Линейная алгебра и геометрия

Харитонцев-Беглов Сергей

24 июня 2022 г.

Содержание

1. Векторные пространства

Рассмотрим простейшую систему уравнений:

$$\begin{cases} ax + by = e \\ cx + dy = f. \end{cases} \iff x \cdot \begin{pmatrix} a \\ c \end{pmatrix} + y \cdot \begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} e \\ f \end{pmatrix}$$

По сути задача: выразить $\binom{e}{f}$ через $\binom{a}{c}$, $\binom{b}{d}$: так как $x \cdot \binom{a}{c} = \binom{xa}{xc}$, тогда $\binom{xa}{xc} + \binom{yb}{yd} = \binom{xa+yb}{xc+yd}$.

***Определение* 1.1.** $x\binom{a}{c} + y\binom{b}{d}$ — линейная комбинация $\binom{a}{c}$ и $\binom{b}{d}$.

***Определение* 1.2.** $\left\{x\binom{a}{c} + y\binom{b}{d}\right\}$ — линейная оболочка $\binom{a}{c}$ и $\binom{b}{d}$. Она обозначается $\langle\binom{a}{c}, \binom{b}{d}\rangle$.

***Определение* 1.3.** Пусть R — кольцо.
Множество $\left\{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \mid a_1, a_2, \ldots, a_n \in R \right\}$ — называется n-мерным арифметическим (координатным) пространством (пространством столбцов) над R, обозначается R^n.

на котором мы ещё определяем операции сложения и умножения на скаляр:

- $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{pmatrix}$
- $r \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} ra_1 \\ ra_2 \\ \vdots \\ ra_n \end{pmatrix} \forall r \in R$

***Определение* 1.4.** Аналогично пространству столбцов, можно определить пространство строк. Всё ровно аналогично, но теперь элементы расположены в строку. Обозначается ${}^nK$

***Определение* 1.5.** Пусть K — поле. Векторное пространство над K — тройка $(V, +, \cdot)$, где V — множество, $+\colon V \times V \to V$, $\cdot\colon K \times V \to V$. Причем:

1–4 $(V, +)$ — абелева группа.

1. $a + b = b + a \ \forall a, b \in V$.
2. $(a + b) + c = a + (b + c) \forall a, b, c \in V$
3. $\exists \overline{0}\colon a + \overline{0} = a \forall a \in V$
4. $\forall a \in V \ \exists (-a) \in V : a + (-a) = \overline{0}$
5. $(k_1 k_2)v = k_1(k_2 v)$ (ассоциативность умножения на скаляр)
6. $(k_1 + k_2)v = k_1 v + k_2 v$ (дистрибутивность умножения вектора на скаляр относительно сложения скаляров)

7. $k(v_1 + v_2) = kv_1 + kv_2$ (дистрибутивность умножения вектора на скаляр относительно сложения векторов)

8. $1_K \cdot v = v$ (унитарность, единица поля K является единицей и относительно умножения вектора на скаляр)

Здесь и далее (и немного ранее) скалярами называются элементы поля K, а векторами — элементы множества V.

Замечание. V — векторное пространство над K. Тогда:

- $0 \cdot v = \overline{0}\ \forall v \in V$.
- $k \cdot \overline{0} = \overline{0}\ \forall k \in K$.
- $(-1) \cdot v = -v\ \forall v \in V$.

Замечание. Из определений 2–8 следует 1.

***Определение* 1.6.** Пусть R — кольцо.
Тройка $(V, +, \cdot)$ с аксиомами 1-8 называется модулем над R.

Замечание. Абелевы группы(V — абелева, а умножение на скаляр выкинули) $\implies$ модули над $\mathbb{Z}$.

***Определение* 1.7.** V — векторное пространство над K. $v_1, v_2, \ldots, v_n \in V$. $a_1, a_2, \ldots, a_n \in K$. Тогда $\sum a_i v_i$ — линейная комбинация $v_1, v_2, \ldots, v_n$.

***Определение* 1.8.** Пусть M — множество векторов: $M \subset V$, тогда линейная оболочка множества M $\langle M \rangle = \{a_1v_1 + a_2v_2 + \ldots + a_kv_k \mid a_i \in K, v_i \in M\}$.

***Определение* 1.9.** Подпространство V — подмножество $U \subset V$, такое что $(U, +_V, \cdot_V)$ — векторное пространство.

Утверждение 1.1. $U \subset V$ — подпространство $\iff$ U — замкнуто, т.е. все операции с элементами U лежат в U.

Пример. ${}^nK$ — арифметическое пространство строк.

Пусть $v_1, v_2, \ldots, v_m \in K^n$, т.е. векторы в пространстве столбцов. Рассмотрим $x_1v_1 + x_2v_2 + \ldots + x_mv_m = 0 = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ — однородную систему линейных уравнений (x_i — неизвестные). Рассмотрим всё множество решений — строк $(x_1, x_2, \ldots, x_m) \in {}^nK$. Утверждение — оно является подпространством в ${}^nK$. Для этого нужно просто проверить, что сумма двух решений — тоже решение, и решение, умноженное на какой-либо скаляр всё ещё остаётся решением. Доказывается просто расписав почленно $x_iv_i + y_iv_i = (x_i + y_i)v_i$ и получив итоговое равенство 0. Домножение на скаляр очевидно.

Полученное пространство не является всем пространством строк (${}^nK$), но является его подпространством, как мы только что доказали.

Обозначение: U — подпространство V: $U \leqslant V$.

Утверждение 1.2. $V_1, V_2, \leqslant V \implies V_1 \cap V_2 \leqslant V$.

Доказательство. Очевидно! □

***Определение* 1.10.** Сумма по Минковскому: $A, B \subset V : A + B \coloneqq \{a + b \mid a \in A \wedge b \in B\}$.

Утверждение 1.3 (Сумма по Минковскому)**.** $V_1, V_2 \leqslant V \implies V_1 + V_2 \leqslant V$.

Доказательство.

- $x, y \in V_1 + V_2 \iff x = v_1 + v_2, y = v_1' + v_2'$, где $v_1, v_1' \in V_1,\ v_2, v_2' \in V_2$. Тогда $x + y = (v_1 + v_1') + (v_2 + v_2'), (v_1 + v_1') \in V_1, (v_2 + v_2') \in V_2 \implies x + y \in V_1 + V_2$
- $k \cdot x$ — очевидно.

□

Замечание. $M \subset V$, $\langle M \rangle = \bigcap\limits_{\substack{U \leqslant V \\ U \supset M}} U$, доказывается как аналогичное утверждение из первого семестра.

***Определение* 1.11.** V_1, V_2 — векторные пространства над K. Тогда $f \colon V_1 \to V_2$ — гомоморфизм (линейное отображение), если

1. $f(v_1 + v_2) = f(v_1) + f(v_2)\ \forall v_1, v_2 \in V_1$.
2. $f(kv) = kf(v)$.

Если при этом f — биекция, то f — изоморфизм.

***Определение* 1.12.** Координатизация — сопоставление элементам векторного пространства координат пространства, являющимся изоморфным этому пространству, ака построение гомоморфизма:

$$\forall v \in V, v \to \begin{pmatrix} k_1 \\ k_2 \\ \vdots \\ k_n \end{pmatrix}, k_i \in K$$

Верно ли, что любое векторное пространство изоморфно какому-то K^n? Да, если правильно понимать, что за n, и вообще, мы это чуть позже докажем.

