Конспект по линейной алгебре

Подготовка к экзамену. 4 модуль
by АкЕб (feat. Qwen3)

24 июня 2025 г.

Содержание

1 Двойственность между подпространствами и двойственным пространством

Определение 1 (Двойственное пространство)**.** *Пусть V — векторное пространство над полем $\mathbb{F}$. Тогда двойственным пространством V^* называется множество всех линейных функционалов на V, то есть отображений $f : V \to \mathbb{F}$, удовлетворяющих:*

$$f(\alpha v + \beta w) = \alpha f(v) + \beta f(w), \quad \forall v, w \in V,\ \alpha, \beta \in \mathbb{F}.$$

Пример 1. *Если $V = \mathbb{R}^n$, то любой линейный функционал можно записать как $f(x_1, ..., x_n) = a_1x_1 + ... + a_nx_n$ для некоторых $a_i \in \mathbb{R}$.*

Определение 2 (Аннулятор подпространства)**.** *Пусть $U \subseteq V$ — подпространство. Тогда его аннулятор определяется как:*

$$U^0 := \{f \in V^* \mid f(u) = 0\ \forall u \in U\}.$$

Свойство 1 (Основная двойственность)**.** *Если $\dim V < \infty$, то:*

$$\dim U^0 = \dim V - \dim U.$$

Замечание 1. *Таким образом, каждому подпространству $U \subseteq V$ соответствует подпространство $U^0 \subseteq V^*$, и эта связь взаимна: если мы возьмём аннулятор U^0 в V^*, то получим исходное U при подходящих условиях.*

2 Билинейные отображения и формы

Определение 3 (Билинейное отображение)**.** *Отображение $B : V \times W \to \mathbb{F}$ называется билинейным, если оно линейно по каждой переменной при фиксированной другой:*

$$B(\alpha v_1 + \beta v_2, w) = \alpha B(v_1, w) + \beta B(v_2, w),$$
$$B(v, \alpha w_1 + \beta w_2) = \alpha B(v, w_1) + \beta B(v, w_2).$$

Определение 4 (Билинейная форма)**.** *Если $V = W$, то $B : V \times V \to \mathbb{F}$ называется билинейной формой.*

Пример 2. *Стандартный пример билинейной формы — скалярное произведение:*

$$B(v, w) = v \cdot w = \sum_{i=1}^{n} v_i w_i.$$

Определение 5 (Матрица Грама)**.** *Пусть B — билинейная форма на V, $\{e_1, ..., e_n\}$ — базис V. Тогда матрицей Грама формы B в этом базисе называется матрица $G = (g_{ij})$, где:*

$$g_{ij} = B(e_i, e_j).$$

3 Вычисление формы через матрицу Грама

Предложение 1 (Формула вычисления). *Пусть* $v = \sum_{i=1}^{n} v_i e_i$, $w = \sum_{j=1}^{n} w_j e_j$. *Тогда:*

$$B(v, w) = \sum_{i,j=1}^{n} g_{ij} v_i w_j = [v]^T G [w],$$

где $[v]$, $[w]$ — *столбцы координат векторов* v, w *в данном базисе.*

Замечание 2. *То есть формулу можно читать так: "умножь транспонированный вектор слева на матрицу Грама, а потом справа на второй вектор".*

Предложение 2 (Изменение матрицы Грама при замене базиса). *Пусть* P — *матрица перехода от старого базиса к новому. Тогда новая матрица Грама:*

$$G' = P^T G P.$$

4 Симметрические билинейные формы и квадратичные формы

Определение 6 (Симметрическая билинейная форма). *Форма* B *называется симметрической, если:*

$$B(v, w) = B(w, v) \quad \forall v, w \in V.$$

Определение 7 (Квадратичная форма). *Функция* $Q : V \to \mathbb{F}$ *называется квадратичной формой, если существует симметричная билинейная форма* B, *такая что:*

$$Q(v) = B(v, v).$$

Предложение 3 (Биекция между симметричными билинейными и квадратичными формами). *Если* $\operatorname{char} \mathbb{F} \neq 2$, *то между симметричными билинейными формами и квадратичными формами существует взаимно однозначное соответствие:*

$$B(v, w) = \frac{1}{2}(Q(v + w) - Q(v) - Q(w)).$$

5 Невырожденные формы

Определение 8 (Невырожденная билинейная форма). *Форма* B *называется невырожденной, если из равенства* $B(v, w) = 0$ *для всех* $w \in V$ *следует* $v = 0$.

Или другими словами: ядро отображения $v \mapsto B(v, \cdot)$ *тривиально.*

Предложение 4 (Равносильные условия невырожденности). *Следующие утверждения равносильны:*

(1) Форма B *невырожденна.*

(2) Отображение $\varphi_B : V \to V^*$, *заданное как* $\varphi_B(v)(w) = B(v, w)$, *является изоморфизмом.*

(3) Матрица Грама G *невырожденна (т.е.* $\det G \neq 0$*).*

Замечание 3. *Таким образом, невырожденная форма позволяет нам «перепрыгивать» между пространством и двойственным к нему без потерь информации.*

6 Аксиомы евклидова и унитарного пространства, КБШ, длины и углы, ортогональность/нормированность

Определение 9 (Евклидово пространство)**.** *Евклидовым пространством называется вещественное векторное пространство V, на котором задано скалярное произведение — симметричная положительно определённая билинейная форма $(\cdot,\cdot): V\times V\to\mathbb{R}$, удовлетворяющая следующим аксиомам:*

1. $(x+y,z)=(x,z)+(y,z)$,
2. $(\alpha x,y)=\alpha(x,y)$ *для любого* $\alpha\in\mathbb{R}$,
3. $(x,y)=(y,x)$,
4. $(x,x)>0$ *при* $x\neq 0$.

Такое пространство обозначается $(V,(\cdot,\cdot))$.

Определение 10 (Унитарное пространство)**.** *Унитарным пространством называется комплексное векторное пространство V, на котором задана эрмитова форма, то есть отображение $(\cdot,\cdot): V\times V\to\mathbb{C}$, удовлетворяющее следующим аксиомам:*

1. $(x+y,z)=(x,z)+(y,z)$,
2. $(\alpha x,y)=\alpha(x,y)$ *для любого* $\alpha\in\mathbb{C}$,
3. $(x,y)=\overline{(y,x)}$,
4. $(x,x)>0$ *при* $x\neq 0$.

[Неравенство Коши–Буняковского–Шварца (КБШ)] Для любых $x,y\in V$:

$$|(x,y)|\leq\|x\|\cdot\|y\|.$$

Равенство достигается тогда и только тогда, когда x и y линейно зависимы.

Определение 11 (Длина (норма), угол между векторами)**.** *Длина (или норма) вектора x:*

$$\|x\|=\sqrt{(x,x)}.$$

Угол θ между двумя ненулевыми векторами x и y определяется как:

$$\cos\theta=\frac{(x,y)}{\|x\|\cdot\|y\|}.$$

Определение 12 (Ортогональность)**.** *Два вектора x,y в евклидовом или унитарном пространстве называются ортогональными, если $(x,y)=0$. Обозначение: $x\perp y$.*

Вектор x называется нормированным, если $\|x\|=1$.

Определение 13 (Нормированное пространство)**.** *Пространство V называется нормированным, если на нём задана функция $\|\cdot\|: V\to\mathbb{R}_{\geq 0}$, удовлетворяющая аксиомам:*

1. $\|x\|=0\iff x=0$,
2. $\|\alpha x\|=|\alpha|\cdot\|x\|$,
3. $\|x+y\|\leq\|x\|+\|y\|$ *(неравенство треугольника).*

7 Процесс ортогонализации Грама–Шмидта. Изометрия евклидовых пространств

Предложение 5 (Метод Грама–Шмидта). *Любой базис $\{e_1, ..., e_n\}$ евклидова пространства можно преобразовать в ортонормированный базис $\{f_1, ..., f_n\}$ следующим образом:*

$$\begin{aligned} u_1 &= e_1, \\ u_2 &= e_2 - \frac{(e_2, u_1)}{(u_1, u_1)} u_1, \\ u_3 &= e_3 - \frac{(e_3, u_1)}{(u_1, u_1)} u_1 - \frac{(e_3, u_2)}{(u_2, u_2)} u_2, \\ &\vdots \\ f_i &= \frac{u_i}{\|u_i\|}. \end{aligned}$$

Определение 14 (Изометрия евклидовых пространств). *Отображение $T : V \to W$ между евклидовыми пространствами называется изометрией, если оно сохраняет скалярное произведение:*

$$(Tx, Ty)_W = (x, y)_V \quad \forall x, y \in V.$$

Замечание 4. *Изометрия сохраняет длины, углы и ортогональность.*

8 Свойства координат в ортонормированном базисе, теорема Пифагора

Предложение 6 (Координаты в ОНБ). *Если $\{e_1, ..., e_n\}$ — ортонормированный базис (ОНБ), то для любого $x \in V$:*

$$x = \sum_{i=1}^{n} (x, e_i) e_i.$$

Коэффициенты разложения — это просто проекции x на базисные векторы.

