Коллоквиум по алгебре
ФКН ПИ 1 курс

Арунова Анастасия

Содержание

1-й модуль

1 Определения

1.1 Дать определение умножения матриц. Коммутативна ли эта операция?

Определение. Рассмотрим A типа $n \times p$ и B типа $p \times k$. Привидением матриц A и B называют матрицу C типа $n \times k$ с элементами $c_{ij} = \sum\limits_{l=1}^{p} a_{il} \cdot b_{lj}$, $\forall i = \overline{1, n}, j = \overline{1, k}$

Замечание. Операция умножения матриц *не является коммутативной.*

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

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

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

$$A \cdot B \neq B \cdot A$$

1.2 Дать определения ступенчатого вида матрицы и канонического (улучшенного ступенчатого) вида матрицы.

Определение. Матрица M имеет ступенчатый вид, если номера столбцов первых ненулевых элементов всех строк (такие элементы будем называть ведущими) возрастают, а нулевые строки расположены в нижней части матрицы.

Определение. Матрица M имеет улучшенный ступенчатый (канонический) вид, если:

1) она имеет ступенчатый вид
2) все ведущие элементы равны 1
3) в столбце с ведущим элементом все остальные элементы равны 0

1.3 Перечислить элементарные преобразования строк матрицы.

Определение. Элементарными преобразованиями строк матрицы называют:

1) умножение i-ой строки матрицы на $\alpha \neq 0$:
   $\alpha \cdot (i) \to (i)$

2) перестановка двух строк в матрице:
   $(i) \leftrightarrow (k)$
3) добавление к i-ой строке k-ой строки с коэффициентом α:
   $(i) + \alpha \cdot (k) \to (i)$

1.4 Сформулировать теорему о методе Гаусса.

Теорема. Любую конечную матрицу можно элементарными преобразованиями привести к ступенчатому (каноническому) виду.

1.5 Дать определения перестановки и подстановки.

Определение. Всякое расположение чисел $1, \ldots, n$ в определённом порядке называют перестановкой $\alpha = (\alpha_1, \ldots, \alpha_2)$.

Определение. Подстановкой называется взаимно-однозначное отображение $1, \ldots, n$ в себя:

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

Здесь $(\sigma(1), \ldots, \sigma(n))$ – перестановка.

1.6 Выписать общую формулу для вычисления определителя произвольного порядка.

Определение. Определителем (детерминантом) порядка n, соответствующим квадратной матрице A называется число, являющееся суммой $n!$ слагаемых:

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

1.7 Выписать формулы для разложения определителя по строке и по столбцу.

Разложение по строке (столбцу):

Для любого фиксированного j справедливо: $\det A = \sum\limits_{i=1}^{n} a_{ij} A_{ij}$ – разложение по столбцу.

Для любого фиксированного i справедливо: $\det A = \sum\limits_{j=1}^{n} a_{ij} A_{ij}$ – разложение по строке.

1.8 Выписать формулы Крамера для квадратной матрицы произвольного порядка. Когда с их помощью можно найти решение СЛАУ?

Теорема. Пусть $Ax = b$ совместная СЛАУ, тогда:

$$x_i \cdot \det A = \Delta_i$$

$$\Delta_i = \det(A_1, ..., A_{i-1}, b, A_{i+1}, ..., A_n)$$

Если $\det A \neq 0$, то $x_i = \dfrac{\Delta_i}{\det A}$, $i = \overline{1, n}$.

1.9 Дать определение обратной матрицы. Сформулировать критерий её существования.

Определение. Обратной к квадратной матрице $A \in M_n(\mathbb{R})$ называется матрица

$$A^{-1} : A \cdot A^{-1} = E = A^{-1} \cdot A$$

Теорема. $\exists A^{-1} \Leftrightarrow \det A \neq 0$.

1.10 Выписать формулу для нахождения обратной матрицы.

Формула: $A^{-1} = \dfrac{1}{\det A} \cdot \widetilde{A}$.

1.11 Выписать формулу для матрицы обратной к произведению двух матриц.

Формула: $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$.

1.12 Дать определение минора.

Определение. Минором k-го порядка матрицы A называют определитель матрицы, составленной из элементов, стоящих на пересечении произвольных k строк и k столбцов из матрицы A.

1.13 Дать определение базисного минора. Какие строки называются базисными?

Определение. Любой отличный от нуля минор, порядок которого равен рангу, называется базисным минором матрицы. Строки, которые попали в базисный минор, называются базисными.

1.14 Дать определение ранга матрицы.

Определение. Рангом матрицы называют наивысший порядок отличного от 0 минора.

Определение означает, что:

1) $\exists M_{i1\ldots ir}^{j1\ldots jr} \neq 0$ (минор r-го порядка $r = \operatorname{Rg} A$)
2) все миноры порядков $r+1, r+2, \ldots$ равны 0 (или не существуют).

1.15 Дать определение линейной комбинации строк. Что такое нетривиальная линейная комбинация?

Определение. Линейной комбинацией строк (или столбцов) $a_1, \ldots, a_s$ одинаковой длины называют выражение вида:

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s = \sum_{k=1}^{s} \alpha_k a_k, \text{ где } \alpha_1, \ldots, \alpha_s \text{ – некоторые числа}$$

Определение. Линейная комбинация $\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s$ называется нетривиальной, если $\alpha_1, \ldots, \alpha_s$ не все равны 0.

1.16 Дать определение линейной зависимости строк матрицы.

Определение. Строки $a_1, \ldots, a_s$ называют линейно зависимыми, если существуют числа $\alpha_1, \ldots, \alpha_s$ не все равные 0, такие что $\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s = 0$

1.17 Дать определение линейно независимых столбцов матрицы.

Определение. Если равенство $\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s = 0$ возможно только в случае, когда $\alpha_1 = \ldots = \alpha_s = 0$, то столбцы матрицы $a_1, \ldots, a_s$ называют линейно независимыми.

1.18 Сформулировать критерий линейной зависимости.

Утверждение. $a_1, \ldots, a_s$ – линейно зависимы $\Leftrightarrow$ хотя бы один из $a_1, \ldots, a_s$ линейно выражается через другие.

1.19 Сформулировать теорему о базисном миноре.

Теорема (о базисном миноре)**.**

1) Базисные строки (столбцы), соответствующие любому базисному минору M матрицы A л.н.з.
2) Строки (столбцы) матрицы A, не входящие в M являются линейной комбинацией базисных строк.

1.20 Сформулировать теорему о ранге матрицы.

Следствие (теорема о ранге матрицы)**.** Ранг матрицы равен максимальному числу её линейно независимых строк и равен максимальному числу линейно независимых столбцов.

1.21 Сформулировать критерий невырожденности квадратной матрицы.

Следствие. Рассмотрим квадратную матрицу $A \in M_n(\mathbb{R})$. Следующие три условия эквивалентны:

(1) $\det A \neq 0$

(2) $\operatorname{Rg} A = n$

(3) все строки A линейно независимы

1.22 Сформулировать теорему Кронекера–Капелли.

Теорема. СЛАУ $Ax = b$ совместна $\Leftrightarrow \operatorname{Rg} A = \operatorname{Rg} \left(A \mid b \right)$.

2 Доказательства

2.1 Что происходит с произведением матриц при транспонировании?

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

Доказательство. A – матрица типа $m \times n$, B – матрица типа $n \times k$

$$[(A \cdot B)^T]_{ij} = [A \cdot B]_{ji} = \sum_{r=1}^{n} [A]_{jr} \cdot [B]_{ri} = \sum_{r=1}^{n} [A^T]_{rj} \cdot [B^T]_{ir} = [B^T \cdot A^T]_{ij}, \quad \begin{matrix} \forall i = \overline{1, m} \\ \forall j = \overline{1, k} \end{matrix}$$

□

2.2 Сформулировать и доказать утверждение о том, что кососимметричность для линейной функции эквивалентна обнулению на паре совпадающих элементов.

Утверждение. Для любой линейной функции кососимметричность (1) эквивалентна обнулению на паре совпадающих элементов (2).

Доказательство. Рассмотрим f – линейная функция (от столбцов).

1) (2) $\Rightarrow$ (1)
   Дано: $f(u, u) = 0$ – обнуление на паре совпадающих элементов
   Доказать: $f(u, v) = -f(v, u)$ – кососимметричность
   $$\underbrace{f(u+v, u+v)}_{=0} \overset{\text{линейность}}{=} \underbrace{f(u, u)}_{=0} + f(u, v) + f(v, u) + \underbrace{f(v, v)}_{=0} \Rightarrow f(u, v) = -f(v, u)$$
2) (1) $\Rightarrow$ (2)
   Дано: $f(u, v) = -f(v, u)$ – кососимметричность
   Доказать: $f(u, u) = 0$ – обнуление на паре совпадающих элементов
   $f(u, v) = -f(v, u)$ по (1)
   $f(a, a) = -f(a, a) \Rightarrow f(a, a) = 0$

□

2.3 Какие три условия достаточно наложить на функцию от столбцов матрицы, чтобы она обязательно была детерминантом?

Утверждение. На функцию от столбцов матрицы достаточно наложить следующие три условия, чтобы она обязательно была детерминантом:

1) Функция должна быть полилинейна (линейна по столбцам)
2) Кососимметрична ($\det A = -\det A$, т.е. равна 0, если есть 2 одинаковых столбца)
3) Равна 1 на E_n

Доказательство. Докажем при $n = 2$. Разложим столбцы:

$$\begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix} = a_{11} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + a_{21} \begin{pmatrix} 0 \\ 1 \end{pmatrix}; \quad \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix} = a_{12} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + a_{22} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Определим, чему равна функция от матрицы:

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

$$= a_{11}a_{22} f\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) + a_{21}a_{12} f\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) + a_{11}a_{12} \underbrace{f\left(\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\right)}_{=0,\text{ кососимметр.}} + a_{21}a_{22} \underbrace{f\left(\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\right)}_{=0,\text{ кососимметр.}} =$$

$$= (a_{11}a_{22} - a_{12}a_{21}) \cdot \underbrace{f\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)}_{f(E_n)=1} = a_{11}a_{22} - a_{12}a_{21} = \det A$$

□

2.4 Чему равен определитель произведения двух квадратных матриц?

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

Доказательство. Рассмотрим функцию $f(B) = \det(A \cdot B)$. Докажем $f(B) = \det B \cdot f(E_n)$

1) Кососимметричность выполнена, т.к. при совпадении двух столбцов матрицы B столбцы матрицы $A \cdot B$ тоже будут совпадать.
2) Если столбец матрицы B имеет вид $\lambda a + \mu b$, то в матрице $A \cdot B$ этот столбец имеет вид $\lambda Aa + \mu Ab$, и определитель тоже линеен $\Rightarrow f(B)$ линейна.
3) Выполнены кососимметричность и линейность, следовательно:

$$f(B) = \det B \cdot f(E_n), \text{ но } f(E_n) = \det(A \cdot E_n) = \det A \Rightarrow \det(A \cdot B) = f(B) = \det B \cdot \det A$$

□

2.5 Выписать формулы Крамера для квадратной матрицы произвольного порядка и доказать их.

Теорема. Пусть $Ax = b$ совместная СЛАУ, тогда:

$$x_i \cdot \det A = \Delta_i$$

$$\Delta_i = \det(A_1, ..., A_{i-1}, b, A_{i+1}, ..., A_n)$$

Если $\det A \neq 0$, то $x_i = \dfrac{\Delta_i}{\det A}$, $i = \overline{1, n}$

Доказательство. Пусть A_i – столбец матрицы. Запишем СЛАУ в векторном виде:

$$x_1 A_1 + x_2 A_2 + ... + x_n A_n = b \Leftrightarrow Ax = b$$

$$\Delta_i = \det(A_1, ..., A_{i-1}, b, A_{i+1}, ..., A_n) = \det(A_1, ..., A_{i-1}, x_1 A_1 + ... + x_n A_n, A_{i+1}, ..., A_n) =$$
$$= \det(A_1, ..., A_{i-1}, \sum_{j=1}^{n} x_j A_j, A_{i+1}, ..., A_n) \overset{\text{линейность}}{=} \sum_{j=1}^{n} x_j \det(A_1, ..., A_{i-1}, A_j, A_{i+1}, ..., A_n)$$

При $j \neq i$ слагаемые $x_j \cdot \underbrace{\det(A_1, ..., A_{i-1}, A_j, A_{i+1}, ..., A_n)}_{=0,\text{ два одинаковых столбца}} = 0$

$$\Delta_i = \sum_{j=1}^{n} x_j \det(A_1, ..., A_{i-1}, A_j, A_{i+1}, ..., A_n) = x_i \det(A_1, ..., A_{i-1}, A_i, A_{i+1}, ..., A_n)$$

□

2.6 Сформулировать и доказать критерий существования обратной матрицы.

Теорема. $\exists A^{-1} \Leftrightarrow \det A \neq 0$.

Доказательство.

Необходимость. Дано: $\exists A^{-1}$

Доказать: $\det A \neq 0$

По определению обратной матрицы: $A \cdot A^{-1} = E \Rightarrow \det(A \cdot A^{-1}) = \det E = 1 \Rightarrow \det A \neq 0$

Достаточность. Дано: $\det A \neq 0$

Доказать: $\exists A^{-1}$

Предъявим матрицу $B = \dfrac{1}{\det A} \cdot \widetilde{A}$, где $\widetilde{A} = \begin{pmatrix} A_{11} & \dots & A_{1n} \\ \vdots & & \vdots \\ A_{n1} & \dots & A_{nn} \end{pmatrix}^T$ – союзная матрица.

Докажем, что B является обратной, т.е. $A \cdot B = E$.

$$[A \cdot B]_{ij} = \sum_{r=1}^{n} [A]_{ir} \cdot [B]_{rj} = \frac{1}{\det A} \cdot \sum_{r=1}^{n} a_{ir} \cdot [\widetilde{A}]_{rj} = \frac{1}{\det A} \cdot \sum_{r=1}^{n} a_{ir} \cdot A_{jr} =$$

$$= \begin{cases} \frac{1}{\det A} \cdot \det A,\ i = j \text{ (разложение по i-й строке)} \\ 0,\ i \neq j \text{ (фальшивое разложение)} \end{cases} = \begin{cases} 1,\ i = j \\ 0,\ i \neq j \end{cases} = [E]_{ij}$$

Аналогично проверяется $B \cdot A = E \Rightarrow$ по определению B – обратная. □

2.7 Сформулировать и доказать критерий линейной зависимости.

Утверждение. $a_1, \dots, a_s$ – линейно зависимы $\Leftrightarrow$ хотя бы один из $a_1, \dots, a_s$ линейно выражается через другие.

Доказательство.

Необходимость. Дано: $a_1, .., a_s$ – л.з.

Доказать: найдутся выражаемые через другие.

По определению:

$$\exists\, \alpha_1, \dots, \alpha_s \text{ (не все 0)}: \alpha_1 a_1 + \dots + \alpha_s a_s = 0$$

Пусть $\alpha_1 \neq 0$. Тогда:

$$a_1 = -\frac{\alpha_2}{\alpha_1} a_2 + \dots + \left(-\frac{\alpha_s}{\alpha_1}\right) a_s$$

Достаточность. Дано: один линейно выражается через другие.

Доказать: они линейно зависимы.

Пусть $a_1 = \beta_2 a_2 + \dots + \beta_s a_s$. Тогда $\underbrace{1 \cdot a_1 - \beta_2 a_2 - \dots - \beta_s a_s}_{\text{нетривиальная лин.комб.}} = 0 \Rightarrow$ по определению они л.з. □

2.8 Как связан ранг транспонированной матрицы с рангом исходной матрицы?

Утверждение. $\operatorname{Rg} A^T = \operatorname{Rg} A$.

Доказательство. Покажем, что $\operatorname{Rg} A^T \geq \operatorname{Rg} A$. Пусть $\operatorname{Rg} A = r \overset{\text{опр}}{\Rightarrow} \exists$ минор $M_{i1\ldots ir}^{j1\ldots jr} \neq 0$. В матрице A есть минор $N_{j1\ldots jr}^{i1\ldots ir} \neq 0$, получается из M операцией транспонирования.

Минор $N \neq 0$ по свойствам определителя ($\det N = \det M^T = \det M \neq 0$). Тогда по определению $\operatorname{Rg} A^T \geq r = \operatorname{Rg} A$.

Таким образом:

$$\operatorname{Rg} A \leq \operatorname{Rg} A^T \leq \operatorname{Rg}(A^T)^T = \operatorname{Rg} A \Rightarrow \operatorname{Rg} A^T = \operatorname{Rg} A$$

□

2.9 Сформулировать и доказать следствие теоремы о базисном миноре для квадратных матриц (критерий невырожденности).

Следствие. Рассмотрим квадратную матрицу $A \in M_n(\mathbb{R})$. Следующие три условия эквивалентны:

(1) $\det A \neq 0$

(2) $\operatorname{Rg} A = n$

(3) все строки A линейно независимы

Доказательство.

1) (1) $\Rightarrow$ (2)

Пусть $\det A \neq 0 \Rightarrow$ в A есть минор порядка n, он $\neq 0 \Rightarrow$ по определению $\operatorname{Rg} A = n$.

2) (2) $\Rightarrow$ (3)

Пусть $\operatorname{Rg} A = n \Rightarrow$ все строки базисные $\Rightarrow$ по первому пункту теоремы о базисном миноре (строки базисного минора л.н.з) они все л.н.з.

3) (3) $\Rightarrow$ (1)

Пусть строки A л.н.з. Предположим противное: $\det A = 0 \Rightarrow \operatorname{Rg} A < n \Rightarrow$ по второму пункту теоремы о базисном миноре (строки, не входящие в базисный минор являются лин. комб. базисных) по крайней мере одна из строк является линейной комбинацией остальных $\Rightarrow$ по критерию л.з все строки л.з – $\perp$.

□

2.10 Сформулируйте и докажите теорему о базисном миноре.

Теорема.

1) Базисные строки (столбцы), соответствующие любому базисному минору M матрицы A л.н.з.

2) Строки (столбцы) матрицы A, не входящие в M являются линейной комбинацией базисных строк.

Доказательство.

1) Предположим, что они л.з. Тогда по критерию линейной зависимости одна из них является линейной комбинацией остальных $\Rightarrow M = 0$ – $\perp$ с определением базисного минора.
2) Без ограничения общности, будем считать, что базисный минор M матрицы A расположен в левом верхнем углу. Пусть $\operatorname{Rg} A = r$.

$$A = \begin{array}{c} r\left\{\begin{array}{c}\\ \\ \\ \end{array}\right. \\ \\ \\ \\ \end{array} \begin{pmatrix} \multicolumn{4}{c|}{\overbrace{\qquad\qquad}^{r}} & a_{1\,r+1} & \dots & a_{1n} \\ \multicolumn{4}{c|}{\mathrm{M}} & \vdots & \dots & \vdots \\ \multicolumn{4}{c|}{} & a_{r\,r+1} & \dots & a_{rn} \\ \hline a_{r+1\,1} & \dots & & \dots & & \dots & a_{r+1\,n} \\ \vdots & \dots & & \dots & & \dots & \vdots \\ a_{m1} & \dots & & \dots & & \dots & a_{mn} \end{pmatrix}$$

Возьмём строку $a_k, k > r$ и покажем, что $\exists \lambda_1, \dots, \lambda_r : a_k = a_1\lambda_1 + \dots + a_r\lambda_r$

Составим определитель $\Delta = \begin{vmatrix} a_{11} & \dots & a_{1r} & a_{1j} \\ \vdots & \dots & \vdots & \vdots \\ a_{r1} & \dots & a_{rr} & a_{rj} \\ a_{k1} & \dots & a_{kr} & a_{kj} \end{vmatrix}$ и покажем, что $\Delta = 0 \ \forall j = \overline{1, n}$

Если $j \leq r$, то в Δ есть 2 одинаковых столбца и $\Delta = 0$.

Если $j > r$, то Δ является минором исходной матрицы A. Тогда $\Delta = 0$, т.к. является минором порядка $r + 1$ в матрице ранга r.