Пример векторных пространств.

1. K — векторное пространство над K (следует из аксиом поля)
2. Векторы над плоскостью/пространством.
3. $K[x]_n = \{f \in K[x] \mid \deg f \leqslant n\}$. Тогда $K[x]_n \cong K^{n+1}$.
4. M — множество, K — поле. Тогда $V = \{f : M \to K\}$ (множество функций из M в K) — векторное пространство:
   - $(f_1 + f_2)(m) \coloneqq f_1(m) + f_2(m)\ \forall m \in M$.
   - $(kf)(m) = k \cdot f(m)\ \forall k \in K$.

   По сути, каждая такая функция задаётся значениями в каждой точке M, и тогда получаем f — $\{f(m) \in K | m \in M\}$, что есть, по сути, $K^{|M|}$

4'. $M = K = \mathbb{R}$, $C_0(\mathbb{R})$ — непрерывные функции $\mathbb{R} \to \mathbb{R}$. $C_0(\mathbb{R}) \leqslant (a_0, a_1, \ldots)$. Значения во всех рациональных точках. (Любая такая функция задаётся своими значениями во всех рациональных точках, а все рациональные точки можно пронумеровать и составить последовательность, и тогда каждая такая фукнция задаётся последовательностью значений во всех своих рациональных точках)

5. Последовательность фиббоначиевого типа: $a_n = a_{n-1} + a_{n-2}$. Тогда множество таких последовательностей — векторное пространство $\cong \mathbb{R}^2$

6. M — множество. $V = 2^M$, $K = \mathbb{Z}/2\mathbb{Z}$, $M_1 + M_2 \coloneqq M_1 \triangle M_2,\ 0 \cdot M = \varnothing, 1 \cdot M = M$. Тогда V — векторное пространство над $\mathbb{Z}/2\mathbb{Z}$, $V \cong {}^n(\mathbb{Z}/2\mathbb{Z})$, а координатизация тут — битовая строка из 0 и 1.

Но в любом ли векторном пространстве есть координатизация? Да, это мы докажем, но чуть позже, смотри дальше.

***Определение* 1.13.** V — векторное пространство над K. $\{v_i\}_{i\in I}$ (множество векторов) называется базисом V, если $\forall v \in V\ \exists! \{a_i\}_{i \in I}$(множество коэффициентов)$, a_i \in K : v = \sum_{i\in I} a_i v_i$, из которых почти все (т.е. все, кроме какого-то конечного числа) $a_i = 0$

Замечание. В терминах этого определения $I = \{1, 2, \ldots, n\}$ $V \leftrightarrow \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$, то есть $V \cong K^n$.

***Определение* 1.14.** V — векторное пространство над полем K, тогда $\{v_i\}_{i\in I}$ называется линейно независимой системой (ЛНЗ), если выполнено одно из равносильных утверждений:

1. $\nexists i \in I \colon v_i = \sum\limits_{j \neq i} a_j v_j$

2. $\forall \{a_i\} \in K \colon \sum a_i v_i = 0 \implies a_i = 0\ \forall i \in I$.

Доказательство. $2 \implies 1$. Пусть $\exists i \colon v_i = \sum a_j v_j \implies \sum a_j v_j - v_i = 0 \xRightarrow{a_i = -1}$ не выполняется второе (не все коэффициенты равны нулю).

$1 \implies 2$. Пусть $a_i v_i = 0$, причем $\exists a_j \neq 0$. Тогда перенесём $a_j v_j$ в левую часть и разделим на $-a_j$ и получить $v_j = \sum\limits_{i \neq j} b_i v_i$, т.е. выразили, противоречие с первым пунктом. $\square$

Теорема 1.4 (Равносильное определение базиса)**.** $\{v_i\}_{i \in I}, v_i \in V$, V — векторное пространство над K.

1. $\{v_i\}$ — базис.

2. $\{v_i\}$ — линейно независимая система и $\langle\{v_i\}\rangle = V$. $\{v_i\}$ — порождающая система.

3. $\{v_i\}$ — максимальная линейно независимая система, т.е. $\forall v \in V : \{v_i\}_{i\in I} \cup \{v\}$ — линейно зависимая.

4. $\{v_i\}$ — минимальная порождающая система. То есть выкидывание любого вектора делает систему не порождающей.

Доказательство.

- $1 \implies 2$. $\{v_i\}$ — базис $\implies$ $\{v_i\}$ порождающая по определению. Причем если $\sum a_i v_i = 0$, то $a_i = 0$, иначе получили два разложения для нуля (всегда есть разложение со всеми нулевыми коэффициентами), тогда получили, что $\{v_i\}$ — Л.Н.С.

- $2 \implies 1$. $\forall v \in V : v = \sum a_i v_i$, так как $\{v_i\}$ — порождающая. Тогда докажем единственность: пусть существуют $\sum a_i' v_i = v = \sum a_i v_i$. Тогда возьмем разность: $0 = \sum (a_i - a_i')v_i \iff a_i - a_i' = 0 \iff a_i = a_i'$.

- $3 \implies 2$. Нужно доказать, что $\{v_i\}$ — порождающая система. Рассмотрим произвольный $v \in V$. Знаем, что $v_i \cup v$ — линейно зависимая, значит $\exists a : \sum a_i v_i + av = 0$ и не все a равны нулю. Легко понять, что $a \neq 0$, иначе исходная система линейно зависимая, а тогда можно выразить вектор v — $v = \sum \frac{a_i}{-a} v_i$, умеем выражать любой вектор — значит мы порождающая система.

- $2 \implies 4$. Пусть наша $\{v_i\}$ — ЛНЗ и порождающая, хотим доказать, что тогда она минимальная порождающая. Пусть это не так, тогда если она не минимальная порождающая, то убрав один вектор, мы сможем его получить при помощи других наших векторов $\Rightarrow$ исходная система линейно зависима, противоречие.

- $4 \implies 2$. Пусть $\{v_i\}$ — ЛЗ. Тогда $\exists i : v_i = \sum_{j \neq i} a_j v_j$. Тогда можно выкинуть v_i, система уменьшится и останется порождающей (v_i заменяем на линейную комбинацию остальных), противоречие. Значит, $\{v_i\}$ — ЛНЗ.

- $2 \implies 3$. $\forall v \in V : v = \sum a_i v_i \Rightarrow \{v_i\} \cup \{v\}$ — ЛЗ.

$\square$

***Определение* 1.15.** V — векторное пространство над K.

V называется конечномерным, если $\exists$ конечная порождающая система, т.е. $V = \langle v_1, v_2, \cdots, v_n \rangle$.

Лемма. Из любой конечной порождающей системы $V = \langle v_1, v_2, \ldots, v_n \rangle$ можно выбрать базис.

Доказательство. Во-первых, если она линейно независима, то все очевидно, вот и базис.

Иначе, пусть $\exists v_i = \sum\limits_{j \neq i} a_j b_j$. Тогда заметим, что система никак не пострадает, если убрать v_i из системы: мы все равно можем его получить при помощи остальных векторов.

Теперь можно продолжить этот процесс до момента, когда эта система станет линейно независимой. Так как система была конечной, то этот процесс когда-либо закончится (например, если выкинем все вектора). $\square$

Замечание. Пример пространства с пустым базисом: у множества $V = \{0\}$ базис равен $\varnothing$.