[Теорема Пифагора] Если $x \perp y$, то:

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2.$$

Если $x_1, ..., x_k$ попарно ортогональны, то:

$$\left\| \sum_{i=1}^{k} x_i \right\|^2 = \sum_{i=1}^{k} \|x_i\|^2.$$

9 Ортогональное дополнение к подпространству: основная теорема

Определение 15 (Ортогональное дополнение). *Пусть $U \subseteq V$ — подпространство евклидова пространства. Тогда его ортогональным дополнением называется множество:*

$$U^\perp := \{v \in V \mid (v, u) = 0 \ \forall u \in U\}.$$

[Основная теорема об ортогональном разложении] Для любого подпространства $U \subseteq V$ имеет место ортогональное разложение:

$$V = U \oplus U^{\perp}.$$

То есть любой вектор $v \in V$ можно единственным образом представить в виде $v = u + w$, где $u \in U$, $w \in U^{\perp}$.

10 Расстояние от точки до подпространства

Определение 16 (Расстояние от точки до подпространства)**.** *Пусть $U \subseteq V$ — подпространство евклидова пространства, $v \in V$. Тогда расстоянием от v до U называется:*

$$\operatorname{dist}(v, U) = \min_{u \in U} \|v - u\|.$$

[Формула расстояния через ортогональную проекцию] Если $p_U(v)$ — ортогональная проекция v на U, то:

$$\operatorname{dist}(v, U) = \|v - p_U(v)\|.$$

Пример 3. *Пусть $U = \operatorname{span}\{e_1, e_2\} \subset \mathbb{R}^3$, $v = (1, 2, 3)$. Тогда $p_U(v) = (1, 2, 0)$, и $\operatorname{dist}(v, U) = \|v - p_U(v)\| = \|(0, 0, 3)\| = 3$.*

11 Полуторалинейные формы, унитарное пространство, эрмитовость

Определение 17 (Полуторалинейная форма)**.** *Отображение $\alpha : V \times V \to \mathbb{C}$ называется полуторалинейной формой, если оно:*

1. *линейно по второму аргументу:*

$$\alpha(v, w + w') = \alpha(v, w) + \alpha(v, w'), \quad \alpha(v, \lambda w) = \lambda \alpha(v, w),$$

2. *полулинейно (сопряжённо-линейно) по первому аргументу:*

$$\alpha(v + v', w) = \alpha(v, w) + \alpha(v', w), \quad \alpha(\lambda v, w) = \overline{\lambda} \alpha(v, w).$$

Определение 18 (Эрмитова форма)**.** *Полуторалинейная форма α называется эрмитовой, если она удовлетворяет условию симметрии:*

$$\alpha(v, w) = \overline{\alpha(w, v)}.$$

Определение 19 (Унитарное пространство)**.** *Комплексное векторное пространство V, на котором задана положительно определённая эрмитова форма, называется унитарным пространством. Формально, это значит:*

$$(v, v) > 0 \text{ для всех } v \neq 0.$$

12 Необходимое условие положительной определенности квадратичных форм

Определение 20 (Квадратичная форма)**.** *Функция $Q : V \to \mathbb{R}$ называется квадратичной формой, если существует симметричная билинейная форма B, такая что:*

$$Q(v) = B(v, v).$$

Определение 21 (Положительно определённая квадратичная форма)**.** *Квадратичная форма Q называется положительно определённой, если:*

$$Q(v) > 0 \text{ для всех } v \neq 0.$$

Предложение 7 (Необходимое условие положительной определённости)**.** *Если матрица A соответствует квадратичной форме $Q(x) = x^T Ax$, то необходимым условием положительной определённости является положительность всех главных миноров матрицы A.*

13 Критерий Сильвестра. Разложение Холецкого

[Критерий Сильвестра] Симметричная матрица $A \in \mathbb{R}^{n\times n}$ положительно определена тогда и только тогда, когда все её угловые миноры положительны:

$$\Delta_1 = a_{11} > 0, \quad \Delta_2 = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} > 0, \quad ..., \quad \Delta_n = \det A > 0.$$

[Разложение Холецкого] Если A — симметричная положительно определённая матрица, то её можно представить в виде:

$$A = LL^T,$$

где L — нижняя треугольная матрица с положительными диагональными элементами.

14 Теорема Лагранжа о диагонализации квадратичных форм

[Лагранжа] Любую квадратичную форму $Q(x_1, ..., x_n)$ можно привести к сумме квадратов новых переменных с помощью невырожденной замены координат:

$$Q(x) = \sum_{i=1}^{r} \lambda_i y_i^2,$$

где $r = \mathrm{rk}(Q)$, $\lambda_i \in \mathbb{R} \setminus \{0\}$.

Замечание 5. *Это утверждение часто называют диагонализацией квадратичной формы. Оно работает над любыми полями характеристики не 2.*

15 Закон инерции квадратичных форм

[Закон инерции квадратичных форм] Число положительных и отрицательных коэффициентов при квадратах в нормальном виде квадратичной формы не зависит от способа приведения к этому виду.

Другими словами, *число положительных и отрицательных собственных значений* матрицы формы инвариантно.

Определение 22 (Индекс инерции)**.** *Число положительных (соответственно, отрицательных) слагаемых в нормальном виде квадратичной формы называется положительным (отрицательным) индексом инерции.*

[Следствие из закона инерции] Для любой квадратичной формы:

$$\mathrm{rk}(Q) = \text{положительный индекс} + \text{отрицательный индекс}.$$

16 Двойственность как функтор, дуальный оператор

Определение 23 (Двойственное пространство)**.** *Пусть V — векторное пространство над полем $\mathbb{F}$. Тогда двойственным пространством к нему называется множество всех линейных отображений из V в $\mathbb{F}$, то есть:*

$$V^* = \mathrm{Lin}(V, \mathbb{F}).$$

Элементы этого пространства называются линейными функционалами.

Замечание 6. *Если $\dim V < \infty$, то $\dim V^* = \dim V$.*

Определение 24 (Дуальный оператор)**.** *Пусть $f : V \to W$ — линейный оператор между конечномерными векторными пространствами. Тогда ему соответствует дуальный оператор $f^\circ : W^* \to V^*$, определённый правилом:*

$$f^\circ(\varphi)(v) = \varphi(f(v)), \quad \forall \varphi \in W^*,\ v \in V.$$

Замечание 7. *То есть если φ «берёт» элемент из W и возвращает число, то $f^*(\varphi)$ «берёт» элемент из V, отправляет его через f в W, а потом применяет φ.*

Предложение 8 (Функториальность двойственности)**.** *Если $f : V \to W$, $g : W \to U$ — линейные отображения, то:*

$$(g \circ f)^\circ = f^\circ \circ g^\circ.$$

Также $(\mathrm{id}_V)^\circ = \mathrm{id}_{V^*}$.

Замечание 8. *Это означает, что переход к двойственному пространству — это контравариантный функтор на категории векторных пространств.*

17 Определение сопряженного оператора через дуальный, простейшие свойства

Определение 25 (Сопряжённый оператор)**.** *Пусть V и W — евклидовы пространства (или унитарные). Тогда для любого линейного оператора $f : V \to W$ можно определить сопряжённый оператор $f^* : W \to V$, удовлетворяющий соотношению:*

$$(f(v), w)_W = (v, f^*(w))_V \quad \forall v \in V,\ w \in W.$$

Замечание 9. *Сопряжённый оператор — это аналог дуального оператора, но действующий между исходными пространствами, а не их двойственными.*

Предложение 9 (Простейшие свойства сопряжённого оператора)**.** *1. Если $f : V \to W$, $g : W \to U$, то $(g \circ f)^* = f^* \circ g^*$,*

2. $(\alpha f + \beta g)^* = \overline{\alpha} f^* + \overline{\beta} g^*$,

3. $(f^*)^* = f$.

