену переменных, которая устроена так:

$x_1 = x_1'$
...
$x_i = x_1' - x_j'$
...
$x_j = x_i' + x_j'$
...
$x_n = x_n'$

$X = TX'$

Пример:
$Q(x) = x_1^2 - 4x_1x_2 = x_1^2 - 4x_1x_2 + 4x_1^2 + 4x_2^2 = (x_1 - x_2)^2 - 4x_2^2$
$x_1' = x_1 - x_2$
$x_2' = 2x_2$
$Q(x) = (x_1')^2 - (x_2')^2$ — нормальный вид

Теор. **Закон инерции в квадратичной форме**
Для $\forall$ двух канонических видов одной и той же квадратичной формы:
$Q_1(y_1, .., y_m) = \lambda_1 y_1^2 + .. + \lambda_m y_m^2$, где $\lambda_i \neq 0, i = \overline{1,m}$
$Q_1(z_1, .., z_k) = \mu_1 z_1^2 + .. + \mu_k z_k^2$, где $\mu_j \neq 0, j = \overline{1,k}$
Справедливо:

1. $m = k =$ рангу квадратичной формы (доказано ранее)
2. Количество положительных λ_i равно количеству положительных μ_j , называется **положительным индексом инерции** и *обозначается* i_+
   Количество отрицательных λ_i равно количеству отрицательных μ_j , называется **отрицательным индексом инерции** и *обозначается* i_-
   Пара (i_+, i_-) называется **сигнатурой квадратичной формы**

Зам. Ранг квадратичной формы равен сумме индексов инерации: $i_+ + i_-$

Зам. Если зафиксировать (i_+, i_-), то найдется *ровно одна* квадратичная форма с такими индексами инерции *с точностью до выбора базиса*

Лекция #24

Зам. $\forall$ Квадратичная форма при $x = 0$: $Q(x) = 0$, так как квадратичная форма — однородный многочлен

Квадратичная форма $Q(x)$ называется **положительно определенной**,
если $\forall x \neq 0 : Q(x) > 0$, **отрицательно определенной**, если $\forall x \neq 0 : Q(x) < 0$
Знакопеременной, если $\exists x \neq y : Q(x) < 0 < Q(y)$

Критерий Сильвестра

Квадратичная форма положительно определена $\Leftrightarrow$ последовательность главных угловых миноров *положительна*: $\Delta_1 > 0,\ \Delta_2 > 0,\ ..,\ \Delta_n > 0$

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdot & a_{1n} \\ a_{21} & a_{22} & \cdot & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

Пример:
$Q_1 = 2x_1^2 + 3x_2^2 + 4x_3^2$ над $V = \mathbb{R}^3$

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix} \Rightarrow \begin{cases} \Delta_1 = 2 \\ \Delta_2 = 6 \\ \Delta_3 = 24 \end{cases} \Rightarrow Q_1 \text{ определена положительно}$$

Следствие

Квадратичная форма отрицательно определена $\Leftrightarrow \Delta_1 < 0,\ \Delta_2 > 0,\ \Delta_3 < 0,\ ..,\ (-1)^n\Delta_n > 0$

Линейные отображения и линейные операторы

Пусть V — линейное пространство, тогда ϕ называется линейным оператором (л.о.), если $\forall x, y \in V$ и $\forall \alpha \in \mathbb{F}$ справедливо:

1. $\phi(x + y) = \phi(x) + \phi(y)$
2. $\phi(\alpha x) = \alpha\phi(x)$

(это линейность)
Обозначение: $\phi : V \to V$

Матрица линейного оператора

Фиксируем базис $e_1, .., e_n$ в V
Найдем векторы $\phi(e_1), .., \phi(e_n)$ — образы базисных векторов
Результат разложим по базису:

$$\begin{cases} \phi(e_1) = a_{11}e_1 + a_{21}e_2 + .. + a_{n1}e_n \\ \vdots \\ \phi(e_n) = a_{1n}e_1 + a_{2n}e_2 + .. + a_{nn}e_n \end{cases}, \text{ где } a_{ij} \in \mathbb{F}$$

Матрицей л.о. Называется $A = \begin{pmatrix} a_{11} & . & . & a_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & . & . & a_{nn} \end{pmatrix}$, где столбцы — векторы $\phi(e_1), .., \phi(e_n)$

Пример:
$\phi(x) = \text{пр}_L x$ — проекция на ось абсцисс
$L = L(i)$, где i — вектор из $\mathbb{R}^3$

$$\begin{cases} \phi(i) = i = 1 \cdot i + 0 \cdot j + 0 \cdot k \\ \phi(j) = 0 = 0 \cdot i + 0 \cdot j + 0 \cdot k \\ \phi(k) = 0 = 0 \cdot i + 0 \cdot j + 0 \cdot k \end{cases} \Rightarrow A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Утв. Пусть ϕ — л.о. в V, $e = \{e_1, .., e_n\}$ — базис в V и $x^e = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ — координаты вектора x в базисе e, A^e — матрица л.о. в том же базисе
Тогда $(\phi(x))^e = A^e x^e$

<u>*Док-во:*</u>
Разложим по базису:
$\phi(x) = \phi(x_1 e_1 + .. + x_n e_n)$
Применим свойства линейности:
$\phi(x_1 e_1 + .. + x_n e_n) = x_1 \phi(e_1) + .. + x_n \phi(e_n)$
Запишем через компоненты матрицы л.о.:
$x_1 \phi(e_1) + .. + x_n \phi(e_n) = x_1(a_{11} e_1 + .. + a_{n1} e_n) + .. + x_n(a_{1n} e_1 + .. + a_{nn} e_n) =$
$= (a_{11} x_1 + .. + a_{1n} x_n) e_1 + .. + (a_{n1} x_1 + .. + a_{nn} x_n) e_n$

$$\Rightarrow \begin{pmatrix} a_{11} x_1 + .. + a_{1n} x_n \\ \vdots \\ a_{n1} x_1 + .. + a_{nn} x_n \end{pmatrix} \Rightarrow A^e x^e$$

#

Утв. Пусть $e = \{e_1, .., e_n\}$ и $e' = \{e'_1, .., e'_n\}$ — два базиса в одном пространстве V,
A^e и $A^{e'}$— матрицы л.о. в этих базисах соответсвенно, T — матрица перехода от базиса e к e', тогда $A^{e'} = T^{-1} A^e T$

<u>*Док-во:*</u>
$x = Tx'$, где x — координаты в базисе e, а x' — координаты в базисе e', тогда

$$(\phi(x))^e = A^e x^e = A^e T x^{e'}$$
$$(\phi(x))^{e'} = T^{-1} (\phi(x))^e = T^{-1} A^e T x^{e'}$$

$\Rightarrow A^{e'} = T^{-1} A^e T$
#

Лекция #25

Линейные отображения

Пусть V_1 и V_2 — линейные пространства

Тогда ϕ называется **линейным отображением**, если $\phi : V_1 \to V_2$ и:

1. $\forall x \in V_1, \alpha \in \mathbb{F}: \phi(\alpha x) = \alpha\phi(x)$
2. $\forall x_1, x_2 \in V_1: \phi(x_1 + x_2) = \phi(x_1) + \phi(x_2)$

Утв. Пусть ϕ — линейное отображение из V_1 в V_2 , а $A_{\varepsilon_1\varepsilon_2}$ — матрица линейного отображения в паре базисов ε_1 (базис V_1) и ε_2 (базис V_2), то есть берем элементы из базиса $\varepsilon_1 : e_1, .., e_n$, рассматриваем их образы $\phi(e_1), .., \phi(e_n)$ и раскладываем их по базису ε_2, то есть в V_2, по столбцам матрицы стоят коэффициенты этого разложения

Пусть T_1 — матрица перехода от ε_1 к ε_1', а T_2 — матрица перехода от ε_2 к ε_2'

Тогда $A_{\varepsilon_1'\varepsilon_2'} = T_2^{-1}A_{\varepsilon_1\varepsilon_2}T_1$

Зам. Если $V_1 = V_2$, $\varepsilon_1 = \varepsilon_2 = \varepsilon$ и $\varepsilon_1' = \varepsilon_2' = \varepsilon'$, то формула принимает следующий вид: $A_{\varepsilon'} = T^{-1}A_\varepsilon T$, это формула для линейного оператора

<u>Док-во:</u>

$[x]_{\varepsilon_1'} = T_1^{-1}[x]_{\varepsilon_1}$ **(1)**

$[y]_{\varepsilon_2'} = T_2^{-1}[y]_{\varepsilon_2}$ **(2)**

Пусть $y = \phi(x)$, то есть образу x под действием ϕ

Тогда $[y]_{\varepsilon_2} = A_{\varepsilon_1\varepsilon_2}[x]_{\varepsilon_1}$ и $[y]_{\varepsilon_2'} = A_{\varepsilon_1'\varepsilon_2'}[x]_{\varepsilon_1'}$

Подставим **(1)** и **(2)** и домножим на T_2 слева:

$T_2^{-1}[y]_{\varepsilon_2} = A_{\varepsilon_1'\varepsilon_2'}T_1^{-1}[x]_{\varepsilon_1}$

$[y]_{\varepsilon_2} = T_2A_{\varepsilon_1'\varepsilon_2'}T_1^{-1}[x]_{\varepsilon_1}$

$[y]_{\varepsilon_2} = A_{\varepsilon_1\varepsilon_2}[x]_{\varepsilon_1}$

$\Rightarrow\ T_2A_{\varepsilon_1'\varepsilon_2'}T_1^{-1} = A_{\varepsilon_1\varepsilon_2}$

$\Rightarrow\ A_{\varepsilon_1'\varepsilon_2'} = T_2^{-1}A_{\varepsilon_1\varepsilon_2}T_1$

#

Зам. С каждым линейным преобразованием $\phi : V_1 \to V_2$ связаны два подпространства: $\operatorname{Ker}\phi \subseteq V_1$ и $\operatorname{Im}\phi \subseteq V_2$

Утв. Пусть $\phi : V_1 \to V_2$, $\dim V_1 = m$, $\dim V_2 = n$, тогда $\dim \operatorname{Ker}\phi + \dim \operatorname{Im}\phi = m$

<u>Док-во:</u>

Выберем в V_1 базис $e = \{e_1, .., e_m\}$

$\forall x \in V_1 : x = x_1e_1 + .. + x_me_m$

Разложим по линейности:

$\phi(x) = x_1\phi(e_1) + .. + x_m\phi(e_m)$

$\phi(e_1), .., \phi(e_m)$ — столбцы матрицы линейного отображения

$\Rightarrow \operatorname{Im}\phi = L(\phi(e_1), .., \phi(e_m))$

$\Rightarrow \dim \operatorname{Im}\phi = \operatorname{Rg} A_e$

Ядро ϕ описывается СЛАУ $A_ex = 0$ это однородная СЛАУ и размерность пространства ее решений $\dim \operatorname{Ker}\phi = m - \operatorname{Rg} A_e$

$\Rightarrow \dim \operatorname{Ker}\phi + \dim \operatorname{Im}\phi = m$

#

Зам. Пусть $\phi : V \to V$ — л.о. Тогда, вообще говоря, $V \neq \operatorname{Im} \phi \oplus \operatorname{Ker} \phi$

Пример:
$D : f \to f'$ в $\mathbb{R}_n[x]$ — многочлены степени не выше n с коэффициентами из $\mathbb{R}$
$\operatorname{Im} D = \mathbb{R}_{n-1}[x]$ — многочлены степени не выше $n-1$ с коэффициентами из $\mathbb{R}$
$\operatorname{Ker} D = L(1)$ — константы
$\dim \mathbb{R}_n[x] = n + 1$ $\quad \dim \operatorname{Im} D = n$ $\quad \dim \operatorname{Ker} D = 1$
Но при этом $\operatorname{Im} D + \operatorname{Ker} D = \mathbb{R}_{n-1}[x] \neq \mathbb{R}_n[x]$

<u>Собственные числа и собственные векторы</u>

Число $\lambda \in \mathbb{F}$ называется **собственным числом (с.з.)** линейного оператора $\phi : V \to V$, если существует вектор $v \in V, v \neq 0 : \phi(v) = \lambda v$, то есть $Av = \lambda v$, где A — матрица л.о.
При этом v называется **собственным вектором (с.в)**

Зам. Собственный вектор — это ненулевой вектор, переходящий под действием л.о. ϕ в коллинеарный себе

Множество *всех* собственных значений ϕ называется **спектром** ϕ

Примеры:
1. $A_e = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$, e_1 и e_2 — с.в., 2 и 3 — с.з.
2. $A_e = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$ — поворот на $\dfrac{\pi}{4}$ над $\mathbb{R}$ — нет с.в. и с.з.

Для произвольной квадратной матрицы A определитель $\chi_A(\lambda) = \det(A - \lambda E)$ называется **характеристическим многочленом**, а $\chi_A(\lambda) = 0$ — **характеристическим уравнением**

Матрицы A и B называются **подобными**, если существует невырожденная матрица C такая, что $B = C^{-1}AC$

Утв. Характеристические многочлены подобных матриц совпадают

<u>*Док-во:*</u>
Пусть матрицы A и B подобны, по определению $\exists C : \det C \neq 0$ и $B = C^{-1}AC$
$\chi_B(\lambda) = \det(B - \lambda E) =$
$= \det(C^{-1}AC - \lambda E) = \det(C^{-1}AC - \lambda C^{-1}C) =$
$= \det(C^{-1}(A - \lambda E)C) = \det C^{-1} \det(A - \lambda E) \det C = \det C^{-1} \det C \det(A - \lambda E) =$
$= \det(A - \lambda E) = \chi_A(\lambda)$
#

Утв. Характеристическое уравнение оператора *не зависит* от выбора базиса

<u>*Док-во:*</u>
Матрицы л.о. в разных базисах подобны: $A' = T^{-1}AT$
$\Rightarrow$ характеристическое уравнение не зависит от выбора матрицы
#

$\Rightarrow$ Можно говорить о характеристическом уравнении л.о., а не матрицы

Зам. Свободный коэффициент χ_A — это определитель матрицы A_e, а след матрицы $\operatorname{tr} A_e$ — это коэффициент при λ^{n-1} с точностью до знака $\Rightarrow$ они не зависят от базиса

Лекция #26

Теор. λ — с.з. $\Leftrightarrow$ λ — корень характеристического уравнения $\chi_A(\lambda) = 0$, когда все корни принадлежат полю

Зам. Всегда верно над $\mathbb{C}$, потому что $\mathbb{C}$ алгебраически замкнуто

Док-во:
«→» *Необходимость:*

Дано: λ — *с.з.*
Доказать: λ — *корень* $\chi_A(\lambda) = 0$
По определению с.з.: $\exists x \neq 0 : Ax = \lambda x = \lambda I x$, где I — тождественный оператор
Это все равно, что:
(1) $(A - \lambda I)x = 0$
Запишем **(1)** в некотором базисе:
$(A_e - \lambda E)x = 0$ — это однородная СЛАУ
По критерию существования ненулевого решения однородной СЛАУ с квадратной матрицей, так как СЛАУ совместна $\Rightarrow \det(A_e - \lambda E) = \chi_A(\lambda) = 0$

«←» *Достаточность:*

Дано: λ — *корень* $\chi_A(\lambda) = 0$
Доказать: λ — *с.з.*
Если λ — корень характеристического уравнения, то в заданном базисе выполняется равенство $\chi_A(\lambda) = \det(A_e - \lambda E) = 0$
Можно рассмотреть СЛАУ с матрицей $(A_e - \lambda E)$, она имеет ненулевое решение x
Это решение — набор координат некоторого вектора, для которого выполняется равенство **(1)**: $(A - \lambda I)x = 0 \Leftrightarrow Ax = \lambda x, x \neq 0$ — это определение с.з.

#

Алгебраической характеристикой собственного значения называется его *кратность* как корня характеристического уравнения

Пример:
$\chi_A(\lambda) = (\lambda - 5)^3(\lambda - 6)^2(\lambda + 3)$
$\lambda_1 = 5$ — алгебраическая кратность **3**
$\lambda_2 = 6$ — алгебраическая кратность **2**
$\lambda_3 = -3$ — алгебраическая кратность **1**

Собственным подпространством, отвечающим с.з. λ_i л.о. A, называется множество: $V_{\lambda_i} = \{x \in V \,|\, Ax = \lambda_i x\}$

Зам. V_{λ_i} — это все с.в., отвечающие $\lambda_i \cup \{0\}$
Зам. V_{λ_i} — это действительно подпространство, потому что $\forall u, v \in V$ и $\forall \alpha \in \mathbb{F}$ верно:

1. $A(u + v) = Au + Av = \lambda_i u + \lambda_i v = \lambda_i(u + v)$,
   то есть если $u, v \in V\lambda_i$, то и $(u + v) \in V\lambda_i$
2. $A(\alpha v) = \alpha Av = \alpha \lambda_i v = \lambda_i \alpha v$
   то есть если $v \in V\lambda_i$, то и $(\alpha v) \in V\lambda_i$

$\Rightarrow V\lambda_i$ замкнуто относительно сложения и умножения на число

Зам. $V\lambda_i = \operatorname{Ker}(A - \lambda_i E)$

Размерность подпространства $V\lambda_i$ называется **геометрической кратностью** с.з. λ_i

Зам. Геометрическая кратность $\lambda_i = \dim \operatorname{Ker}(A - \lambda_i E)$ и это максимальное количество л.н.з. с.в., отвечающих λ_i

Зам. Геометрическая кратность с.з. λ_i равна количеству элементов в ФСР однородной СЛАУ $(A-\lambda_i E)x = 0$

Теорема (без доказательства)
Геометрическая кратность с.з. не превышает его алгебраической кратности и всегда $\geqslant 1$

Утв. Пусть $\lambda_1,..,\lambda_k$ — с.з. л.о. A и $\lambda_i \neq \lambda_j$, где $i, j = \overline{1,k}$, а $v_1,..,v_k$ — соответствующие им с.в., тогда $v_1,..,v_k$ л.н.з.

Док-во:
Нужно доказать, что с.в., отвечающие разным с.з., л.н.з.
Докажем, применив принцип матиндукции
При $k = 1$ это верно, так как с.в. по определению $\neq 0 \Rightarrow$ л.н.з
Пусть утверждение уже верно при $k = m$
Добавим еще один вектор e_{m+1}, соответствующий λ_{m+1}
Докажем, что система $e_1, e_2, .., e_m, e_{m+1}$ осталась л.н.з.:
(2) $\alpha_1 e_1 + \alpha_2 e_2 + .. + \alpha_m e_m + \alpha_{m+1} e_{m+1} = 0$
Применим к **(2)** оператор A:
$A(\alpha_1 e_1 + \alpha_2 e_2 + .. + \alpha_m e_m + \alpha_{m+1} e_{m+1}) = A(0) = 0$
|| **(3)**
$A(\alpha_1 e_1 + \alpha_2 e_2 + .. + \alpha_m e_m + \alpha_{m+1} e_{m+1}) = \alpha_1 Ae_1 + \alpha_2 Ae_2 + .. + \alpha_m Ae_m + \alpha_{m+1} Ae_{m+1}$
Так как $Ae_i = \lambda_i e_i$
$\alpha_1 Ae_1 + \alpha_2 Ae_2 + .. + \alpha_m Ae_m + \alpha_{m+1} Ae_{m+1} = \alpha_1 \lambda_1 e_1 + \alpha_2 \lambda_2 e_2 + .. + \alpha_m \lambda_m e_m + \alpha_{m+1} \lambda_{m+1} e_{m+1}$
Умножим **(2)** на λ_{m+1} и вычтем из **(3)**:
$\alpha_1(\lambda_1 - \lambda_{m+1})e_1 + \alpha_2(\lambda_2 - \lambda_{m+1})e_2 + .. + \alpha_m(\lambda_m - \lambda_{m+1})e_m = 0$
$\Rightarrow$ По индукции векторы $e_1, .., e_m$ л.н.з.
Из определения линейной независимости:
$$\begin{cases} \alpha_1(\lambda_1 - \lambda_{m+1}) = 0 \\ \vdots \\ \alpha_m(\lambda_m - \lambda_{m+1}) = 0 \end{cases}$$
Так как все с.з. различны $\Rightarrow$ все $\alpha_i = 0, i = \overline{1,m}$
$\Rightarrow$ (2) можно записать в виде: $\alpha_{m+1} e_{m+1} = 0$
И так как e_{m+1} это с.в. , он $\neq 0$ по определению $\Rightarrow \alpha_{m+1} = 0 \Rightarrow \alpha_1 = \alpha_2 = .. = \alpha_m = \alpha_{m+1} = 0$
$\Rightarrow$ По определению $e_1, e_2, .., e_m, e_{m+1}$ образуют л.н.з. систему
$\Rightarrow$ По определению матиндукции это верно $\forall k$
#

Утв. Матрица л.о. A является диагональной в данном базисе $\Leftrightarrow$ все векторы этого базиса являются с.в. для A

Док-во:
«→» Необходимость:

Дано: A_e диагональна

Доказать: базис e состоит из с.в. л.о. A

По определению матрицы л.о. в j-том столбце A_e стоят координаты вектора $A(e_j)$ — образа j-того базисного вектора

Если матрица диагональна, столбец имеет вид $\begin{pmatrix} 0 & .. & 0 & \lambda_j & 0 & .. & 0 \end{pmatrix}^T$

$A(e_j) = 0 + .. + \lambda_j e_j + .. + 0$, то есть по определению e_j — с.в. с с.з. λ_j

$e_j \neq 0$ так как является элементом базиса

Это верно $\forall j \Rightarrow$ все e_j — собственные, а на диагонали стоят соответствующие с.з.