Следствие. В любом конечном пространстве есть базис.

Замечание. В любом пространстве есть базис.

Пример.

$$K[x] = \langle 1, x, x^2, \ldots \rangle$$
$$K[[x]] = \langle ??? \rangle$$

У $K[[x]]$ есть базис, но на человеческом нельзя задать.

У $\mathbb{R}$ над $\mathbb{Q}$ тоже есть базис, но как его задать — вопрос.

***Определение* 1.16.** Размерность пространства $\dim V$ — количество элементов в базисе.

Это хорошо, но непонятно, почему это определение корректное, т.е. почему во всех базисах пространста одинаковое количество элементов.

Теорема 1.5. Все базисы имеют поровну элементов.

Лемма (Лемма о линейной зависимости линейных комбинаций)**.** Пусть $u_1, \dots, u_m \in \langle v_1, v_2, \dots, v_n \rangle$, $m > n$. Тогда $u_1, \dots, u_m$ линейно зависима.

Доказательство.

Лемма (О замене)**.** $\langle v_1, v_2, \dots v_n \rangle = \langle \sum a_i v_i, v_2, \dots, v_n \rangle$, т.е. можно заменить элемент на линейную комбинацию элементов без изменения линейной оболочки, если $a_1 \neq 0$

Доказательство. $\sum a_i v_i, v_2, \dots, v_n \in \langle v_1, v_2, \dots, v_n \rangle$, это очевидное доказательство в одну сторону. А для другой стороны заметим, что $v_2, v_3, \cdots, v_n \in \{v_1, v_2, \cdots, v_n\}$, а $v_1 = \frac{(\sum a_i v_i) - a_2 v_2 - \dots - a_n v_n}{a_1}$ □

Доказательство ЛЗЛК:

Рассмотрим u_1. Если $u_1 = \overline{0}$, то система сразу линейно зависимая, конец. Иначе можно представить $u_1 = \sum a_i v_i$, и $\exists i : a_i \neq 0$ По лемме произведем замену v_i на сумму. Получили $\langle v_1, \cdots, v_{i-1}, u_1, v_{i+1}, \cdots v_n \rangle = \langle v_1, v_2, \cdots, v_n \rangle$. Давайте продолжать подобную операцию: на k-ом шаге заменяем/выражаем $u_k = \sum_{v_i \text{ — не заменен}} a_i v_i + \sum_{i<k} b_i u_i$ Если все $a_i = 0$, то мы выражаем u_k через остальные u, т.е. получили линейную зависимость. Иначе будем там заменять, и через n шагов получим:

$u_{n+1}, \cdots, u_m \in \langle v_1, v_2, \cdots, v_n \rangle = \langle u_1, u_2, \cdots, u_n, \rangle$, т.е. умеем выражать остальные u через первые n, т.е. система всё же линейно зависимая. □

Из доказанной леммы очевидно следует теорема о равенстве количеств элементов во всех базисах оного пространства, а значит и корректность определения.

Пример. Рассмотрим $\mathbb{Z}/6\mathbb{Z}$. Пусть R — модуль над R.

$\{1\}$ — минимальная порождающая система. При этом, $\{2, 3\}$ — тоже минимальная порождающая система (пример показывает что лемма работает только для векторных пространств, но не для модулей).

Лемма. Пусть V — конечномерное пространство.

1. $\forall$ ЛНЗ систему можно дополнить до базиса.
2. $V_1 \leqslant V_2 \Rightarrow \dim V_1 \leqslant V_2$, причем $\dim V_1 = \dim V_2 \Rightarrow V_1 = V_2$.

Доказательство. Пусть $\dim V_1 = n$, $v_1, \dots, v_k$ — ЛНЗ система. Тогда заметим, что $k \leqslant n$ по лемме о линейной зависимости.

Процесс: $\exists v \notin \langle v_1, \dots, v_k \rangle$. Положим $v_{k+1} = v$. Если v не существует, то $v_1, \dots, v_k$ — базис. Причем, заметим, что $v_1, \dots, v_{k+1}$ — ЛНЗ система.

Продолжаем данный процесс. Заметим, что данный процесс будет длиться не более $n - k$ шагов, так как, если размер станет $n + 1$, то система точно будет ЛЗ.

Докажем второй пункт. Рассмотрим $v_1, \dots, v_k$ — базис V_1. Заметим, что $\{v_i\}$ — ЛНЗ и каждый $v_i \in V_2$. Тогда $\{v_i\}$ можно дополнить до базиса $V_2 \Rightarrow k \leqslant \dim V_2$. □

Замечание Напоминание. Пусть V — векторное пространство, причем $\dim V = n$, $v_1, \dots, v_n$ — базис $V \Rightarrow \exists$ изоморфизм векторных пространств.

$f: K^n \to V$, причем $f(\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}) = f(\begin{pmatrix} a_1+b_1 \\ \vdots \\ a_n+b_n \end{pmatrix}) = \sum(a_i+b_i)v_i = \sum a_iv_i + \sum b_iv_i = f(\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}) + f(\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix})$.

Плюс есть домножение на скаляр: $f(k\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}) = kf(\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix})$

***Определение* 1.17.** $a \in \mathbb{C}$ называется алгебраическим, если $\exists f \in \mathbb{Z}[x]$, такой что $f(a) = 0 \wedge f \not\equiv 0$ (a — корень какого-то многочлена с целыми коэффициентами, отличного от тождественного нуля)

Замечание. Если разрешить коэффициентам многочлена быть рациональными, получим то же самое (можно домножить все коээфициенты на их общий знаменатель)

Утверждение 1.6. a — алгебраическое $\Rightarrow \langle 1, a, a^2, \dots\rangle$ над $\mathbb{Q}$ — конечномерное.

Доказательство. $\exists P = \sum\limits_{i=0}^{n} k_ix^i$, такое что $k_n = 1, P(a) = 0$. Тогда $a^n = -\sum\limits_{i=0}^{n-1} k_ia^i \in \langle 1, a, \dots, a^{n-1}\rangle$, $a^{n+1} = -\sum\limits_{i=0}^{n-1} k_ia^{i+1} \in \langle 1, a, \dots, a^{n-1}\rangle$ (a^n выражается через первые n) и так далее для $\forall N > n$. $a^N \in \langle 1, a, \dots, a^{n-1}\rangle$ $\square$

Утверждение 1.7. a, b — алгебраические. Тогда $\langle a^ib^k\rangle$ над $\mathbb{Q}$ — конечномерное.

Доказательство. a — корень f: $\deg f = m$. b — корень g: $\deg g = n$.

Тогда $a^i \cdot b^k = (\sum\limits_{j=0}^{m-1} k_ja^j)(\sum\limits_{s=0}^{n-1} l_sb^s) = \sum\sum(k_jb_s)a^jb^s \Rightarrow \{a^jb^s\}_{\substack{j=0..m-1 \\ s=0..n-1}}$ — порождает $\langle\{a^ib^k\}\rangle$. $\square$

Теорема 1.8. Алгебраические числа образуют кольцо. По факту хочется доказать: a, b — алгебраические $\Rightarrow a+b, ab$ — алгебраические.

Доказательство. $\mathbb{C}$ — векторное пространство над $\mathbb{Q}$.