Разложим Δ по последнему столбцу:

$$a_{1j}A_1 + \dots + a_{rj}A_j + a_{kj}A_k = \underbrace{0}_{\Delta=0}$$

где $A_1, \dots, A_k$ – алгебраические дополнения в Δ (A_k – базисный минор $\Rightarrow A_k \neq 0$).

$$a_{kj} = -\frac{A_1}{A_k}a_{1j} - \dots - \frac{A_r}{A_k}a_{rj}, \ j = \overline{1, n}, \ k > r$$

Отсюда следует, что справедлива формула для строк (a_j – это j-я строка):

$$(a_{k1}, \dots, a_{kn}) = \lambda_1(a_{11}, \dots, a_{1n}) + \dots + \lambda_r(a_{r1}, \dots, a_{rn}) \Leftrightarrow a_k = \lambda_1 a_1 + \dots + \lambda_r a_r$$

□

2.11 Сформулируйте и докажите теорему о ранге матрицы.

Следствие (теорема о ранге матрицы)**.** Ранг матрицы равен максимальному числу её линейно независимых строк и равен максимальному числу линейно независимых столбцов.

Доказательство. Пусть $\operatorname{Rg} A = r$, а максимальное количество л.н.з. строк k. Покажем, что $r = k$.

1) Т.к. в A есть r л.н.з. строк (т.к. $\operatorname{Rg} A = r$, то это базисные строки по первому пункту теоремы о базисном миноре) $\Rightarrow k \geq r$ (по определению k).
2) Вычеркнем из A все сроки, кроме k л.н.з. Получим матрицу A_1, в которой k строк. При этом $\operatorname{Rg} A_1 = k$ (т.к. если бы $\operatorname{Rg} A_1 < k$, то по второму пункту теоремы о базисном миноре одна из строк будет являться линейной комбинацией остальных $\Rightarrow$ по критерию линейной зависимости они будут л.з. – $\perp$).

   Базисный минор в A_1 имеет порядок k и является не равным нулю минором порядка k в исходной матрице $\Rightarrow k \leq r = \operatorname{Rg} A \Rightarrow k = r$.

□

2.12 Сформулируйте теорему Кронекера–Капелли и докажите её.

Теорема (Кронекера-Капелли)**.** СЛАУ $Ax = b$ совместна $\Leftrightarrow \operatorname{Rg} A = \operatorname{Rg} \begin{pmatrix} A \mid b \end{pmatrix}$.

Доказательство.

Необходимость. Дано: СЛАУ совместна.

Доказать: $\operatorname{Rg} A = \operatorname{Rg} \begin{pmatrix} A \mid b \end{pmatrix}$

По определению СЛАУ совместна $\Leftrightarrow \exists$ столбец $x^0 = \begin{pmatrix} x_1^0 \\ \vdots \\ x_n^0 \end{pmatrix} : Ax^0 = b$.

И выполнено $Ax^0 = b \Leftrightarrow x_1^0 a_1 + \ldots + x_n^0 a_n = b$, где a_j – j-й столбец матрицы A.

Предположим, что базисный минор матрицы A расположен в левом верхнем углу матрицы $\Rightarrow$ столбцы $a_1, \ldots, a_r$ являются базисными, а столбцы $a_{r+1}, \ldots, a_n$ являются их линейными комбинациями (по второму пункту теоремы о базисном миноре).

$$\begin{cases} a_{r+1} = \lambda_{1\,r+1} a_1 + \ldots + \lambda_{r\,r+1} a_r \\ \vdots \\ a_n = \lambda_{1n} a_1 + \ldots + \lambda_{rn} a_r \end{cases}$$

Отсюда:

$$b = x_1^0 a_1 + \ldots + x_r^0 a_r + x_{r+1}^0(\lambda_{1\,r+1} a_1 + ... + \lambda_{rn} a_r) + \ldots + x_n^0(\lambda_{1n} a_1 + \ldots + \lambda_{rn} a_r) =$$
$$= (x_1^0 + x_{r+1}^0 \lambda_{1\,r+1} + \ldots + x_n^0 \lambda_{1n}) a_1 + \ldots + (x_r^0 + x_{r+1}^0 \lambda_{1\,r+1} + \ldots + x_n^0 \lambda_{1n}) a_r$$

Т.е. столбец b является линейной комбинацией базисных столбцов матрицы A. Тогда $a_1, \ldots, a_r$ – базисные $\Rightarrow$ M – базисный минор и для $\Big(A \mid b\Big)$. Он $\neq 0$, и все окаймляющие миноры равны 0, т.к. у них один из столбцов – линейная комбинация столбцов $a_1, \ldots, a_r$ (столбцы $a_{r+1}, \ldots, a_n$ – линейная комбинация по определению базисного минора в матрице A, b – по доказанному). Значит, выполняется:

$$\operatorname{Rg}\Big(A \mid b\Big) = r = \operatorname{Rg} A$$

Достаточность. Дано: $\operatorname{Rg} A = \operatorname{Rg}\Big(A \mid b\Big)$

Доказать: СЛАУ совместна.

Пусть $\operatorname{Rg} A = r$. Пусть M – базисный минор A. Предположим, что он расположен в левом верхнем углу матрицы A. Очевидно, что M - является базисным минором и для $\Big(A \mid b\Big)$ $\Rightarrow$ по теореме о базисном миноре столбец b – линейная комбинация столбцов $a_1, \ldots, a_r$:

$$b = \lambda_1 a_1 + \ldots + \lambda_r a_r \Rightarrow x = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_r \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ – решение СЛАУ } Ax = b$$

$$\lambda_1 a_1 + \ldots + \lambda_r a_r + 0 \cdot a_{r+1} + \ldots + 0 \cdot a_n = b$$

$\square$

2-й модуль

1 Определения

1.1 Дать определение фундаментальной системы решений (ФСР) однородной СЛАУ

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

Определение. Любые $n - r$ линейно независимых столбцов, являющиеся решениями однородной СЛАУ $Ax = 0$, где n – число неизвестных, $r = \operatorname{Rg} A$, называют фундаментальной системой решений (ФСР).

1.2 Сформулируйте теорему о структуре общего решения однородной СЛАУ.

Теорема. 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 $c_1, \ldots, c_k$ – некоторые постоянные.

1.3 Сформулируйте теорему о структуре общего решения неоднородной системы линейных алгебраических уравнений.

Теорема. Пусть известно частное решение $\widetilde{x}$ СЛАУ $Ax = b$. Тогда любое решение этой СЛАУ может быть представлено в виде: $x = \widetilde{x} + c_1\Phi_1 + \ldots + c_k\Phi_k$, где $c_1, \ldots, c_k$ –некоторые постоянные, а $\Phi_1, \ldots, \Phi_k$ – ФСР соответствующей однородной системы $Ax = 0$.

1.4 Дайте определения модуля и аргумента комплексного числа. Что такое главное значение аргумента комплексного числа?

Пусть z – комплексное число. Его запись в алгебраической и тригонометрической формах соответственно:

$$z = x + iy = r(\cos\varphi + i\sin\varphi)$$

$x = r\cos\varphi$, $y = r\sin\varphi$

$r = \sqrt{x^2 + y^2} = |z|$ – модуль комплексного числа.

$\varphi = \operatorname{Arg} z = \{\arg z + 2\pi k | k \in \mathbb{Z}\}$ – аргумент комплексного числа (угол между r и положительным направлением Re).

Главное значение аргумента комплексного числа: $\arg z$, $\arg z \in [0; 2\pi)$ или $\arg z \in (-\pi; \pi]$.

1.5 Что происходит с аргументами и модулями комплексных чисел при умножении и при делении?

Пусть z_1, z_2 – комплексные числа.

При умножении комплексных чисел их модули умножаются, аргументы складываются:

$$z = z_1 \cdot z_2 = r_1 r_2 (\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2))$$

При делении комплексных чисел их модули делятся, аргументы вычитаются:

$$z = \frac{z_1}{z_2} = \frac{r_1}{r_2} (\cos(\varphi_1 - \varphi_2) + i \sin(\varphi_1 - \varphi_2))$$

1.6 Выпишите формулу Муавра.

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

1.7 Как найти комплексные корни n-ой степени из комплексного числа? Сделайте эскиз, на котором отметьте исходное число и все корни из него.

Извлечение комплексных корней

Пусть дано комплексное число $w = \rho(\cos \psi + i \sin \psi)$ и число $n \in \mathbb{N}$. Нужно найти $\sqrt[n]{w}$.

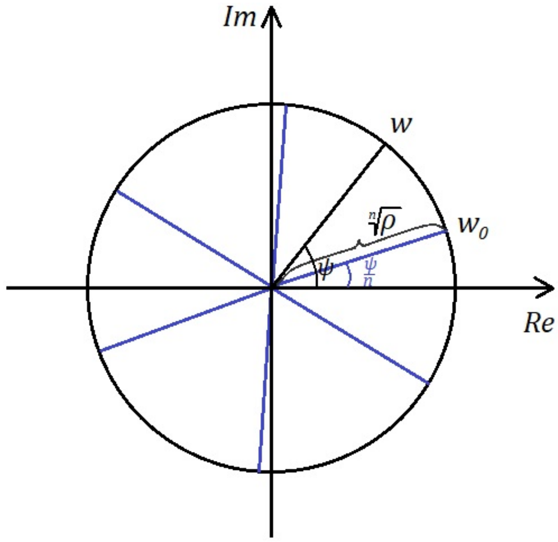
По формуле Муавра: $z^n = r^n(\cos n\varphi + i \sin n\varphi) = \rho(\cos \psi + \sin \psi)$

$$\begin{cases} \rho = r^n \\ \psi + 2\pi k = n\varphi, \ k \in \mathbb{Z} \end{cases} \Rightarrow \begin{cases} r = \sqrt[n]{\rho} \leftarrow \text{ арифметический корень из } \rho > 0 \\ \varphi = \frac{\psi + 2\pi k}{n}, \ k \in \mathbb{Z} \end{cases}$$

Достаточно рассмотреть только $k = 0, 1, 2, \ldots, n-1$. Их ровно n штук. Тогда:

$$\sqrt[n]{w} = \{ \sqrt[n]{\rho} \cdot \left(\cos\left(\frac{\psi + 2\pi k}{n}\right) + i \sin\left(\frac{\psi + 2\pi k}{n}\right) \right) \mid k = \overline{0, n-1} \}$$

Корни $\sqrt[n]{w}$ лежат в вершинах правильного n-угольника, вписанного в окружность радиуса $\sqrt[n]{\rho}$.



1.8 Сформулируйте основную теорему алгебры. Сформулируйте теорему Безу.

Теорема. Для любого многочлена $a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$, где $a_i \in \mathbb{C}$, $a_n \neq 0$, существует корень $z_0 \in \mathbb{C}$, т.е. решение уравнения $a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0 = 0$

Теорема (Безу)**.** Остаток от деления многочлена $f(x)$ на $x - c$ равен $f(c)$.

1.9 Какие многочлены называются неприводимыми?

Определение. Многочлен называется приводимым, если существует его нетривиальное разложение $f = g \cdot h$ и неприводимым в противном случае.

1.10 Сформулируйте утверждение о разложении многочленов на неприводимые множители над полем комплексных чисел.

Для любого непостоянного многочлена из $\mathbb{C}[x]$ существует разложение на неприводимые множители первой степени.

Неприводимым над $\mathbb{C}$ являются только многочлены 1-ой степени: $z - z_1$.

Любой многочлен степени $n > 0$ разлагается в произведение неприводимых многочленов. Комплексный многочлен степени n разлагается в произведение:

$$P_n(z) = a_n \cdot (z - z_1)^{\alpha_1} \cdot \ldots \cdot (z - z_k)^{\alpha_k}, \ \ n = \alpha_1 + \ldots + \alpha_k$$

1.11 Сформулируйте утверждение о разложении многочленов на неприводимые множители над действительными числами.

Утверждение. Все многочлены 1-ой и все многочлены 2-ой степени с $D < 0$ являются неприводимыми над $\mathbb{R}$, а все остальные приводимы.

1.12 Дайте определение векторного произведения векторов в трёхмерном пространстве

Определение. Вектор $\vec{c}$ называют векторным произведением векторов $\vec{a}$ и $\vec{b}$, если:

1) $|\vec{c}| = |\vec{a}| \cdot |\vec{b}| \cdot \sin\varphi$, где φ – угол между $\vec{a}$ и $\vec{b}$
2) $\vec{c} \perp \vec{a}$, $\vec{c} \perp \vec{b}$
3) тройка $\vec{a}$, $\vec{b}$, $\vec{c}$ – правая

Обозначение. $\vec{c} = \vec{a} \times \vec{b}$ или $\vec{c} = [\vec{a}, \vec{b}]$

1.13 Выпишите формулу для вычисления векторного произведения в координатах, заданных в ортонормированном базисе.

Утверждение. Пусть $\vec{i}$, $\vec{j}$, $\vec{k}$ – правый ОНБ, $\vec{a} = a_x\vec{i} + a_y\vec{j} + a_z\vec{k}$, $\vec{b} = b_x\vec{i} + b_y\vec{j} + b_z\vec{k}$. Тогда:

$$[\vec{a}, \vec{b}] = \begin{vmatrix} i & j & k \\ a_x & a_y & a_z \\ b_x & b_y & b_z \end{vmatrix} = \vec{i}(a_yb_z - a_zb_y) + \vec{j}(a_zb_x - a_xb_z) + \vec{k}(a_xb_y - a_yb_x)$$

1.14 Что такое уравнение поверхности и его геометрический образ?

Определение. Рассмотрим ПДСК O_{xyz} и некоторую поверхность S. Уравнение $F(x, y, z) = 0$ называют уравнением поверхности S, если этому уравнению удовлетворяют координаты любой точки, лежащей на поверхности, и не удовлетворяют координаты ни одной точки, не лежащей на поверхности. При этом поверхность S называют геометрическим образом уравнения $F(x, y, z) = 0$.

1.15 Сформулируйте теорему о том, что задает любое линейное уравнение на координаты точки в трехмерном пространстве.

Теорема.

1) Любая плоскость в пространстве определяется уравнением $Ax + By + Cz + D = 0$, в котором A, B, C, D — некоторые числа.

2) Любое уравнение $Ax + By + Cz + D = 0$, где $A^2 + B^2 + C^2 > 0$, определяет в пространстве плоскость.

1.16 Что такое нормаль плоскости?

Определение. Вектор $\vec{n} = (A, B, C)$ перпендикулярен плоскости $Ax + By + Cz + D = 0$ и называется ее нормальным вектором.

2 Доказательства

2.1 Сформулируйте теорему о структуре общего решения неоднородной системы линейных алгебраических уравнений и докажите её.

Теорема. Пусть известно частное решение $\widetilde{x}$ СЛАУ $Ax = b$. Тогда любое решение этой СЛАУ может быть представлено в виде:

$$x = \widetilde{x} + c_1\Phi_1 + \ldots + c_k\Phi_k$$

где $c_1, \ldots, c_k$ –некоторые постоянные, а $\Phi_1, \ldots, \Phi_k$ – ФСР соответствующей однородной системы $Ax = 0$.

Доказательство.

$$X_{\text{общ.неодн.}} = X_{\text{част.неодн.}} + X_{\text{общ.однород.}}$$

Пусть x^0 – произвольное решение СЛАУ $Ax = b \Rightarrow x^0 - \widetilde{x}$ – решение СЛАУ $Ax = 0$ (по свойствам решений СЛАУ).

К $x^0 - \widetilde{x}$ применим теорему о структуре общего решения ОСЛАУ:

$$x^0 - \widetilde{x} = c_1\Phi_1 + \ldots + c_k\Phi_k \Rightarrow x^0 = \widetilde{x} + c_1\Phi_1 + \ldots + c_k\Phi_k$$

□

2.2 Выпишите формулу Муавра и докажите её.

Утверждение. Формула Муавра: $z^n = r^n(\cos n\phi + i \sin n\phi)$, $n \in \mathbb{N}$

Доказательство. Применим принцип математической индукции.

1) $n = 2$:
$$z^2 = z \cdot z = r \cdot r \cdot (\cos(\varphi + \varphi) + i \sin(\varphi + \varphi)) = r^2(\cos 2\varphi + i \sin 2\varphi)$$

2) Предположим, что формула верна для всех $n \le k$. Покажем, что из этого следует, что оно верно для всех $n = k + 1$:

$$z^{k+1} = z^k \cdot z = r^k(\cos k\varphi + i \sin k\varphi) \cdot r(\cos \varphi + i \sin \varphi) = r^{k+1} (\cos(k\varphi + \varphi) + i \sin(k\varphi + \varphi)) =$$
$$= r^{k+1}(\cos((k + 1)\varphi) + i \sin((k + 1)\varphi))$$

Таким образом, формула верна $\forall n \in \mathbb{N}$.

□

2.3 Докажите, что если у многочлена с вещественными коэффициентами есть корень с ненулевой мнимой частью, то число, комплексно сопряжённое к этому корню, также будет корнем этого многочлена

Утверждение. Если $c \in \mathbb{C}$ – корень кратности k многочлена $P_n(x)$ с действительными коэффициентами, то $\bar{c}$ тоже является корнем $P_n(x)$ кратности k.

Доказательство. Пусть $P_n(c) = a_n \cdot c^n + \ldots + a_1 \cdot c + a_0 = 0$. Сопряжём обе части:

$$\bar{0} = \bar{a_n} \cdot \bar{c^n} + \ldots + \bar{a_1} \cdot \bar{c} + \bar{a_0}$$

Откуда $\bar{c}$ – тоже будет корнем:

$$0 = a_n \cdot \bar{c^n} + \ldots + a_1 \cdot \bar{c} + a_0 = a_n \cdot c^n + \ldots + a_1 \cdot c + a_0$$

Если c – корень кратности 1, то всё доказано. Если кратность > 1, то делим на $x - \bar{c}$, по теореме Безу остаток будет нулевым и к многочлену применяем ту же процедуру. □

2.4 Выпишите формулу для вычисления векторного произведения в правом ортонормированном базисе трехмерного пространства и приведите её вывод.

Утверждение. Пусть $\vec{i}$, $\vec{j}$, $\vec{k}$ – правый ОНБ, $\vec{a} = a_x\vec{i} + a_y\vec{j} + a_z\vec{k}$, $\vec{b} = b_x\vec{i} + b_y\vec{j} + b_z\vec{k}$. Тогда:

$$[\vec{a}, \vec{b}] = \begin{vmatrix} i & j & k \\ a_x & a_y & a_z \\ b_x & b_y & b_z \end{vmatrix} = \vec{i}(a_yb_z - a_zb_y) + \vec{j}(a_zb_x - a_xb_z) + \vec{k}(a_xb_y - a_yb_x)$$

Доказательство. Т.к. $\vec{i}$, $\vec{j}$, $\vec{k}$ – ОНБ, то

$$\vec{i} \times \vec{i} = \vec{j} \times \vec{j} = \vec{k} \times \vec{k} = \vec{0}, \vec{i} \times \vec{j} = \vec{k}, \vec{j} \times \vec{i} = -\vec{k}, \vec{i} \times \vec{k} = -\vec{j}, \vec{k} \times \vec{i} = \vec{j}, \vec{j} \times \vec{k} = \vec{i}, \vec{k} \times \vec{j} = -\vec{i}$$

$$\begin{aligned}
\vec{a} \times \vec{b} &= (a_x\vec{i} + a_y\vec{j} + a_z\vec{k}) \times (b_x\vec{i} + b_y\vec{j} + b_z\vec{k}) = \\
&= a_xb_y\, \vec{i} \times \vec{j} + a_xb_z\, \vec{i} \times \vec{k} + a_yb_x\, \vec{j} \times \vec{i} + a_yb_z\, \vec{j} \times \vec{k} + a_zb_x\, \vec{k} \times \vec{i} + a_zb_y\, \vec{k} \times \vec{j} = \\
&= \vec{i}(a_yb_z - b_ya_z) + \vec{j}(a_zb_x - a_xb_z) + \vec{k}(a_xb_y - a_yb_x) = \begin{vmatrix} i & j & k \\ a_x & a_y & a_z \\ b_x & b_y & b_z \end{vmatrix}
\end{aligned}$$

□

2.5 Докажите теорему о том, что любое линейное уравнение на координаты точки в трехмерном пространстве задает плоскость и что любая плоскость определяется линейным уравнением.