«←» Достаточность:

Дано: базис $e = \{e_1, .., e_n\}$ состоит из с.в.

Доказать: A_e диагональна

По определению с.в. $Ae_j = \lambda_j e_j$

$\Rightarrow$ по определению в матрице л.о. все элементы в j-том столбце равны 0, кроме элементов на диагонали

$\Rightarrow$ матрица диагональна

#

Оператор, для которого существует базис, в котором его матрица диагональна, называется **диагонализируемым**

Зам. Диагонализируемость эквивалентна существованию базиса из с.в.

Пример:

Существуют л.о., не являющиеся диагонализируемыми:

$A = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix}, \phi \neq \pi k, k \in \mathbb{Z}$

$\chi_A(\lambda) = \begin{vmatrix} \cos\phi - \lambda & -\sin\phi \\ \sin\phi & \cos\phi - \lambda \end{vmatrix} = \lambda^2 - 2\cos\phi\lambda + \cos^2\phi + \sin^2\phi = \lambda^2 - 2\cos\phi\lambda + 1$

$\chi_A(\lambda) = 0 \Rightarrow \lambda^2 - 2\cos\phi\lambda + 1 = 0 \Rightarrow D = 4(\cos^2\phi - 1) < 0$ при $\phi \neq \pi k$

Лекция #27

Теор. Линейный оператор диагонализируем $\Leftrightarrow$ для $\forall$ его с.з. геометрическая кратность равна алгебраической

Теор. __Достаточное условие диагонализируемости__

Если характеристическое уравнение линейного оператора, действующего в n-мерном линейном пространстве, имеет *n попарно различных* корней, принадлежащих рассматриваемому полю, то линейный оператор *диагонализируем*, т.е. существует базис, в котором матрица этого л.о. является *диагональной*

__Док-во:__

Корень характеристического уравнения принадлежит нашему полю $\Rightarrow$ ему можно сопоставить хотя бы один с.в.: v_k

Система таких векторов будет л.н.з., так как корни попарно различны, а их количество $n = \dim V$

$\Rightarrow$ Эта система образует базис в V

Этот базис состоит из с.в.

$\Rightarrow$ Матрица в нем является диагональной

#

Жорданова клетка размера $m \times m$, отвечающая с.з. λ_i — это матрица, где на диагонали стоят λ_i, а над каждой λ_i — единица, то есть матрица вида: $J_m(\lambda_i) = \begin{pmatrix} \lambda_i & 1 & . & 0 \\ 0 & \lambda_i & . & . \\ . & . & . & 1 \\ 0 & . & 0 & \lambda_i \end{pmatrix}$

Жорданова Нормальная Форма (ЖНФ) матрицы л.о. — это блочно-диагональная матрица с *жордановыми клетками* на диагонали: $J = \begin{pmatrix} J_{m_1}(\lambda_1) & 0 & . & 0 \\ 0 & J_{m_2}(\lambda_2) & . & . \\ . & . & . & 0 \\ 0 & . & 0 & J_{m_s}(\lambda_s) \end{pmatrix}$,

причем $m_1 + .. + m_s = \dim V$

__Теорема О ЖНФ__

$\forall A \in M_n(\mathbb{F})$ заменой базиса *приводится к ЖНФ* над алгебраически замкнутым полем, т.е. $\forall A \in M_n(\mathbb{F})\ \exists C : \det C \neq 0 : A = CJC^{-1}$, где J — ЖНФ, причем эта ЖНФ единственна с точностью до перестановки клеток

Зам. Если $\mathbb{F}$ не является алгебраически замкнутым полем, то эта теорема справедлива в случае, когда все корни характеристического уравнения принадлежат $\mathbb{F}$

Зам. Если матрица диагональна, то пространство V равно прямой сумме собственных подпространств $V_{\lambda_i} = \mathrm{Ker}\,(A - \lambda_i E)$

Корневым подпространством линейного оператора A, соответствующим с.з. λ_i называется множество $K_{\lambda_i} = \mathrm{Ker}\,(A - \lambda_i E)^{m_i}$, где m_i — алгебраическая кратность с.з. λ_i

Зам. K_{λ_i} является инвариантным подпространством для линейного оператора

Подпространство $H \subseteq V$ называется **инвариантным** для линейного оператора A, если $\forall y \in H : Ay \in H$

Зам. Если H — инвариантное подпространство для л.о. A, то корректно определено сужение $A|_H$ (т.е. $A_1 : H \to H$) оператора A на подпространство H

<u>Теорема (без доказательства) О расщеплении</u>
$\forall$ л.о., действующего в линейном пространстве V над $\mathbb{C}$ $V = K_{\lambda_1} \oplus .. \oplus K_{\lambda_s}$, где K_{λ_i} — корневое подпространство, соответствующее λ_i

Можно рассмотреть ограничение $A|_{K_{\lambda_i}}$ и рассмотреть его отдельно

Зам. Каждое K_{λ_i}, в свою очередь, разбивается в прямую сумму циклических подпространств, т.е. подпространств вида $L = (x, (A - \lambda_i E)x, .., (A - \lambda_i E)^{h-1}x)$ — жорданова цепочка длины h

<u>Как найти Жорданову Нормальную Форму оператора A?</u>
Она, с точностью до перестановки клеток, определяются числами q_h — число жордановых клеток $h \times h$ с λ_i на диагонали

Пример ЖНФ:

$$J = \begin{pmatrix} -3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 1 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5 & 1 & 0 \\ 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & 0 & 0 & 0 & 0 & 5 \end{pmatrix}, \text{где } \begin{matrix} \lambda_1 = -3 \\ \lambda_2 = 5 \end{matrix} \quad \Rightarrow \quad \begin{matrix} q_1(\lambda_2) = 0, & q_1(\lambda_1) = 1 \\ q_2(\lambda_2) = 1, & q_2(\lambda_1) = 0 \\ q_3(\lambda_2) = 1, & q_3(\lambda_1) = 0 \\ q_4(\lambda_2) = 0, & q_4(\lambda_1) = 0 \end{matrix}$$

Утв. Для каждого $\lambda_i : q_h = r_{h+1} - 2r_h + r_{h-1}$, где $r_h = \text{Rg}\,(A - \lambda_i E)^h$, а $r_0 = \text{Rg}\,E_n = n$

<u>Какова максимальная длина жордановой цепочки для λ_i?</u>
$\min \text{Rg}\,(A - \lambda_i E)^m = n - m_i$,
где $m \in \mathbb{N}$, n — размерность пространства V, m_i — алгебраическая кратность λ_i
Находим минимальное m, для которого ранг равен $n - m_i$

<u>Теорема Гамильтона-Кэли</u>
$\chi_A(A) = 0$, то есть, если подставить в характеристическое уравнение л.о. матрицу этого же л.о., получится нулевая матрица

Суперпозицией линейных операторов A и B называется линейный оператор $A(B(x))$, то есть последовательное применение л.о.

Зам. Очевидно, что суперпозиция $A \cdot B$ — л.о.

$AB(\lambda u + \mu v) = A(B(\lambda u + \mu v)) = A(\lambda Bu + \mu Bv) = \lambda A(Bu) + \mu A(Bv) = \lambda AB(u) + \mu AB(v)$
Это верно $\forall \lambda, \mu \in \mathbb{F}$ и $\forall u, v \in V$

Утв. Пусть A, B — л.о. на пространстве V, тогда матрицей $A \cdot B$ будет произведение матриц A и B

<u>Док-во:</u>
$(ABx)^e = (AB)^e x^e$, где e — это базис, x — столбец координат, AB — матрица л.о.
По определению: $(AB)^e x^e = A^e (Bx)^e = A^e B^e x^e$
Т.к. x произвольна, то $(AB)^e = A^e B^e$
В качестве x можно взять базисный вектор
#

Лекция #28

В прошлый раз была теорема Гамильтона-Кэли: $\chi_A(A) = 0$, $\deg \chi_A(\lambda) = n$ — размерность пространства

Минимальным многочленом л.о. A называется многочлен $\mu(\lambda) : \mu(A_e) = 0$, $\mu \neq 0$ и коэффициент при старшей степени $= 1$

Пример:

Пусть $A = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$, тогда $\begin{matrix} \chi_A(\lambda) = (\lambda - 3)(\lambda - 3)^5 \\ \mu_A(\lambda) = (\lambda - 3)(\lambda - 3)^3 \end{matrix} \Rightarrow \begin{matrix} \deg \chi_A = 6 \\ \deg \mu_A = 4 \end{matrix}$

Длина максимальной жордановой цепочки

Евклидовы пространства

Евклидово пространство — это линейное пространство над $\mathbb{R}$, в котором задано скалярное произведение, то есть ε — это пара $(V, g(x, y))$, где V, а $g(x, y)$ — это функция от двух векторных аргументов, удовлетворяющих следующим аксиомам:
$\forall x, y \in V, \forall \lambda \in \mathbb{R}$:

1. $g(x, y) = g(y, x)$ — симметричность
2. $g(x + y, z) = g(x, z) + g(y, z)$ — линейность по каждому из аргументов
3. $g(\lambda x, y) = \lambda g(x, y)$ — линейность по каждому из аргументов
   То есть это симметрическая билинейная форма
4. $g(x, x) \geqslant 0$, причем $g(x, x) = 0 \Leftrightarrow x = 0$
   То есь $g(x, x)$ — положительно определенная квадратичная форма

Зам. То есть $g(x, y)$ — билинейная симметрическая положительно определенная $(x = y)$ форма

Примеры:

1. V_3 — геометрические векторы
   $(\overrightarrow{a}, \overrightarrow{b}) = |\overrightarrow{a}| \cdot |\overrightarrow{b}| \cdot \cos \phi$
2. $V = C[a, b]$ — непрерывные функции на $[a, b]$
   $(f_1, f_2) = \int_a^b f_1(x) \cdot f_2(x) \, dx$

Пусть ε — евклидово пространство, тогда величина $\|v\| = \sqrt{(v, v)}$ называется **нормой** (длиной) вектора v в евклидовом пространстве

Примеры:

$$\|f\| = \sqrt{\int_a^b f^2(x) \, dx}$$

$$\|\sin x\| = \sqrt{\int_a^b \sin^2 x \, dx}$$

<u>Неравенство Коши-Буняковского-Шварца</u>

Утв. $\forall x, y \in \varepsilon$: $|(x, y)| \leqslant \|x\| \cdot \|y\|$

<u>Док-во:</u>

$\forall \lambda \in \mathbb{R} : (\lambda x - y, \lambda x - y) \geqslant 0$ по аксиоме 4

$\lambda(x, \lambda x - y) - (y, \lambda x - y) = \lambda^2(x, x) - \lambda(x, y) - \lambda(y, x) + (y, y) = \lambda^2\|x\|^2 - 2\lambda(x, y) + \|y\|^2 \geqslant 0$

$D \leqslant 0$

$D = 4(x, y)^2 - 4\|x\|^2\|y\|^2$

$|(x, y)| \leqslant \|x\| \cdot \|y\|$

#

<u>Следствие 1</u>

Можно определить угол между векторами x и y следующей формулой:

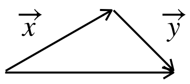
$$\cos\alpha = \frac{(x, y)}{\|x\| \cdot \|y\|} = \frac{(x, y)}{\sqrt{(x, x)} \cdot \sqrt{(y, y)}}$$

<u>Следствие 2</u>

Неравенство треугольника

Утв. $\forall x, y \in \varepsilon : \|x + y\| \leqslant \|x\| + \|y\|$

<u>Док-во:</u>



$\|x + y\|^2 = (x + y, x + y) = (x, x) + 2(x, y) + (y, y) \leqslant \|x\|^2 + 2\|x\| \cdot \|y\| + \|y\|^2 = (\|x\| + \|y\|)^2$

Так как $\|z\| \geqslant 0 \forall z \in \varepsilon$, то $\|x + y\| \leqslant \|x\| + \|y\|$

#

<u>Ортогональость</u>

Два вектора x и y из евклидового пространства ε называют **ортогональными**, если $g(x, y) = 0$, то есть их скалярное произведение равно нулю

Система векторов $\{a_1, .., a_n\}$ называется

(a) **Ортогональной**, если $\forall i, j = \overline{1,n},\ i \neq j : (a_i, a_j) = 0$

(b) **Ортонормированной,** если она ортогональна и $(a_i, a_i) = 1 \forall i = \overline{1,n}$

Утв. Пусть $\{a_1, .., a_k\}$ — ортогональная система, причем $a_i \neq 0, i = \overline{1,k}$, тогда эта система линейно независима

<u>Док-во:</u>

Пусть

(1) $\alpha_1 a_1 + .. + \alpha_k a_k = 0$

Умножим **(1)** на a_i скалярно:

$(\alpha_1 a_1 + .. + \alpha_k a_k, a_i) = (0, a_i) = 0$

$\alpha_1(a_1, a_i) + .. + \alpha_i(a_i, a_i) + .. + \alpha_k(a_k, a_i) = 0$ — тк система ортогональня

$\Rightarrow \alpha_i\|a_i\|^2 = 0$, но $a_i \neq 0$

$\Rightarrow \alpha_i = 0$ и это верно $\forall i = \overline{1,k}$

$\Rightarrow$ все $\alpha_i = 0 \Rightarrow$ по определению $\{a_1, .., a_k\}$ л.н.з.

#

Если $v_1, .., v_k$ — это ортогональная система ненулевых векторов в V, то это **ортогональный базис**

Ортогональный базис всегда можно превратить в **ортонормированный базис** (ОНБ), положив: $e_i = \dfrac{a_i}{\|a_i\|}, i = \overline{1,k}$

Зам. Пусть $x, y \in \varepsilon$ и $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ и $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ — столбцы координат векторов x и y в некотором базисе, тогда $g(x, y) = X^T \Gamma Y$, где Γ — матрица Грама

Матрица Грама $\Gamma = \begin{pmatrix} (a_1, a_1) & . & . & (a_1, a_n) \\ \vdots & \vdots & \vdots & \vdots \\ (a_n, a_1) & . & . & (a_n, a_n) \end{pmatrix}$, где a_i — векторы базиса, то есть это матрица билинейной симметрической формы, которой является скалярное произведение

Зам. В ОНБ: $(x, y) = X^T E Y = X^T Y = x_1 y_1 + .. + x_n y_n$

Зам Пусть $e_1, .., e_n$ — ОНБ в ε и $(x_1, .., x_n)^T$ — столбец координат вектора x в базисе $e_1, .., e_n$, тогда $x_i = (x, e_i), \forall i = \overline{1,n}$

<u>*Док-во:*</u>
$x = x_1 e_1 + .. + x_n e_n$
Скалярно умножим на e_i:
$(x, e_i) = x_1(e_1, e_i) + .. + x_i(e_i, e_i) + .. + x_n(e_n, e_i)$
$(e_i, e_i) = 1$, так как ОНБ
$\Rightarrow x_i = (x, e_i)$
#

<u>Процесс ортогонализации Грама-Шмидта</u>

Утв. Если ε — *конечномерное* евклидово пространство, то в нем *всегда* существует ОНБ

<u>*Док-во:*</u>
Пусть $a_1, .., a_n$ — базис в евклидовом пространстве ε, построим по нему ортогональный базис $b_1, .., b_n$
Положим, $b_1 = a_1$, он не равен нулю, так как это элемент базиса
b_2 будем искать в виде:
$b_2 = a_2 - \alpha b_1$
Коэффициент α найдем из условия ортогональности b_2 и b_1:
$(b_2, b_1) = 0$
$(a_2 - \alpha b_1, b_1) = 0$
$(a_2, b_1) - \alpha(b_1, b_1) = 0$
$\Rightarrow \alpha = \dfrac{(a_2, b_1)}{(b_1, b_1)}$
$b_2 = a_2 - \dfrac{(a_2, b_1)}{(b_1, b_1)} b_1$
Геометрически: мы вычитаем из a_2 его проекцию на b_1
Заметим, что a_1 и a_2 могут быть выражены через b_1 и b_2 и наоборот
$\Rightarrow b_1$ и b_2 л.н.з.
Пусть $b_1, .., b_k$, где $k \geqslant 2$, уже построены
Будем искать b_{k+1} в виде
(2) $b_{k+1} = a_{k+1} - \alpha_{k+1\ 1} b_1 - \alpha_{k+1\ 2} b_2 - .. - \alpha_{k+1\ k} b_k$
Коэффициент $\alpha_{k+1\ i}$ найдем из условия ортогональности b_{k+1} и b_i, где $i = \overline{1,k}$

Домножим **(2)** скалярно на b_i:
$(b_{k+1}, b_i) = (a_{k+1}, b_i) - \alpha_{k+1\ i}(b_i, b_i)$

$$\Rightarrow \alpha_{k+1\ i} = \frac{(a_{k+1}, b_i)}{(b_i, b_i)}$$

$$\Rightarrow b_{k+1} = a_{k+1} - \sum_{i=1}^{k} \frac{(a_{k+1}, b_i)}{(b_i, b_i)} b_i$$

Если переписать по-другому: $b_i = a_i - \sum_{k=1}^{i-1} \frac{(a_i, b_k)}{(b_k, b_k)} b_k$, где $i = \overline{2,n}$

Продолжаем процесс до тех пор, пока не получим ортогональную систему $b_1, .., b_n$
То есть есть система ненулевых ортогональных векторов $b_1, .., b_n$, где $n = \dim V$
Это ортогональный базис в V, так как они л.н.з., и их количество равно размерности
ОНБ получим, разделив каждый вектор на его нормаль:

$$e_i = \frac{b_i}{\|b_i\|}, \text{ где } \|b_i\| = \sqrt{(b_i, b_i)},\ i = \overline{1,n}$$

#

Лекция #29

Свойства матрицы Грама

Скалярное произведение при фиксированном базисе $a_1, .., a_n$

$(x, y) = X^T \Gamma Y$, где

X, Y — столбцы координат векторов x и y,

Γ — матрица Грама $[\Gamma]_{ij} = (a_i, a_j)$

1. Матрица Грама **симметриескас**, то есть $\Gamma = \Gamma^T$
   Это свойство скалярного произведения
   $\forall x \neq 0 : x^T \Gamma x > 0$
   $x^T \Gamma x = (x, x) = \|x\|^2$
2. Пусть e и e' — два базиса, а Γ и Γ' — их матрицы Грама
   Тогда $\Gamma' = U^T \Gamma U$, где U — матрица перехода от e к e'
   Это так, потому что Γ — матрица билинейной формы
3. Определитель матрицы Грама **всегда положителен**: $\det \Gamma > 0$

   Док-во:
   Перейдем в ОНБ
   Он всегда существует по теореме Грама-Шмидта
   Пусть U — матрица перехода от исходного базиса к ОНБ
   Тогда $\Gamma' = U^T \Gamma U$ по свойству (1)
   В ОНБ $\Gamma' = E$ по определению
   $\Rightarrow E = U^T \Gamma U$
   $\det E = 1 = \det(U^T \Gamma U) = \det U^T \det \Gamma \det U = \det \Gamma (\det U)^2$
   $\Rightarrow \det \Gamma > 0$
   #

   Определитель матрицы Грама набора векторов $a_1, .., a_k$ называется **грамианом** и обозначается $\operatorname{Gr}(a_1, .., a_k) = \det \Gamma(a_1, .., a_k)$
4. **Утв.** Определитель матрицы Грама (грамиан) **не меняется** при применения процесса <u>ортогонализации</u> Г-Ш