Докажем, что $a+b$ — алгебраическое: рассмотрим $1, a+b, (a+b)^2, (a+b)^3, \dots$. $(a+b)^i = \sum \binom{i}{k}a^kb^{i-k} \in V$, причем $\dim V = N$. Тогда $1, a+b, \dots, (a+b)^N$ — ЛЗ система. $\Longrightarrow \exists\{c_i\}, c_i \in \mathbb{Q}$: $\sum c_i(a+b)^i = 0 \Rightarrow a+b$ — корень $\sum c_ix^i = 0$ (ЛЗ система $\Longrightarrow \sum c_ix^i \not\equiv 0$). ab — аналогично. $\square$

Пример. SF — последовательности фиб. типа. $SF = \{(a_1, a_2, \dots) \mid {}_{a_{i+1}=a_i+a_{i-1}}^{a_i\in\mathbb{R}}\}$ — векторное пространство над $\mathbb{R}$. $\dim SF = 2$, причем $(1, 0, 1, 1, 2, 3, 5, 8, \dots)$ и $(0, 1, 1, 2, 3, 5, \dots)$ — Базис SF.

Координаты $(1, 1, 2, 3, \dots)$ в базисе, заданном сверху: $\binom{1}{1}$.

При этом есть другой, хороший базис: $\begin{matrix} u_1 = (1, \varphi, \varphi^2, \varphi^3, \dots) \\ u_2 = (1, -\frac{1}{\varphi}, \left(-\frac{1}{\varphi}\right)^2, \dots) \end{matrix}$

Например, $u = au_1 + bu_2 \iff \begin{cases} 1 = a\cdot 1 + b\cdot 1 \\ 1 = a\varphi + b\left(-\frac{1}{\varphi}\right) \end{cases} \rightsquigarrow \binom{a}{b}$ — вектор $\Rightarrow u_n = a\varphi^{n-1} + b\left(-\frac{1}{\varphi}\right)^{n-1}$.

2. Матрицы

***Определение* 2.1.** Пусть R — кольцо, I, J — конечные множества.

Тогда матрица A над R — отображение $I \times J \to R$.

Обычно $I = \{1, \ldots, m\}, J = \{1, \ldots, n\}, (i, j) \mapsto a_{ij} \in R$.

Тогда матрица $m \times n$: $(a_{ij})_{\substack{i=1..m \\ j=1..n}}$

***Определение* 2.2.** Множество матриц $M_{m,n}(R)$.

При $I = J$ мы называем квадратными $M_n(R)$.

Рассмотрим матрицу $A \in M_{m,n}$. Её можно разбить на n столбцов $(c_1 \mid c_2 \mid \ldots \mid c_n), c_i \in K^m$ и m строчек: $\begin{pmatrix} r_1 \\ r_2 \\ \ldots \\ r_n \end{pmatrix}, r_i \in {}^nK$.

Также заметим, что $M_{m,n}(K)$ — векторное пространство над K. Ясно, что $M_{m,1}(K) \cong K^m$ и $M_{1,n}(K) \cong {}^nK$.

***Определение* 2.3.** Умножение матрицы на столбец: $M_{m,n}(K) \times K^n \to K^m$: $(a_{ij}, \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}) \mapsto \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$, где $y_i = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n = \sum\limits_{k=1}^{n} a_{ik}x_k$.

Можно определить умножение строки на столбец: $\begin{pmatrix} a_1 & a_2 & \ldots & a_n \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \rightsquigarrow \sum a_i x_i$. Тогда умножение матрицы на столбец можно записать как $\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_m \end{pmatrix} \cdot X \rightsquigarrow \begin{pmatrix} r_1 \cdot X \\ r_2 \cdot X \\ \vdots \\ r_m \cdot X \end{pmatrix}$, где r_i — строчки, а X - столбец.

Тогда заметим, что умножение матриц: $A \cdot B = \begin{pmatrix} Ac_1 & Ac_2 & \ldots & Ac_l \end{pmatrix}$.

Пример СЛУ. Системы линейных уравнений можно записывать как матрицу.

$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_1 \\ \ldots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_1 \end{cases}$ Тогда $(a_{ij}) = A$, $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = X$, $\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = B$ и матричная запись СЛУ - $AX = B$

Замечание. $A \in M_{m,n}(K)$. Рассмотрим $\mathcal{A}$: $K^n \to K^m$, $X \mapsto A \cdot X$.

Утверждение 2.1. $\mathcal{A}$ — линейное отображение.

Доказательство. $\mathcal{A}(X + Y) = A \cdot X + A \cdot Y \quad \forall X, Y$, $\mathcal{A}(kX) = kA \cdot X$, $k \in K$. $\square$

Однородная СЛУ: $AX = 0$. $A = \begin{pmatrix} c_1 & c_2 & \dots & c_n \end{pmatrix}$. Эта система имеет только тривиальное решение $x = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \iff c_1, \dots, c_n$ — ЛНЗ. $c_i \in K^m, \dim K^m = m$, тогда по ЛЗЛК заметим, что если $n > m$, то $AX = 0$ имеет нетривиальное решение (т.к. неизвестных > уравнений).

2.1. Структура линейных отображений

Пример. $V = R^2$. Поворот вокруг O — линейное отображение. Симметрия относительно прямой — линейное отображение, если $0 \in l$. Проекция на l — линейное отображение.

Свойства. 1. $\mathcal{A}(0) = 0 (x = 0 \Rightarrow \mathcal{A}(0) = 0)$.

2. $\mathcal{A}$ — инъекция $\iff \mathcal{A}(x) = 0 \Rightarrow x = 0$.

3. $x_1, x_2, \dots, x_n$ — ЛЗ $\Rightarrow \mathcal{A}(x_i)$ — ЛЗ.

3'. $\mathcal{A}$ — инъекция: $\{x_i\}$ — ЛНЗ $\Rightarrow \{\mathcal{A}(x_i)\}$ — ЛНЗ.

4. $u_1, u_2, \dots, u_n$ — базис U. $v_1, v_2, \dots, v_n \in V$. Тогда $\exists! \mathcal{A} \colon U \to V$ такое что $\mathcal{A}(u_i) = v_i$.

Доказательство. 1. $\mathcal{A}(0) = \mathcal{A}(0 + 0) = \mathcal{A}(0) + \mathcal{A}(0)$

2. $\Rightarrow$: $\mathcal{A}$ — инъекция, $\mathcal{A}(x) = 0, \mathcal{A}(0) = 0 \Rightarrow x = 0$.

   $\Leftarrow$: От противного, пусть $x \neq y \in U : \mathcal{A}(x) = \mathcal{A}(y) \Rightarrow \mathcal{A}(x) - \mathcal{A}(y) = \mathcal{A}(x - y) = 0 \Rightarrow x - y = 0$. Противоречие.

3. $\sum a_i x_i = 0 \implies \sum a_i \mathcal{A}(x_i) = \sum \mathcal{A}(a_i x_i) = \mathcal{A}(\sum a_i x_i) = \mathcal{A}(0) = 0$.

3'. Пусть $0 = \sum a_i \mathcal{A}(x_i) = \mathcal{A}(\sum a_i x_i) \implies \sum a_i x_i = 0 \Rightarrow a_i = 0$.