Теорема.

1) Любая плоскость в пространстве определяется уравнением $Ax + By + Cz + D = 0$, в котором A, B, C, D — некоторые числа.
2) Любое уравнение $Ax + By + Cz + D = 0$, где $A^2 + B^2 + C^2 > 0$, определяет в пространстве плоскость.

Доказательство.

1) Рассмотрим плоскость π. Пусть точка $M_0(x_0, y_0, z_0)$ ей принадлежит. Рассмотрим $\vec{n} \perp \pi$. Пусть $\vec{n} = (A, B, C)$.

$$M(x, y, z) \in \pi \Leftrightarrow (\vec{n}, \overrightarrow{M_0M}) = 0 \Leftrightarrow A(x_0 - x) + B(y_0 - y) + C(z_0 - z) = 0$$

Т.е. $Ax + By + Cz + D = 0$, где $D = -Ax_0 - By_0 - Cz_0$. Таким образом, координаты точки M удовлетворяют уравнению $Ax + By + Cz + D = 0$.

2) Рассмотрим уравнение $Ax + By + Cz + D = 0$, где $A^2 + B^2 + C^2 > 0$. Оно имеет хотя бы одно решение (например, если $A \neq 0$, то $x_0 = -\frac{D}{A}, y_0 = z_0 = 0$). Обозначим за M_0 точку (x_0, y_0, z_0). Пусть точка $M(x, y, z)$ удовлетворяет уравнению $Ax + By + Cz + D = 0$. Вычтем из него равенство $Ax_0 + By_0 + Cz_0 + D = 0$:

$$A(x_0 - x) + B(y_0 - y) + C(z_0 - z) = 0 \Leftrightarrow (\vec{n}, \overrightarrow{M_0M}) = 0, \text{ где } \vec{n} = (A, B, C)$$

$(\vec{n}, \overrightarrow{M_0M}) = 0 \Leftrightarrow \vec{n} \perp \overrightarrow{M_0M} \Leftrightarrow$ точка M лежит в плоскости, проходящей через M_0 и перпендикулярной вектору $\vec{n} \Rightarrow$ уравнение $Ax + By + Cz + D = 0$ определяет плоскость.

$\square$

2.6 Дайте определение фундаментальной системы решений (ФСР) однородной системы линейных уравнений. Докажите теорему о существовании ФСР.

Определение. Любые $n - r$ линейно независимых столбцов, являющиеся решениями однородной СЛАУ $Ax = 0$, где n – число неизвестных, $r = \operatorname{Rg} A$, называют фундаментальной системой решений (ФСР).

Теорема (о существовании ФСР)**.** Рассмотрим однородную СЛАУ $Ax = 0$. У неё существует $k = n - r$ линейно независимых решений, где n – число неизвестных, а $r = \operatorname{Rg} A$.

Доказательство. Будем предполагать, что базисный минор расположен в левом верхнем углу:

$$A = \begin{array}{c} \\ r\left\{\begin{array}{c}\\ \\ \\ \end{array}\right. \\ \\ \\ \\ \end{array} \begin{pmatrix} \overbrace{}^{r} & & & \\ \boxed{\quad \mathrm{M} \quad} & a_{1\,r+1} & \ldots & a_{1n} \\ & \vdots & \ldots & \vdots \\ & a_{r\,r+1} & \ldots & a_{rn} \\ a_{r+1\,1} & \ldots & \ldots & \ldots & a_{r+1\,n} \\ \vdots & \ldots & \ldots & \ldots & \vdots \\ a_{m1} & \ldots & \ldots & \ldots & a_{mn} \end{pmatrix}$$

Тогда строки $a_1, \ldots, a_r$ являются базисными. А строки $a_{r+1}, \ldots, a_m$ являются линейными комбинациями:

$$\begin{cases} a_{r+1} = \lambda_1 a_1 + \ldots + \lambda_r a_r \\ \vdots \\ a_m = \mu_1 a_1 + \ldots + \mu_r a_r \end{cases}$$

Сделаем элементарные преобразования:

$$\left.\begin{array}{l} a_{r+1} - \lambda_1 a_1 - \ldots - \lambda_r a_r \to a_{r+1} \\ \vdots \\ a_m - \mu_1 a_1 - \ldots - \mu_r a_r \to a_m \end{array}\right\} \Rightarrow \text{получим матрицу, где последние } m - r \text{ строк нулевые}$$

$$A = \begin{array}{c} r\left\{\begin{array}{c}\\ \\ \\ \end{array}\right. \\ \\ \\ \\ \end{array} \begin{pmatrix} \overbrace{\boxed{\quad \mathrm{M} \quad}}^{r} & \begin{matrix} \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots \end{matrix} \\ \begin{matrix} 0 & \ldots \\ \vdots & \ldots \\ 0 & \ldots \end{matrix} & \begin{matrix} \ldots & \ldots & 0 \\ \ldots & \ldots & \vdots \\ \ldots & \ldots & 0 \end{matrix} \end{pmatrix}$$

Заметим, что элементарные преобразования соответствуют эквивалентным преобразованиям исходной СЛАУ $\Rightarrow$ СЛАУ $Ax = 0$ эквивалентна:

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

Мы называем переменные $(x_1, \ldots, x_r)$, отвечающие базисным столбцам, базисными (главными), а остальные переменные – свободными $(x_{r+1}, \ldots, x_n)$

В $(*)$ слева – базисные, а справа – свободные.

Придадим свободным переменным следующий набор значений:

1-й набор	2-й набор	...	$(n-r)$-й набор
$x_{r+1} = 1$	$x_{r+1} = 0$	...	$x_{r+1} = 0$
$x_{r+2} = 0$	$x_{r+2} = 1$	...	$x_{r+2} = 0$
$\vdots$	$\vdots$	...	$\vdots$
$x_n = 0$	$x_n = 0$	...	$x_n = 1$

Для каждого набора свободных переменных решим СЛАУ относительно $x_1, \ldots, x_r$. Эта СЛАУ всегда имеет единственное решение, т.к. её определитель $(r \times r)$ – это базисный минор M и он не равен 0 (например, есть решение по формуле Крамера).

Получаем следующее решение:

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

Столбцы: $\Phi_1 = \begin{pmatrix} \phi_{11} \\ \vdots \\ \phi_{1r} \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \Phi_k = \begin{pmatrix} \phi_{k1} \\ \vdots \\ \phi_{kr} \\ 0 \\ \vdots \\ 1 \end{pmatrix}$ – решения СЛАУ $(*) \Rightarrow$ решения исходной СЛАУ.

Покажем, что они л.н.з. Рассмотрим равенство из определения $\alpha_1\Phi_1 + \ldots + \alpha_k\Phi_k = 0$

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

Это может быть выполнено только при $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 0 \overset{\text{опр.}}{\Rightarrow} \Phi_1, \ldots, \Phi_k$ являются л.н.з. Значит, $\Phi_1, \ldots, \Phi_k$ – л.н.з., их $n-r$ и они являются решениями $\Rightarrow$ это ФСР. $\square$

2.7 Сформулируйте критерий существования ненулевого решения однородной системы линейных уравнений с квадратной матрицей и докажите его.

Следствие. Однородная СЛАУ $Ax = 0$ имеет ненулевые решения $\Leftrightarrow \det A = 0$, т.е. A – вырожденная матрица.

Доказательство.

Необходимость. Дано: $Ax = 0$ имеет решение x $(\neq 0)$

Доказать: $\det A = 0$

Предположим, что $\det A \neq 0 \Rightarrow$ СЛАУ имеет единственное решение (по правилу Крамера) и это решение $x = 0$ – $\perp \Rightarrow \det A = 0$

Достаточность. Дано: $\det A = 0$

Доказать: $\exists x \neq 0 : Ax = 0$

Определитель $\det A = 0 \Rightarrow \operatorname{Rg} A < n$. Пусть $\operatorname{Rg} A = r$. По теореме о существовании ФСР, существуют $n - r > 0$ л.н.з. (ненулевых) решений СЛАУ $Ax = 0$. Это и есть ненулевые решения. □

2.8 Докажите теорему о структуре общего решения однородной системы линейных алгебраических уравнений.

Теорема (о структуре общего решения однородной СЛАУ)**.** 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 $c_1, \ldots, c_k$ – некоторые постоянные.

Доказательство.

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

Будем предполагать, что базисный минор расположен в левом верхнем углу:

$$A = \left(\begin{array}{c|ccc} \overbrace{\quad \text{M} \quad}^{r} & a_{1\,r+1} & \ldots & a_{1n} \\ & \vdots & \ldots & \vdots \\ & a_{r\,r+1} & \ldots & a_{rn} \\ \hline \begin{matrix} a_{r+1\,1} & \ldots & \ldots \\ \vdots & \ldots & \ldots \\ a_{m1} & \ldots & \ldots \end{matrix} & \ldots & \ldots & \begin{matrix} a_{r+1\,n} \\ \vdots \\ a_{mn} \end{matrix} \end{array}\right)$$

Тогда строки $a_1, \dots, a_r$ являются базисными. А строки $a_{r+1}, \dots, a_m$ являются линейными комбинациями:

$$\begin{cases} a_{r+1} = \lambda_1 a_1 + \ldots + \lambda_r a_r \\ \vdots \\ a_m = \mu_1 a_1 + \ldots + \mu_r a_r \end{cases}$$

Сделаем элементарные преобразования:

$$\left.\begin{matrix} a_{r+1} - \lambda_1 a_1 - \ldots - \lambda_r a_r \to a_{r+1} \\ \vdots \\ a_m - \mu_1 a_1 - \ldots - \mu_r a_r \to a_m \end{matrix}\right\} \Rightarrow \text{ получим матрицу, где последние } m-r \text{ строк нулевые}$$

$$A = \begin{array}{c} r\left\{\begin{matrix} \\ \\ \\ \end{matrix}\right. \\ \\ \\ \\ \end{array} \begin{pmatrix} \overbrace{\boxed{\quad \text{M} \quad}}^{r} & \begin{matrix} \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \end{matrix} \\ \begin{matrix} 0 & \dots \\ \vdots & \dots \\ 0 & \dots \end{matrix} & \begin{matrix} \dots & \dots & 0 \\ \dots & \dots & \vdots \\ \dots & \dots & 0 \end{matrix} \end{pmatrix}$$

Заметим, что элементарные преобразования соответствуют эквивалентным преобразованиям исходной СЛАУ $\Rightarrow$ СЛАУ $Ax = 0$ эквивалентна:

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

Решим СЛАУ (1) относительно неизвестных $x_1, \dots, x_r$ (выразим главные через свободные):

$$(2) \begin{cases} x_1 = \alpha_{1\,r+1}x_{r+1} + \ldots + \alpha_{1n}x_n \\ \vdots \\ x_r = \alpha_{r\,r+1}x_{r+1} + \ldots + \alpha_{rn}x_n \end{cases} \qquad \text{где } \alpha_{ij} \text{ – числа}$$

Составим новую матрицу D (ϕ_{ij} – координаты столбцов, образующих ФСР):

$$D = \begin{pmatrix} x_1^0 & \phi_{11} & \dots & \phi_{k1} \\ \vdots & \vdots & \dots & \vdots \\ x_r^0 & \phi_{1r} & \dots & \phi_{kr} \\ x_{r+1}^0 & \phi_{1\,r+1} & \dots & \phi_{k\,r+1} \\ \vdots & \vdots & \dots & \vdots \\ x_n^0 & \phi_{1n} & \dots & \phi_{kn} \end{pmatrix}$$
$$\qquad \underbrace{\qquad}_{x^0} \quad \underbrace{\qquad}_{\Phi_1} \qquad\quad \underbrace{\qquad}_{\Phi_k}$$

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

1) $\operatorname{Rg} D \geq k$, т.к. $\Phi_1, \ldots, \Phi_k$ – л.н.з. (по определению ФСР), а по теореме о ранге матрицы $\operatorname{Rg} D$ равен максимальному числу л.н.з. столбцов.

2) Покажем, что $\operatorname{Rg} D \leq k$. Столбцы $x^0, \Phi_1, \ldots, \Phi_k$ – решения СЛАУ $Ax = 0$. Тогда для них верна система (2). На место x в системе (2) последовательно подставим столбцы $x^0, \Phi_1, \ldots, \Phi_k$. Тогда x_i переменная ($i = \overline{1, r}$) из системы (2) после подстановки в неё столбцов $x^0, \Phi_1, \ldots, \Phi_k$ будет выглядеть:

$$\begin{cases} x_i^0 = \alpha_{i\,r+1} x_{r+1}^0 + \ldots + \alpha_{in} x_n^0 \\ \phi_{1i} = \alpha_{i\,r+1} \phi_{1\,r+1} + \ldots + \alpha_{ir} \phi_{1n} \\ \vdots \\ \phi_{ki} = \alpha_{i\,r+1} \phi_{k\,r+1} + \ldots + \alpha_{in} \phi_{kn} \end{cases}$$

Таким образом, первая строка d_i матрицы является линейной комбинацией строк $d_{r+1}, \ldots, d_n$.

$$\begin{cases} d_1 = \alpha_{1\,r+1} d_{r+1} + \ldots + \alpha_{1n} d_n \\ \vdots \\ d_r = \alpha_{r\,r+1} d_{r+1} + \ldots + \alpha_{rn} d_n \end{cases}$$

Сделаем элементарные преобразования:

$$\begin{cases} d_1 - \alpha_{1\,r+1} d_{r+1} - \ldots - \alpha_{1n} d_n \to d_1 \\ \vdots \\ d_r - \alpha_{r\,r+1} d_{r+1} - \ldots - \alpha_{rn} d_n \to d_r \end{cases}$$

Получаем матрицу D_1, у которой первые r строк нулевые:

$$D \sim D_1 = \begin{pmatrix} 0 & \ldots & \ldots & 0 \\ \vdots & \ldots & \ldots & \vdots \\ 0 & \ldots & \ldots & 0 \\ x_{r+1}^0 & \phi_{1\,r+1} & \ldots & \phi_{k\,r+1} \\ \vdots & \vdots & \ldots & \vdots \\ x_n^0 & \phi_{1n} & \ldots & \phi_{kn} \end{pmatrix} \begin{array}{l} \left.\vphantom{\begin{matrix}0\\0\\0\end{matrix}}\right\} r \\ \left.\vphantom{\begin{matrix}0\\0\\0\end{matrix}}\right\} n - r = k \end{array}$$

$\operatorname{Rg} D_1 \leq n - r = k$. При элементарных преобразованиях ранг не меняется $\Rightarrow \operatorname{Rg} D \leq k$.

Таким образом, $\operatorname{Rg} D = k$ (т.к. $\operatorname{Rg} D \geq k$ и $\operatorname{Rg} D \leq k$).

Заметим, что $\Phi_1, \ldots, \Phi_k$ являются базисными (они л.н.з. и их $k = \operatorname{Rg} D$) $\Rightarrow$ по теореме о базисном миноре столбец x^0 – их линейная комбинация, т.е. $\exists c_1, \ldots, c_k : x^0 = c_1 \Phi_1 + \ldots + c_k \Phi_k$. $\square$

3-й модуль

1 Определения

1.1 Какие бинарные операции называются ассоциативными, а какие коммутативными?

Определение. Пусть X – множество с заданной на нём бинарной операцией $*$. $*$ – ассоциативна, если: $\forall a, b, c \in X \;\; a * (b * c) = (a * b) * c$.

Бинарная операция $*$ – коммутативна, если: $\forall a, b \in X \;\; a * b = b * a$

1.2 Дайте определения полугруппы и моноида. Приведите примеры.

Определение. Множество X с заданной на нём бинарной ассоциативной операцией называется полугруппой.

Определение. Полугруппа, в которой есть нейтральный элемент – моноид.

Пример полугруппы. $(\mathbb{N} \setminus \{1\}, \cdot)$, $\cdot$ – умножение натуральных чисел.
Пример моноида. $(\mathbb{N}, \cdot)$

1.3 Сформулируйте определение группы. Приведите пример.

Определение (эквивалентное)**.** Множество G с корректно определённой на нём бинарной операцией $*$ называется группой, если:

1) операция ассоциативна: $\forall x, y, z \in G \; x * (y * z) = (x * y) * z$
2) $\exists e \in G \; \forall x \in G : x * e = e * x = x$
3) $\forall x \in G \; \exists x^{-1} \in G : x * x^{-1} = x^{-1} * x = e$

Пример. $(\mathbb{Z}, +)$

1.4 Что такое симметрическая группа? Укажите число элементов в ней.

Определение. Симметрическая группа S_n – множество всех подстановок длинны n: $\sigma = \begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix}$ с операцией композиции. Число элементов в S_n равно числу перестановок: $n!$

1.5 Что такое общая линейная и специальная линейная группы?

Определение. Общая линейная группа – множество всех невырожденных матриц A с операцией матричного умножения: $GL_n(\mathbb{R})$ (n – размер матрицы).

Определение. Специальная линейная группа – $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\}$, $SL_n(\mathbb{R}) \subset GL_n(\mathbb{R})$. Это множество замкнуто относительно умножения и взятия обратного.

1.6 Сформулируйте определение абелевой группы. Приведите пример.

Определение. Группа с коммутативной операцией называется абелевой.

Пример. $(\mathbb{Z}, +)$

1.7 Дайте определение подгруппы. Приведите пример группы и её подгруппы.

Определение. Подмножество $H \subseteq G$ называется подгруппой в G, если:

1) $e \in H$
2) Если $h_1, h_2 \in H \Rightarrow h_1 \cdot h_2 \in H$, т.е. множество H замкнуто относительно умножения.
3) Если $h \in H \Rightarrow h^{-1} \in H$, т.е. H замкнуто относительно взятия обратного.

Пример. Специальная линейная группа: $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\}$, $SL_n(\mathbb{R}) \subset GL_n(\mathbb{R})$. Это множество замкнуто относительно умножения и взятия обратного.

1.8 Дайте определение гомоморфизма групп. Приведите пример.

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

Пример. $G_1 = (\mathbb{R}_+, \cdot)$, $G_2 = (\mathbb{R}, +)$ и гомоморфизмом $f = \ln x$. Является гомоморфизмом по определению $\forall a, b \in G_1 \ \ln(a \cdot b) = \ln a + \ln b$.

1.9 Дайте определение изоморфизма групп. Приведите пример.

Определение. Биективный гомоморфизм называется изоморфизмом.

Пример. $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$ и изоморфизмом $f = e^x$.

1.10 Дайте определение порядка элемента.

Определение. Пусть q – наименьшее натуральное ($\neq 0$) число, для которого $a^q = e$, где $a \in G$, оно называется порядком элемента. Если такого числа не существует, то говорят об элементе бесконечного порядка.

1.11 Сформулируйте определение циклической группы. Приведите пример.

Определение. Пусть g – элемент G. Если любой элемент $g \in G$ имеет вид $g = a^n$, где $a \in G$, то G называют циклической группой.

1.12 Сколько существует, с точностью до изоморфизма, циклических групп данного порядка?

Утверждение. Все циклические группы одного порядка изоморфны.

Утверждение. Для каждого числа существует единственная (с точностью до изоморфизма) циклическая группа такого порядка. Также существует ровно одна бесконечная циклическая группа.

1.13 Что такое ядро гомоморфизма групп? Приведите пример.

Определение. Ядром гомоморфизма $f : G \to F$ называется множество элементов группы G, которые переходят в e_F (нейтральный элемент во второй группе).

$$\operatorname{Ker} f = \{g \in G \mid f(g) = e_F\}$$

Пример. $\varphi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, $\varphi(x) = x \mod 3$, $\operatorname{Ker}\varphi = \{x \in \mathbb{Z} \mid x \,\vdots\, 3\}$

Пример. $\det : GL_n(\mathbb{R}) \to \mathbb{R}^* = \{\mathbb{R} \setminus \{0\}, \cdot\}$, $\operatorname{Ker}\det = SL_n(\mathbb{R}) = \{A \mid \det A = 1\}$

1.14 Сформулируйте утверждение о том, какими могут быть подгруппы группы целых чисел по сложению.

Утверждение. Любая подгруппа в $(\mathbb{Z}, +)$ имеет вид $k\mathbb{Z}$ (числа, кратные k) для $k \in \mathbb{N} \cup \{0\}$.