18 Сопряженный оператор, определение формулой и явное вычисление

Предложение 10 (Вычисление сопряжённого оператора в координатах)**.** *Пусть $V = \mathbb{R}^n$ или $\mathbb{C}^n$, и пусть A — матрица линейного оператора f в некотором ортонормированном базисе. Тогда матрицей сопряжённого оператора f^* будет:*

- A^T — транспонированная матрица, если $V = \mathbb{R}^n$, - $A^* = \overline{A^T}$ — эрмитово сопряжённая матрица, если $V = \mathbb{C}^n$.

Пример 4. *Пусть* $A = \begin{pmatrix} 1 & i \\ -i & 2 \end{pmatrix}$. *Тогда:*

$$A^* = \begin{pmatrix} 1 & i \\ -i & 2 \end{pmatrix}^* = \begin{pmatrix} 1 & i \\ -i & 2 \end{pmatrix}^T = \begin{pmatrix} 1 & -i \\ i & 2 \end{pmatrix}.$$

Замечание 10. *В унитарном случае сопряжённый оператор играет роль аналога комплексно-сопряжённого числа.*

19 Самосопряженные операторы, самосопряженность в матричных терминах. Собственные числа ССО

Определение 26 (Самосопряжённый оператор)**.** *Линейный оператор $f : V \to V$ на евклидовом или унитарном пространстве называется самосопряжённым, если:*

$$f^* = f.$$

Предложение 11 (Матричная форма самосопряжённого оператора)**.** *Если f — самосопряжённый оператор, и A — его матрица в ортонормированном базисе, то:*

$$A^* = A.$$

В вещественном случае это значит, что A — симметричная матрица; в комплексном — эрмитова.

[Собственные числа самосопряжённого оператора] Все собственные значения самосопряжённого оператора вещественны.

Идея доказательства. Если $f(v) = \lambda v$, то:

$$(f(v), v) = (\lambda v, v) = \lambda (v, v),$$

но также:

$$(f(v), v) = (v, f(v)) = (v, \lambda v) = \overline{\lambda}(v, v).$$

Значит, $\lambda = \overline{\lambda}$, то есть $\lambda \in \mathbb{R}$. □

20 Теорема о канонической форме самосопряжённого оператора (с леммой)

[О существовании собственного вектора] Всякий самосопряжённый оператор f на ненулевом евклидовом или унитарном пространстве имеет хотя бы один собственный вектор.

Идея доказательства. Рассмотрим функцию $Q(x) = (f(x), x)$ при условии $\|x\| = 1$. Эта функция достигает максимума, и в точке максимума можно показать, что $f(x) = \lambda x$. $\square$

[Каноническая форма самосопряжённого оператора] В любом конечномерном евклидовом или унитарном пространстве существует ортонормированный базис, в котором матрица самосопряжённого оператора диагональна, и на диагонали стоят его собственные значения:

$$A = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}.$$

Замечание 11. *Это означает, что самосопряжённый оператор всегда приводится к диагональному виду в подходящем ортонормированном базисе.*

Если f — самосопряжённый оператор, то он диагонализируем.

21 Оценка квадратичной формы

Определение 27 (Квадратичная форма)**.** *Пусть V — векторное пространство над $\mathbb{R}$. Функция $Q : V \to \mathbb{R}$ называется квадратичной формой, если она задаётся однородным многочленом второй степени от координат вектора $x \in V$.*

Можно также записать:

$$Q(x) = x^T A x,$$

где A — симметричная матрица.

Определение 28 (Оценка квадратичной формы на единичной сфере)**.** *Часто нас интересует, какую максимальную или минимальную величину может принимать $Q(x)$ при условии $\|x\| = 1$. Это помогает понять поведение формы в целом.*

Формально:

$$\max_{\|x\|=1} Q(x), \quad \min_{\|x\|=1} Q(x).$$

Предложение 12 (Экстремальные значения квадратичной формы)**.** *Если $Q(x) = x^T A x$, то:*

- Максимальное значение $Q(x)$ на единичной сфере равно наибольшему собственному значению матрицы A, - Минимальное значение $Q(x)$ на единичной сфере равно наименьшему собственному значению матрицы A.

Пример 5. *Рассмотрим $Q(x_1, x_2) = 3x_1^2 + 2x_1x_2 + 3x_2^2$. Тогда её матрица:*

$$A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}.$$

Собственные значения: $\lambda_1 = 4,\ \lambda_2 = 2$. Значит:

$$\max_{\|x\|=1} Q(x) = 4, \quad \min_{\|x\|=1} Q(x) = 2.$$

22 Ортогональные и унитарные операторы, равносильные матричные и геометрические переформулировки

Определение 29 (Ортогональный оператор)**.** *Линейный оператор $f : V \to V$ на евклидовом пространстве V называется ортогональным, если он сохраняет скалярное произведение:*

$$(f(v), f(w)) = (v, w) \quad \forall v, w \in V.$$

Определение 30 (Унитарный оператор)**.** *Аналогично, линейный оператор $f : V \to V$ на унитарном пространстве V называется унитарным, если:*

$$(f(v), f(w)) = (v, w) \quad \forall v, w \in V.$$

Предложение 13 (Равносильные условия)**.** *Для линейного оператора f следующие условия равносильны:*

1. *f ортогонален (унитарен),*
2. *$f^* = f^{-1}$,*
3. *f сохраняет длину любого вектора: $\|f(v)\| = \|v\|$,*
4. *f переводит ортонормированный базис в ортонормированный.*

Замечание 12. *Ортогональные операторы — это изометрии евклидова пространства; унитарные — аналог для комплексного случая.*

23 Ортогональная/унитарная группа, примеры

Определение 31 (Ортогональная группа)**.** *Множество всех ортогональных операторов на $\mathbb{R}^n$ образует группу относительно композиции, обозначаемую $O(n)$.*

Аналогично, множество всех унитарных операторов на $\mathbb{C}^n$ образует группу $U(n)$.

Свойство 2 (Свойства групп)**.**

1. *$O(n) \subset GL(n, \mathbb{R})$ — подгруппа невырожденных матриц,*
2. *$U(n) \subset GL(n, \mathbb{C})$ — подгруппа,*
3. *Для любой матрицы $A \in O(n)$ выполняется $A^T A = I$,*
4. *Для $A \in U(n)$ выполняется $A^* A = I$.*

Пример 6. *Матрица поворота на угол θ в $\mathbb{R}^2$:*

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

является элементом $O(2)$.

24 Собственные числа и каноническая форма унитарного оператора

[Собственные числа унитарного оператора] Все собственные значения унитарного оператора имеют модуль 1, то есть являются комплексными числами вида $e^{i\theta}$.

То есть если λ — собственное значение, то $|\lambda| = 1$.

Идея доказательства. Если $f(v) = \lambda v$, то:

$$\|v\|^2 = (v, v) = (f(v), f(v)) = (\lambda v, \lambda v) = |\lambda|^2 (v, v) = |\lambda|^2 \|v\|^2.$$

Отсюда $|\lambda|^2 = 1$. □

[Канонический вид унитарного оператора] В подходящем ортонормированном базисе матрица унитарного оператора имеет вид:

$$\begin{pmatrix} e^{i\theta_1} & 0 & \cdots & 0 \\ 0 & e^{i\theta_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e^{i\theta_n} \end{pmatrix}.$$

То есть диагональная матрица с комплексными числами модуля 1 на диагонали.

Замечание 13. *Это аналог жордановой формы для унитарных операторов.*

25 Канонический вид ортогонального оператора — геометрический смысл и маломерные примеры

[Канонический вид ортогонального оператора] В подходящем ортонормированном базисе матрица ортогонального оператора в $\mathbb{R}^n$ имеет блочно-диагональный вид, где каждый блок размера 1×1 или 2×2:

- ± 1 — для собственных значений ± 1, - $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ — для пар комплексно-сопряжённых собственных значений $e^{\pm i\theta}$.