4. Определим $\mathcal{A}$: пусть $u \in U$. $\exists! \{a_i\} : \ u = \sum a_i u_i$. Положим, $\mathcal{A}(u) = \sum a_i v_i$. $\mathcal{A}$ — линейно (очевидно/упражнение).

   Единственность: пусть $\mathcal{A}_2(u_i) = v_i$, тогда по линейности $\mathcal{A}_2(\sum a_i u_i) = \sum a_i \mathcal{A}_2(u_i) = \sum a_i v_i = \mathcal{A}(\sum a_i u_i)$.

□

***Определение* 2.4.** $\mathcal{A} \colon U \to V$ — линейное отображение.

Тогда $\ker \mathcal{A} = \{u \in U \mid \mathcal{A}(u) = 0\}$ — ядро $\mathcal{A}$. $\operatorname{Im} A = \{v \in V \mid \exists u : \mathcal{A}(u) = v\}$.

Свойства. 1. $\ker \mathcal{A} \leqslant U$, $\operatorname{Im} \mathcal{A} \leqslant U$.

2. $\operatorname{Im} \mathcal{A} = V \iff \mathcal{A}$ — сюръекция.

3. $\ker \mathcal{A} = \{0\} \iff \mathcal{A}$ — инъекция.

Доказательство. 1. Нам нужно собственно проверить замкнутость $\ker \mathcal{A}$. Пусть $x, y \in \ker \mathcal{A} \Rightarrow \mathcal{A}(x + y) = \mathcal{A}(x) + \mathcal{A}(y) = 0$ по определению ядра. Осталось проверить замкнутость домножения на скаляр. Ну действительно, пусть $x \in \ker \mathcal{A} \Rightarrow \mathcal{A}(kx) = k \cdot \mathcal{A}(x) = 0$.

   $\operatorname{Im} \mathcal{A} \leqslant U$ аналогично. Пусть $X, Y \in \operatorname{Im} \mathcal{A} \Rightarrow \exists x, y \in U : \begin{cases} \mathcal{A}(x) = X \\ \mathcal{A}(y) = Y \end{cases} \Rightarrow \mathcal{A}(x + y) = X + Y$.

   Замкнутость по домножению на скаляр: пусть $x \in \operatorname{Im} \mathcal{A} \Rightarrow \exists x \in U : \mathcal{A}(x) = X \Rightarrow \mathcal{A}(kx) = kX$.

2. Это абсолютно тривиально – просто перефразирования одного и того же: если достигаются все значения, то у каждого значения хотя бы один достигающий его аргумент и наоборот.

3. $\Leftarrow$: Очевидно, так как тогда только $\mathcal{A}(0) = 0$.
$\Rightarrow$: Предположим от противного: $x \neq y \in U : \mathcal{A}(x) = \mathcal{A}(y) \Rightarrow \mathcal{A}(x-y) = 0 \Rightarrow 0 \neq x-y \in \ker \mathcal{A}$. Противоречие.

$\square$

Теорема 2.2 (О ядре и образе)**.** $\mathcal{A}$ — линейное отображение.

1. $\exists$ базис $u_1, u_2, \ldots, u_k, u_{k+1}, \ldots u_n$. Причем $u_1, \ldots, u_k$ — базис $\ker \mathcal{A}$, а $\mathcal{A}(u_{k+1}), \ldots, \mathcal{A}(u_n)$ — базис $\operatorname{Im} \mathcal{A}$.

2. $\dim(\ker \mathcal{A}) + \dim(\operatorname{Im} \mathcal{A}) = \dim U$.

Доказательство. Рассмотрим базис $u_1, u_2, \ldots, u_k$ — базис $\ker \mathcal{A}$. По лемме эту систему можно дополнить до базиса U. Рассмотрим $u_{k+1}, \ldots, u_n$ из нового базиса.

Хотим доказать, что $\mathcal{A}(u_{k+1}), \ldots, \mathcal{A}(u_n)$ — базис $\operatorname{Im} \mathcal{A}$. Докажем по определению, доказав линейную независимость и порождение всех векторов в пространстве.

- ЛНЗ-ть: Пусть $\sum a_{k+i}\mathcal{A}(u_{k+i}) = 0 \Rightarrow \mathcal{A}(\sum a_{k+i}u_{k+i}) = 0 \Rightarrow \sum a_{k+i}u_{k+i} \in \ker A \Rightarrow \exists a_1, a_2, ..., a_k :$ $\sum a_{k+i}u_{k+i} = \sum\limits_{i=1}^{k}(-a_i)u_i \Rightarrow \sum\limits_{i=1}^{n} a_iu_i = 0$. Противоречие, так как $u_1, u_2, ..., u_n$ – базис в U.

- Порождение: Возьмём какой-нибудь $u \in U$. Докажем, что $\mathcal{A}(u)$ выражается через базис. Разложим u через базис: $u = \sum\limits_{i=1}^{n} a_iu_i \Rightarrow \mathcal{A}(u) = \mathcal{A}\left(\sum\limits_{i=1}^{n} a_iu_i\right) = \mathcal{A}\left(\sum\limits_{i=1}^{k} a_iu_i\right) + \sum\limits_{i=k+1}^{n} a_i\mathcal{A}(u_i)$. Но $\mathcal{A}\left(\sum\limits_{i=1}^{k} a_iu_i\right) = 0$, так как оно лежит в ядре. Значит действительно $\mathcal{A}(u) = \sum\limits_{i=k+1}^{n} a_i\mathcal{A}(u_i)$.

$\square$

***Определение* 2.5.** Пусть U, V — векторные пространства над полем K.

Тогда $U \oplus V \coloneqq U \times V$ как множества. То есть $(u_1, v_1) + (u_2, v_2) = (u_1 + u_2, v_1 + v_2)$, $k(u, v) \coloneqq (ku, kv)$.

Замечание. Пусть $\begin{matrix} u_1, \ldots, u_n & \text{— Базис } U \\ v_1, \ldots, v_m & \text{— Базис } V \end{matrix}$, $\widetilde{u_i} = (u_i, 0), \widetilde{v_i} = (0, v_i)$,

Тогда $\{\widetilde{u_i}\} \cup \{\widetilde{v_i}\}$ — Базис $U \oplus V$.

Доказательство. $\forall (u, v) \in U \oplus V : \exists!(a_i)\exists!(b_i)\ (u, v) = (\sum a_iu_i, \sum b_iv_i)$.

$(u, 0) = (\sum a_i\widetilde{u_i})$, $(0, v) = (\sum b_i\widetilde{v_i})$. $\square$

Замечание. $i_u : U \to U \oplus V$, $u \mapsto (u, 0)$, i_v — аналогично. Инъективный гомоморфизм векторных пространств.

$P_u : U \oplus V \to U, (u, v) \mapsto u$ — проекция. $\operatorname{Im} P_u = U, \ker P_u = \operatorname{Im} i_v$.

Диаграмма прямой суммы: $U \underset{i_u}{\overset{P_u}{\longleftrightarrow}} U \oplus V \underset{i_v}{\overset{P_v}{\longleftrightarrow}} V$. $P_ui_u = \mathrm{id}_u$, $P_vi_v = \mathrm{id}_v$, $P_vi_u = 0_v$, $P_ui_v = 0_u$, $i_uP_u + i_vP_v = \mathrm{id}_{u\oplus v}$

Теорема 2.3 (Формула Грассмана)**.** Пусть $U, V \leqslant W$, U, V — конечномерные.