1.15 Дайте определение левого смежного класса по некоторой подгруппе.

Определение. Пусть G – группа и H – её подгруппа. Пусть фиксирован $g \in G$. Левым смежным классом элемента g по подгруппе H называется множество $gH = \{g \cdot h | h \in H\}$ (а правым смежным класс: $Hg = \{h \cdot g \mid h \in H\}$).

1.16 Дайте определение нормальной подгруппы.

Определение. Подгруппа H группы G называется нормальной, если $gH = Hg$, $\forall g \in G$.

1.17 Что такое индекс подгруппы?

Определение. Индексом подгруппы H в группе G называется количество левых смежных классов G по H.

1.18 Сформулируйте теорему Лагранжа.

Теорема (Лагранжа)**.** Пусть G – конечная группа и $H \subseteq G$ – её подгруппа. Тогда

$$|G| = |H| \cdot [G : H]$$

1.19 Сформулируйте три следствия из теоремы Лагранжа.

Следствие. Пусть G – конечная группа и $g \in G$. Тогда $\operatorname{ord} g$ делит $|G|$.

Следствие. Пусть G – конечная группа и $g \in G$. Тогда

$$g^{|G|} = e$$

Следствие (Малая теорема Ферма)**.** Пусть $\bar{a}$ – ненулевой вычет по простому модулю p. Тогда

$$\bar{a}^{p-1} = \bar{1} \text{ (или } \bar{a}^p = \bar{a})$$

1.20 Сформулируйте критерий нормальности подгруппы, использующий сопряжение.

Утверждение. Пусть $H \subseteq G$. Тогда три условия эквивалентны:

(1) H нормальная

(2) $gHg^{-1} \subseteq H$, $\forall g \in G$

(3) $\forall g \in G$ $gHg^{-1} = H$

1.21 Сформулируйте определение простой группы.

Определение. Группа называется простой, если она не имеет собственных (т.е. отличных от единичной и самой группы) нормальных групп.

1.22 Дайте определение факторгруппы.

Определение. Пусть H – нормальная подгруппа в G. G/H – множество левых смежных классов по H с операцией умножения $(g_1H)(g_2H) = g_1g_2H$ называется факторгруппой.

1.23 Что такое естественный гомоморфизм?

Определение. Отображение $\varepsilon : G \to G/H$ называется естественным гомоморфизмом.

$\varepsilon : a \longmapsto aH$, где $a \in G$, aH – смежный класс, содержащий a

1.24 Сформулируйте критерий нормальности подгруппы, использующий понятие ядра гомоморфизма.

Утверждение. H – нормальная подгруппа в $G \Leftrightarrow H = \operatorname{Ker} f$, f – гомоморфизм.

1.25 Сформулируйте теорему о гомоморфизме групп. Приведите пример.

Теорема (о гомоморфизме). Пусть $f : G \to F$ – гомоморфизм групп. Тогда $\operatorname{Im} f$ изоморфен факторгруппе $G/\operatorname{Ker} f$, т.е. $G/\operatorname{Ker} f \cong \operatorname{Im} f$, где $\operatorname{Im} f = \{a \in F \mid \exists g \in G : f(g) = a\}$ – образ f.

Пример:

$$f : GL_n(\mathbb{R}) \xrightarrow{\det A} \mathbb{R}^* = \{\mathbb{R} \setminus \{0\}, \cdot\}$$

$$\operatorname{Ker} \det = SL_n(\mathbb{R}) = \{A \mid \det A = 1\} \Rightarrow GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \underbrace{\mathbb{R}^*}_{\operatorname{Im} \det}$$

1.26 Что такое прямое произведение групп?

Определение. Прямым произведением двух групп G_1 и G_2 называется их прямое (декартовое) произведение как множеств с покомпонентным умножением:

$$(x_1, y_1) \circ (x_2, y_2) = (x_1 * x_2, y_1 \star y_2)$$

$*$ – произведение в G_1, $\star$ – произведение в G_2

1.27 Сформулируйте определение автоморфизма и внутреннего автоморфизма.

Определение. Автоморфизм – это изоморфизм из G в G.

Определение. Внутренним автоморфизмом называют отображение $I_n : g \mapsto aga^{-1}$

1.28 Что такое центр группы? Приведите пример.

Определение. Центр группы G – это множество $Z(G) = \{a \in G \mid ab = ba\, \forall b \in G\}$, т.е. множество элементов, которые коммутируют со всеми.

Пример. Центр группы кватернионов $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ равен $\{1, -1\}$.

1.29 Что можно сказать про факторгруппу группы по её центру?

$G/Z(G) \cong I_{nn}(G)$, $I_{nn}(G)$ – внутренние автоморфизмы.

1.30 Сформулируйте теорему Кэли.

Теорема (Кэли)**.** Любая конечная группа порядка n изоморфна некоторой подгруппе группы S_n.

1.31 Дайте определение кольца.

Определение. Пусть $K \neq \varnothing$ – множество на котором заданы две бинарные операции: $+$ и $\cdot$, что:

1) $(K, +)$ – абелева группа.
2) $(K, \cdot)$ – полугруппа.
3) Умножение дистрибутивно по сложению: $\forall a, b, c$

$$(a + b)c = ac + bc$$
$$c(a + b) = ca + cb$$

1.32 Что такое коммутативное кольцо? Приведите примеры коммутативного и некоммутативного колец.

Определение. Если $\forall x, y \in K$ $xy = yx$ (т.е. умножение коммутативно), то кольцо $(K, +, \cdot)$ называется коммутативным.

Пример. $(\mathbb{Z}, +, \cdot)$ – коммутативное кольцо.

Пример. $(M_n(\mathbb{R}), +, \cdot)$ – некоммутативное кольцо.

1.33 Дайте определение делителей нуля.

Определение. Если $ab = 0$ при $a \neq 0$ и $b \neq 0$ в кольце K, то a называется левым, b – правым делителем нуля.

1.34 Какие элементы кольца называются обратимыми?

Определение. Элемент коммутативного кольца с "1" называется обратимым (по умножению), если существует $a^{-1} : aa^{-1} = a^{-1}a = 1$.

1.35 Дайте определение поля. Приведите три примера.

Определение. Поле P – это коммутативное кольцо с единицей ($1 \neq 0$), в котором каждый элемент $a \neq 0$ обратим.

Пример. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

1.36 Дайте определение подполя. Привести пример пары: поле и его подполе.

Определение. Подполе – подмножество поля, которое само является полем относительно тех же операций.

Пример. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Пример. $\mathbb{Z}_p$, где p – простое, тоже является полем.

1.37 Дайте определение характеристики поля. Привести примеры: поля конечной положительной характеристики и поля нулевой характеристики.

Определение. Пусть P – поле. Характеристикой поля называется такое наименьшее $q \in \mathbb{N}$, что $\underbrace{1 + 1 + \ldots + 1}_{q} = 0$. Если такого q нет, то характеристика равна 0.

Пример. $\operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = \operatorname{char} \mathbb{Q} = 0$

Пример. $\operatorname{char} \mathbb{Z}_p = p$

1.38 Сформулируйте утверждение о том, каким будет простое подполе в зависимости от характеристики.

Утверждение. Пусть P – поле, а P_0 – его простое подполе. Тогда:

1) Если характеристика поля $\operatorname{char} P = p > 0$, то $P_0 \cong \mathbb{Z}_p$
2) Если $\operatorname{char} P = 0$, то $P_0 \cong \mathbb{Q}$.

1.39 Дайте определение идеала. Что такое главный идеал?

Определение. Подмножество I кольца K называется (двусторонним) идеалом, если оно:

1) является подгруппой $(K, +)$ по сложению
2) $\forall a \in I \, \forall r \in K \; ra \in I$ и $ar \in I$

Определение. Идеал I называется главным, если $\exists a \in K : I = \{ra \mid r \in K\}$. Говорят, что идеал I порождён a.

1.40 Сформулируйте определение гомоморфизма колец.

Определение. $\varphi : K_1 \to K_2$ – гомоморфизм колец, если $\forall a, b \in K_1$:

1) $\varphi(a + b) = \varphi(a) \oplus \varphi(b)$
2) $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$

1.41 Сформулируйте теорему о гомоморфизме колец. Приведите пример.

Теорема (о гомоморфизме колец)**.** Пусть K_1, K_2 – два кольца, $\varphi : K_1 \to K_2$ – гомомрфизм. Тогда

$$\underbrace{K_1/\operatorname{Ker}\varphi}_{\text{факторкольцо}} \cong \underbrace{\operatorname{Im}\varphi}_{\text{кольцо}}$$

Пример. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, любому целому числу сопоставляем его остаток от деления на число n, $\operatorname{Ker}\varphi = n\mathbb{Z}$.

1.42 Сформулируйте критерий того, что кольцо вычетов по модулю n является полем.

Утверждение. $\mathbb{Z}_p$ является полем $\Leftrightarrow$ p –простое.

1.43 Сформулируйте теорему о том, когда факторкольцо кольца многочленов над полем само является полем.

Теорема. Пусть P – поле, а $f(x) \in P[x]$. Тогда факторкольцо $P[x]/\langle f(x)\rangle$ является полем $\Leftrightarrow$ многочлен $f(x)$ – неприводим над P.

1.44 Дайте определение алгебраического элемента над полем.

Определение. Элемент $\alpha \in P$ называется алгебраическим элементом над полем $F \subset P$, если существует $f(x) \neq 0$ (многочлен, т.е. $f(x) \in F[x]$) : $f(\alpha) = 0$. Если это не так, то α – трансцендентный элемент над F.

Пример. Пусть $F = \mathbb{Q}$. И $\sqrt{2} \in \mathbb{R}$ – алгебраическое число: $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Элемент $\pi \in \mathbb{R}$ – трансцендентный.

1.45 Сформулируйте утверждение о том, что любое конечное поле может быть реализовано как факторкольцо кольца многочленов по некоторому идеалу.

Теорема. Любое конечное поле F_q, где $q = p^n$, а p – простое можно, реализовать в виде $\mathbb{Z}_p[x]/\langle h(x)\rangle$, где $h(x)$ – неприводимый многочлен степени n над $\mathbb{Z}_p$.

1.46 Дайте определение линейного (векторного) пространства.

Пусть F – поле, пусть V – произвольное множество, на котором задано 2 операции: сложение и умножение на число (т.е. элемент из F). Это означает, что $\forall x, y \in V$ существует элемент $x+y \in V$ и $\forall \lambda \in F\, \exists \lambda \cdot x \in V$. Множество V называется линейным пространством, если выполнены следующие 8 свойств:

$\forall x, y, z \in V$ и $\forall \lambda, \mu \in F$:

1) $(x + y) + z = x + (y + z)$ – ассоциативность сложения.
2) Найдется нейтральный элемент по сложению: $\exists 0 \in V : \forall x \in V : x + 0 = 0 + x = x$
3) Существует противоположный элемент по сложению: $\forall x \in V\ \exists (-x) \in V : x + (-x) = 0$
4) $x + y = y + x$ – коммутативность сложения
5) $\forall x \in V : 1 \cdot x = x$, нейтральный $1 \in F_1$
6) Ассоциативность умножения на число: $\mu(\lambda x) = (\mu\lambda)x$
7) Дистрибутивность относительно сложения чисел: $(\lambda + \mu)x = \lambda x + \mu x$
8) Дистрибутивность относительно сложения векторов: $\lambda(x + y) = \lambda x + \lambda y$

1.47 Дайте определение базиса линейного (векторного) пространства.

Определение. Базисом линейного пространства V называется упорядоченный набор векторов $b_1, \ldots, b_n$ такой, что:

1) $b_1, \ldots, b_n$ – л.н.з.
2) Любой вектор из V представляется линейной комбинацией векторов $b_1, \ldots, b_n$, то есть $\forall x \in V$ $x = x_1 b_1 + \ldots x_n b_n$. При этом $x_1, \ldots, x_n$ называется координатами вектора в базисе $b_1, \ldots, b_n$.

1.48 Что такое размерность пространства?

Определение. Максимальное количество л.н.з. векторов в данном линейном пространстве V называется размерностью этого линейного пространства.

1.49 Дайте определение матрицы перехода от старого базиса линейного пространства к новому.

Определение. Матрицей перехода от базиса $\mathcal{A}$ к базису $\mathcal{B}$ называется матрица:

$$T_{\mathcal{A}\to\mathcal{B}} = \begin{pmatrix} t_{11} & \cdots & t_{1n} \\ \vdots & & \vdots \\ t_{n1} & \cdots & t_{nn} \end{pmatrix}$$

$$(b_1, \ldots, b_n)_{1\times n} = (a_1, \ldots, a_n) \cdot T_{\mathcal{A}\to\mathcal{B}}$$

$b = a \cdot T_{\mathcal{A}\to\mathcal{B}}$ – матричная форма записи определения матрицы перехода, где $b = (b_1, \ldots, b_n)$, $a = (a_1, \ldots, a_n)$

1.50 Выпишите формулу для описания изменения координат вектора при изменении базиса.

Утверждение. Пусть $x \in L$, $\mathcal{A}$ и $\mathcal{B}$ – базисы в L.
$x^a = (x_1^a, \ldots, x_n^a)^T$ – столбец координат вектора x в базисе $\mathcal{A}$.
$x^b = (x_1^b, \ldots, x_n^b)^T$ – столбец координат вектора x в базисе $\mathcal{B}$.
Тогда $x^b = T_{\mathcal{A}\to\mathcal{B}}^{-1} x^a \Leftrightarrow X' = T^{-1}X$, где X' – координаты в новом базисе.

1.51 Дайте определение подпространства в линейном пространстве.

Определение. Подмножество W векторного пространства V называется подпространством, если оно само является пространством относительно операций в V.

1.52 Дайте определения линейной оболочки конечного набора векторов и ранга системы векторов.

Определение. Множество $L(a_1, \ldots, a_k) = \{\lambda_1 a_1 + \ldots \lambda_k a_k \mid \lambda_i \in F\}$ – множество всех линейных комбинаций векторов $a_1, \ldots, a_k$ называется линейной оболочкой набора $a_1, \ldots, a_k$.

Определение. Рангом системы векторов $a_1, \ldots, a_k$ в линейном пространстве называется размерность их линейной оболочки.

$$\mathrm{Rg}(a_1, \ldots, a_k) = \dim(L(a_1, \ldots, a_k))$$

1.53 Дайте определения суммы и прямой суммы подпространств.

Определение. Множество $H_1 + H_2 = \{x_1 + x_2 \mid x_1 \in H_1, x_2 \in H_2\}$ называется суммой подпространств H_1 и H_2.

Определение. Сумма подпространств $H_1 + H_2$ называется прямой и обозначается $H_1 \oplus H_2$, где $H_1 \cap H_2 = \{0\}$, т.е. тривиально.

1.54 Сформулируйте утверждение о связи размерности суммы и пересечения подпространств.

Утверждение. Пусть H_1 и H_2 – подпространства в L. Тогда:

$$\dim(H_1 + H_2) = \dim(H_1) + \dim(H_2) - \dim(H_1 \cap H_2)$$

1.55 Дайте определение билинейной формы.

Пусть V – линейное пространство над $\mathbb{R}$.

Определение. Функцию $b : V \times V \to \mathbb{R}$ называют билинейной формой, если $\forall \alpha, \beta \in \mathbb{R}$:

1) $b(\alpha x + \beta y, z) = \alpha b(x, z) + \beta b(y, z)$
2) $b(x, \alpha y + \beta z) = \alpha b(x, y) + \beta b(x, z)$

1.56 Как меняется матрица билинейной формы при замене базиса? Как меняется матрица квадратичной формы при замене базиса?

Утверждение. Пусть U – матрица перехода от базиса e к базису f. Пусть B_e – матрица билинейной формы в базисе e. Тогда:

$$B_f = U^T B_e U$$

2 Доказательства

2.1 Сформулируйте и докажите утверждение о связи порядка элемента, порождающего циклическую группу, с порядком группы.

Утверждение. Пусть G – группа и $g \in G$. Тогда $|\langle g \rangle| = \mathrm{ord}(g)$

Доказательство. Заметим, что если $\forall k, s \in \mathbb{N}\ g^k = g^s \Rightarrow g^{k-s} = e$ (т.к. $\exists g^{-1}$), то $\mathrm{ord}\, g \leq k-s \Rightarrow$ если g имеет бесконечный порядок, то все элементы g^n, $n \in \mathbb{Z}$ различны $\Rightarrow \langle g \rangle$ содержит бесконечного много элементов $\Rightarrow$ в бесконечном случае доказано.

Если же $\mathrm{ord}(g) = m$, то из минимальности $m \in N \Rightarrow e = g^0$, $g = g^n, \ldots, g^{m-1}$ попарно различны. Покажем, что $\langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\}$. Т.к. $\forall n \in \mathbb{Z}$ представимо в виде $n = qm + r$, где $0 \leq r < m$, $g^n = g^{qm+r} = (g^m)^q \cdot g^r = e^q \cdot g^r = g^r \Rightarrow \langle g \rangle = \{e, g, \ldots, g^{m-1}\}$ и $|\langle g \rangle| = m = \mathrm{ord}(g)$. □

2.2 Сформулируйте и докажите утверждение о том, какими могут быть подгруппы группы целых чисел по сложению.

Утверждение. Любая подгруппа в $(\mathbb{Z}, +)$ имеет вид $k\mathbb{Z}$ (числа, кратные k) для $k \in \mathbb{N} \cup \{0\}$.

Доказательство. $k\mathbb{Z}$ является подгруппой. Докажем, что других нет.

Если $H = \{0\}$ (H – подгруппа, 0 – нейтральный элемент), то положим, что $k = 0$. Иначе $k = \min(H \cap \mathbb{N})$ ($\neq \varnothing$, т.к. $H \neq \{0\}$). Тогда $k\mathbb{Z} \subseteq H$.

Рассмотрим $a \in H$ и $a = qk + r$, $0 \leq r < k$. Тогда $r = \underbrace{a}_{\in H} - \underbrace{qk}_{\in H} \in H \Rightarrow r = 0$ (так как $r < k = \min(H \cap \mathbb{N})$). Получаем, что $a = qk \Rightarrow H \subseteq k\mathbb{Z}$.

Доказана принадлежность в обе стороны: $k\mathbb{Z} \subseteq H$ и $H \subseteq k\mathbb{Z}$. Значит, $k\mathbb{Z} = H$. □

2.3 Сформулируйте и докажите теорему Лагранжа (включая две леммы).

Лемма. Левые смежные классы G по подгруппе H либо не пересекаются, либо совпадают:

$$\forall g_1, g_2 \in G \text{ либо } g_1H = g_2H, \text{ либо } g_1H \cap g_2H = \varnothing$$

Доказательство. Докажем, что если классы пересекаются, то они совпадают. Если $g_1H \cap g_2H \neq \varnothing$, то $\exists h_1, h_2 \in H : g_1 \cdot h_1 = g_2 \cdot h_2 \Rightarrow g_1 = g_2 \cdot \underbrace{h_2 \cdot h_1^{-1}}_{\in H} \Rightarrow g_1H = g_2 \underbrace{h_2 h_1^{-1} H}_{\text{лежит в } H} \in g_2H \Rightarrow g_1H \subseteq g_2H$. Аналогично есть обратное включение $\Rightarrow g_1H = g_2H$. □

Лемма. $|gH| = |H|$, $\forall g \in G$ (и любой конечной подгруппы H).

Доказательство. Пусть $H = \{h_1, \dots, h_n\}$, H – конечная подгруппа. Тогда смежный класс

$$gH = \{g \cdot h \mid h \in H\} = \{gh_1, \dots, gh_n\}$$

Тогда $|gH| \le |H|$ (т.к. некоторые из $gh_1, \dots, gh_n$ могут совпасть).