   Док-во:
   $a_1, .., a_n$ — исходный базис
   С помощью ортогонализации Г-Ш получаем ортогональный базис $b_1, .., b_n$
   $$U_{a \to b} = \begin{pmatrix} 1 & . & . & * \\ \cdot & 1 & & \cdot \\ \cdot & & \cdot & \cdot \\ 0 & . & . & 1 \end{pmatrix} \text{— верхнетреугольная матрица с 1 на диагонали}$$
   $\operatorname{Gr}(b_1, .., b_n) = \det \Gamma_b = \det(U^T \Gamma_a U) = \det U^T \det \Gamma_a \det U = 1 \cdot \det \Gamma_a \cdot 1 = \det \Gamma_a = \operatorname{Gr}(a_1, .., a_n)$
   #

<u>Сдедствие</u>

$\operatorname{Gr}(a_1, .., a_n) = (b_1, b_1) \cdot \ldots \cdot (b_n, b_n) = \|b_1\|^2 \cdot \ldots \cdot \|b_n\|^2$

Зам. Если a_1, a_2, a_3 — это столбцы координат некоторых линейно независимых. векторов, то $\Gamma(a_1, a_2, a_3) = A^T A$ (матрица, составленная из скалярных произведений в ОНБ), где A -- матрица, составленная и столбцов координат a_1, a_2, a_3

$\operatorname{Gr}(a_1, a_2, a_3) = \det \Gamma(a_1, a_2, a_3) = \det(A^T A) = \det A^T \det A = (\det A)^2$

Но $\det A = \langle a_1, a_2, a_3 \rangle$, а это ориентированный объем

$\Rightarrow \operatorname{Gr}(a_1, a_2, a_3) = V^2(a_1, a_2, a_3) \Rightarrow V(a_1, a_2, a_3) = \sqrt{\operatorname{Gr}(a_1, a_2, a_3)}$

Аналогично: $S(a_1, a_2) = |\det A| = \sqrt{\operatorname{Gr}(a_1, a_2)}$

Зам. В n-мерном случае принимают в виде определения: $V(a_1, .., a_n) = \sqrt{\text{Gr}\,(a_1, .., a_n)}$

Ортогональное дополнение

Пусть H — некоторое подпространство в V
Множество $\{x \in V \,|\, (x, y) = 0 \forall y \in H\} = H^{\perp}$, то есть множество векторов из V, ортогональных к каждому вектору из H, называется **ортогональным дополнением** H

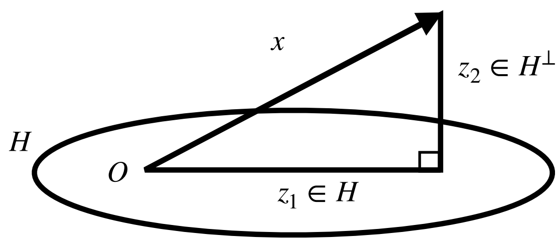
Утв. $H^{\perp}$ является линейным подпространством в V и $V = H \oplus H^{\perp}$
$\Rightarrow \dim V = \dim H + \dim H^{\perp}$

Док-во:
$\forall x, y \in H^{\perp}$ и $\forall \alpha \in \mathbb{F}$
Проверим заменутость относительно сложения и умножения на число $h \in H$:

1. $(x + y, h) = (x, h) + (y, h) = 0 \Rightarrow x + y \in H^{\perp}$
2. $(\alpha x, h) = \alpha(x, h) = 0 \Rightarrow \alpha x \in H^{\perp}$

$\Rightarrow H^{\perp}$ подпространство
Тогда можно рассматривать $H + H^{\perp}$
Покажем, что сумма прямая и равна V
Если $x \in H \cap H^{\perp}$, то $(x, x) = 0 \Leftrightarrow x = 0$ (по 4 аксиоме)
$\Rightarrow H \cap H^{\perp} = \{0\}$ и сумму прямая
Пусть $f_1, .., f_m$ — ОНБ в H (он всегда существует)
Дополним его до базиса в пространстве V векторами $f_{m+1}, .., f_n$
Применим ортогонализацию Г-Ш к $f_1, .., f_m, f_{m+1}, .., f_n$
Получим: $f_1, .., f_m, b_{m+1}, .., b_n$, где $b_{m+1}, .., b_n$ ортогональны каждому из векторов $f_1, .., f_m$
$\Rightarrow$всему H
Они принадлежат $H^{\perp}$
$\forall x \in V$ можно представить в виде: $x = x_1 f_1 + .. + x_m f_m + x_{m+1} b_{m+1} + .. + x_n b_n$
$x_1 f_1 + .. + x_m f_m = z_1 \in H$
$x_{m+1} b_{m+1} + .. + x_n b_n = z_2 \in H^{\perp}$
Значит, $V = H \oplus H^{\perp}$
#

Пусть $x = z_1 + z_2$, тогда
$z_1 \in H$ — **ортогональная проекция** x на H
$z_2 \in H^{\perp}$ — **ортогональная составляющая** x относительно H



Утв. $(L^{\perp})^{\perp} = L$, где L — подпространство

Док-во:
$\forall x \in L$ ортогонален любому вектору из $L^{\perp}$
$\Rightarrow L \subseteq (L^{\perp})^{\perp}$
А по утверждению у них одинаковая размрность
$\Rightarrow L = (L^{\perp})^{\perp}$
#

5 свойство матрицы Грама:

Утв. $a_1, .., a_k$ — л.н.з. (это может быть не базис) $\Leftrightarrow$ Gr $(a_1, .., a_k) \neq 0$

Док-во:

Пусть $\alpha_1 a_1 + .. + \alpha_k a_k = 0$ **(1)**

Умножаем **(1)** последовательно на $a_1, .., a_k$ скалярно:

$$\begin{cases} \alpha(a_1, a_1) + .. + \alpha_k(a_1, a_k) = 0 \\ \vdots \\ \alpha(a_k, a_1) + .. + \alpha_k(a_k, a_k) = 0 \end{cases}, \text{ то есть } \Gamma(a_1, .., a_k) \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{pmatrix} = 0$$

У этой ОСЛАУ существует нетривиальное решение $\Leftrightarrow$ $\det \Gamma(a_1, .., a_k) = \text{Gr}\,(a_1, .., a_k) \neq 0$

#

Лекция #30

Как найти проекцию вектора на подпространство $H = L(a_1, . . , a_k)$?

Утв. Пусть $a_1, . . , a_k$ — л.н.з., так как это базис в H, x — произвольный вектор из V.
Тогда $x = h + h^{\perp}$, где

$h = \text{пр}_H x$ — ортогональная проекция вектора x на подпространство H,

$h^{\perp}$ — ортогональная составляющая вектора относительно H.

Тогда $\text{пр}_H x = A(A^T A)^{-1} A^T x$, где

A — матрица, составленная по столбцам из $a_1, . . , a_k$

Док-во:

Так как $a_1, . . , a_k$ — базис в H, то $h = \alpha_1 a_1 + . . + \alpha_k a_k$

$x = \alpha_1 a_1 + . . + \alpha_k a_k + h^{\perp}$

Последовательно скалярно умножаем это выражение на векторы $a_1, . . , a_k$

Заметим, что $\forall i = \overline{1,n}$: $(a_i, h^{\perp}) = 0$, так как $h^{\perp} \in H^{\perp}$

$\Rightarrow$ Получаем СЛАУ относительно $\alpha_1, . . , \alpha_k$:

$$\begin{cases} \alpha_1(a_1, a_1) + . . + \alpha_k(a_1, a_k) = (a_1, x) \\ . \\ . \alpha_1(a_k, a_1) + . . + \alpha_k(a_k, a_k) = (a_k, x) \end{cases},$$

В матричной форме: $\Gamma(a_1, . . , a_k) \cdot \alpha = A^T x$, где $\alpha = (\alpha_1 . . \alpha_k)^T$

Применим свойство (5) матрицы Грама: так как $a_1, . . , a_k$ — л.н.з. $\Rightarrow \det \Gamma(a_1, . . , a_k) \neq 0$

$\Rightarrow \exists \Gamma^{-1}$, так как $\Gamma(a_1, . . , a_k) = A^T A \Rightarrow \exists (A^T A)^{-1}$

В матричной форме: $h = \text{пр}_H x = A\alpha = a_1\alpha_1 + . . + a_k\alpha_k$

$A^T A\alpha = A^T x \Rightarrow \alpha = (A^T A)^{-1} A^T x$

И окончательно: $h = A\alpha = A(A^T A)^{-1} A^T x$

#

Расстоянием от точки M, заданной вектором x, **до линейного могообразия** P называется $\rho(M, P) = \inf\limits_{n \in P} \rho(x, u) = \min\limits_{n \in P} \|x - u\|$

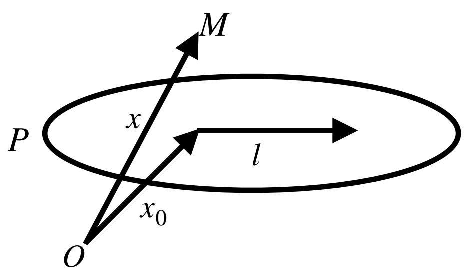
Множество решений неоднородной СЛАУ $Ax = b$ называется **линейным многообразием**

Зам. По теореме о структуре решений неоднородной СЛАУ P — линейное многообразие $\Leftrightarrow$ $P = x_0 + L$, где L — некоторое подпространсво

Зам. $\rho(M, P) =$ длине ортогональной составляющей вектора $x - x_0$, где $P = x_0 + L$

Мы ищем $\min\limits_{u \in P} \|x - u\|$, где $x - u = x - (x_0 + l) = x - x_0 + l' = \text{пр}_L(x - x_0 + l) + (x - x_0 + l)^{\perp}$, $l \in L$

$\|y\| \leqslant \|x - u\| + \|z\| \Rightarrow \min\limits_{u \in P} \|x - u\| = \|(x - x_0)^{\perp}\|$



То есть расстояние — это длина «перпендикуляра», опущенного из x на P

Утв. Расстояние $\rho(x, P)$ между точкой x и линейным многообразием $P = x_0 + L$, где $L = L(a_1, .. a_k)$, может быть найдено по формуле:
$\rho^2(x, P) = \dfrac{\mathrm{Gr}(a_1, .., a_k, x - x_0)}{\mathrm{Gr}(a_1, .., a_k)}$