$\dim(U + V) = \dim U + \dim V - \dim(U \cap V)$

Доказательство. Построим линейное $f\colon U\oplus V \to W, (u,v)\mapsto u+v$. f — линейное (очев/упражнение).

Заметим, что $\operatorname{Im} f = U+V$, $\ker f = \{(u,-u) \mid \begin{matrix} u\in U \\ -u\in V\end{matrix}\} = \{(u,-u)\mid u\in U\cap V\}$.

Очевидно, что $\ker f \cong U\cap V \implies \dim(\ker f) = \dim(U\cap V)$. А по теореме о размерности ядра и образа: $\dim V + \dim U = \dim(U\oplus V) = \dim(U+V) + \dim(U\cap V)$ $\square$

Пример. K^n, $U = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mid a_1x_1 + \ldots + a_nx_n = 0 \right\}$ — гиперплоскость $\dim U = n-1$.

СЛУ — m уравнений, m гиперплоскостей — $u_1, u_2, \ldots, u_m$. Ответ — $\bigcap\limits_{i=1}^{n} u_i$.

$\dim u_1 = n-1$. $\dim(u_1\cap u_2) = \dim u_1 + \dim u_2 - \dim(u_1+u_2) \geqslant n-1+n-1-n \geqslant n-2$. Можно продолжить процесс.

Следствие. Множество решений однородной СЛУ (n неизвестных, m уравнений) — пространство размерности $\geqslant n-m$.

Замечание. Аналогия $(+,\cap)$ с $(\cup,\cap)$ — неполная: $(V_1+V_2)\cap V_3 \neq (V_1\cap V_3)+(V_2\cap V_3)$, пример: три прямые на плоскости.

Пусть $A\in M_{m,n}(K), A = (a_{ij})_{\substack{i=1..m \\ j=1..n}}$, $\mathcal{A}\colon \begin{matrix} K^n \to K^m \\ X \mapsto A\cdot X\end{matrix}$ — линейное отображение.

$K^n - \langle e_1,\ldots,e_n\rangle, K^m = \langle \widetilde{e_1}, \ldots \widetilde{e_m}\rangle$, где e_i — вектор нулей с 1 на i строчке. Тогда $Ae_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj}\end{pmatrix}$.

Тогда можно сказать, что $A = \left(\mathcal{A}(e_1) \mid \mathcal{A}(e_2) \mid \ldots \mid \mathcal{A}(e_n) \right)$

Следствие. $A, B\in M_{m,n}(K)$. $\mathcal{A},\mathcal{B}$ — линейные отображения, $\mathcal{A}=\mathcal{B} \implies A = B$.

Утверждение 2.4. $A\in M_{m,n}(K)$, $\mathcal{A}$ — соответствующее отображение.

$\ker\mathcal{A}$ — множество решений однородной СЛУ с матрицей A
$\operatorname{Im}\mathcal{A}$ — линейная оболочка столбцов A.

Доказательство. $A = \left(\begin{array}{c|c|c|c} C_1 & C_2 & \ldots & C_n \end{array} \right) = \left(\begin{array}{c|c|c} \mathcal{A}(e_1) & \mathcal{A}(e_2) & \ldots \mathcal{A}(e_n) \end{array} \right)$

$\langle C_1, C_2, \ldots, C_n\rangle = \langle\{Ae_i\}\rangle = \operatorname{Im}\mathcal{A}$. $\sum a_i\mathcal{A}(e_i) = \mathcal{A}(\sum a_ie_i) = \mathcal{A}(V)$. V — вектор $\in K^n$. $\square$

Определение 2.6. $A = \left(\begin{array}{c|c|c|c} C_1 & C_2 & \ldots & C_n \end{array} \right)$.

$\dim\langle C_1,\ldots,C_n\rangle$ — называется рангом матрицы.

Обозначение $\operatorname{rank} A, \operatorname{rk} A, \operatorname{rg} A$.

При $n = m$ $n - \operatorname{rk} A$ называется дефектом матрицы. Дефект $\dim\ker A$.

Теорема 2.5 (Принцип Дирихле для векторных пространств)**.** $\mathcal{A}\colon V\to V$ — линейное отображение. V — конечномерное.

Тогда $\mathcal{A}$ — инъекция $\iff$ $\mathcal{A}$ — сюръекция.

Доказательство. $\dim V = n$, $\mathcal{A}$ — инъекция $\iff$ $\ker\mathcal{A} = 0$ $\iff$ $\dim\ker A = 0$ $\iff$ $\dim\operatorname{Im} A = n - 0 = n \iff \operatorname{Im} A = V \iff \mathcal{A}$ — сюръекция. $\square$

***Определение* 2.7.** Неоднородная система: $AX = B$, $A \in M_{m,n}(K), B \in K^m$.

Теорема 2.6. Решение неоднородной и соответствующей ей однородной системы связаны:

Доказательство. Пусть X_0 — решение $AX = B$, тогда $AX = B \land AX_0 = B \iff A(X - X_0) = 0 \iff X - X_0 \in \ker\mathcal{A}$ — решения соответствующей однородной A.

$X = X_0 + v, v \in \ker\mathcal{A}$. Множество решений $X_0 + \ker\mathcal{A} = X_0 + \ker A = X_0 + \mathcal{A}^{-1}\{0\}$.

$\mathcal{A}^{-1}(\{AX_0\}) = X_0 + \mathcal{A}^{-1}\{0\}$. $\square$

Теорема 2.7 (Альтернатива Фредгольма)**.** $\forall n = m$. СЛУ: n уравнений, n неизвестных, $AX = B$. Пусть A — фиксировано, B — нефиксировано, K — бесконечное.

Тогда верно одно из двух:

1. Однородное СЛУ имеет только тривиальное решение и неоднородное СЛУ имеет единственное решение при любом B.

2. $AX = 0$ имеет бесконечно много решений, тогда 0 или бесконечное множество решений в зависимости от B.

Теорема 2.8. $B \in M_{n,m}(K), A \in M_{l,n}(K)$. Причем $K^m \xrightarrow[\mathcal{B}]{\cdot B} K^n \xrightarrow[\mathcal{A}]{\cdot A} K^l$.

Рассмотрим $C = A \cdot B$, $\mathcal{C}\colon K^m \to K^l$. $C \coloneqq A \cdot B$, тогда $\mathcal{C}$ — отображения домножения C.

Доказательство. Докажем, что $C_1(X) = (A \cdot B) \cdot X$, $C(X) = A \cdot (B \cdot X)$. Достаточно проверить для какого-то базиса K^m.

e_i — все нули, но на i-ой строчке единица, без волны в K^m, с — в K^n. Тогда $Be_i = \begin{pmatrix} b_{1i} \\ b_{2i} \\ \vdots \\ b_{ni} \end{pmatrix} = \sum_k b_{ki}\widetilde{e_k}$.

Тогда $A(Be_i) = A(\sum b_{ki}\widetilde{e_k}) = \sum b_{ki}(A\widetilde{e_k}) = \sum b_{ki} \begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{lk} \end{pmatrix} = \begin{pmatrix} \sum_k a_{1k}b_{ki} \\ \sum_k a_{2k}b_{ki} \\ \vdots \\ \sum_k a_{lk}b_{ki} \end{pmatrix}$, где i — фиксированный столбец. $\square$

Следствие. Умножение матриц ассоциативно:

$A \in M_{k,l}(K), B \in M_{l,m}(K), C \in M_{m,n}(K)$.