Предположим, что $|gH| < |H|$. Т.е. найдутся такие элементы $h_1, h_2 \in H$, что $h_1 \neq h_2$ и выполнено $gh_1 = gh_2$. Но тогда

$$gh_1 = gh_2 \Rightarrow g^{-1}gh_1 = g^{-1}gh_2 \Rightarrow h_1 = h_2$$

Получили противоречие. Следовательно, $|gH| = |H|$. □

Теорема (Лагранжа)**.** Пусть G – конечная группа и $H \subseteq G$ – её подгруппа. Тогда

$$|G| = |H| \cdot [G : H]$$

Доказательство. Любой элемент группы G лежит в некотором левом смежном классе по H (gH). Т.к. левые смежные классы не пересекаются и любой из них содержит по $|H|$ элементов, группа G распределяется на непересекающиеся левые смежные классы порядка $|H| \Rightarrow |G| = |H| \cdot [G : H]$. □

2.4 Докажите, что гомоморфизм инъективен тогда и только тогда, когда его ядро тривиально.

Утверждение. Пусть $f : G \to F$ – гомоморфизм. Тогда f – инъективно (является мономорфизмом) $\Leftrightarrow \operatorname{Ker} f = e_G$.

Доказательство.

Необходимость. Дано: f – инъективно

Доказать: $\operatorname{Ker} f = e_G$

$\forall x_1 \neq x_2 : f(x_1) \neq f(x_2) \Rightarrow f(e_G) = e_F$ (и для $x \in G$ и $x \neq e_G$ $f(x) \neq f(e_G) = e_F$)

Достаточность. Дано: $\operatorname{Ker} f = e_G$

Доказать: f – инъективно

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

$$f(x_1 x_2^{-1}) = e_F = f(x_1) \cdot f(x_2^{-1}) = f(x_1) \cdot f(x_2)^{-1} \Rightarrow x_1 \cdot x_2^{-1} = e_G \Leftrightarrow x_1 = x_2$$

Противоречие с предположением $\Rightarrow f$ – мономорфизм (инъективно). □

2.5 Сформулируйте и докажите критерий нормальности подгруппы, использующий сопряжение.

Утверждение. Пусть $H \subseteq G$. Тогда три условия эквивалентны:

(1) H нормальная

(2) $gHg^{-1} \subseteq H, \forall g \in G$

(3) $\forall g \in G \ gHg^{-1} = H$

Доказательство.

1) (1) $\Rightarrow$ (2)

Т.к. $gH = Hg$, то $\forall h \in H \ gh = hg \Rightarrow ghg^{-1} = h \in H \Rightarrow gHg^{-1} \subseteq H$

2) (2) $\Rightarrow$ (3)

Для $\forall h \in H \ h = gg^{-1}hgg^{-1} = g(g^{-1}hg)g^{-1} = g\underbrace{((g^{-1})h(g^{-1})^{-1})}_{\in H}g^{-1} \in gHg^{-1}$.

Тогда $H \subseteq gHg^{-1}$, и, т.к. $gHg^{-1} \subseteq H$, $H = gHg^{-1}$

3) (3) $\Rightarrow$ (1)

$gHg^{-1} = H \Leftrightarrow gHg^{-1}g = Hg \Leftrightarrow gH = Hg$ – условие нормальности.

□

2.6 Сформулируйте и докажите критерий нормальности подгруппы, использующий понятие ядра гомоморфизма.

Утверждение. H – нормальная подгруппа в $G \Leftrightarrow H = \operatorname{Ker} f$, f – гомоморфизм.

Доказательство.

Необходимость. Дано: H – нормальная подгруппа в G

Доказать: существует гомоморфизм f такой, что $H = \operatorname{Ker} f$

В роли гомоморфизма f может выступать естественный гомоморфизм $\varepsilon : G \to G/H$. Он существует, т.к. H – нормальная подгруппа и G/H корректно определена. $\operatorname{Ker} f$ – это множество всех элементов, которые перешли в $eH = H$ – исходная нормальная подгруппа.

Достаточность. Дано: H – нормальная подгруппа в $GH = \operatorname{Ker} f$

Доказать: H – нормальная подгруппа в G

Пусть $f : G \to F$ – гомоморфизм. Покажем, что $\forall g \in G$ и $\forall z \in \operatorname{Ker} f$ выполняется $g^{-1}zg \in \operatorname{Ker} f$

$f(g^{-1}zg) = f(g^{-1})f(z)f(g) \overset{\text{св-во гомоморф.}}{=} f(g)^{-1}\underbrace{f(z)}_{e_F}f(g) = (f(g))^{-1}f(g) = e_F \overset{\text{опр.}}{\Rightarrow} g^{-1}zg \in \operatorname{Ker} f$.

Так как $g^{-1} \operatorname{Ker} fg \subseteq \operatorname{Ker} f$, $\operatorname{Ker} f$ – нормальная группа. □

2.7 Сформулируйте и докажите теорему о гомоморфизме групп.

Теорема (о гомоморфизме)**.** Пусть $f : G \to F$ – гомоморфизм групп. Тогда $\operatorname{Im} f$ изоморфен факторгруппе $G/\operatorname{Ker} f$, т.е. $G/\operatorname{Ker} f \cong \operatorname{Im} f$, где $\operatorname{Im} f = \{a \in F \mid \exists g \in G : f(g) = a\}$ – образ f.

Доказательство. Рассмотрим отображение $\tau : G/\operatorname{Ker} f \to F$, заданное формулой

$$\tau(g \operatorname{Ker} f) = f(g) \in \operatorname{Im} f$$

где $g \operatorname{Ker} f$ – смежный класс $H = \operatorname{Ker} f$.

Докажем, что τ и есть исходный изоморфизм. Проверим корректность (т.е. покажем, что τ не зависит от выбора представителя смежного класса):

$$\forall h_1, h_2 \in \operatorname{Ker} f \ f(gh_1) = f(g)f(h_1) = f(g) \cdot e_F = f(g) = f(g) \cdot \underbrace{f(h_2)}_{e_F} = f(gh_2)$$

Значит, τ – определён корректно.

Отображение τ сюръективно ($\tau : G/\operatorname{Ker} f \to \operatorname{Im} f$) и покажем, что оно инъективно.

По утверждению $f(g) = e_F \Leftrightarrow g \in \operatorname{Ker} f = H$, т.е. ядро гомоморфизма состоит только из нейтрального элемента в факторгруппе. Воспользуемся критерием инъективности: τ – инъективно тогда и только тогда, когда $\operatorname{Ker} \tau$ тривиально (состоит из $e \cdot \operatorname{Ker} f$) $\Rightarrow \tau$ – биективно.

Остаётся проверить, что τ – гомоморфизм:

$$\tau((g_1 \operatorname{Ker} f) \cdot (g_2 \cdot \operatorname{Ker} f)) \underset{\substack{\uparrow \\ \text{по определению} \\ \text{произведения в} \\ \text{факторгруппе}}}{=} \tau(g_1 g_2 \operatorname{Ker} f) \underset{\substack{\uparrow \\ \text{по определению } \tau}}{=} f(g_1 g_2) \underset{\substack{\uparrow \\ f \text{ – гомоморфизм}}}{=} f(g_1) f(g_2) \underset{\substack{\uparrow \\ \text{по определению } \tau}}{=} \tau(g_1 \operatorname{Ker} f) \tau(g_2 \operatorname{Ker} f)$$

Таким образом, τ – биективный гомоморфизм, т.е. изоморфизм. □

2.8 Докажите, что центр группы является её нормальной подгруппой.

Утверждение. $Z(G)$ всегда является нормальной подгруппой в G.

Доказательство. Покажем, что $Z(G)$ является подгруппой. Для того, чтобы H было подгруппой нужно, чтобы $\forall a, b \in H \ ab^{-1} \in H$. Для того, чтобы проверить:

- что $e \in H$, берём $b = a \Rightarrow aa^{-1} = e \in H$
- что $ab \in H$, берём $b = b^{-1} \Rightarrow ab \in H$
- что $a^{-1} \in H$, берём $a = e, b = a \Rightarrow a \in H$

1) Проверим, что $\forall a, b \in Z(G)$ выполнено $ab^{-1} \in Z(G)$.

$$ab^{-1}g = ab^{-1}(g^{-1})^{-1} = a(g^{-1}b)^{-1} \overset{b \in Z(G)}{=} a(bg^{-1})^{-1} = a(g^{-1})^{-1}b^{-1} = agb^{-1} \overset{a \in Z(G)}{=} gab^{-1}$$

2) Это нормальная подгруппа, т.к. элементы коммутируют с любыми из G и $gZ(G) = Z(G)g$.

□

2.9 Сформулируйте и докажите утверждение о том, чему изоморфна факторгруппа группы по её центру.

Утверждение. $G/Z(G) \cong I_{nn}(G)$

Доказательство. Факторгруппа $G/Z(G)$ является нормальной подгруппой. Рассмотрим отображение $f : G \to \operatorname{Aut}(G)$, заданнное формулой $f : g \mapsto \varphi_g(h) = ghg^{-1}$.

Тогда $\operatorname{Im} f = I_{nn}(G)$ по определению и $\operatorname{Ker} f = Z(G)$, т.к. $ghg^{-1} = h \Leftrightarrow gh = hg$ ($\varphi_g(h) = id(h)$ – нейтральный элемент во второй группе).

Тогда $gh = hg$ верно для тех элементов, которые коммутируют с любым, т.е. элементов центра.

Применим теорему о гомоморфизме групп:

$$G/\operatorname{Ker} f \cong \operatorname{Im} f \Leftrightarrow G/Z(G) \cong I_{nn}(G) \qquad \square$$

2.10 Сформулируйте и докажите теорему Кэли.

Теорема (Кэли)**.** Любая конечная группа порядка n изоморфна некоторой подгруппе группы S_n.

Доказательство. Пусть $|G| = n$, и $\forall a \in G$ рассмотрим отображение $L_a : G \to G$, определённое формулой $L_a(g) = a \cdot g$ (умножение слева на a). Покажем, что L_a – это биекция.

Пусть $e, g_1, g_2, \ldots, g_{n-1}$ элементы группы тогда $a \cdot e, a \cdot g, \ldots, a \cdot g_{n-1}$ – те же самые элементы, но в другом порядке ($ag_i = ag_j \Leftrightarrow a^{-1}ag_i = a^{-1}ag_j \Leftrightarrow g_i = g_j$) $\Rightarrow L_a$ – перестановка элементов группы.

Существует нейтральный элемент: $id = L_e$.

По ассоциативности в G: $L_{ab}(g) = (ab)g = a(bg) \Leftrightarrow L_{ab} = L_a \circ L_b$.

При этом относительно операции композиции отображений: $\forall L_a\ \exists (L_a)^{-1} = L_{a^{-1}}$

Таким образом, множество $L_e, L_{g_1}, L_{g_2}, \ldots, L_{g_{n-1}}$ образуют группу H в группе $S(G)$ всех биективных отображений G на себя, т.е. в S_n.

Искомый изоморфизм: $\underbrace{a}_{\in G} \mapsto \underbrace{L_a}_{\in H \subseteq S_n}$ $\square$

2.11 Докажите, что характеристика поля может быть либо простым числом, либо нулем.

Утверждение. $\operatorname{char} P = \begin{cases} 0 \\ p, \ p \text{ – простое} \end{cases}$

Доказательство. Пусть $p \neq 0 \Rightarrow p \geq 2$ ($p \neq 1$, т.к. $1 \neq 0$)

Если $p = mk$, где $1 < m, k < p$, то $0 = \overbrace{1 + \ldots + 1}^{mk} = \overbrace{(1 + \ldots + 1)}^{m}\overbrace{(1 + \ldots + 1)}^{k}$. Обе скобки $\neq 0$, так как p по определению минимальное натуральное число при котором $1 + \ldots + 1 = 0$, а $m, k < p$ $\Rightarrow$ m и k делители нуля, а их нет в поле по определению. □

2.12 Сформулируйте и докажите утверждение о том, каким будет простое подполе в зависимости от характеристики.

Утверждение. Пусть P – поле, а P_0 – его простое подполе. Тогда:

1) Если характеристика поля $\operatorname{char} P = p > 0$, то $P_0 \cong \mathbb{Z}_p$
2) Если $\operatorname{char} P = 0$, то $P_0 \cong \mathbb{Q}$.

Доказательство. Рассмотрим $1 \in P$ (нейтральный элемент по умножению) $\Rightarrow \langle 1 \rangle \subseteq (P, +)$, $\langle 1 \rangle$ – циклическая группа по сложению, порождённая 1.

Кольцо $\langle 1 \rangle$ является подкольцом в P.

Т.к. любое подполе поля P содержит 1, то оно содержит и $\langle 1 \rangle$, т.е. $\langle 1 \rangle \subseteq P_0$.

1) Если $\operatorname{char} P = p > 0$, то $\langle 1 \rangle \cong \mathbb{Z}_p$ – поле $\Rightarrow P_0 = \langle 1 \rangle \cong \mathbb{Z}_p$

   Пример. $\underbrace{\mathbb{Z}_p}_{P_0} \subset \underbrace{\mathbb{Z}_p(x)}_{P}$

2) Если $\operatorname{char} P = 0$, то $\langle 1 \rangle \cong \mathbb{Z}$ (это не поле), значит, в P_0 должны быть все дроби $\dfrac{a}{b}$, где $a, b \in \langle 1 \rangle, b \neq 0$. Они все образуют подполе изоморфное $\mathbb{Q}$.

□

2.13 Сформулируйте и докажите критерий того, что кольцо вычетов по модулю n является полем.

Утверждение. $\mathbb{Z}_p$ является полем $\Leftrightarrow p$ –простое.

Доказательство. Для любого n $\mathbb{Z}_n$ является кольцом с 1. Если n является составным, то $n = mk$, $1 \leq m, k \leq n$, и, следовательно, $\overline{m}\overline{k} = \overline{n} = \overline{0} \Rightarrow$ в кольце есть делители нуля $\Rightarrow$ это не поле.

Если p – простое, рассмотрим $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ – все классы вычетов, кроме $\overline{0}$. Возьмём произвольный элемент $\overline{s}$ и докажем, что $\exists \overline{s}^{-1} : \overline{s} \cdot \overline{s}^{-1} = \overline{1}$. Рассмотрим множество $A = \{\overline{s} \cdot \overline{1}, \overline{s} \cdot \overline{2}, \ldots, \overline{s} \cdot \overline{p-1}\}$ в A нет $\overline{0}$ (т.к. p – простое, а среди чисел нет 0 или кратных 0). Заметим, что в A стоят те же элементы, но в другом порядке (если $\overline{k_1} \cdot \overline{s} = \overline{k_2} \cdot \overline{s} \Leftrightarrow (\overline{k_1} - \overline{k_2})\overline{s} = \overline{0}$, а это возможно только при $\overline{k_1} = \overline{k_2}$) $\Rightarrow$ в наборе $\overline{s}, \overline{s} \cdot \overline{2}, \ldots, \overline{s} \cdot \overline{p-1}$ найдётся 1 $\Rightarrow$ существует элемент $\overline{s}^{-1} : \overline{s} \cdot \overline{s}^{-1} = \overline{1} \Rightarrow \overline{s}$ (он произвольный) обратим. □

2.14 Докажите, что ядро гомоморфизма колец является идеалом.

Лемма. $\operatorname{Ker}\varphi$, где φ – гомоморфизм колец, всегда является идеалом в кольце K_1 ($\varphi : K_1 \to K_2$)

Доказательство.

Идеал:

1) Подгруппа в $(K_1, +)$
2) $\forall a \in \operatorname{Ker}\varphi\, \forall r \in K_1\ ar \in \operatorname{Ker}\varphi$ и $ra \in \operatorname{Ker}\varphi$

Любой гомоморфизм колец является гомоморфизмом их аддитивных групп $(K_1, +)$ и $(K_2, +) \Rightarrow$ $\operatorname{Ker}\varphi$ является нормальной подгруппой в $(K_1, +)$ ($(K_1, +)$ коммутативна). Пусть $a \in \operatorname{Ker}\varphi$, т.е. $\varphi(a) = 0$. Возьмём ar и рассмотрим выражение $\varphi(ar) = \varphi(a) \cdot \varphi(r) = 0 \cdot \varphi(r) = 0$. И аналогично $\varphi(ra) = \varphi(r) \cdot 0 = 0$. □

2.15 Сформулируйте и докажите утверждение о том, когда факторкольцо кольца многочленов над полем само является полем.

Теорема. Пусть P – поле, а $f(x) \in P[x]$. Тогда факторкольцо $P[x]/\langle f(x)\rangle$ является полем $\Leftrightarrow$ многочлен $f(x)$ – неприводим над P.

Доказательство. Если $f(x) = f_1(x) \cdot f_2(x)$ (т.е. не является неприводимым), где $0 < \deg f_i < \deg f$, $\overline{f}_1, \overline{f}_2 \in P[x]/\langle f(x)\rangle$, отличаются от нуля, но $\overline{f_1(x)} \cdot \overline{f_2(x)} = \overline{f(x)} = \overline{0} \Rightarrow$ в $P[x]/\langle f(x)\rangle$ есть делители нуля и это не поле.

Покажем, что если $f(x)$ неприводим, то любой класс вычетов $\overline{a(x)} \neq \overline{0}$ обратим. Представитель $\overline{a(x)}$ это некоторый многочлен $a(x)$ с $\deg a(x) < \deg f(x)$. Т.к. $f(x)$ неприводим, он взаимно прост с $a(x) \Rightarrow \exists b(x), c(x) : a \cdot b + c \cdot f = 1$ (НОД), т.е. $\overline{a}\overline{b} + \overline{c}\overline{f} = \overline{1}$, т.е. $\overline{a} \cdot \overline{b} = \overline{1} \mod \langle f(x)\rangle$, т.е. $\overline{b}$ – обратный элемент к $\overline{a}$ в $P[x]/\langle f(x)\rangle$. □

2.16 Выпишите и докажите формулу для описания изменения координат вектора при изменении базиса.

Утверждение. Пусть $x \in L$, $\mathcal{A}$ и $\mathcal{B}$ – базисы в L.

$x^a = (x_1^a, \ldots, x_n^a)^T$ – столбец координат вектора x в базисе $\mathcal{A}$.

$x^b = (x_1^b, \ldots, x_n^b)^T$ – столбец координат вектора x в базисе $\mathcal{B}$.

Тогда $x^b = T_{\mathcal{A}\to\mathcal{B}}^{-1}\, x^a \Leftrightarrow X' = T^{-1}X$, где X' – координаты в новом базисе.

Доказательство. Докажем, что $x^b = T_{\mathcal{A}\to\mathcal{B}}^{-1}\, x^a$ (из невырожденности матрицы перехода будет следовать нужная формула).

$$x = a \cdot x^a = (a_1, \ldots, a_n) \begin{pmatrix} x_1^a \\ \vdots \\ x_n^a \end{pmatrix} = x_1^a a_1 + \ldots + x_n^a a_n = bx^b$$

$$b = a \cdot T_{\mathcal{A} \to \mathcal{B}} \Rightarrow a \cdot x^a = b \cdot x^b, ax^a = a \cdot T_{\mathcal{A} \to \mathcal{B}} \cdot x^b$$

$$x^a = T_{\mathcal{A} \to \mathcal{B}} \cdot x^b \Rightarrow x^b = T_{\mathcal{A} \to \mathcal{B}}^{-1} \cdot x^a$$

□

2.17 Выпишите формулу для преобразования матрицы билинейной формы при замене базиса и докажите её.

Утверждение. Пусть U – матрица перехода от базиса e к базису f. Пусть B_e – матрица билинейной формы в базисе e. Тогда:

$$B_f = U^T B_e U$$

Доказательство. $b(x, y) = (x^e)^T \cdot B_e \cdot y^e$, где x^e – столбец координат в базисе e

$x^e = Ux^f$ (x^e – старые координаты, а x^f – новые)

$y^e = Uy^f$ (y^e – старые координаты, а y^f – новые)

$$(Ux^f)^T \cdot B_e \cdot (U \cdot y^f) = (x^f)^T \cdot \underbrace{U^T \cdot B_e \cdot U}_{B_f} \cdot y^f = (x^f)^T B_f y^f \Rightarrow B_f = U^T B_e U$$

□

2.18 Сформулируйте и докажите теорему о гомоморфизме колец.