Замечание 14. *Геометрически это означает, что ортогональный оператор можно представить как комбинацию отражений и поворотов.*

Пример 7 (Пример в $\mathbb{R}^2$)**.** *Матрица поворота:*

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

соответствует повороту плоскости на угол θ, и является ортогональной матрицей.

Пример 8 (Пример в $\mathbb{R}^3$)**.** *Матрица вращения вокруг оси z:*

$$A = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

сохраняет ориентацию и является элементом $SO(3) \subset O(3)$.

26 Переход от жорданова базиса унитарного оператора к вещественному

Определение 32 (Жорданов базис)**.** *Пусть $f : V \to V$ — линейный оператор на комплексном пространстве V. Тогда существует базис (не обязательно ортонормированный), в котором матрица f имеет жорданову нормальную форму:*

$$J = \begin{pmatrix} \lambda_1 & * & & \\ & \lambda_2 & * & \\ & & \ddots & * \\ & & & \lambda_n \end{pmatrix},$$

где звёздочки обозначают либо 0, либо 1 (на первой наддиагонали).

Замечание 15. *Для унитарных операторов собственные значения имеют модуль 1, то есть они имеют вид $e^{i\theta}$.*

Предложение 14 (Переход к вещественному представлению)**.** *Если f — унитарный оператор на комплексном пространстве V, и его матрица в некотором базисе имеет жорданову форму, то при переходе к вещественному представлению комплексные собственные значения $e^{i\theta}$ заменяются на блоки вида:*

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Эти блоки соответствуют поворотам на угол θ в двумерных вещественных подпространствах.

Пример 9. *Пусть $\lambda = i$ — собственное значение унитарного оператора. Тогда в вещественном виде ему соответствует блок:*

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

что соответствует повороту на $90°$.

27 Превращение вещественного базиса для унитарного вещественного оператора в канонический вид ортогонального оператора

Определение 33 (Унитарный вещественный оператор)**.** *Оператор $f : V \to V$ на вещественном евклидовом пространстве называется унитарным вещественным, если он сохраняет скалярное произведение:*

$$(f(v), f(w)) = (v, w) \quad \forall v, w \in V,$$

то есть является ортогональным оператором.

[Канонический вид ортогонального оператора] В подходящем ортонормированном базисе матрица ортогонального оператора имеет блочно-диагональный вид, где каждый блок — это либо ± 1, либо поворотная матрица:

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Такой вид достигается путём перехода от комплексных собственных значений к их вещественным представлениям.

Пример 10. *Рассмотрим унитарный оператор с собственными значениями $e^{\pm i\theta}$. В вещественном базисе он представляется как:*

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Это элемент группы $SO(2)$, то есть поворот плоскости на угол θ.

28 Матричные переформулировки теорем о каноническом виде для ортогональных, унитарных и самосопряжённых операторов

[Каноническая форма самосопряжённого оператора] Любая эрмитова матрица A приводится к диагональному виду через унитарное преобразование:

$$A = UDU^*, \quad D = \mathrm{diag}(\lambda_1, ..., \lambda_n),$$

где $\lambda_i \in \mathbb{R}$ — собственные значения A, $U \in U(n)$ — унитарная матрица.

[Каноническая форма унитарного оператора] Любая унитарная матрица A приводится к диагональному виду через унитарное преобразование:

$$A = UDU^*, \quad D = \mathrm{diag}(e^{i\theta_1}, ..., e^{i\theta_n}).$$

[Каноническая форма ортогонального оператора] Любая ортогональная матрица $A \in O(n)$ приводится к блочно-диагональному виду:

$$A = QBQ^T, \quad B = \bigoplus_{j=1}^{k} \begin{cases} \pm 1, \\ \begin{pmatrix} \cos\theta_j & -\sin\theta_j \\ \sin\theta_j & \cos\theta_j \end{pmatrix} \end{cases}$$

с помощью ортогональной матрицы Q.

Замечание 16. *Таким образом, все три типа операторов допускают диагонализацию или блочную диагонализацию с помощью унитарных/ортогональных преобразований.*

29 Приведение квадратичной формы к каноническому виду

Определение 34 (Канонический вид квадратичной формы)**.** *Квадратичная форма $Q(x) = x^T Ax$ называется приведённой к каноническому виду, если она записана как сумма квадратов новых переменных:*

$$Q(y) = \sum_{i=1}^{n} \lambda_i y_i^2.$$

[Метод Лагранжа] Любую квадратичную форму можно привести к каноническому виду с помощью невырожденной замены переменных:

$$x = Cy, \quad C \in GL(n, \mathbb{R}),$$

после чего матрица формы становится диагональной.

Пример 11. *Рассмотрим* $Q(x_1, x_2) = 3x_1^2 + 4x_1x_2 + 2x_2^2$. *После замены:*

$$y_1 = x_1 + \frac{2}{3}x_2, \quad y_2 = x_2,$$

форма принимает вид:

$$Q(y_1, y_2) = 3y_1^2 - \frac{2}{3}y_2^2.$$

Замечание 17. *ПриведениеКанонический вид не единственен, но количество положительных и отрицательных коэффициентов (знакопеременная часть) определяется законом инерции.*

30 Положительный самосопряженный оператор – переформулировка через собственные числа, извлечение квадратного корня

Определение 35 (Положительный самосопряжённый оператор)**.** *Самосопряжённый оператор* A *на евклидовом или унитарном пространстве называется положительным, если для любого ненулевого вектора* v *выполняется:*

$$(Av, v) > 0.$$

Если вместо строгого неравенства стоит нестрогое (≥ 0*), то оператор называется неотрицательным.*

Предложение 15 (Через собственные значения)**.** *Самосопряжённый оператор положителен тогда и только тогда, когда все его собственные значения положительны.*

Пример 12. *Рассмотрим матрицу:*

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Её собственные значения: $\lambda_1 = 3,\ \lambda_2 = 1$. *Оба положительны* A *— положительный самосопряжённый оператор.*

[Извлечение квадратного корня] Для любого положительного самосопряжённого оператора A существует единственный положительный самосопряжённый оператор B, такой что:

$$B^2 = A.$$

Такой B обозначают $\sqrt{A}$ или $A^{1/2}$.

Идея доказательства. В ортонормированном базисе, где A диагональна, достаточно взять квадратные корни из собственных значений. Полученная диагональная матрица будет искомым B. □

Пример 13. *Для матрицы:*

$$A = \begin{pmatrix} 4 & 0 \\ 0 & 9 \end{pmatrix}, \quad \sqrt{A} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}.$$

31 Полярное разложение матрицы, геометрический смысл

[Полярное разложение] Любую невырожденную матрицу $A \in GL(n, \mathbb{R})$ можно представить в виде:

$$A = UP,$$

где $U \in O(n)$ — ортогональная матрица («поворот»), а P — положительно определённая симметричная матрица («растяжение»).

Замечание 18. *Можно также записать $A = QV$, где $V \in O(n)$, Q — положительно определённая.*

Пример 14. *Пусть:*

$$A = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}.$$

Тогда можно найти U и P, такие что $A = UP$, где $P = \sqrt{A^T A}$, а $U = AP^{-1}$.

Замечание 19 (Геометрический смысл)**.** *Полярное разложение показывает, что любое линейное преобразование можно представить как «сначала растяжение», потом «поворот» (или наоборот). Это полезно в компьютерной графике, физике и анализе данных.*

32 SVD-разложение

[Singular Value Decomposition, SVD] Любая матрица $A \in \mathbb{R}^{m \times n}$ допускает разложение вида:

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

где:

- $U \in \mathbb{R}^{m \times m}$ — ортогональная матрица, - $V \in \mathbb{R}^{n \times n}$ — ортогональная матрица, - $\Sigma \in \mathbb{R}^{m \times n}$ — прямоугольная диагональная матрица с *сингулярными числами* $\sigma_i \geq 0$ на диагонали.