Тогда $(AB)C = A(BC)$.

***Определение* 2.8.** При $m = n$,

$M_n(K)$ — кольцо квадратных матриц. Ассоциативное, но не коммутативное кольцо.

Пример. $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

2.2. Матрица линейного отображения

U, V — векторные пространства над K. $\mathcal{A}\colon U \to V$ — линейное. $u_1, \dots, u_m$ — базис U, $v_1, \dots, v_n$ — базис V.

$\mathcal{A}(u_i) \in V \Rightarrow \mathcal{A}(u_i)$ — линейная комбинация $\{v_i\}$.

Тогда (a_{ij}) — матрица линейного отображения $\mathcal{A}$ в базисах $\{u_i\}, \{v_i\}$. $A = [\mathcal{A}]_{\{u_i\},\{v_i\}}$. Столбцы A — столбцы координат $\mathcal{A}(u_i)$ в базисе $\{v_i\}$.

Утверждение 2.9. $u \in U$, u — столбец координат в базисе $\{u_i\}$.

Тогда $A \cdot u$ — столбец координат $\mathcal{A}(u)$ в базисе $\{v_i\}$.

Доказательство. Для u_i это так по определению, а для остальных векторов по дистрибутивности/линейности. □

Замечание. $\{u_i\}$ задает изоморфизм $u \underset{f_u}{\longrightarrow} K^m$, $v \underset{f_v}{\longrightarrow} K^n$ — координатизации. Тогда верно:

$$\begin{array}{ccc} U & \underset{\mathcal{A}}{\longrightarrow} & V \\ f_u \downarrow & & \downarrow f_v. \\ K^m & \underset{\cdot A}{\longrightarrow} & K^n \end{array}$$

2.3. Матрица перехода и формулы пересчета

V — векторное пространство. id_v — линейное. $\mathrm{id}_v : V \to V$, $\{v_i\}$ — базис. $[\mathrm{id}]_{\{v_i\},\{v_i\}} = \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix} = E_n$. Причем E_n — единица в кольце матриц.

Пусть теперь $\{u_i\}, \{v_i\}$ — базисы V. Тогда $[\mathrm{id}]_{\{u_i\},\{v_i\}} = C = (c_{ij})$. $u_i = \sum_j c_{ji} v_j$. $\big(u_1, \dots, u_n\big) = \big(v_1, \dots, v_n\big) \cdot C$.

$x \in V$, $x = \sum a_i u_i$, $X = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = (X)_{u_i}$.

$x = \big(u_1, \dots, u_n\big) \cdot X = \big(v_1, \dots, v_n\big) \cdot C \cdot X$

CX — координаты x в базисе v_i

C — матрица перехода от базиса u_i к базису v_i.

Замечание. (*Свойства матриц перехода*)

- $C_{\{u_i\},\{u_i\}} = E$
- $\{u_i\}, \{v_i\}, \{w_i\}$ — базисы. Тогда $C_{\{u_i\}\{w_i\}} = C_{\{v_i\}\{w_i\}} \cdot C_{\{u_i\}\{v_i\}}$.
- $C_1 = C_{\{u_i\},\{v_i\}}, C_2 = C_{\{v_i\},\{u_i\}}$.
  $C_1 \cdot C_2 = C_2 \cdot C_1 = E$. C_1, C_2 — взаимообратные.

Пусть $\mathcal{A}\colon U \to V$, U, V — векторные пространства над K.

Пусть e_i, f_i — базисы U и V, тогда существует матрица $A = [\mathcal{A}]_{\{e_i\},\{f_i\}}$

Причем важный момент, что если бы было два отображения: $U \xrightarrow{\mathcal{A}} V \xrightarrow{\mathcal{B}} W$, причем $\{e_i\}, \{f_i\}, \{g_i\}$ — базисы U, V, W соответственно. Тогда $[\mathcal{B}\mathcal{A}]_{\{e_i\},\{g_i\}} = [\mathcal{B}]_{\{f_i\}\{g_i\}} \cdot [\mathcal{A}]_{\{e_i\},\{f_i\}}$.

Тогда пусть V — векторное пространство, тогда $[\mathrm{id}_V]_{\{e_i\},\{f_i\}} = C$ — матрица перехода от e_i к f_i,

$x \in V$ X — координаты относительно $\{e_i\} \implies C \cdot X$ — координаты x относительно $\{f_i\}$.

$[\mathrm{id}]_{\{e_i\},\{e_i\}} = E = \begin{pmatrix} 1 & \dots & 0 \\ 0 & 1 & \dots \\ 0 & \dots & 1 \end{pmatrix}$. $EA = A, AE = A$.

$[\mathrm{id}]_{\{f_i\},\{e_i\}} = C^{-1}$, $CC^{-1} = C^{-1}C = E$. Матрица перехода — обратимы.

***Определение* 2.9.** V — векторное пространство над K.

$\mathcal{A}\colon V \to V$ называется линейным оператором.

Множество операторов на V — кольцо относительно $(+, \circ)$. $(\mathcal{A}+\mathcal{B})(V) \coloneqq \mathcal{A}(V)+\mathcal{B}(V) \quad \forall v \in V$.

$C \circ (\mathcal{A}+\mathcal{B}) = C \circ \mathcal{A} + C \circ \mathcal{B}$ — из линейности C.

***Определение* 2.10.** $\mathrm{End}(V)$ — эндоморфизм — множество операторов на V, $\dim V = n \implies \mathrm{End}\ V \cong M_n(K)$.

Так как $[\mathcal{A}+\mathcal{B}]_{\{e_i\}} = [\mathcal{A}]_{\{e_i\}} + [\mathcal{B}]_{\{e_i\}}$.

$[\mathcal{A}\circ\mathcal{B}]_{\{e_i\}} = [\mathcal{A}]_{\{e_i\}} \circ [\mathcal{B}]_{\{e_i\}}$. Говоря об операторах, будем писать $[\mathcal{A}]_{\{e_i\}}$.

$(M_n(K))^*$ — группа обратимых матриц, обозначение $GL_n(K), GL(n, K)$.

Пример. $GL_1(K) = K^* = K \setminus \{0\}$.

$$\begin{array}{llll} \mathcal{A}\colon & U & \to & V \text{ — линейно} \\ & \{e_i\} & & \{f_i\} \\ & \{e_i'\} & & \{f_i'\} \end{array}$$

Пусть $A = [\mathcal{A}]_{\{e_i\},\{f_i\}}$. Чему тогда равно $[\mathcal{A}]_{\{e_i'\},\{f_i'\}} =?$

$U(\{e'\}) \xrightarrow{\mathrm{id}} U(\{e_i\}) \xrightarrow{\mathcal{A}} V(\{f_i\}) \xrightarrow{\mathrm{id}} V(\{f_i'\})$.

Тогда $[\mathcal{A}]_{\{e_i'\},\{f_i'\}} = [\mathrm{id}_v \circ \mathcal{A} \circ \mathrm{id}_u]_{\{e_i'\},\{f_i'\}} = [\mathrm{id}_v]_{\{f_i\},\{f_i'\}} \cdot [\mathcal{A}]_{\{e_i\},\{f_i\}} \cdot [\mathrm{id}_u]_{\{e_i'\},\{e_i\}} = CA \cdot D^{-1}$, где C — матрица перехода от f_i к f_i', D — матрица перехода от e_i к e_i'.