Теорема (о гомоморфизме колец)**.** Пусть K_1, K_2 – два кольца, $\varphi : K_1 \to K_2$ – гомомрфизм. Тогда

$$\underbrace{K_1 / \operatorname{Ker} \varphi}_{\text{факторкольцо}} \cong \underbrace{\operatorname{Im} \varphi}_{\text{кольцо}}$$

Доказательство. Ядро $\operatorname{Ker} \varphi$ является идеалом (по лемме*) $\Rightarrow K_1 / \operatorname{Ker} \varphi$ корректно определён. Рассмотрим отображение $\tau : k_1 / \operatorname{Ker} \varphi \to \operatorname{Im} \varphi$. Выполняется $\tau(a + I) = \varphi(a)$ из доказательства теоремы о гомоморфизме групп $\Rightarrow \tau$ – корректно определено и является гомоморфизмом групп по сложению. Остаётся проверить, что τ сохраняет умножение:

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

Значит, τ – гомоморфизм колец. И, т.к. τ является биекцией (из теоремы о гомомрфизме групп), то это изоморфизм (между $K_1 / \operatorname{Ker} \varphi$ и $\operatorname{Im} \varphi$).

Лемма. * Ядро $\operatorname{Ker}\varphi$, где φ – гомоморфизм колец, всегда является идеалом в кольце K_1 ($\varphi : K_1 \to K_2$)

□

2.19 Что такое сумма и прямая сумма подпространств? Сформулируйте и докажите критерий того, что сумма подпространств является прямой.

Определение. Множество $H_1 + H_2 = \{x_1 + x_2 \mid x_1 \in H_1, x_2 \in H_2\}$ называется суммой подпространств H_1 и H_2.

Определение. Сумма подпространств $H_1 + H_2$ называется прямой и обозначается $H_1 \oplus H_2$, где $H_1 \cap H_2 = \{0\}$, т.е. тривиально.

Утверждение. $H_1 + H_2$ является прямой суммой $\Leftrightarrow \forall x \in H_1 + H_2$ единственным образом представляется $x_1 \in H_1$ и $x_2 \in H_2$ в виде $x = x_1 + x_2$.

Доказательство.

Необходимость. Дано: сумма прямая, т.е. $H_1 \cap H_2 = \{0\}$

Доказать: $x = x_1 + x_2$ представляется единственным образом

Предположим, что есть 2 разложения: $x = x_1 + x_2$ и $x = y_1 + y_2$, $x_1, y_1 \in H_1$, $x_2, y_2 \in H_2$. Вычтем их друг из друга:

$$x_1 - y_1 = y_2 - x_2 = 0 \Rightarrow \begin{cases} x_1 = y_1 \\ x_2 = y_2 \end{cases}$$

Достаточность. Дано: $x = x_1 + x_2$ представляется единственным образом

Доказать: сумма прямая

Если мы предположим, что $\exists x \neq 0 : x \in H_1 \cap H_2$, то $\forall \alpha \in F : \alpha x \in H_1$ и $\alpha x \in H_2$. Тогда $\forall \beta \in F : x = x - \beta x + \beta x = \underbrace{(1-\beta)x}_{\in H_1} + \underbrace{\beta x}_{\in H_2} \Rightarrow$ представление не единственно. □

2.20 Сформулируйте и докажите утверждение о связи размерности суммы и пересечения подпространств.

Утверждение. Пусть H_1 и H_2 – подпространства в L. Тогда:

$$\dim(H_1 + H_2) = \dim(H_1) + \dim(H_2) - \dim(H_1 \cap H_2)$$

Доказательство. Рассмотрим базис $H_1 \cap H_2$. Дополним его до базиса в H_1 и до базиса в H_2. Пусть $\dim H_1 = n$, $\dim H_2 = m$, $\dim(H_1 \cap H_2) = r$.

Обозначим базисные векторы следующим образом:

$$\underbrace{e_1, \ldots, e_r}_{\text{базис в } H_1 \cap H_2}, \quad \underbrace{v_1, \ldots, v_{n-r}}_{\text{дополнение до } H_1}, \quad \underbrace{w_1, \ldots, w_{m-r}}_{\text{дополнение до } H_2}$$

Это базис в $H_1 + H_2$, т.к. любой вектор из $H_1 + H_2$ может быть выражен через них, и они л.н.з. Таким образом, можем найти размерность $H_1 + H_2$:

$$\dim(H_1 + H_2) = r + (n - r) + (m - r) = n + m - r = \dim H_1 + \dim H_2 - \dim(H_1 \cap H_2)$$

$\square$

4-й модуль

1 Определения

1.1 Дайте определение квадратичной формы.

Определение. Однородный многочлен от n переменных, то есть:

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

называют квадратичной формой.

1.2 Дайте определения положительной и отрицательной определенности квадратичной формы.

Определение. Квадратичную форму $Q(x)$ будем называть:

- Положительно определенной, если $\forall x \neq 0\ \ Q(x) > 0$
- Отрицательно определенной, если $\forall x \neq 0\ \ Q(x) < 0$

1.3 Дайте определения канонического и нормального вида квадратичной формы.

Определение. Квадратичную форму $Q(x) = \alpha_1 x_1^2 + \dots + \alpha_n x_n^2, \alpha_i \in \mathbb{R}, i = \overline{1, n}$ (т.е. не имеющую попарных произвольных элементов) называют квадратичной формой канонического вида. Если $\alpha_i \in \{0, 1, -1\}$ то канонический вид называют нормальным.

1.4 Сформулируйте критерий Сильвестра и его следствие.

Теорема (критерий Сильвестра)**.** Квадратичная форма $Q(x)$ от n переменных $x = (x_1, \dots, x_n)$ положительно определена $\Leftrightarrow \Delta_1 > 0, \dots, \Delta_n > 0$

$$\Delta_1 = a_{11}, \Delta_2 = \begin{vmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{vmatrix}, \dots, \Delta_n = \det A \text{ – последовательность главных угловых миноров.}$$

Следствие. $Q(x)$ отрицательно определена $\Rightarrow \Delta_1 < 0, \Delta_2 > 0, \Delta_3 < 0, \dots, (-1)^n \Delta_n > 0$, т.е. знаки главных угловых миноров чередуются, начиная с минуса.

1.5 Сформулируйте закон инерции квадратичных форм. Что такое индексы инерции?

Теорема (Закон инерции квадратичных форм)**.** Для любых двух канонических видов:

$$Q_1(y_1, \ldots, y_n) = \lambda_1 y_1^2 + \ldots + \lambda_m y_m^2,\ \lambda_i \neq 0,\ i = \overline{1, m}$$

$$Q_2(z_1, \ldots, z_n) = \mu_1 z_1^2 + \ldots + \mu_k z_k^2,\ \mu_j \neq 0,\ j = \overline{1, k}$$

одной и той же квадратичной формы выполнено:

1) $m = k =$ рангу квадратичной формы
2) количество положительных $\lambda_i =$ количеству положительных $\mu_j = i_+$
3) количество отрицательных $\lambda_i =$ количеству отрицательных $\mu_j = i_-$

Числа i_+ и i_- называют положительными и отрицательными индексами инерции (они являются инвариантами квадратичной формы).

1.6 Дайте определение линейного отображения. Приведите пример.

Пусть V_1 и V_2 два линейных (конечномерных) пространства.

Определение. Отображение $\varphi : V_1 \to V_2$ называется линейным, если $\forall \alpha, \beta \in \mathbb{R}$:

1) $\forall x, y \in V_1\ \varphi(x + y) = \varphi(x) + \varphi(y)$
2) $\forall x \in V_1,\ \forall \alpha \in F\ \varphi(\alpha x) = \alpha \varphi(x)$

Пример. $D : g \to g'$ в $\mathbb{R}[x]$ (дифференцирование)

$$\dim \mathbb{R}_n[x] = n + 1$$

$$\operatorname{Im} D = \mathbb{R}_{n-1}[x] \Rightarrow \dim \operatorname{Im} D = n$$

$$\operatorname{Ker} D = L(1) \text{ – константы}$$

$$\dim \operatorname{Ker} D = 1 \text{ (и } \dim \operatorname{Im} D + \dim \operatorname{Ker} D = n + 1)$$

Но $\operatorname{Ker} D \cap \operatorname{Im} D \neq \{0\}$ и $\operatorname{Ker} D + \operatorname{Im} D = \mathbb{R}_{n-1}[x] \neq \mathbb{R}_n[x]$.

1.7 Дайте определение матрицы линейного отображения.

Пусть $e_1, \ldots, e_n$ – базис в V_1, $\dim V_1 = n$, $f_1, \ldots, f_m$ – базис в V_2 ($\dim V_2 = m$). Рассмотрим образы $\varphi(e_1), \ldots, \varphi(e_n) \in V_2$ и разложим их по базису $f_1, \ldots, f_m$ в V_2.

$$\begin{cases} \varphi(e_1) = a_{11} f_1 + a_{21} f_2 + \ldots + a_{m1} f_m \\ \vdots \\ \varphi(e_n) = a_{1n} f_1 + a_{2n} f_2 + \ldots + a_{mn} f_m \end{cases}$$

Определение. Матрица линейного отображения – это матрица:

$$A_{ef} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{12} & \dots & a_{2n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

По столбцам матрицы стоят координаты образов векторов базиса V_1 в базисе V_2.

1.8 Выпишите формулу для преобразования матрицы линейного отображения при замене базисов. Как выглядит формула в случае линейного оператора?

Утверждение. Пусть φ – линейное отображение из линейного пространства V_1 в V_2. Пусть матрица $A_{\varepsilon_1\varepsilon_2}$ – матрица линейного отображения в паре базисов: ε_1 – базис в V_1, ε_2 – в V_2. И пусть даны две матрицы перехода: T_1 – матрица перехода от ε_1 к ε_1' в V_1, T_2 – матрица перехода от ε_2 к ε_2' в V_2. Тогда

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

Для линейного оператора:

$$A' = T^{-1} \cdot A \cdot T$$

1.9 Сформулируйте утверждение о связи размерностей ядра и образа линейного отображения.

Утверждение. Пусть $\varphi : V_1 \to V_2$ – линейное отображение. Тогда $\dim \operatorname{Ker} \varphi + \dim \operatorname{Im} \varphi = \dim V_1$.

1.10 Дайте определения собственного вектора и собственного значения линейного оператора.

Определение. Число λ называется собственным числом (значением, с.з.) линейного оператора $\varphi : V \to V$, если существует вектор $x \in V$, $x \neq 0$ такой, что $\varphi x = \lambda x$. При этом вектор x называется собственным вектором (с.в.), отвечающим с.з. λ.

1.11 Дайте определения характеристического уравнения и характеристического многочлена квадратной матрицы.

Определение. Для произвольной квадратной матрицы A определитель $\chi_A(\lambda) = \det(A - \lambda E)$ называют характеристическим многочленом матрицы A.

Определение. Характеристическое уравнение – $\chi_A(\lambda) = \det(A - \lambda E) = 0$.

1.12 Сформулируйте утверждение о связи характеристического уравнения и спектра линейного оператора.

Теорема. λ – с.з. линейного оператора $A \Leftrightarrow \lambda$ – корень характеристического многочлена (над алгебраически замкнутым полем или, если корень принадлежит рассматриваемую полю F).

1.13 Дайте определение собственного подпространства.

Утверждение. Пусть $A : V \to V$ – л.о. и λ – его с.з. Тогда множество $V_\lambda = \{x \in V \mid Ax = \lambda x\}$ – подпространство в V (называется собственным подпространством, отвечающим λ).

1.14 Дайте определения алгебраической и геометрической кратности собственного значения. Какое неравенство их связывает?

Определение. Алгебраической кратностью называется кратность λ как корня характеристического уравнения.

Определение. Размерность подпространства V_λ называется геометрической кратностью с.з. λ. Геометрическая кратность равна $\dim V_\lambda = \dim \operatorname{Ker}(A - \lambda I)$

Утверждение. Геометрическая кратность с.з. не превышает его алгебраической кратности.

1.15 Каким свойством обладают собственные векторы линейного оператора, отвечающие различным собственным значениям?

Утверждение. Пусть $\lambda_1, \ldots, \lambda_k$ – с.з. линейного оператора A, $\lambda_i \neq \lambda_j$, $i \neq j$ (они различны), а $v_1, \ldots, v_k$ – соответствующие с.в. Тогда $v_1, \ldots, v_k$ – линейно независимые. Т.е. с.в., отвечающие различным с.з. линейно независимы.

1.16 Сформулируйте критерий диагональности матрицы оператора.

Утверждение. Матрица л.о. является диагональной в данном базисе $\Leftrightarrow$ все векторы этого базиса являются собственными векторами для данного л.о.

1.17 Сформулируйте критерий диагонализируемости матрицы оператора с использованием понятия геометрической кратности.

Теорема. Л.о. диагонализируем $\Leftrightarrow$ для любого его с.з. λ_j $a_{\lambda_j} = g_{\lambda_j}$ (алгебраическая кратность λ_j равна геометрической).

1.18 Дайте определение евклидова пространства.

Определение. Евклидово пространство – это пара, состоящая из пространства V над $\mathbb{R}$ и функции $g(x, y) : V \times V \to \mathbb{R}$ (скалярное произведение).

1) $\forall x, y \in V$ $g(x, y) = g(y, x)$ – симметричность.
2) Линейность по каждому из аргументов: $g(x + y, z) = g(x, z) + g(y, z)$.
3) $\forall \alpha \in \mathbb{R}$ $g(\alpha x, y) = \alpha g(x, y)$.
4) Положительная определённость: $\forall x \in V$, $x \neq 0$ $g(x, x) > 0$
   $g(x, x) = 0 \Leftrightarrow x = 0$ (невырожденность).

1.19 Выпишите неравенства Коши-Буняковского и треугольника.

Теорема. $\forall x, y \in E$ справедливо неравенство: $|g(x, y)| \leq \|x\|\|y\|$.

Следствие (неравенство треугольника)**.** $\forall x, y \in E$ $\|x + y\| \leq \|x\| + \|y\|$

1.20 Дайте определения ортогонального и ортонормированного базисов.

Определение. Если $k = \dim V$, то система ненулевых векторов $v_1, \ldots, v_k$ будет базисом

1) ортогональным, если $(v_i, v_j) = 0$, $\forall i, j = \overline{1, k}$, $i \neq j$ (все векторы попарно ортогональны).
2) ортонормированным, если он ортогональный и $(v_i, v_i) = 1$, $i = \overline{1, k}$ (все векторы нормированы).

1.21 Дайте определение матрицы Грама.

Пусть $a_1, \ldots, a_n$ – базис в евклидовом пространстве E. Тогда скалярное произведение в координатах записывается следующим образом:

$$g(x, y) = X^T \Gamma Y$$

где X, Y – столбцы координат векторов x и y в базисе $a_1, \ldots, a_n$, а Γ – это матрица скалярного произведения как билинейной формы.

$$\Gamma = \begin{pmatrix} g(a_1, a_1) & \ldots & g(a_1, a_n) \\ \vdots & & \vdots \\ g(a_1, a_n) & \ldots & g(a_n, a_n) \end{pmatrix}$$

1.22 Выпишите формулу для вычисления скалярного произведения векторов, заданных своими координатами в произвольном базисе трехмерного пространства.

Теорема. Пусть $\vec{a} = a_1\vec{e_1} + \ldots + a_n\vec{e_n}$, $\vec{b} = b_1\vec{e_1} + \ldots + b_n\vec{e_n}$ – разложение векторов $\vec{a}$ и $\vec{b}$ по базису. Тогда их скалярное произведение может быть вычислено по формуле:

$$(\vec{a}, \vec{b}) = \begin{pmatrix} a_1 & \ldots & a_b \end{pmatrix} \cdot \begin{pmatrix} (\vec{e_1}, \vec{e_1}) & \ldots & (\vec{e_1}, \vec{e_n}) \\ \vdots & \ddots & \vdots \\ (\vec{e_n}, \vec{e_1}) & \ldots & (\vec{e_n}, \vec{e_n}) \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_3 \end{pmatrix} = a^T \Gamma b$$

1.23 Выпишите формулу для преобразования матрицы Грама при переходе к новому базису.

Матрицы Грама двух базисов e и e' связаны между собой так:

$$\Gamma' = U^T \Gamma U$$

где U – матрица перехода от e к e'.

1.24 Как меняется определитель матрицы Грама (грамиан) при применении процесса ортогонализации Грама-Шмидта?

Утверждение. Определитель матрицы Грама (грамиан) не изменяется при применении процесса ортогонализации Грама-Шмидта.

1.25 Сформулируйте критерий линейной зависимости с помощью матрицы Грама.

Утверждение. Векторы $a_1, \ldots, a_k \in E$ – л.н.з. $\Leftrightarrow$ $\mathrm{Gr}(a_1, \ldots, a_k) \neq 0$.

1.26 Дайте определение ортогонального дополнения.

Определение. Пусть $H \subseteq V$ – подпространство в линейном пространстве V. Тогда множество

$$H^{\perp} = \{x \in V \mid (x, y) = 0 \,\forall y \in H\}$$

называется ортогональным дополнением.

1.27 Дайте определения ортогональной проекции вектора на подпространство и ортогональной составляющей.

Определение. $\forall x \in V$ доказано, что $\exists y \in H, z \in H^{\perp} : x = y + z$.

Тогда y называется ортогональной проекцией x на H, а z называется ортогональной составляющей x относительно H.

Оба вектора y и z определены однозначно (для данного x).

1.28 Выпишите формулу для ортогональной проекции вектора на подпространство, заданное как линейная оболочка данного линейно независимого набора векторов.

Утверждение. Пусть $H = L(a_1, \ldots, a_k)$ и $a_1, \ldots, a_k$ – л.н.з. Тогда

$$y = \text{пр}_H x = A(A^T A)^{-1} A^T x$$

где A составлена из столбцов координат векторов $a_1, \ldots, a_k$ в ОНБ.

1.29 Выпишите формулу для вычисления расстояния с помощью определителей матриц Грама.

Утверждение. Расстояние $\rho(P, M)$ между линейным многообразием P и точкой M (с радиус-вектором x), где $P = x_0 + L(\underbrace{a_1, \ldots, a_k}_{\text{л.н.з.}})$ $(a_1, \ldots, a_k$ – ФСР ОСЛАУ) может быть найден по формуле:

$$\rho(P, M) = \sqrt{\frac{\mathrm{Gr}(a_1, \ldots, a_k, x - x_0)}{\mathrm{Gr}(a_1, \ldots, a_k)}}$$

1.30 Дайте определение сопряженного оператора в евклидовом пространстве.

Определение. Линейный оператор $A^* : E \to E$ называется сопряжённым к л.о. $A : E \to E$, если:

$$\forall x, y \in E : (\mathcal{A}x, y) = (x, \mathcal{A}^* y)$$

1.31 Дайте определение самосопряженного (симметрического) оператора.

Определение. Л.о. A называется самосопряжённым (симметрическим), если:

$$\forall x, y \in E : (\mathcal{A}x, y) = (x, \mathcal{A}y)$$

1.32 Как найти матрицу сопряженного оператора в произвольном базисе?

Теорема. Для любого линейного оператора в евклидовом пространстве существует единственный сопряжённый оператор $A^* : E \to E$, причём его матрицей в базисе b будет матрица $A^*_b = \Gamma^{-1} A^T_b \Gamma$, где Γ – матрица Грама базиса b.

1.33 Каким свойством обладают собственные значения самосопряженного оператора?

Теорема. Все корни характеристического уравнения самосопряжённого линейного оператора являются действительными числами.

1.34 Что можно сказать про собственные векторы самосопряженного оператора, отвечающие разным собственным значениям?

Утверждение. С.в. самосопряжённого л.о., отвечающее различным с.з., ортогональны.

1.35 Сформулируйте определение ортогональной матрицы.

Определение. Квадратную матрицу O называют ортогональной, если $O^T O = E$.

1.36 Сформулируйте определение ортогонального оператора.

Определение. Линейный оператор $A : E \to E$ называется ортогональным, если:

$$\forall x, y \in E\ (Ax, Ay) = (x, y)$$

Т.е. A сохраняет скалярное произведение.

1.37 Сформулируйте критерий ортогональности оператора, использующий его матрицу.

Теорема. Матрица л.о. A в ОНБ ортогональна $\Leftrightarrow$ A – ортогональный л.о.

1.38 Каков канонический вид ортогонального оператора? Сформулируйте теорему Эйлера.