Замечание 20. *Сингулярные числа — это квадратные корни из собственных значений матрицы $A^T A$ (или AA^T).*

Пример 15. *Пусть:*

$$A = \begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix}.$$

Тогда:

$$U = I, \quad \Sigma = A, \quad V = I.$$

Замечание 21. *SVD используется в машинном обучении, компрессии данных, рекомендательных системах и многом другом.*

33 Группы, порожденные набором элементов, два описания

Определение 36 (Группа, порожденная множеством)**.** *Пусть G — группа, $S \subseteq G$. Тогда подгруппа $\langle S \rangle$, порожденная множеством S, состоит из всех элементов группы G, которые можно получить, применяя конечное число операций умножения и взятия обратного элемента к элементам S.*

Формально:

$$\langle S \rangle = \bigcap_{\substack{H \leq G \\ S \subseteq H}} H.$$

Замечание 22. *Это наименьшая подгруппа, содержащая S.*

Пример 16. *$\langle 2\rangle$ в аддитивной группе $(\mathbb{Z},+)$ — это множество всех чётных чисел.*

Предложение 16 (Альтернативное описание)**.** *Множество $\langle S\rangle$ состоит из всевозможных произведений:*

$$s_1^{\pm 1}s_2^{\pm 1}\cdots s_k^{\pm 1},\quad k\in\mathbb{N},\ s_i\in S.$$

34 Группы как множества слов в абелевом и неабелевом случае, графы Кэли, примеры

Определение 37 (Свободная группа)**.** *Пусть S — некоторый алфавит. Свободная группа $F(S)$ состоит из всех конечных слов в алфавите $S\cup S^{-1}$, таких что рядом не стоят символы вида aa^{-1} или $a^{-1}a$.*

Операция — приписывание одного слова к другому, с последующим сокращением.

Пример 17. *Слово $ab^{-1}ba^{-1}c$ после сокращений превратится в ac.*

Определение 38 (Граф Кэли)**.** *Пусть G — группа, $S\subseteq G$ — порождающее множество. Граф Кэли $\Gamma(G,S)$ имеет вершины, соответствующие элементам G, и ребро из g в gs помеченное символом $s\in S$.*

Пример 18. *Граф Кэли $\Gamma(\mathbb{Z},\{1\})$ — бесконечная цепочка: $\cdots\to -2\to -1\to 0\to 1\to 2\to\cdots$*

Замечание 23. *Графы Кэли помогают визуализировать группу и понять её структуру.*

35 Теорема Кэли

[Кэли] Любая конечная группа G изоморфна подгруппе группы перестановок S_n для некоторого n.

Идея доказательства. Каждому элементу $g\in G$ сопоставим перестановку $\varphi_g: G\to G$, заданную правилом $\varphi_g(x)=gx$. Отображение $g\mapsto\varphi_g$ является инъективным гомоморфизмом. □

Пример 19. *Группа $\mathbb{Z}_3=\{0,1,2\}$ изоморфна циклической подгруппе $\langle(1\ 2\ 3)\rangle\subset S_3$.*

Замечание 24. *Теорема Кэли позволяет рассматривать любую группу как группу перестановок, что даёт мощный аппарат для анализа.*

36 Левые и правые смежные классы, теорема Лагранжа

Определение 39 (Смежный класс)**.** *Пусть G — группа, $H\subseteq G$ — её подгруппа, $a\in G$. Тогда:*

- Левым смежным классом элемента a по подгруппе H называется множество:

$$aH=\{ah\mid h\in H\}.$$

- Правым смежным классом элемента a по подгруппе H называется множество:

$$Ha=\{ha\mid h\in H\}.$$

Замечание 25. *Левые и правые смежные классы могут не совпадать, если группа не абелева.*

[Теорема Лагранжа] Если G — конечная группа, $H \leq G$, то порядок H делит порядок G, и число левых (или правых) смежных классов равно:

$$[G : H] = \frac{|G|}{|H|}.$$

Это число называется *индексом* подгруппы H в группе G.

Пример 20. *Рассмотрим группу S_3 перестановок трёх элементов ($|S_3| = 6$), и пусть $H = \{e, (12)\}$. Тогда:*

$$[G : H] = \frac{6}{2} = 3.$$

Имеем три левых смежных класса: $H, (13)H, (23)H$.

37 Индекс, биекция между левыми и правыми классами, примеры их несовпадения

Определение 40 (Индекс подгруппы)**.** *Число левых смежных классов группы G по подгруппе H обозначается $[G : H]$ и называется индексом подгруппы H в группе G.*

Предложение 17 (Биекция между левыми и правыми классами)**.** *Между множеством левых смежных классов G/H и множеством правых смежных классов $H\backslash G$ существует естественная биекция:*

$$aH \mapsto Ha^{-1}.$$

Поэтому число левых и правых смежных классов всегда совпадает.

Пример 21 (Несовпадение левых и правых классов)**.** *Рассмотрим группу S_3 и подгруппу $H = \{e, (12)\}$. Возьмём $a = (13)$. Тогда:*

$$aH = \{(13), (13)(12) = (123)\}, \quad Ha = \{(13), (12)(13) = (132)\}.$$

Очевидно, $aH \neq Ha$, хотя мощность у них одинаковая.

38 Нормальность, равносильные определения, примеры

Определение 41 (Нормальная подгруппа)**.** *Подгруппа $H \leq G$ называется нормальной, если для любого $g \in G$ выполняется:*

$$gHg^{-1} = H.$$

Обозначение: $H \triangleleft G$.

Предложение 18 (Равносильные условия нормальности)**.** *Для подгруппы $H \leq G$ следующие условия равносильны:*

1. *$gHg^{-1} = H$ для всех $g \in G$,*
2. *$gH = Hg$ для всех $g \in G$,*
3. *Разбиения на левые и правые смежные классы совпадают.*

Пример 22. *В любой абелевой группе любая подгруппа нормальна, так как $gh = hg$ $gH = Hg$.*

Пример 23. *В группе S_3 подгруппа A_3 чётных перестановок нормальна, поскольку имеет индекс 2, и разбиения на левые и правые классы совпадают.*

39 Факторгруппа, примеры

Определение 42 (Факторгруппа)**.** *Пусть $H \triangleleft G$. Тогда множество левых смежных классов G/H можно превратить в группу относительно операции:*

$$(aH)(bH) = (ab)H.$$

Эта группа называется факторгруппой G по H.

Предложение 19. *Факторгруппа G/H является группой тогда и только тогда, когда $H \triangleleft G$.*

Пример 24. *Пусть $G = \mathbb{Z}$, $H = 2\mathbb{Z}$. Тогда $G/H = \{2\mathbb{Z}, 1+2\mathbb{Z}\}$ — это циклическая группа из двух элементов, изоморфная $\mathbb{Z}_2$.*

Пример 25. *$G = S_3$, $H = A_3$. Тогда $G/H = \{A_3, (12)A_3\}$ — также группа из двух элементов, изоморфная $\mathbb{Z}_2$.*

40 Простые группы, гомоморфизмы, ядро и образ

Определение 43 (Простая группа)**.** *Группа G называется простой, если она неабелева и не имеет нетривиальных нормальных подгрупп, то есть единственными нормальными подгруппами являются $\{e\}$ и G.*

Пример 26. *Группа A_5 — простая. Это первая нетривиальная простая группа.*

Определение 44 (Гомоморфизм групп)**.** *Отображение $f : G \to H$ называется гомоморфизмом, если:*

$$f(ab) = f(a)f(b) \quad \forall a, b \in G.$$

Определение 45 (Ядро и образ)**.** *Для гомоморфизма $f : G \to H$:*
- Ядро: $\ker f = \{g \in G \mid f(g) = e_H\}$, *- Образ:* $\operatorname{Im} f = \{f(g) \mid g \in G\}$.

Предложение 20. $\ker f \triangleleft G$, *и* $\operatorname{Im} f \leq H$.

Пример 27. *Рассмотрим гомоморфизм $f : \mathbb{Z} \to \mathbb{Z}_n$, заданный как $f(k) = k \mod n$. Тогда:*

$$\ker f = n\mathbb{Z}, \quad \operatorname{Im} f = \mathbb{Z}_n.$$

[Первая теорема о гомоморфизмах] Для любого гомоморфизма $f : G \to H$:

$$G/\ker f \cong \operatorname{Im} f.$$

41 Теорема о гомоморфизме и её применения

На самом деле это билеты 41-45...

Определение 46 (Гомоморфизм групп)**.** *Отображение $f : G \to H$ между группами называется гомоморфизмом, если оно сохраняет операцию:*

$$f(ab) = f(a)f(b) \quad \forall a, b \in G.$$

Если f также биективно, то он называется изоморфизмом.