Док-во:
Расстояние равно длине ортогональной составляющей вектора $x - x_0$
Применим к $a_1, .., a_k, x - x_0$:
$\mathrm{Gr}(a_n, .., a_k, x - x_0) = (b_1, b_1) \cdot ... \cdot (b_k, b_k)((x - x_0)^\perp, (x - x_0)^\perp)$
По свойству (4)
$((x - x_0)^\perp, (x - x_0)^\perp) = \rho^2$
$\mathrm{Gr}(a_1, .., a_k) \neq 0$ по свойству (5)
$\Rightarrow \rho^2 = \dfrac{\mathrm{Gr}(a_1, .., a_k, x - x_0)}{\mathrm{Gr}(a_1, .., a_k)}$
#

Линейные операторов в евклидовых пространствах

Линейный оператор $A^* : \varepsilon \to \varepsilon$ называется **сопряженным** к линейному оператору $A : \varepsilon \to \varepsilon$, если $\forall x, y \in \varepsilon$ (евклидово пространство): $(Ax, y) = (x, A^*y)$

Линейный оператор называется **самосопряжённым,** если $A = A^*$, то есть и $\forall x, y \in \varepsilon$: $(Ax, y) = (x, Ay)$

Теорема
Для любого линейного оператора $A : \varepsilon \to \varepsilon$ $\exists!$ сопряженный оператор $A^* : \varepsilon \to \varepsilon$, причем пего матрица вычисляется так: $(A^*)_b = \Gamma^{-1}(A_b)^T\Gamma$, где Γ — матрица Грама в базисе b

Следствие
Если b — ОНБ, то $(A^*)_b = (A_b)^T$

Док-во:
Покажем, что л.о. с матрицей $B = \Gamma^{-1}A^T\Gamma$ является сопряженным к данному л.о. С матрицей A
Для этого проверяем выполнение равенства $(Ax, y) = (x, By)$ $\forall x, y \in \varepsilon$
Пусть x^b, y^b — столбцы координат векторов x и y в базисе b
Тогда по доказанному ранее $(Ax)^b = A_b x^b$
$\Rightarrow$ Запишем скалярные произведения в матричной форме: $(((Ax)^b)^T\Gamma y^b) = (x^b)^T\Gamma(By)^b$,
так как $(x, y) = (x^b)^T\Gamma_b y^b$
$(x^b)^T A_b^T y^b = (x^b)^T\Gamma B_b y^b$
$\Rightarrow$ По лемме для квадратичных форм $A_b^T\Gamma = \Gamma B_b$
Так как базис состоит из л.н.з. векторов $\Rightarrow \exists\Gamma^{-1}$ по (5) свойству $\Rightarrow B_b = \Gamma^{-1}A_b^T\Gamma$ — определено однозначно
#

Следствие
Матрица линейного оператора в ОНБ является симметрической $\Leftrightarrow$ л.о. самосопряженный

Утв. Все корни характеристического уравнения самосопряженного оператора являются действительными числами

Док-во:

Пусть $\lambda_i \in \mathbb{C}$ — корень $\chi_A(\lambda) = 0$

Тогда СЛАУ $(A - \lambda_i E)x = 0$ **(1)** имеет ненулевое решение

Пусть $x = (x_1, .., x_n)^T$ — такое решение, $x_i \in \mathbb{C}, k = \overline{1,n}$

Умножим (1) на $\overline{x}^T = x^*$ (транспонированный и комплексно сопряженный вектор)

$\overline{x}^T(A - \lambda_i E)x = 0$

$\Rightarrow \overline{x}^T A x = \lambda_i \overline{x}^T x$

$\overline{x}^T x = \overline{x}_1 x_1 + .. + \overline{x}_n x_n = |x_1|^2 + .. + |x_n|^2$

Так как вектор ненулевой $\lambda_i = \dfrac{\overline{x}^T A x}{\overline{x}^T x} = \dfrac{x^* A x}{x^* x}$ — отношение Рэлея

$\overline{x}^T x$ — вещественное положительное число

$w = \overline{x}^T A x$

Покажем, что $w \in \mathbb{R}$, то есть $\overline{w} = w$

$w = w^T$ (так как это число)

$w = \underline{w^T =} (\overline{x}^T A x)^T = x^T A^T (\overline{x}^T)^T = x^T A \overline{x}$ (мы в ОНБ)

$\overline{w} = \overline{\overline{x}^T A x} = \overline{\overline{x}}^T \overline{A} \overline{x} = x^T A \overline{x} = w$

$\overline{A} = A$, так как матрица вещественная

$\Rightarrow w \in \mathbb{R} \Rightarrow \lambda_i = \dfrac{w}{\overline{x}^T x} \in \mathbb{R}$

#

Лекция #31

Теорема

Пусть λ_i — с.з. самосопряжённого оператора A

Тогда его алгебраическая кратность равна геометрической

Утв. Собственные векторы самосопряжённого л.о., отвечающие различным с.з. ортогональны

Док-во:

Пусть x_1, x_2 — с.в.

По определению: $Ax_i = \lambda_i x_i, x_i \neq 0$

$(Ax_1, x_2) = (\lambda_1 x_1, x_2) = \lambda_1(x_1, x_2)$

$||$ — так как A самосопряженный

$(x_1, Ax_2) = (x_1, \lambda_2 x_2) = \lambda_2(x_1, x_2)$

$\Rightarrow \overline{(\lambda_1 - \lambda_2)}(x_1, x_2) = 0$, где $\lambda_1 \neq \lambda_2$ по условию

#

Теорема

Для любого **самосопряжённого линейного оператора** A существует **ОНБ**, состоящий из собственных векторов. Матрица A_e нашего линейного оператора в этом базисе **диагональна**, а на диагонали стоят собственные значения, повторяющиеся *столько раз, какова их алгебраическая кратность*

Теорема (частный случай предыдущей теоремы)

Если собственные значения $\lambda_1, .., \lambda_n$ самосопряжённого линейного оператора $A : \varepsilon \to \varepsilon$, где $\dim \varepsilon = n$ попарно различны, то в ε существует ОНБ, в котором матрица имеет диагональный вид

Док-во:

Так как $\lambda_1, .., \lambda_n$ попарно различны, то выбрав для каждого λ_i соответствующий ему собственный вектор v_i, мы получим систему из n ненулевых векторов

По утверждению об ортогональности собственных векторов самосопряжённого линейного оператора это будет ортогональная система

$\Rightarrow$ По ранее доказанному утверждению она л.н.з. и в ней n векторов ($n = \dim \varepsilon$)

$\Rightarrow$ Она является базимом

Этот базис является ортогональным

ОНБ получим, взяв $e_i = \dfrac{v_i}{\|v_i\|}, i = \overline{1,n}$

Итак, существует ОНБ из собственных векторов

По ранее доказанному утверждению матрица л.о. в нем диагональна

#

Ортогональные преобразования и ортогональные матрицы

Квадратную матрицу O называют **ортогональной**, если $O^T O = E$

Пример:

$O_4 = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix}$ — матрица поворота

Свойства ортогональных матриц

1. $|\det O| = 1 \ \Rightarrow O$ невырожденна

   Док-во:
   $\det(O^T O) = \det E = 1$
   $\det(O^T O) = (\det O)^2 \Rightarrow |\det O| = 1$
   #

2. $O^{-1} = O^T$

   Док-во:
   По (1) O^{-1} существует
   Умножим определение на O^{-1} справа:
   $(O^T O)O^{-1} = EO^{-1} \quad \Rightarrow \quad O^T(OO^{-1}) = O^T E = O^T$
   $\Rightarrow O^{-1} = O^T$
   #

3. O^T тоже ортогональная матрица

   Док-во:
   $(O^T)^T O^T = E$, где $(O^T)^T = O$, а $O^T = O^{-1}$
   #

4. Произведение двух ортогональных матриц O и Q одинакового размера — ортогональная матрица

   Док-во:
   $(OQ)^T OQ = Q^T O^T OQ = Q^T EQ = Q^T Q = E$
   #

Зам. Множество всех ортогональных матриц размера $n \times n$ над $\mathbb{R}$ с матричным умножением *образует группу* $O_n(\mathbb{R})$

Линейный оператор $A : \varepsilon \to \varepsilon$ называется **ортогональным** линейным оператором, если $\forall x, y \in \varepsilon : (Ax, Ay) = (x, y)$

Зам. Говорят, что A *«сохраняет скалярное произведение»*
Зам. Ортогональный оператор мохраняет длины и угол между векторами

Док-во:
$\|Ax\|^2 = (Ax, Ax) = (x, x) = \|x\|^2$,
то есть длины не поменялись
$$\cos(Ax, Ay) = \frac{(Ax, Ay)}{\|Ax\| \cdot \|Ay\|} = \frac{(x, y)}{\|x\| \cdot \|y\|} = \cos(x, y)$$
#

<u>Теорема</u>

Пусть $A : \varepsilon \to \varepsilon$

A — ортогональный л.о. $\Leftrightarrow A$ переводит ОНБ $e_1, .., e_n$ в ОНБ $Ae_1, .., Ae_n$

<u>Док-во:</u>

«→» Необходимость:

Дано: $e_1, .., e_n$ — ОНБ, A — ортогональный л.о.

Доказать: $Ae_1, .., Ae_n$ — ОНБ

$(Ae_i, Ae_j) = (e_i, e_j) = \delta^i_j = \begin{cases} 1, \ i = j \\ 0, \ i \neq j \end{cases}$

То есть система $\{Ae_j\}$ состоит из ненулевых векторов и ортогональна $\Rightarrow$ она л.н.з.

Так как количество элементов равно $\dim \varepsilon = n$, это базис

«←» Достаточность:

Дано: $e_1, .., e_n$ и $Ae_1, .., Ae_n$ — ОНБ

Доказать: A — ортогональный л.о.