Теорема (о каноническом виде ортогонального оператора)**.** Для любого ортогонального линейного оператора существует ОНБ, в котором его матрица имеет следующий блочно-диагональный вид:

$$A' = \begin{pmatrix} A_1 & & & & & & & & \\ & \ddots & & & & \text{\Huge 0} & & & \\ & & A_k & & & & & & \\ & & & 1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & 1 & & & \\ & \text{\Huge 0} & & & & & -1 & & \\ & & & & & & & \ddots & \\ & & & & & & & & -1 \end{pmatrix}, \text{ где } A_k = \begin{pmatrix} \cos\varphi_k & -\sin\varphi_k \\ \sin\varphi_k & \cos\varphi_k \end{pmatrix} \text{ – матрица поворота}$$

Следствие (теорема Эйлера)**.** Любой ортогональный оператор в $\mathbb{R}^3$ может быть приведён к следующему каноническому виду:

$$A' = \begin{pmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}$$

Т.е. любой ортогональный оператор является либо поворотом на некоторый угол вокруг некоторой оси, либо композицией поворота и отражения.

1.39 Сформулируйте теорему о существовании для самосопряженного оператора базиса из собственных векторов.

Теорема. Для любого самосопряжённого л.о. A существует ОНБ, состоящий из его с.в. В этом базисе матрица л.о. диагональна, а на диагонали стоят собственные значения, повторяющиеся столько, какова их алгебраическая кратность.

1.40 Сформулируйте теорему о приведении квадратичной формы к диагональному виду при помощи ортогональной замены координат.

Теорема. Любую квадратичную форму можно ортогональным преобразованием привести к каноническому виду.

1.41 Сформулируйте утверждение о QR-разложении.

Утверждение (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, такие что $A = QR$, где Q – ортогональные матрицы, R – верхнетреугольные.

1.42 Сформулируйте теорему о сингулярном разложении.

Теорема (о сингулярном разложении)**.** Для любой прямоугольной матрицы $A \in M_{mn}(\mathbb{R})$ имеет место следующее разложение:

$$A = V\Sigma U^T$$

Оно называется сингулярным (SVD). Здесь $U \in O_n(\mathbb{R})$, $V \in O_m(\mathbb{R})$ – ортогональные матрицы, $\Sigma \in M_{mn}(\mathbb{R})$ – диагональная матрица с $\sigma_i \geq 0$ на диагонали. Причём, что $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_r > 0$, $r = \operatorname{Rg} A$. Числа σ_i называются сингулярными.

1.43 Сформулируйте утверждение о полярном разложении.

Утверждение (полярное разложение)**.** Любой линейный оператор в евклидовом пространстве представляется в виде композиции симметрического и ортогонального $A = S \cdot U$, S – симметрический л.о., U – ортогональный л.о.

1.44 Дайте определение сопряжённого пространства

Определение. Пространством, сопряженным (двойственным) к линейному пространству L называется множество всех линейных функционалов на L с операциями сложения и умножения на число $\forall x \in V, \lambda \in F$:

$$(f_1 + f_2)(x) = f_1(x) + f_2(x)$$

$$(\lambda f)(x) = \lambda f(x)$$

Обозначение. L^* – сопряжённое к линейному пространство.

1.45 Выпишите формулу для преобразования координат ковектора при переходе к другому базису.

Утверждение. Пусть e и g – два базиса в V. Тогда

$$[f]_g = [f]_e \cdot T_{e \to g}$$

1.46 Дайте определение взаимных базисов

Определение. Базис $e = (e_1, \dots, e_n)$ в линейном пространстве L и базис $f = (f^1, \dots, f^n)$ в L^* называются взаимными, если

$$f^i(e_j) = \delta^i_j = \begin{cases} 1, \ i = j \\ 0, \ i \neq j \end{cases}$$

1.47 Дайте определение биортогонального базиса

Определение. Если отождествить E и E^*, то базис взаимный к данному, называется биортогональным.

1.48 Что можно сказать про ортогональное дополнение к образу сопряженного оператора?

Утверждение. $(\operatorname{Im} A^*)^\perp = \operatorname{Ker} A$

2 Доказательства

2.1 Сформулируйте и докажите (включая лемму) теорему об инвариантности ранга матрицы квадратичной формы.

Лемма. Пусть $A, S \in M_n(\mathbb{R})$, $\det S \neq 0$. Тогда $\operatorname{Rg}(A \cdot S) = \operatorname{Rg} A = \operatorname{Rg}(S \cdot A)$, т.е. умножение на невырожденную матрицу S не меняет ранг матрицы A

Доказательство. $\operatorname{Rg}(A \cdot S) \leq \operatorname{Rg} A$, т.к. столбцы матрицы $A \cdot S$ – это линейные комбинации столбцов матрицы A, а ранг равен максимальному количеству л.н.з. столбцов (теорема о ранге матрицы) $\Rightarrow$ число л.н.з. столбцов не может вырасти и $\operatorname{Rg}(A \cdot S) \leq \operatorname{Rg} A$.

$$\operatorname{Rg} A = \operatorname{Rg}(A \cdot \underbrace{S \cdot S^{-1}}_{E}) \leq \operatorname{Rg}(A \cdot S) \Rightarrow \operatorname{Rg} A = \operatorname{Rg}(A \cdot S)$$

□

Утверждение (об инвариантности ранга)**.** Пусть Q – квадратичная форма на линейном пространстве V, $a = \{a_1, \dots, a_n\}$, $b = \{b_1, \dots, b_n\}$ – базисы в V.

Пусть A – матрица $Q(x)$ в базисе a, B – матрица $Q(x)$ в базисе b. Тогда $\operatorname{Rg} A = \operatorname{Rg} B$ (ранги матриц квадратичных форм).

Доказательство. Мы знаем, что $B = S^T \cdot A \cdot S$, где $S = T_{a \to b}$ – матрица перехода, и она всегда невырождена. По лемме при умножении A на невырожденные матрицы S и S^T её ранг не изменится, значит, $\operatorname{Rg} B = \operatorname{Rg} A$. □

2.2 Сформулируйте и докажите утверждение о связи размерностей ядра и образа линейного отображения.

Утверждение. Пусть $\varphi : V_1 \to V_2$ – линейное отображение. Тогда

$$\dim \operatorname{Ker} \varphi + \dim \operatorname{Im} \varphi = m = \dim V_1$$

Доказательство. Выберем базис в $V_1 : e = \{e_1, \dots, e_m\}$. Тогда $\forall x \in V_1$ можно представить в виде: $x = x_1 e_1 + \ldots + x_m e_m$. Следовательно, $\varphi(x) = x_1 \varphi(e_1) + \ldots + x_m \varphi(e_m)$, где $\varphi(e_1), \dots, \varphi(e_m)$ – столбцы матрицы линейного отображения φ.

Т.е. $\operatorname{Im} \varphi = L(\varphi(e_1), \dots, \varphi(e_m)) \Rightarrow \dim \operatorname{Im} \varphi = \operatorname{Rg} A$ – ранг матрицы линейного отображения. Ядро отображения записывается однородной системой (СЛАУ): $Ax = 0 \Rightarrow \dim \operatorname{Ker} \varphi$ – это число элементов ФСР $Ax = 0$. Но число элементов в ФСР:

$$m - \operatorname{Rg} A = \dim \operatorname{Ker} \varphi \Rightarrow \dim \operatorname{Ker} \varphi + \dim \operatorname{Im} \varphi = m$$

□

2.3 Сформулируйте и докажите утверждение о связи характеристического уравнения и спектра линейного оператора.

Теорема. λ – с.з. линейного оператора $A \Leftrightarrow \lambda$ – корень характеристического многочлена (над алгебраически замкнутым полем или, если корень принадлежит рассматриваемую полю F).

Доказательство.

Необходимость. Дано: λ – с.з.

Доказать: λ – корень характеристического многочлена

По определению $\exists x \neq 0 : Ax = \lambda x$, т.е. $Ax = \lambda \cdot I \cdot x \Leftrightarrow (A - \lambda I)x = 0$, где I – тождественный оператор.

Запишем равенство $(A - \lambda I)x = 0$ в некотором базисе e:

$$(A_e - \lambda E)x^e = 0$$

Это однородная СЛАУ, и она имеет ненулевое решение $\Rightarrow \det(A_e - \lambda E) = 0$, т.е. λ – корень характеристического уравнения.

Достаточность. Дано: λ – корень характеристического многочлена

Доказать: λ – с.з.

Если λ – корень, то в заданном базисе выполняется равенство: $\det(A_e - \lambda E) = 0 \Rightarrow$ соответствующая СЛАУ с матрицей $(A_e - \lambda E)$ имеет ненулевое решение (используется критерий существования решения однородной СЛАУ с квадратной матрицей).

Это решение можно интерпретировать как набор координат некоторого вектора, для которого выполняется $(A - \lambda I)x = 0, x \neq 0$. Это по определению означает, что x – с.в., а λ – с.з. $\square$

2.4 Сформулируйте и докажите утверждение о том, каким свойством обладают собственные векторы линейного оператора, отвечающие различным собственным значениям.

Утверждение. Пусть $\lambda_1, \ldots, \lambda_k$ – с.з. линейного оператора A, $\lambda_i \neq \lambda_j$, $i \neq j$ (они различны), а $v_1, \ldots, v_k$ – соответствующие с.в. Тогда $v_1, \ldots, v_k$ – линейно независимые. Т.е. с.в., отвечающие различным с.з. линейно независимы.

Доказательство. Применим принцип математической индукции. При $k = 1$ верно, т.к. с.в. по определению не 0 и, соответственно, л.н.з.

Пусть уравнение верно для $k = m$. Добавим ещё один с.в. v_{m+1}. Докажем, что система из векторов $v_1, \dots, v_m, v_{m+1}$ осталась л.н.з. Рассмотрим равенство

$$(1) : \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_m v_m + \alpha_{m+1} v_{m+1} = 0$$

Применим к (1) линейный оператор A:

$$\alpha_1 A v_1 + \ldots + \alpha_m A v_m + \alpha_{m+1} A v_{m+1} = 0 \Rightarrow \ (2) : \alpha_1 \lambda_1 v_1 + \ldots + \alpha_m \lambda_m v_m + \alpha_{m+1} \lambda_{m+1} v_{m+1} = 0$$

Умножим (1) на λ_{m+1} и вычтем его из (2):

$$\alpha_1(\lambda_1 - \lambda_{m+1}) v_1 + \ldots + \alpha_m(\lambda_m - \lambda_{m+1}) v_m = 0$$

Т.к. все λ_i различны, а $v_1, \dots, v_m$ – л.н.з., то:

$$\begin{cases} \alpha_1(\lambda_1 - \lambda_{m+1}) = 0 \\ \ldots \\ \alpha_m(\lambda_m - \lambda_{m+1}) = 0 \end{cases} \Rightarrow \begin{cases} \alpha_1 = 0 \\ \ldots \\ \alpha_m = 0 \end{cases} \Rightarrow (1) \text{ можно записать в виде } \alpha_{m+1} v_{m+1} = 0$$

Т.к. v_{m+1} – с.в., то $v_{m+1} \neq 0 \Rightarrow \alpha_{m+1} = 0$.

По определению (л.н.з. векторов) $v_1, \dots, v_{m+1}$ – л.н.з. Индукционный переход выполнен, значит утверждение верно всегда. □

2.5 Сформулируйте и докажите критерий диагональности матрицы оператора.

Утверждение. Матрица л.о. является диагональной в данном базисе $\Leftrightarrow$ все векторы этого базиса являются собственными векторами для данного л.о.

Доказательство.

Необходимость. Дано: A_e – диагональна.

Доказать: базис e состоит из собственных векторов.

По определению матрицы линейного оператора в j-ом столбце стоят координаты вектора $A(e_j)$ в базисе e. Если матрица диагональна, то j-й столбец имеет вид:

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \\ \lambda_j \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \lambda_j \text{ стоит на } j\text{-ом месте.}$$

Т.е. $A(e_j) = 0 \cdot e_1 + \ldots + 0 \cdot e_{j-1} + \lambda_j e_j + 0 \cdot e_{j+1} + \ldots \Rightarrow Ae_j = \lambda_j e_j$, т.е. по определению собственного вектора e_j – с.в. с с.з. λ_j. Он не равен 0, т.к. это элемент базиса.

Т.к. это верно для $\forall j = \overline{1, n}$, то все базиснве векторы – собственные, а на диагонали стоят с.з.

Достаточность. Дано: $(e_1, \ldots, e_n)$ – базис, и он состоит из с.в.

Доказать: A_e – диагональная.

$Ae_j = \lambda_j e_j$ (по определению с.в.) $\Rightarrow$ если записать по определению матрицу л.о., то все элементы, кроме диагональных, будут нулевыми, а на диагонали стоит число λ_j. □

2.6 Каким свойством обладает оператор в n-мерном вещественном пространстве, у характеристического многочлена которого есть n различных действительных корней?

Теорема (достаточное условие диагонализируемости)**.** Если характеристическое уравнение л.о., действующего в V, где $\dim V = n$, имеет n попарно различных корней, то л.о. диагонализируем (корни лежат в том же поле, над которым рассматривается V).

Доказательство. Если $\lambda_i \in F$ – корень характеристического уравнения, то ему можно сопоставить хотя бы 1 собственный вектор. Но система векторов $v_1, \ldots, v_n$ (отвечающая различным с.з.) будет л.н.з., и их число равно $\dim V \Rightarrow$ они образуют базис, и этот базис состоит из с.в. $\Rightarrow$ в нём есть матрица л.о. диагональная. □

2.7 Выпишите и докажите неравенство Коши–Буняковского. Выпишите и докажите неравенство треугольника.

Теорема. $\forall x, y \in E$ справедливо неравенство: $|g(x, y)| \leq \|x\|\|y\|$.

Доказательство. $\forall \alpha \in \mathbb{R}$ $g(\alpha x - y, \alpha x - y) \geq 0$ (положительная определённость).

$$g(\alpha x - y, \alpha x - y) = \alpha g(x, \alpha x - y) - g(y, \alpha x - y) = \alpha^2 g(x, x) - \alpha g(x, y) - \alpha g(x, y) + g(y, y) =$$
$$= \alpha^2 g(x, x) - 2\alpha g(x, y) + g(y, y) = \alpha\|x\|^2 - 2\alpha g(x, y) + \|y\|^2 \geq 0, \ \forall \alpha \in \mathbb{R}$$

Дискриминант данного уравнения $D \leq 0$ (неравенство на α). Тогда:

$$D = 4g(x, y)^2 - 4\|x\|^2\|y\|^2 \leq 0 \Rightarrow \|g(x, y)\| \leq \|x\|\|y\|$$

□

Следствие (неравенство треугольника)**.** $\forall x, y \in E \ \|x+y\| \leq \|x\| + \|y\|$

Доказательство.

$\|x+y\|^2 = g(x+y, x+y) = g(x,x) + 2g(x,y) + g(y,y) \leq \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 = (\|x\| + \|y\|)^2$

Обе части неотрицательные, следовательно, выполнено неравенство треугольника. □

2.8 Докажите теорему о том, что евклидово пространство можно представить в виде прямой суммы подпространства и его ортогонального дополнения.

Теорема. Ортогональное дополнение $H^\perp$ является линейным подпространством в V и $V = H \oplus H^\perp$ $(\dim V = \dim H + \dim H^\perp)$.

Доказательство. $H^\perp$ является подпространством, т.к. замкнуто относительно операции сложения и умножения на число: $\forall h \in H$, $\forall x, y \in H^\perp$, $\alpha \in \mathbb{R}$

$$(x+y, h) = (x,h) + (y,h) = 0 + 0 = 0 \Rightarrow x + y \in H^\perp$$

$$(\alpha x, h) = \alpha(x,h) = \alpha \cdot 0 = 0 \Rightarrow \alpha x \in H^\perp$$

Т.к. $H^\perp$ является подпространством, то можно рассматривать $H + H^\perp$. Осталось показать, что сумма прямая и что $V = H + H^\perp$.

Если $x \in H \cap H^\perp$, то $(x,x) = 0 \Leftrightarrow x = 0$, т.е. $H \cap H^\perp = \{0\} \Rightarrow$ сумма прямая.

Пусть $f_1, \ldots, f_m$ – ОНБ в H (он всегда существует). Дополним его до базиса в V векторами $f_{m+1}, \ldots, f_n$. Применим принцип ортогонализации Грама-Шмидта:

$f_1, \ldots, f_m, \underbrace{e_{m+1}, \ldots, e_n}_{\text{новые}} \Rightarrow e_{m+1}, \ldots, e_n$ – ортогональны $f_1, \ldots, f_m$ (базис в H) $\Rightarrow$ они ортогональны всему H.

И $\forall x \in V$ можно представить в виде:

$$x = \underbrace{x_1 f_1 + \ldots x_m f_m}_{y \in H} + \underbrace{x_{m+1} e_{m+1} + \ldots + x_n e_n}_{z \in H^\perp}$$

Т.е. $\forall x \in V \ x = y + z$, $y \in H$, $z \in H^\perp$, но это и означает, что всё пространство V равно $H \oplus H^\perp$. □

2.9 Выпишите формулу для преобразования матрицы Грама при переходе к новому базису и докажите её. Что происходит с определителем матрицы Грама при применении процесса ортогонализации Грама-Шмидта? Что можно сказать про знак определителя матрицы Грама? Ответы обоснуйте.

1) Матрицы Грама двух базисов e и e' связаны между собой так:

$$\Gamma' = U^T \Gamma U$$

где U – матрица перехода от e к e'.

Это формула верна, т.к. Γ – матрица билинейной формы $g(x, y)$.

2) $\det \Gamma > 0$

Доказательство. Рассмотрим $\det \Gamma'$:

$$\det \Gamma' = \det(U^T \Gamma U) = \underbrace{\det U^T}_{U} \cdot \det \Gamma \cdot \det U = \underbrace{(\det U)^2}_{>0} \cdot \det \Gamma$$

Перейдём к ОНБ (это всегда можно сделать в конечномерном пространстве). В нём $\Gamma' = E \Rightarrow \det \Gamma' = 1$.

$$1 = \underbrace{(\det U)^2}_{>0} \cdot \det \Gamma \Rightarrow \det \Gamma > 0$$

□

3) Определитель матрицы Грама (грамиан) не изменяется при применении процесса ортогонализации Грама-Шмидта.

Доказательство. $\mathrm{Gr}(a_1, \ldots, a_n) = \det \Gamma(a_1, \ldots, a_n)$.

Матрица перехода от базиса $a_1, \ldots, a_n$ к базису $b_1, \ldots, b_n$ (ортогональный не нормированный) имеет следующий вид:

$$U_{a \to b} = \begin{pmatrix} 1 & & * & \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \Rightarrow \det U_{a \to b} = 1$$

$$\det \Gamma'_b = \det(U^T \Gamma_a U) = (\det U)^2 \cdot \det \Gamma_a = 1 \cdot \det \Gamma_a = \det \Gamma_a$$

□

2.10 Сформулируйте и докажите критерий линейной зависимости набора векторов с помощью матрицы Грама.

Утверждение. Векторы $a_1, \ldots, a_k \in E$ – л.н.з. $\Leftrightarrow \mathrm{Gr}(a_1, \ldots, a_k) \neq 0$.

Доказательство. Рассмотрим линейную комбинацию векторов $a_1, \ldots, a_k$.

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

Умножим (1) скалярно на векторы $(a_1, \ldots, a_k)$:

$$\begin{cases} \alpha_1(a_1, a_1) + \alpha_2(a_1, a_2) + \ldots + \alpha_k(a_1, a_k) = 0 \\ \vdots \\ \alpha_1(a_k, a_1) + \alpha_2(a_k, a_2) + \ldots + \alpha_k(a_k, a_k) = 0 \end{cases}$$

Это однородная СЛАУ на коэффициенты $\alpha_1, \ldots, \alpha_k$, т.е. СЛАУ вида $\Gamma_{k\times k}(a_1, \ldots, a_k) \cdot \alpha = 0$.
У неё существует нетривиальное решение (векторы л.з.) $\Leftrightarrow \det \Gamma_{k\times k} = 0$.
И, соответственно, $a_1, \ldots, a_k$ – л.н.з $\Leftrightarrow \det \Gamma_{k\times k} \neq 0$. □

2.11 Выпишите формулу ортогональной проекции вектора на её подпространство, заданное как линейная оболочка данного линейного независимого набора векторов, и докажите её

Утверждение. Пусть $H = L(a_1, \ldots, a_k)$ и $a_1, \ldots, a_k$ – л.н.з. Тогда

$$y = \text{пр}_H x = A(A^T A)^{-1} A^T x$$

где A составлена из столбцов координат векторов $a_1, \ldots, a_k$ в ОНБ.