Определение 47 (Ядро и образ гомоморфизма)**.** *Для гомоморфизма $f : G \to H$:*

- Ядро — это множество $\ker f = \{g \in G \mid f(g) = e_H\}$*, - Образ — это множество* $\operatorname{Im} f = \{f(g) \mid g \in G\}$*.*

Предложение 21. $\ker f \triangleleft G$ *— нормальная подгруппа, а* $\operatorname{Im} f \leq H$ *— подгруппа.*

[Основная теорема о гомоморфизме] Пусть $f : G \to H$ — гомоморфизм. Тогда имеет место изоморфизм:

$$G/\ker f \cong \operatorname{Im} f.$$

Этот изоморфизм задаётся правилом:

$$\varphi(g \ker f) = f(g).$$

Пример 28 (Примеры применения теоремы о гомоморфизме)**.** *Рассмотрим несколько важных случаев:*

1. ***Вещественные числа и положительные числа****: Рассмотрим гомоморфизм* $f : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$*, заданный как* $f(x) = e^x$*. Тогда:*

$$\ker f = \{0\}, \quad \operatorname{Im} f = \mathbb{R}_{>0}, \Rightarrow \mathbb{R}/\{0\} \cong \mathbb{R}_{>0}.$$

2. ***Симметрическая группа и знакопеременная группа****: Пусть* $f : S_n \to \{\pm 1\}$ *— гомоморфизм, сопоставляющий перестановке её знак. Тогда:*

$$\ker f = A_n, \quad \operatorname{Im} f = \{\pm 1\}, \Rightarrow S_n/A_n \cong \{\pm 1\}.$$

3. ***Плоскость и прямая****: Рассмотрим проекцию* $f : \mathbb{R}^2 \to \mathbb{R}$*, заданную как* $f(x, y) = x$*. Тогда:*

$$\ker f = \{(0, y) \mid y \in \mathbb{R}\}, \quad \operatorname{Im} f = \mathbb{R}, \Rightarrow \mathbb{R}^2/\ker f \cong \mathbb{R}.$$

4. ***Полная и специальная линейная группы****: Рассмотрим гомоморфизм* $f : GL(n, \mathbb{R}) \to \mathbb{R}^*$*, заданный как* $f(A) = \det A$*. Тогда:*

$$\ker f = SL(n, \mathbb{R}), \quad \operatorname{Im} f = \mathbb{R}^*, \Rightarrow GL(n, \mathbb{R})/SL(n, \mathbb{R}) \cong \mathbb{R}^*.$$

5. ***Целые числа и корни из единицы****: Рассмотрим гомоморфизм* $f : \mathbb{Z} \to \mathbb{C}^*$*, заданный как* $f(k) = e^{2\pi i k/n}$*. Тогда:*

$$\ker f = n\mathbb{Z}, \quad \operatorname{Im} f = \{z \in \mathbb{C} \mid z^n = 1\}, \Rightarrow \mathbb{Z}/n\mathbb{Z} \cong \mu_n,$$

где μ_n *— группа корней из единицы порядка* n*.*

Замечание 26. *Таким образом, теорема о гомоморфизме позволяет находить структуру факторгрупп и упрощать вычисления с группами.*

Определение 48 (Прямое произведение групп)**.** *Пусть* G_1, G_2 *— группы. Их прямым произведением называется множество всех пар* (g_1, g_2) *с покомпонентной операцией:*

$$(g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2 h_2).$$

Обозначается $G_1 \times G_2$*.*

Предложение 22 (Критерий разложимости группы)**.** *Группа* G *разлагается в прямое произведение* $G = H \times K$*, если:*

1. $H, K \triangleleft G$,

2. $H \cap K = \{e\}$,

3. $HK = G$.

Пример 29. *Группа $\mathbb{Z}_6$ разлагается как $\mathbb{Z}_2 \times \mathbb{Z}_3$, так как эти подгруппы нормальны, их пересечение тривиально, и их произведение совпадает со всей группой.*

Пример 30. *Факторгруппа $\mathbb{Z}_6/\mathbb{Z}_2 \cong \mathbb{Z}_3$, что соответствует разложению $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.*

Определение 49 (Циклы в группе перестановок)**.** *Перестановка $\sigma \in S_n$ называется циклом длины k, если существуют такие элементы $i_1, ..., i_k \in \{1, ..., n\}$, что:*

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

а все остальные элементы остаются на месте.

Пример 31. *Перестановка $(1\ 2\ 3) \in S_4$ действует так: $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$, $4 \mapsto 4$.*

Определение 50 (Независимые циклы)**.** *Циклы $c_1, ..., c_m$ называются независимыми, если множества их перемещаемых точек не пересекаются.*

Любую перестановку можно однозначно представить как произведение независимых циклов.

Пример 32. *Перестановка $\sigma \in S_6$, заданная как:*

$$\sigma(1) = 3,\ \sigma(3) = 5,\ \sigma(5) = 1,\ \sigma(2) = 4,\ \sigma(4) = 2,\ \sigma(6) = 6,$$

записывается как $\sigma = (1\ 3\ 5)(2\ 4)$.

Определение 51 (Цикловой тип)**.** *Цикловой тип перестановки — это набор длин её циклов, записанный в порядке возрастания.*

Например, для $\sigma = (1\ 3\ 5)(2\ 4) \in S_6$ цикловой тип равен $(2, 3)$.

Предложение 23. *Две перестановки в S_n сопряжены тогда и только тогда, когда они имеют одинаковый цикловой тип.*

Определение 52 (Транспозиция)**.** *Транспозицией называется цикл длины 2. Например, $(1\ 2)$ — это транспозиция, меняющая местами 1 и 2.*

Любая перестановка может быть представлена как произведение транспозиций.

Пример 33. *Перестановка $(1\ 2\ 3) \in S_3$ раскладывается как $(1\ 3)(1\ 2)$.*

Предложение 24. *Четность числа транспозиций, необходимого для записи перестановки, инвариантна. Это определяет понятие чётности перестановки.*

Определение 53 (Четные перестановки)**.** *Перестановка называется чётной, если она представляется чётным числом транспозиций. Множество чётных перестановок образует подгруппу $A_n \subset S_n$.*

Любая чётная перестановка может быть представлена как произведение 3-циклов.

Пример 34. *Чётная перестановка $(1\ 2\ 3)(4\ 5\ 6) \in S_6$ может быть представлена как произведение 3-циклов:*

$$(1\ 2\ 3)(4\ 5\ 6).$$

42 Действия групп: определения, примеры, орбиты и стабилизаторы

На самом деле это билеты 46-50...

Группы часто «работают» не только сами по себе, но и на других множествах. Это называется *действием группы на множестве*. Давайте разберёмся, что это значит.

Определение 54 (Действие группы)**.** *Пусть G — группа, X — некоторое множество. Действием группы G на множество X называется отображение:*

$$G \times X \to X, \quad (g, x) \mapsto g \cdot x,$$

удовлетворяющее двум условиям:

1. $e \cdot x = x$ для любого $x \in X$, где e — единица группы G; 2. $(gh) \cdot x = g \cdot (h \cdot x)$ для любых $g, h \in G$ и $x \in X$.

То есть: единичный элемент ничего не меняет, и порядок действий важен.

Определение 55 (Гомоморфизм в группу перестановок)**.** *Другой способ задать действие группы — через гомоморфизм:*

$$\varphi : G \to S(X),$$

где $S(X)$ — группа всех перестановок множества X. Для каждого $g \in G$, $\varphi(g)$ — правило, по которому g перемешивает элементы из X.

Эти два определения равносильны: каждое действие можно превратить в такой гомоморфизм, и наоборот.

Пример 35 (Примеры действия групп)**.** *Вот несколько важных примеров:*

- Группа S_n (все перестановки чисел от 1 до n) естественно действует на множестве $\{1, 2, ..., n\}$: если $\sigma \in S_n$ и $i \in \{1, ..., n\}$, то $\sigma \cdot i = \sigma(i)$.

- Группа G может действовать на себе самой. Например:

- Левое умножение: $g \cdot h = gh$,

- Сопряжение: $g \cdot h = ghg^{-1}$.

Это даёт нам понимание того, как группа "видит"саму себя.