Пусть $x \mapsto \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ в базисе $e_1, .., e_n$, тогда $Ax \mapsto \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ в базисе $Ae_1, .., Ae_n$

Так как $Ax = A(x_1e_1 + .. + x_ne_n) = x_1Ae_1 + .. + x_nAe_n$

$\Rightarrow \forall x, y, \in \varepsilon : (x, y) = x_1y_1 + .. + x_ny_n$ (мы в ОНБ)

(Ax, Ay) точно так же выражаются через координаты в $\{Ae_j\}$

$\Rightarrow$ Верно соотношение $(Ax, Ay) = (x, y) \forall x, y \in \varepsilon$

#

<u>Теорема</u>

Матрица линейного оператора A в ОНБ ортогональна $\Leftrightarrow A$ — ортогональный оператор

<u>Док-во:</u>

«→» Необходимость:

Дано: A_e — ортогональная матрица

Доказать: A — ортогональный л.о.

Т$A_e^TA_e = E \Rightarrow \forall x, y \in \varepsilon$

$x^T(A_e^TA_e) = x^TEy \Leftrightarrow (A_ex)^TA_ey = x^Ty$ — матричная запись скалярного произведения

$(Ax, Ay) = (x, y) \Rightarrow A$ — ортогональный линейный оператор по определению

«←» Достаточность:

Дано: A — ортогональный л.о.

Доказать: A_e — ортогональная матрица

Рассмотрим определение: $(Ax, Ay) = (x, y) \Leftrightarrow (A_ex)^T(A_ey) = x^Ty$

$x^TA_e^TA_ey = x^TEy = x^Ty \Rightarrow$ По лемме $A_e^TA_e = E$

#

Утв. В евклидовом пространстве матрица перехода от одного ОНБ к другому ОНБ является ортогональной

<u>Док-во:</u>

Пусть O — матрица перехода от $e = (e_1, .., e_n)$ к базису $b = (b_1, .., b_n)$, оба ОНБ

По определению матрицы перехода в U по столбцам стоят координаты векторов базиса b в старом

Тогда U^TU — матрица Грама базиса b (скалярное произведение взято в ОНБ)

Второй базис тоже является ОНБ $\Rightarrow U^TU = E$, то есть U ортогональная

#

<u>Теорема о каноническом или спектральном разложении</u>

Для любой симметрической матрицы M существует такая ортогональная матрица U, что $M = U\Lambda U^T$, где $\Lambda = \begin{pmatrix} \lambda_1 & . & . & 0 \\ . & \lambda_2 & & . \\ . & & . & . \\ 0 & . & . & \lambda_n \end{pmatrix}$ — диагональная матрица, где $\lambda_1, .., \lambda_n$ — с.з. л.о. с матрицей M и они повторяются в соответствии с их кратностью

Зам. Говорят, что $\forall$ симметрическая матрица ортогональным преобразованием приводится к диагональному виду

<u>Док-во:</u>

Рассмотрим матрицу M, как матрицу некоторого самосопряжённого линейного оператора в некотором ОНБ $f = \{f_1, .., f_n\}$ — это возможно, так как M симметрична

Для самосопряжённого л.о. Всегда существует ОНБ из собственных векторов, в котором его матрица диагональна

То есть $\Lambda = T_{f\to e}^{-1} M T_{f\to e}$, где $T_{f\to e}$ — матрица перехода между двумя ОНБ

$\Rightarrow$ Она ортогональная и ее можно взять в качестве U

Так как U ортогональная, то $U^{-1} = U^T$

$\Rightarrow M = U\Lambda U^T$

#

<u>Теорема о каноническом виде ортогонального преобразования</u>

Для любого ортогонального преобразования существует ОНБ, в котором его матрица имеет следующий блочно-диагональный вид:

$$A' = \begin{pmatrix} A_{\phi_1} & . & . & . & . & . & . & . & 0 \\ . & . & & & & & & & . \\ . & & A_{\phi_k} & & & & & & . \\ . & & & 1 & & & & & . \\ . & & & & . & & & & . \\ . & & & & & 1 & & & . \\ . & & & & & & -1 & & . \\ . & & & & & & & . & . \\ 0 & . & . & . & . & . & . & . & -1 \end{pmatrix}, \text{ где } A_{\phi_j} = \begin{pmatrix} \cos\phi_j & -\sin\phi_j \\ \sin\phi_j & \cos\phi_j \end{pmatrix}$$

<u>Следствие</u>

<u>Теорема Эйлера</u>

При $n = 3$ любое ортогональное преобразование в $\mathbb{R}^3$ имеет вид

$$\begin{pmatrix} \cos\phi_j & -\sin\phi_j & 0 \\ \sin\phi_j & \cos\phi_j & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}$$

То есть является поворотом на некоторый угол ϕ относительно некоторой оси, либо композиция поворота с отражением

Лекция #32
Теорема о приведении квадратичной формы к каноническому виду ортогональным преобразованием
Приведение к главным осям
Любую квадратичную форму ортогональным преобразованием можно привести к каноническому виду

Док-во:
Матрица квадратичной формы является симметрической: $B^T = B$
Рассмотрим n-мерное евклидово пространство ε (n — число переменных в квадратичной форме Q) и некоторый ОНБ в нем
Матрица квадратичной формы B является матрицей некоторого самосопряжённого оператор в данном базисе по критерию самосопряженности в ОНБ
По теореме для самосопряжённого линейного оператора существует новый ОНБ f такой, что матрица A' линейного оператора в этом базисе диагональна, а сам он состоит из собственных векторов A
Матрица линейного оператора преобразуется по формуле:
$A' = S^{-1}AS$, где S - матрица перехода из исходного базиса в новый
Так как S является матрицей переходя от одного ОНБ к другому, то она является ортогональной и $S^{-1} = S^T$
При этом матрица квадратичной формы преобразуется по формуле: $B' = S^TBS$
$\Rightarrow A' = B'$ и матрица квадратичной формы тоже является диагональной при такой замени координат
$\Rightarrow$ Это и есть канонический вид
#

Зам. Диагональными элементами B', то есть коэффициентами канонического вида квадратичной формы являются собственные качения самосопряжённого оператора A (оператора с той же матрицей)

Утв. О QR-разложении
Пусть $A \in M_m(\mathbb{R})$ и столбцы $A_1, \ldots, A_m$ л.н.з.
Тогда существуют матрицы Q и R: $A = QR$, причем

Q - ортогональная матрица

R - верхрнетреугольная матрица с положительными элементами на главной диагонали

Док-во:
Рассмотрим $A_1, \ldots, A_m$ — столбцы матрицы A и применим к ним процесс ортогоналищации Грама-Шмидта
Получим столбцы $B_1, \ldots, B_m$, потом нормируем их и получим столбцы $Q_1, \ldots, Q_m$
$Q_1, \ldots, Q_m$ является ортонормированной системой
$\Rightarrow$ Если составить из ним матрицу $Q = (Q_1 \,|\, Q_2 \,|\, \ldots \,|\, Q_m)$, то она будет ортогональной
$A_k \in L(Q_1, \ldots, Q_m), k = \overline{1,m}$ — по формулам Грама-Шмидта, так как не берем векторы с большими номерами

$$\Rightarrow A_k = \sum_{i=1}^{k} r_{ik}Q_i, k = \overline{1,m}$$

В матричной форме$A = QR$, где $R = \begin{pmatrix} \Gamma_{11} & . & . & \Gamma_{1m} \\ . & \Gamma_{22} & & . \\ . & & . & . \\ 0 & . & . & \Gamma_{mm} \end{pmatrix}$

$\Gamma_{kk} > 0$, так как это длина соответствующего вектора B_k
#

<u>Теорема о сингулярном разложении (SVD)</u>
Для любой матрицы $A \in M_{mn}(\mathbb{R})$ справедливо сингулярное разложение: $A = V\Sigma U^T$,

где U - ортогональная матрица размера $n \times n$
V - ортогональная матрица размера $m \times m$
Σ - диагональная размера $m \times n$с числами $\sigma_i \geqslant 0$ на диагонали

σ_i называется сингулярными числами A
При этом по договорённости σ_i располагают в порядке невозростания:
$\sigma_1 \geqslant \sigma_2 \geqslant .. \geqslant \sigma_r \geqslant \sigma_{r+1} = .. = 0$

<u>Док-во:</u>
Рассмотрим матрицу A^TA, она симметрична, соответсвует квадратичной форме и неотрицательно определена
$(A^TA)^T = A^T(A^T)^T = A^TA$ — симметрична
$Q(x) = x^TA^TAx = (Ax)^TAx = (Ax, Ax) = \|Ax\|^2 \geqslant 0$ — неотрицательно определена
$\Rightarrow$ л.о. с матрицей A^TA является самосопряженным
$\Rightarrow$ Все с.з. A^TA вещественны и они $\geqslant 0$
Так как $\lambda_i = \dfrac{x^TA^TAx}{x^Tx} \geqslant 0$
Запишем с.з. A^TA в виде σ_i^2, то есть $\sigma_i = \sqrt{\lambda_i(A^TA)}$, и нумеруем их по невозрастанию
$\sigma_1 \geqslant \sigma_2 \geqslant .. \geqslant \sigma_r \geqslant \sigma_{r+1} = .. = 0$
Так как A^TA — самосопряжённый, для него существует ОНБ из собственных векторов
$A^TAu_i = \begin{cases} \sigma_i^2 u_i & ,1 \leqslant i \leqslant r \\ 0 & ,r+1 \leqslant i \leqslant n \end{cases}$, где u_i — нормированный собственный вектор
Положим $v_i = \dfrac{Au_i}{\sigma_i}$, $1 \leqslant i \leqslant r$
$(v_i, v_j) = \begin{cases} 1 & ,i = j \\ 0 & ,i \neq j \end{cases}$
Дополним систему $v_1, .., v_r$ векторами $v_{r+1}, .., v_m$ до ОНБ в $\mathbb{R}^m$
В итоге $u_i = v_i \cdot \sigma_i \;\Rightarrow\; A \cdot [u_1, .., u_n] = [v_1, .., v_m] \cdot \Sigma$

$$\Sigma = \begin{pmatrix} \sigma_1 & . & . & . & . & 0 \\ . & . & & & & . \\ . & & \sigma_r & & & . \\ . & & & 0 & & . \\ . & & & & . & . \\ 0 & . & . & . & . & 0 \end{pmatrix}$$ — диагональная матрица, на диагонали $\sigma_1 \geqslant .. \geqslant \sigma_r \geqslant 0$

$AU = V\Sigma \Rightarrow AUU^{-1} = V\Sigma U^{-1}$
$U^{-1} = U^T$
$\Rightarrow A = V\Sigma U^T$
#

Утв. <u>О полярном разложении</u>
Любой л.о. В евклидовом пространстве представляется в виде композиции симметрического и ортогонального: $A = SU$, где
S - Симметрический л.о.
U - Ортогональный л.о.