Доказательство. Пусть $y = \text{пр}_H x = \alpha_1 a_1 + \ldots + \alpha_k a_k \in H$ (т.е. $x = \underbrace{\alpha_1 a_1 + \ldots + \alpha_k a_k}_{\in H} + \underbrace{h^\perp}_{\in H^\perp}$).

Теперь последовательно умножим x на $a_1, \ldots, a_k$:

$$\begin{cases} \alpha_1(a_1, a_1) + \alpha_2(a_1, a_2) + \ldots + \alpha_k(a_1, a_k) = (a_1, x) \\ \vdots \\ \alpha_1(a_k, a_1) + \alpha_2(a_k, a_2) + \ldots + \alpha_k(a_k, a_k) = (a_k, x) \end{cases}$$

В матричной форме с матрицей $A = [a_1, \ldots, a_k]$:

$$\Gamma_{k\times k}(a_1, \ldots, a_k) \cdot \alpha = A^T x \Leftrightarrow \underbrace{A^T A}_{\Gamma_{k\times k}} \cdot \alpha = A^T x$$

Т.к. $a_1, \dots, a_k$ – л.н.з. $\Rightarrow \Gamma(a_1, \dots, a_k)$ невырождена $\Rightarrow$ к ней существует обратная. Тогда

$$\Gamma \cdot \alpha = A^T x \Rightarrow \alpha = \Gamma^{-1} \cdot A^T \cdot x = (A^T \cdot A)^{-1} \cdot A^T \cdot x$$

$$y = A\alpha = A(A^T A)^{-1} A^T x$$

□

2.12 Докажите, что для любого оператора в конечномерном евклидовом пространстве существует единственный сопряженный оператор.

Теорема. Для любого линейного оператора в евклидовом пространстве существует единственный сопряжённый оператор $A^* : E \to E$, причём его матрицей в базисе b будет матрица $A_b^* = \Gamma^{-1} A_b^T \Gamma$, где Γ – матрица Грама базиса b.

Доказательство. Покажем, что л.о. с матрицей $B = \Gamma^{-1} A \Gamma$ является сопряжённой к данному л.о. Проверим выполнение равенства:

$$\forall x, y \in E \; (Ax, y) = (x, By)$$

Пусть x^b, y^b – столбцы координат векторов в базисе b. Тогда $(Ax)^b = A_b x^b$ и $(x, y) = x^T \Gamma y$ – матричная запись скалярного произведения. Тогда:

$$\underbrace{((Ax)^b)^T \Gamma y^b}_{(x^b)^T \cdot A_b^T \cdot \Gamma \cdot y^b} = (x^b)^T \Gamma (By)^b \text{ – скалярное произведение в матричной форме}$$

$$(x^b)^T \cdot A_b^T \cdot \Gamma \cdot y^b = (x^b)^T \Gamma (By)^b \overset{\text{лемма}}{\Rightarrow} \Gamma B_b = A_b^T \Gamma \Rightarrow B_b = \Gamma^{-1} A_b^T \Gamma \; (\exists \Gamma^{-1}, \text{ т.к. } \det \Gamma > 0)$$

□

2.13 Сформулируйте и докажите свойство собственных векторов самосопряженного оператора, отвечающих разным собственным значениям.

Утверждение. С.в. самосопряжённого л.о., отвечающее различным с.з., ортогональны.

Доказательство. Пусть $Ax_1 = \lambda_1 x_1$, $x_1 \neq 0$, $Ax_2 = \lambda_2 x_2$, $x_2 \neq 0$, $\lambda_1 \neq \lambda_2$ (т.е. x_1, x_2 – с.в., соответствующие с.з. λ_1, λ_2).

$$\begin{cases} (Ax_1, x_2) = (\lambda_1 x_1, x_2) = \lambda_1 (x_1, x_2) \\ (x_1, Ax_2) = (x_1, \lambda_2 x_2) = \lambda_2 (x_1, x_2) \end{cases} \Rightarrow \underbrace{(\lambda_1 - \lambda_2)}_{\neq 0} (x_1, x_2) = 0 \Rightarrow x_1, x_2 \text{ ортогональны}$$

□

2.14 Каким свойством обладают собственные значения самосопряженного оператора?

Теорема. Все корни характеристического уравнения самосопряжённого линейного оператора являются действительными числами.

Доказательство. Пусть $\widetilde{\lambda} \in \mathbb{C}$ – корень характеристического уравнения $\chi_a(\lambda) = 0$, то есть выполнено $\det(A - \widetilde{\lambda}E) = 0$.

Тогда СЛАУ $(A - \widetilde{\lambda}E)x = 0$ имеет ненулевое решение, состоящее из $x_k \in \mathbb{C}$, $k = \overline{1, n}$:

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Рассмотрим столбец сопряжённых (комплексно) элементов:

$$\overline{x} = \begin{pmatrix} \overline{x_1} \\ \vdots \\ \overline{x_n} \end{pmatrix}$$

Умножим СЛАУ на $\overline{x}^T$ ($= x^*$ обозначение) слева:

$$\overline{x}^T(A - \widetilde{\lambda}E)x = 0 \Leftrightarrow \overline{x}^T Ax - \widetilde{\lambda}\overline{x}^T x = 0$$

$$\bar{x}^T x = \overline{x}_1 x_1 + \ldots + \overline{x}_n x_n = \underbrace{|x_1|^2 + \ldots + |x_n|^2}_{\in \mathbb{R}} > 0, \text{ т.к. решение ненулевое (с.в.)}$$

Тогда:

$$\widetilde{\lambda} = \frac{\overline{x}^T Ax}{\overline{x}^T x} \text{ – отношение Релея}$$

Если докажем, что $z = \overline{x}^T Ax$ является вещественным числом, то $\widetilde{\lambda}$ тоже будет вещественным:

$$z = \overline{x}^T Ax = z^T = (\overline{x}^T Ax)^T = x^T A^T (\overline{x}^T)^T = x^T A^T \overline{x} \overset{A = A^T}{=} x^T A \overline{x}$$

Т.к. матрица вещественная:

$$\overline{z} = \overline{\overline{x}^T Ax} = \overline{\overline{x}}^T \cdot \overline{A} \cdot \overline{x} = x^T A \overline{x} \Rightarrow z = \overline{z} \Rightarrow z \in \mathbb{R} \Rightarrow \widetilde{\lambda} = \frac{z}{\overline{x}^T x} \in \mathbb{R}$$

□

2.15 Сформулируйте теорему о существовании для самосопряженного оператора базиса из собственных векторов. Приведите доказательство в случае различных вещественных собственных значений.

Теорема. Если с.з. $\lambda_1, \ldots, \lambda_n$ самосопряжённого л.о. $A : E \to E$, $\dim E = n$, попарно различны, то в E существует ОНБ, в котором матрица оператора A имеет диагональный вид.

Доказательство. Т.к. $\lambda_1, \ldots, \lambda_n$ – попарно различны, то, выбрав для каждого с.з. соответствующий ему с.в., получим систему ненулевых векторов. По утверждению об ортогональности с.в., отвечающих различным с.з., это будет ортогональная система. Она л.н.з. и содержит n векторов. Значит, она является базисом в E (т.к. $\dim E = n$). Это ортогональный базис. Чтобы получить ОНБ нужно разделить каждый вектор на его норму. Векторы не перестают быть собственными, значит, это исходный базис. □

2.16 Сформулируйте и докажите теорему о том, что ортогональный оператор переводит ортонормированный базис в ортонормированный. Верно ли обратно?

Теорема. Пусть л.о. $A : E \to E$. Тогда A – ортогональный л.о. $\Leftrightarrow$ ОНБ $e_1, \ldots, e_n$ переходит в ОНБ $Ae_1, \ldots, Ae_n$.

Доказательство.

Необходимость. Дано: A – ортогональный л.о. и $e_1, \ldots, e_n$ – ОНБ.

Доказать: $Ae_1, \ldots, Ae_n$ – ОНБ.

$$(Ae_i, Ae_j) = (e_i, e_j) \underset{\substack{\uparrow \\ e_1, \ldots, e_n \text{ – ОНБ}}}{=} \delta^i_j = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}$$

Т.е. система векторов $\{Ae_j\}_{j=1}^n$ состоит из ненулевых векторов и попарно ортогональна – это ОНБ из n векторов $\Rightarrow$ базис в E.

Достаточность. Дано: $Ae_1, \ldots, Ae_n$ – ОНБ и $e_1, \ldots, e_n$ – ОНБ.

Доказать: A – ортогональный л.о.

Рассмотрим соответствие $x \mapsto (x_1, x_2, \ldots, x_n)^T$ в базисе $e_1, \ldots, e_n$.

Заметим, что $Ax \mapsto (x_1, x_2, \ldots, x_n)^T$ в базисе $Ae_1, \ldots, Ae_n$, т.к. для линейного оператора выполняется: $Ax = A(x_1e_1 + \ldots + x_ne_n) = x_1Ae_1 + \ldots + x_nAe_n$.

Найдём скалярное произведение в ОНБ $e_1, \ldots, e_n$ и $Ae_1, \ldots, Ae_n$ соответственно:

$$(x, y) = x_1y_1 + \ldots + x_ny_n \text{ в ОНБ } e_1, \ldots, e_n$$

$$(Ax, Ay) = x_1y_1 + \ldots + x_ny_n \text{ в ОНБ } Ae_1, \ldots, Ae_n$$

$$\forall x, y \in E (Ax, Ay) = (x, y) \Rightarrow \text{ оператор по определению ортогональный}$$

$\square$

2.17 Сформулируйте и докажите критерий ортогональности оператора, использующий его матрицу.

Теорема. Матрица л.о. A в ОНБ ортогональна $\Leftrightarrow$ A – ортогональный л.о.

Доказательство.

Необходимость. Дано: Матрица л.о. A ортогональна в ОНБ e.

Доказать: A – ортогональный линейный оператор.

Так как $A_e^T \cdot A_e = E \Rightarrow \forall x, y \in E$, для их координат в базисе e

$$x \mapsto \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, y \mapsto \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

выполнено:

$$(Ax, Ay) = \left(A_e \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \right)^T A_e \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 & \ldots & x_n \end{pmatrix} (A_e^T \cdot A_e) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 & \ldots & x_n \end{pmatrix} E \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = (x, y)$$

Т.е. $\forall x, y \in E$ $(Ax, Ay) = (x, y) \Rightarrow A$ – ортогональный линейный оператор по определению.

Достаточность. Дано: A – ортогональный линейный оператор.

Доказать: Матрица л.о. A ортогональна в ОНБ e.

По определению: $\forall x, y \in E$ $(Ax, Ay) = (x, y)$.

В любом ОНБ в координатах это можно записать так:

$$(A_ex^e)^T \cdot E \cdot (A_ey^e) = (x^e)^T \cdot y^e \Rightarrow (x^e)^T \cdot A_e^T \cdot A_e \cdot y^e = (x^e)^T \cdot E \cdot y^e$$

По лемме: $A_e^T \cdot A_e = E$. $\square$

2.18 Сформулируйте и докажите утверждение о QR-разложении.

Утверждение (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, такие что $A = QR$, где Q – ортогональные матрицы, R – верхнетреугольные.

Доказательство. Применим к столбцам $A_1, \ldots, A_m$ процесс ортогонализации Грама-Шмидта. Получим столбцы $Q_1, \ldots, Q_m$ – ОНБ в $\operatorname{Im} A$. Заметим, что $A_k \in L(Q_1, \ldots, Q_m)$, $k = \overline{1, m}$ (по формулам Грама-Шмидта мы используем только столбцы с меньшими или равными номерами). Тогда

$$A_k = \sum_{i=1}^{k} r_{ik} Q_i, \ k = \overline{1, m}$$

В матричной форме:

$$A = QR, \text{ где } Q = (Q_1 | \ldots | Q_m), \ R = \begin{pmatrix} r_{11} & \ldots & r_{1m} \\ & \ddots & \vdots \\ \Large 0 & & r_{mm} \end{pmatrix}$$

Матрица Q является ортогональной, так как $Q_1, \ldots, Q_m$ образуют ОНБ. □

2.19 Сформулируйте и докажите теорему о сингулярном разложении.

Теорема (о сингулярном разложении)**.** Для любой прямоугольной матрицы $A \in M_{mn}(\mathbb{R})$ имеет место следующее разложение:

$$A = V \Sigma U^T$$

Оно называется сингулярным (SVD). Здесь $U \in O_n(\mathbb{R})$, $V \in O_m(\mathbb{R})$ – ортогональные матрицы, $\Sigma \in M_{mn}(\mathbb{R})$ – диагональная матрица с $\sigma_i \geq 0$ на диагонали. Причём, что $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_r > 0$, $r = \operatorname{Rg} A$. Числа σ_i называются сингулярными.

Доказательство. Рассмотрим $A^T A$ (матрица Грама). Она является симметрической и соответствующая квадратичная форма неотрицательна определена, т.е. $x^T A^T A x = (Ax, Ax) = \|Ax\|^2 > 0$, $\forall x \in \mathbb{R}^n$.

Тогда существуют (т.е. принадлежат $\mathbb{R}$) с.з. для самосопряжённого оператора $A^T A$, и они все ≥ 0, так как

$$\lambda = \frac{x^T A^T A x}{x^T x} = \frac{\|Ax\|^2}{\|x\|^2} > 0, \text{ где } \lambda \text{ – с.з., } x \text{ – с.в. (используется отношение Релея)}$$

Запишем эти с.з. в виде σ_i^2 (это можно сделать для любого неотрицательного числа). Пронумеруем их так, чтобы: $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_r > \sigma_{r+1} = \ldots = \sigma_n = 0$. Так как $A^T A$ самосопряжён, существует ОНБ из с.в. – $u_1, \ldots, u_n$.

$$A^T A u_i = \begin{cases} \sigma_i^2 u_i,\ 1 \leq i \leq r \\ 0,\ r+1 \leq 0 \leq n \end{cases}$$

Положим

$$v_i = \frac{Au_i}{\sigma_i},\ 1 \leq i \leq r$$

Тогда

$$(v_i, v_j) = \begin{cases} (\frac{Au_i}{\sigma_i}, \frac{Au_j}{\sigma_j}) = 1,\ i = j \\ 0,\ i \neq j \end{cases}$$

Получаем векторы $v_1, \ldots, v_r$ – образуют ортонормированную систему. Дополним её векторами $v_{r+1}, \ldots, v_m$ до ОНБ в $\mathbb{R}^m$. Тогда $v_1, \ldots, v_m$ и $u_1, \ldots, u_n$ – ОНБ. В итоге:

$$A \underbrace{[u_1, \ldots, u_n]}_{U} = \underbrace{[v_1, \ldots, v_m]}_{V} \begin{pmatrix} \sigma_1 & & & & & \\ & \ddots & & & \mathbf{0} & \\ & & \sigma_r & & & \\ & & & 0 & & \\ & \mathbf{0} & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

$$v_i = \frac{Au_i}{\sigma_i} \Leftrightarrow Au_i = v_i \cdot \sigma_i$$

Матрицы U и V являются ортонормированными. □

2.20 Сформулируйте и докажите теорему о полярном разложении.

Утверждение (полярное разложение)**.** Любой линейный оператор в евклидовом пространстве представляется в виде композиции симметрического и ортогонального $A = S \cdot U$, S – симметрический л.о., U – ортогональный л.о.

Доказательство. Возьмём сингулрное разложение $A = Q\Sigma P^T$, где Q, P – ортогональные. Пусть $S = Q\Sigma Q^T$, а $U = QP^T$. Тогда выполнено:

$$A = SU = Q\Sigma Q^T \cdot QP^T = Q\Sigma \cdot E \cdot P^T = Q\Sigma P^T \text{ – верно}$$

Проверим, является ли S симметрической:

$$S^T = (Q\Sigma Q^T)^T = (Q^T)^T \Sigma^T Q^T = Q\Sigma Q^T = S$$

Матрица U является ортогональной, так как она является произведением двух ортогональных матриц. □

2.21 Выпишите и докажите формулу для преобразования координат ковектора при переходе к другому базису.

Утверждение. Пусть e и g – два базиса в V. Тогда

$$[f]_g = [f]_e \cdot T_{e\to g}$$

Доказательство. Результат действия f не зависит от базиса:

$$[f]_g \cdot x_g = [f]_e \cdot x_e$$

$$x_g = T_{e\to g}^{-1} \cdot x_e \Leftrightarrow x_e = T_{e\to g} \cdot x_g$$

Разложение по базису единственно:

$$[f]_g = [f]_e \cdot T_{e\to g}$$

□

2.22 Сформулируйте и докажите теорему о приведении квадратичных форм к диагональному виду при помощи ортогональной замены координат.

Теорема. Любую квадратичную форму можно ортогональным преобразованием привести к каноническому виду.

Доказательство. Матрица квадратичной формы является симметрической (матрица $n \times n$). Рассмотрим n-мерное евклидово пространство E и некоторый ОНБ в нём. Тогда матрица квадратичной формы B является матрицей некоторого самосопряжённого линейного оператора, так как $B = B^T$.

Пусть матрица л.о. A совпадает с B. Так как по теореме для самосопряжённого л.о. существует ОНБ из с.в., для л.о. с матрицей A существует новый ОНБ, в котором его матрица диагональна. Пусть U – матрица перехода к этому базису. Она ортогональна.

Тогда в новом базисе матрица л.о. будет иметь вид:

$$A' = U^{-1}AU$$

А матрица квадратичной формы – B в новом базисе имеет вид:

$$B' = U^TBU$$

Но $U^T = U^{-1}$, т.к. U – ортогональная матрица. Значит, если $A = B$, то:

$$A' = U^{-1}AU = U^TAU = U^TBU = B'$$

Т.е. матрица квадратичной формы тоже будет диагональной. Это означает, что в этом базисе матрица квадратичной формы B' приведена к каноническому виду. $\square$

2.23 Что можно сказать про ортогональное дополнение к образу сопряженного оператора?

Утверждение. $(\operatorname{Im} A^*)^\perp = \operatorname{Ker} A$

Доказательство. Докажем, что $\operatorname{Ker} A = (\operatorname{Im} A^*)^\perp$. Если $x \in \operatorname{Ker} A$, то $Ax = 0$. Рассмотрим в V ОНБ. В нём $A^* = E^{-1}A^TE$ Тогда

$$\forall y \in V \;\; (y, Ax) = y^TEAx = y^TAEx = (A^Ty)^TEx = (A^Ty, x) = (A^*y, x)$$

Так как $(y, Ax) = (y, 0) = 0$, $(A^*y, x) = (y, Ax) = 0$. Значит, $x \perp \operatorname{Im} A^* \Rightarrow \operatorname{Ker} A \subseteq (\operatorname{Im} A^*)^\perp$.

Пусть $x \in (\operatorname{Im} A^*)^\perp$. Тогда

$$\forall y \in V \;\; 0 = (x, A^*y) = (Ax, y)$$

Рассмотрим $y = Ax$, $y \in V$. По доказанному:

$$0 = (Ax, y) = (Ax, Ax) = \|Ax\|^2 = 0 \Rightarrow Ax = 0 \Rightarrow x \in \operatorname{Ker} A$$

Отсюда $(\operatorname{Im} A^*)^\perp \subseteq \operatorname{Ker} A$.

Таким образом, $(\operatorname{Im} A^*)^\perp \subseteq \operatorname{Ker} A$ и $\operatorname{Ker} A \subseteq (\operatorname{Im} A^*)^\perp \Rightarrow \operatorname{Ker} A = (\operatorname{Im} A^*)^\perp$. $\square$

Удачи на коллоквиуме!

Автору на ИУП: **2200 2407 6615 8246**

Большое спасибо тем, кто задонатил! Вы лучшие, мне очень приятно!