Теперь давай посмотрим, что происходит с конкретными элементами множества при действии группы.

Определение 56 (Орбита элемента)**.** *Пусть группа G действует на множество X. Орбитой элемента $x \in X$ называется множество всех тех элементов, куда он может попасть под действием группы:*

$$\mathrm{Orb}(x) = \{g \cdot x \mid g \in G\}.$$

Определение 57 (Стабилизатор элемента)**.** *Стабилизатор элемента $x \in X$ — это те элементы группы G, которые «оставляют x на месте», то есть:*

$$\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\}.$$

Можно проверить, что $\mathrm{Stab}(x)$ — это всегда подгруппа в G.

Пример 36. *Рассмотрим группу $G = S_3$, действующую на $X = \{1, 2, 3\}$. Возьмём $x = 1$.*

- Орбита $\mathrm{Orb}(1) = \{1, 2, 3\}$, потому что перестановками можно перевести 1 в любой номер. - Стабилизатор $\mathrm{Stab}(1)$ — это те перестановки, которые не двигают 1, то есть $\{(1), (23)\}$.

Так что $|\mathrm{Orb}(1)| = 3$, $|\mathrm{Stab}(1)| = 2$, а размер всей группы $|S_3| = 6$.

Теперь расскажем про важную связь между орбитами и стабилизаторами.

Предложение 25 (Биекция между орбитой и смежными классами)**.** *Для любого $x \in X$ существует биекция между элементами орбиты* $\mathrm{Orb}(x)$ *и левыми смежными классами группы G по подгруппе* $\mathrm{Stab}(x)$*.*

Формально:

$$\mathrm{Orb}(x) \leftrightarrow G/\mathrm{Stab}(x).$$

Поэтому длина орбиты равна индексу стабилизатора:

$$|\mathrm{Orb}(x)| = [G : \mathrm{Stab}(x)].$$

Если группа G конечна, то:

$$|\mathrm{Orb}(x)| = \frac{|G|}{|\mathrm{Stab}(x)|}.$$

Пример 37. *В предыдущем примере $|G| = 6$, $|\mathrm{Stab}(1)| = 2$ длина орбиты:*

$$|\mathrm{Orb}(1)| = \frac{6}{2} = 3.$$

Что совпадает с реальностью: орбита состоит из трёх элементов $\{1, 2, 3\}$.

И наконец, поговорим о важной теореме Коши, связанной с порядками элементов в группе.

[Теорема Коши] Пусть G — конечная группа, и пусть p — простое число, делящее порядок группы $|G|$. Тогда в G существует элемент порядка p.

Замечание 27. *Это очень полезный факт: если размер группы делится на какое-то простое число, то в группе обязательно есть циклическая подгруппа этого порядка.*

Пример 38. *Рассмотрим группу S_3, её порядок равен 6. Простые числа, делящие 6 — это 2 и 3. В S_3 есть элементы порядков 2 (например,* (12)*) и 3 (например,* (123)*). Теорема Коши работает!*

43 Лемма Бернсайда, подсчёт ожерелий, центр p-группы и прочая группа-магия

Это типа билеты 51-55

Определение 58 (Лемма Бернсайда)**.** *Пусть группа G действует на множество X. Тогда число орбит действия равно:*

$$\#\ \textit{орбит} = \frac{1}{|G|} \sum_{g \in G} \textit{число неподвижных точек элемента } g.$$

То есть:

$$\#\ \textit{орбит} = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|,$$

где $\mathrm{Fix}(g) = \{x \in X \mid g \cdot x = x\}$.

Замечание 28. *Эта лемма часто используется для подсчёта объектов с точностью до симметрии. Например, чтобы понять, сколько всего существует уникальных ожерелий из бусинок, если можно поворачивать и переворачивать ожерелье.*

Чтобы найти число неэквивалентных ожерелий, применим лемму Бернсайда: посчитаем, сколько раскрасок остаются неизменными при каждом элементе группы. Например: - Поворот на 0° (единичный элемент): все 64 раскраски неподвижны. - Поворот на 60°: только те раскраски, где все бусины одинаковые — их 2. - Отражения: каждое фиксирует несколько раскрасок — обычно по 8 на одно отражение. И так далее... В конце сложим всё, поделим на 12 и получим число уникальных ожерелий. Это работает, честно! Пример из жизни математиков: таких ожерелий будет ровно 13. Не веришь? Считай сам

Теперь переходим к более серьёзной теме — к центру группы.

Определение 59 (Центр группы)**.** *Пусть G — группа. Её центром называется множество:*

$$Z(G) = \{z \in G \mid zg = gz \ \forall g \in G\}.$$

То есть это те элементы, которые коммутируют со всеми остальными.

Предложение 26. *Центр группы всегда является нормальной абелевой подгруппой.*

Пример 40. *Рассмотрим группу $GL(n, \mathbb{R})$ — невырожденные матрицы размера $n \times n$. Центр этой группы состоит из скалярных матриц:*

$$Z(GL(n, \mathbb{R})) = \{\lambda I \mid \lambda \in \mathbb{R}^\times\}.$$

Все они коммутируют с любой матрицей, потому что просто умножают на число.

А теперь давайте перейдём к чему-то действительно красивому — к p-группам.

Определение 60 (p-группа)**.** *Группа G называется p-группой, если её порядок равен p^n, где p — простое число, $n \geq 1$.*

[Центр p-группы нетривиален] Если G — p-группа ($|G| = p^n$), то её центр содержит хотя бы два элемента:

$$|Z(G)| \geq 2.$$

Более того, $Z(G)$ делится на p, то есть $p \mid |Z(G)|$.

Идея доказательства. Рассматривается действие группы на себе через сопряжение. Используется классовое уравнение:

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} |\mathrm{Orb}(x)|.$$

Каждая орбита имеет размер, делящийся на p, поэтому правая часть минус $|Z(G)|$ делится на p, значит, и $|Z(G)|$ делится на p $Z(G)$ не тривиален. □

Пример 41. *Рассмотрим группу G порядка p^2. Тогда G либо циклическая, либо изоморфна $\mathbb{Z}_p \times \mathbb{Z}_p$, и в любом случае абелева.*

Действительно: если G не абелева, то $Z(G) \subsetneq G$, но тогда $|Z(G)| = p$, и фактор $G/Z(G)$ циклический G абелева — противоречие!

Предложение 27 (Башня подгрупп в p-группе)**.** *В каждой p-группе G существует цепочка подгрупп:*

$$\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_n = G,$$

где $|G_i| = p^i$, и каждый фактор G_i/G_{i-1} имеет порядок p и абелев.

Такие цепочки называются нормальными рядами, и они показывают, что p-группы «почти абелевы».

Замечание 29. *Это говорит нам, что p-группы имеют хорошую внутреннюю структуру — они разрешимы и даже нильпотентны.*

44 Примеры групп порядка p^3, теоремы о группах порядка pq, теоремы Силова

Это билеты 56-60

Начнём с примеров групп порядка p^3. Эти группы не всегда абелевы — это важный факт, который показывает, что даже в мире p-групп может быть интересная структура.

Пример 42 (Группа верхних унитреугольных матриц)**.** *Рассмотрим множество матриц вида:*

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},$$

где $a, b, c \in \mathbb{F}_p$. Такие матрицы образуют группу относительно умножения. Эта группа имеет порядок p^3, ***но не является абелевой*** *— можно проверить, что две такие матрицы не обязательно коммутируют.*

Замечание 30. *Этот пример показывает, что не любая группа порядка p^3 абелева. Однако, если группа порядка p^2, то она всегда абелева.*

Теперь перейдём к группам порядка pq, где p и q — простые числа.

[О группе порядка pq] Пусть G — группа порядка pq, где $p < q$ — простые числа и $p \nmid q - 1$. Тогда G циклическая, то есть $G \cong \mathbb{Z}_{pq}$.

Набросок доказательства. По теореме Коши, в G существуют элементы порядков p и q. Пусть H — подгруппа порядка q. Она нормальна, потому что число Силовых q-подгрупп равно 1 (по теореме Силова). Пусть K — подгруппа порядка p. Тогда HK — вся группа, $H \cap K = \{e\}$, и $G \cong H \rtimes K$. Если $p \nmid q - 1$, то этот полупрямой продукт тривиален $G \cong H \times K \cong \mathbb{Z}_q \times \mathbb{Z}_p \cong \mathbb{Z}_{pq}$. □

Теперь переходим к важнейшим результатам теории групп — теоремам Силова.