Зам. Это аналог тригонометрической формы записи комплексного числа, то есть $z = r(\cos\phi + i\sin\phi)$, где r — аналог S, а $|\cos\phi + i\sin\phi| = 1$

<u>Док-во:</u>
Возьмем сингулярное разложение для A: $A = Q\Sigma P^T$, где Q и P — ортогональные
Тогда $A = Q\Sigma EP^T = Q\Sigma(Q^TQ)P^T = (Q\Sigma Q^T)(QP^T) = SU$
U Является ортогональной, так как это произведение двух ортогональных матриц
$S^T = (Q\Sigma Q^T)^T = (Q^T)^T\Sigma^TQ^T = Q\Sigma Q^T = S$, то есть S — симметрическая
#

Сопряженное пространство

Отображение $f : V \to \mathbb{F}$, где V — линейное пространство, $\mathbb{F}$ — поле (одномерное пространство), называется **линейной формой** или **линейным функционалом**, если $\forall x, y \in V, \forall \alpha \in \mathbb{F}$:

1. $f(x + y) = f(x) + f(y)$
2. $f(\alpha x) = \alpha f(x)$

Зам. Это частный случай линейного отображения

Пусть в V фиксированный базис $e = (e_1, .., e_n)$
Тогда матрицей отображения f является матрица размера $1 \times n$ (строка)
$[f]_e = (f(e_1), .., f(e_n))$

А действие линейной формы в базисе можно записать в виде произведения:
$$f(x) = [f]_e \cdot x_e = (f(e_1), .., f(e_n))\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = f(x_1e_1 + .. + x_ne_n)$$

Лекция #33

Зам. В полярном разложении с.з. симметрическного оператора неотрицательны

Док-во:
$A = SU = (Q\Sigma Q^T)(QP^T)$
У Σ на диагонали стоят числа $\geqslant 0$ — это и есть с.з.
Это так, потому что Σ — это диагональный вид S
#

Что происходит при замене базиса?

Утв. Пусть e и g — два базиса в V, тогда $[f]_g = [f]_e T_{e\to g}$

Док-во:
Результат действия f не зависит от базиса: $[f]_g x_g = [f]_e x_e$
$x_g = T^{-1}_{e\to g} x_e$ — это для векторов
$x_e = T_{e\to g} x_g$
$\Rightarrow [f]_g x_g = [f]_e T_{e\to g} x_g$
Разложение по базису единственно, значит $[f]_g = [f]_e T_{e\to g}$
#

Пространством, **сопряженным** к линейному пространству L называется множество L^* всех линейных форм на L с операциями сложения и умножения на число $\forall x \in L, \forall \lambda \in \mathbb{F}$:

1. $(f_1 + f_2)(x) = f_1(x) + f_2(x)$
2. $(\lambda f)(x) = \lambda f(x)$

$L^* = \mathrm{Hom}\,(L, \mathbb{F})$ — множество гомоморфизмов из L в $\mathbb{F}$

Зам. Если записывать координаты элементов из L^* по столбцам, то при переходе к другому базису они преобразуются по формуле: $[f]_g^{\text{ст}} = T^T_{e\to g}[f]_e^{\text{ст}}$
Поэтому их называют **ковекторами**, а обычные — **контрвекторами**

Зам. Когда ковекторы и контрвекторы преобразуются одинаково?
Когда матрица перехода удовлетворяет условию: $U^{-1}_{e\to g} = U^T_{e\to g}$, то есть $U_{e\to g}$ ортогональна
То есть это может быть матрица перехода от одного ОНБ к другому

Зам. Градиент — ковектор

Базис $e = (e_1, .., e_n)$ в линейном пространстве L и базис $f = (f^1, .., f^n)$ в сопряжённое пространстве L^* называют **взаимными**, если $f^i(e_j) = \delta^i_j = \begin{cases} 1 & , i = j \\ 0 & , i \neq j \end{cases}$

Утв. Пусть $\dim L = n < \infty$, тогда $\forall$ базиса $\exists!$ взаимный базис в L^* и наоборот

Док-во:
Пусть дан базис $e = \{e_1, .., e_n\}$
Запишем матрицу перехода от некоторого стандартного базиса к e: $T_{s\to e}([e_1]_s, .., [e_n]_s)$

Для произвольного базиса $f = (f^1, .., f^n)$ в L^* составим матрицу $F = \begin{pmatrix} [f^1]_s \\ \vdots \\ [f^n]_s \end{pmatrix}$

Условие взаимности базисов в матричной форме: $FT_{s\to e} = E$
$\Rightarrow$ Так как $T_{s\to e}$ обратима, то $F = T^{-1}_{s\to e}$, а обратная матрица единственна
#

Пример:

В $\mathbb{R}^2$ $e_1 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ и $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, найти взаимный базис:

$A = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \Rightarrow FA = E \Rightarrow F = A^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

$\Rightarrow [f^1] = (1,0), [f^2] = (1,1)$

$f^1(x) = x_1$

$f^2(x) = x_1 + x_2$

Утв. $\forall$ евклидово пространство ε изоморфно своему сопряженному

<u>*Док-во:*</u>

Построим изоморфизм: $\forall a \in \varepsilon \mapsto^{\phi} f_a(x) = (a, x) \in \varepsilon^*$

Отображение ϕ является гомоморфизмом, так как если $a = a_1 + a_2$, то

1. $\phi(a) = (a_1 + a_2, x) = (a_1, x) + (a_2, x) = \phi(a_1) + \phi(a_2)$
2. $\phi(\lambda a) = (\lambda a, x) = \lambda(a, x) = \lambda\phi(a)$

ϕ сюръективно, так как $\forall$ линейная функция вида $a_1x_1 + .. + a_nx_n$ может быть записан в виде (a, x), где $a = (a_1, .., a_n)$

И ϕ инъективно, так как разложение по базису единственно

$\Rightarrow$Это изоморфизм

#

Если отожествлять ε и ε^*, то базис взаимный к данному называется **биортогональным**

Утв. Условие биортогональность базисов $e_1, .., e_n$ и $f_1, .., f_n$ в ε:

$$F^T\Gamma A = E, \text{ где } \begin{array}{l} A = ([e_1]_s, .., [e_n]_s) \\ F = ([f_1]_s, .., [f_n]_s) \\ \Gamma \text{ - матрица Грама базиса } S \end{array}$$

<u>*Док-во:*</u>

По определению взаимности базисов $f^i(e_j) = \delta^i_j$

$f^i(e_j) = (f^i, e_j)$

Запишем преобразование в стандартном базисе, используя матрицу Грама

Получаем $F^T\Gamma A = E$

#

Зам. Если пространство L бесконечномерно., то линейная оболочка координатных функционалов любого базиса в V строго меньше всего L^*

Пример:

$L = \mathbb{F}[x]$, то есть L^* не изоморфно L

Любому линейному отображению $A : V_1 \to V_2$ можно сопоставить сопряженное (двойственное) отображение: $V_1 \overset{A}{\to} V_2$

$$\begin{tikzcd} V_1^* & V_2^* \arrow[l, "A^*"'] \\ V_1 \arrow[u, leftrightarrow] \arrow[r, "A"] & V_2 \arrow[u, leftrightarrow] \end{tikzcd}$$

Здесь V_i^* — это пространство, сопряженное к V_i

$$A^* : V_2^* \to V_1^* \text{ по правилу: } (A^*f_2)(v_1) = f_2(Av_1), \text{ где } \begin{array}{l} f_2 \in V_2^* \\ A^*f_2 \in V_1^* \\ v_1 \in V_1 \end{array}$$

Зам. Если вместо $f(x)$, где $x \in V^*$, ввести более симметричную запись $f(x) = \langle f, v \rangle$ (сопряжение), то определение A^* можно записать в следующем виде $\langle A^* f_2, v_1 \rangle = \langle f_2, A v_1 \rangle$
В случае, когда $V_1 = V_2 = \varepsilon$, получим уже известное определение сопряженного оператора

Зам. Если $\dim L < \infty$, то $(L^*)^* \simeq L$, $f(x) = \langle f, x \rangle$

Пусть $\mathbb{F}$ — поле, V — векторное пространство над $\mathbb{F}$, V^* — сопряженное к нему, $p, q \in \mathbb{N} \cup \{0\}$
Тогда любое полилинейное отображение $f : \underbrace{V \times .. \times V}_{p} \times \underbrace{V^* \times .. \times V^*}_{q} \to \mathbb{F}$ называется **тензором** на V типа (p, q) и валентности $p + q$

Примеры:
1. Тензор типа (1,0) — это линейные функции на V, то есть элементы V^*
2. Тензор типа (0,1) — это линейные функции на V^*, то есть элементы $V^{**} \simeq V$
3. Тензор типа (2,0) — это билинейные формы на V
4. Тензор типа (1,1) — можно интерпретировать как л.о. На V

Зам. Координаты тензоров образуют многомерные аналоги обычных двухмерных матриц

Пусть A — векторное пространство над $\mathbb{F}$, снабжение дополнительной операцией умножения $* : A \times A \to A$ называется алгеброй над полем $\mathbb{F}$, если выполняются следующие свойства:
$\forall x, y, z \in A, \forall \alpha, \beta \in \mathbb{F}$
1. $(x + y) * z = x * z + y * z$
2. $x * (y + z) = x * y + x * z$
3. $(\alpha x) * (\beta y) = (\alpha\beta)(x * y)$

Алгебра называется **ассоциативной**, если операция умножения ассоциативна, и алгеброй **с единицей**, если в ней существует нейтральный элемент по умножению

Примеры:
1. Матрицы с операцией умножения — ассоциативная алгебра с единицей
2. $\mathbb{C}$ является двумерной алгеброй над $\mathbb{R}$
3. Алгебра многочленов $\mathbb{F}[x]$ — многочлены можно умножать на число, складывать и умножать друг на друга
4. Кватернионы H — это числа вида $x_1 + x_2 i + x_3 j + x_4 k$, где $x_i \in \mathbb{R}$, $i^2 = j^2 = k^2 = ijk = 1$, $\dim H = 4$ над $\mathbb{R}$

УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА
УРА УРА