[Существование Силовских подгрупп] Пусть $|G| = p^n m$, где p — простое, $p \nmid m$. Тогда:

- В G существует подгруппа порядка p^n (она называется *Силовской p-подгруппой*), - Любая подгруппа порядка p^k, $k \leq n$, содержится в некоторой Силовской p-подгруппе.

Замечание 31. *Другими словами, для любого «разумного» p-порядка внутри группы найдётся подходящая подгруппа.*

[Сопряженность Силовских подгрупп] Все Силовские p-подгруппы группы G сопряжены между собой, то есть для любых двух Силовских p-подгрупп P и Q найдётся такой элемент $g \in G$, что:

$$Q = gPg^{-1}.$$

Если в группе только одна Силовская p-подгруппа, то она нормальна в G.

[Число Силовских подгрупп] Пусть n_p — число Силовских p-подгрупп в G. Тогда выполняются условия:

- $n_p \equiv 1 \mod p$, - $n_p \mid m$, где $|G| = p^n m$, $p \nmid m$.

Пример 43. *Рассмотрим группу S_3, её порядок равен $6 = 2 \cdot 3$. Число Силовских 3-подгрупп n_3 делит 2 и сравнимо с 1 по модулю 3 $n_3 = 1$ или 2. Но $2 \not\equiv 1 \mod 3$, значит $n_3 = 1$: есть единственная Силовская 3-подгруппа, и она нормальна.*

А вот $n_2 \equiv 1 \mod 2$ и делит 3 $n_2 = 1$ или 3. И действительно: есть три подгруппы порядка 2 в S_3, и они не нормальны.

Замечание 32. *Теоремы Силова дают мощный инструмент для анализа внутренней структуры конечных групп. Они часто используются для классификации групп заданного порядка.*

45 Несостоятельность "размерности"в теории групп, подгруппы в S_n, лемма Шрайера и алгоритм Шрайера-Симса

Это оставшиеся 61-66

Если ты думаешь, что в теории групп есть что-то вроде «размерности», как в линейной алгебре — то ты ошибаешься

Замечание 33 (О несостоятельности аналогии "размерности"). *В линейной алгебре размерность — это очень важная вещь: любые два базиса имеют одинаковую длину, и размерность говорит нам почти всё о структуре пространства.*

Но в теории групп такой аналогии нет. Например, в группе перестановок S_n можно найти разные системы образующих, и их количество может быть разным!

То есть: в теории групп не существует чего-то вроде "размерности которая бы однозначно определяла число образующих. Это важно помнить.

Пример 44. *Рассмотрим группу S_3. Её можно породить:*

- двумя элементами: например, (12) *и* (123)*, - или тремя:* $(12), (13), (23)$.

Число образующих зависит от выбора системы. Нет "размерности как в линейной алгебре.

Переходим к более серьёзным вещам: системам образующих для подгрупп симметрической группы.

[О подгруппах в S_n] Любая подгруппа $H \leq S_n$ имеет систему образующих, состоящую не более чем из $n-1$ элементов.

Это слабая форма теоремы, но она уже даёт полезную информацию: мы можем надеяться на то, что работать с подгруппами S_n будет не слишком сложно, если использовать правильный подход.

Идея доказательства: дерево образующих. Можно построить дерево, где вершины соответствуют элементам множества $\{1, ..., n\}$, а рёбра — действиям перестановок. Тогда, двигаясь от корня к листьям, строим последовательность образующих, по одному на каждый уровень дерева.

Получаем не более $n-1$ образующих. Это работает, потому что группа действует на множестве, и мы используем стабилизаторы точек. □

Пример 45. *Допустим, у нас есть подгруппа $H \leq S_4$, действующая на множестве $\{1, 2, 3, 4\}$. Мы выбираем точку 1, находим её стабилизатор H_1, потом переходим к точке, которую 1 переводится, и так далее. Всего нужно не больше трёх шагов система образующих содержит максимум три элемента.*

Хорошо, теперь давай научимся вычислять порядок подгруппы $H \leq S_n$, зная, как она действует.

Предложение 28 (Вычисление порядка подгруппы через стабилизаторы). *Пусть $H \leq S_n$, и пусть H действует на $X = \{1, ..., n\}$. Возьмём точку $x_1 \in X$, найдём её стабилизатор H_{x_1}. Тогда:*

$$|H| = |\mathrm{Orb}(x_1)| \cdot |H_{x_1}|.$$

Применяем это рекурсивно: для H_{x_1} берём следующую точку x_2 вне её орбиты и повторяем процесс.

Пример 46. *Пусть $H \leq S_4$, и H содержит перестановки, которые фиксируют 1 и действуют на $\{2,3,4\}$. Тогда $H \cong S_3$, и $|H| = 6$. Действительно:*

$$|\mathrm{Orb}(1)| = 1, \quad |H_1| = 6.$$

А теперь поговорим о том, как строить образующие подгруппы, зная образующие исходной группы. Для этого нам нужна...

[Лемма Шрайера] Пусть G — группа, $H \leq G$ — подгруппа, R — система представителей смежных классов G/H. Тогда множество:

$$\{rgs^{-1} \mid r, s \in R,\ g \in G,\ rgH = sH\}$$

образует систему образующих подгруппы H.

Замечание 34. *По сути, эта лемма позволяет строить образующие подгруппы, зная образующие всей группы и представителей смежных классов.*

Пример 47. *Пусть $G = S_3$, $H = A_3$. Возьмём систему представителей $R = \{e, (12)\}$. Тогда, применяя правило rgs^{-1}, получаем образующие H — например, $(12)(123)(12)^{-1} = (132)$.*

[Лемма Шрайера в общем случае] Лемма Шрайера работает не только для симметрических групп, но и вообще для любой группы G и её подгруппы H, если задана система представителей смежных классов R.

Это мощный инструмент для построения систем образующих подгрупп.

Замечание 35. *Если хочешь, это как "генератор кода": ты знаешь, как работает вся группа, и как выбраны представители классов — и автоматически получаешь систему образующих подгруппы.*

Теперь переходим к самому интересному — к алгоритму, который делает всю эту красоту практической.

Определение 61 (Сильная система образующих)**.** *Пусть $H \leq S_n$. Сильной системой образующих для H называется набор образующих, построенный относительно цепочки стабилизаторов:*

$$H = H^{(0)} \geq H^{(1)} \geq H^{(2)} \geq \cdots \geq H^{(n)} = \{e\},$$

где $H^{(i)}$ — стабилизатор точки $i+1$ в $H^{(i-1)}$.

Сильная система образующих — это набор генераторов для каждого уровня этой цепочки.

[Алгоритм Шрайера–Симса] Цель: построить сильную систему образующих для подгруппы $H \leq S_n$ и проверить, принадлежит ли перестановка $\sigma \in S_n$ группе H.

Шаги:

1. Начинаем с произвольного набора образующих H. 2. Строим цепочку стабилизаторов $H^{(0)} \geq H^{(1)} \geq \cdots \geq H^{(n)} = \{e\}$. 3. Используем лемму Шрайера, чтобы находить новые образующие для каждого стабилизатора. 4. Применяем технику перебора смежных классов, чтобы проверить принадлежность $\sigma \in H$ — это и есть *membership test.*

Пример 48 (membership test)**.** *Представь, что ты пришёл в клуб перестановок, и тебя спрашивают: «ты свой?» Ты достаешь своё слово в образующих и показываешь, что ты действительно из H. Это и есть membership test*

Пример 49. *Пусть* $H = \langle (123), (12) \rangle \leq S_3$. *Цепочка стабилизаторов:*

$$H^{(0)} = H, \quad H^{(1)} = \mathrm{Stab}_H(1), \quad H^{(2)} = \mathrm{Stab}_{H^{(1)}}(2).$$

На каждом уровне находим образующие, и в конце проверяем, принадлежит ли, скажем, $(23) \in H$. *Ответ: да, потому что* $(23) = (12)(123)(12)$.

Замечание 36. *Алгоритм Шрайера–Симса — один из самых популярных в компьютерной алгебре. Он используется во многих системах компьютерной алгебры, таких как GAP и Magma.*