Формула замены матрицы при замене базиса. Если $\mathcal{A}$ — линейный оператор, то:

$$A_{new} = CAC^{-1}.$$

Тогда A, B — матрицы одного отображения в разных базисах $\iff \exists C, D : B = CAD$, где C, D — обратимые. Это отношение эквивалентности.

Если A, B — квадратные обратимые матрицы, то $B = BAA^{-1}$.

Теорема 2.10 (Канонический вид линейного отображения)**.** $\mathcal{A} : V \to U$ — линейное, V — конечномерное векторное пространство над K.

Тогда $\exists$ базис $\{e_i\}$ в V, базис $\{f_i\}$ в U, $r \in \mathbb{Z}_{\geqslant 0}$, такие что $[\mathcal{A}]_{\{e_i\},\{f_i\}} = \left|\begin{array}{c|c} E_r & 0 \\ \hline 0 & 0 \end{array}\right|$, где E_r — едининичная матрица размера r.

Доказательство. Выберем базис из теоремы о ядре и образа. $v_1, \dots, v_k, v_{k+1}, \dots v_n$ — базис V, причем $v_1, \dots, v_k$ — базис $\ker \mathcal{A} \leqslant V$, $\mathcal{A}(v_{k+1}), \dots \mathcal{A}(v_n)$ — Базис $\mathrm{Im}\,\mathcal{A} \leqslant U$.

На самом деле рассмотрим базис $v_{k+1}, \dots v_n, v_1, v_2, \dots, v_k$. Теперь $\forall i = 1..n-k$ положим $\mathcal{A}(v_k + i) = u_i$. $u_1, u_2, \dots, u_{n-k}$ — базис $\mathrm{Im}\,\mathcal{A} \leqslant U$ — ЛНЗ.

$u_1, u_2, \ldots u_{n-k}, \ldots, u_m$ — базис U (дополнили до базиса).

Тогда для $\mathcal{A}(v_{k+i}) = u_i = 0u_1 + 0u_2 + \ldots + 1 \cdot u_i + 0 \ldots + 0 \cdot u_m \quad \forall i = 1..(n-k)$.

$(v_l) = 0 \quad \forall l = 1..k$.

Значит столбцы $[\mathcal{A}]_{\{v_{k+1},\ldots,v_n,v_1,\ldots,v_k\}\{u_i\}} = \left|\begin{array}{c|c} E_r & 0 \\ \hline 0 & 0 \end{array}\right|$ □

Замечание. $A \in M_{m,n}(K)$, $\operatorname{rk} A = r$, $\exists$ обратимые матрицы C, D: $CAD = \left|\begin{array}{c|c} E_r & 0 \\ \hline 0 & 0 \end{array}\right|$. $A' \in M_{m,n}$, $\operatorname{rk}(A') = \operatorname{rk}(A) = r \implies A' = \widetilde{C} A \widetilde{D}$

Определение 2.11. $A \in M_{m,n}(K)$, транспонированная матрица $A^T \in M_{n,m}(K) (A^T)_{i,j} = (A)_{j,i} \quad {}_{\forall j=1..m}^{\forall i=1..n}$

Свойства.
1. $(A^T)^T = A$.
2. $(A+B)^T = A^T + B^T$
3. $(AB)^T = B^T \cdot A^T$
4. $(A^{-1})^T = (A^T)^{-1}$

Доказательство. $1, 2$ — очевидно.

3. $((AB)^T)_{i,j} = (AB)_{ji} = \sum\limits_{k=1}^{l} a_{jk} b_{ki}$.

   $(B^T \cdot A^T)_{ij} = \sum\limits_{k=1}^{l} (B^T)_{ik} (A^T)_{kj} = \sum\limits_{k=1}^{l} b_{ki} \cdot a_{jk}$ — тоже самое.

4. следует из 3 и $E^R = E$.

□

Определение 2.12. $A \in M_{m,n}(K)$. Строчный ранг A — это $\dim\langle r_1, r_2, \ldots, r_m\rangle$, где $A = \begin{pmatrix} 1 \\ \hline r_2 \\ \hline \vdots \\ \hline r_m \end{pmatrix}$.

Обозначение $\operatorname{rk}_r(A)$.

Теорема 2.11 (Свойства ранга)**.**
1. $\operatorname{rk} A = \operatorname{rk}_r A, \operatorname{rk} A = \operatorname{rk} A^T, A \in M_{m,n}(K)$.
2. $\operatorname{rk}(AB) \leqslant \min(\operatorname{rk} A, \operatorname{rk} B)$.
3. $\operatorname{rk}(A+B) \leqslant \operatorname{rk}(A) + \operatorname{rk}(B)$

2') A — обратима $\implies \operatorname{rk} AB = \operatorname{rk} B, \operatorname{rk} BA = B$.

4. $A \in M_n(K)$ A — обратима $\iff \operatorname{rk} A = n$.

Доказательство. 4) A — обратима $\iff$ соответственно $\mathcal{A}$ — инъективно и сюръективно $\iff \mathcal{A}$ — сюръекция $\iff \operatorname{Im} \mathcal{A} = K^n \iff \operatorname{rk} \mathcal{A} = n, \dim(\operatorname{Im} \mathcal{A}) = n$.

1. $\operatorname{rk} A = r \implies \exists C, D$ — обратимые, такие, что $CAD = \left|\begin{array}{c|c} E_r & 0 \\ \hline 0 & 0 \end{array}\right|$. Тогда $(CAD)^T = D^T A^T C^T = \left|\begin{array}{c|c} E_r & 0 \\ \hline 0 & 0 \end{array}\right| \implies \operatorname{rk} A^T = r$.

   То есть $\operatorname{rk} A = \operatorname{rk} A^T = \operatorname{rk} A$, то есть строчки $A \leftrightarrow$ столбцы A^T.

2. $\operatorname{rk} AB = \dim(\operatorname{Im}(AB)) = \dim\{AB \cdot X \mid X \in K^n\} \leqslant \dim\{AY \mid Y \in K^m\} = \operatorname{rk} A$.

   $\operatorname{rk} AB = \dim(\operatorname{Im} AB) = \dim(\operatorname{Im} A\,|_{\operatorname{Im} B}) \leqslant \dim(\operatorname{Im} B) = \operatorname{rk} B$ ($\leqslant$ — по теореме о размерности ядра и образа)

2') A – обратимый $\exists A^{-1}$. $\operatorname{rk}(AB) \leqslant \operatorname{rk} B$ по 2.

   $\operatorname{rk} B = rk(A^{-1}(AB)) \leqslant \operatorname{rk} AB$ по 2. $\implies$ $\operatorname{rk} AB = \operatorname{rk} B$.

3. $\operatorname{rk}(A+B) = \dim\{(A+B)X \mid X \in U\} = \dim\{AX + BX \mid X \in U\} \leqslant \dim\{AX + BY \mid X, Y \in U\} = \dim(\operatorname{Im} A + \operatorname{Im} B) \overset{\text{Грасс.}}{\leqslant} \dim \operatorname{Im} A + \dim \operatorname{Im} B = \operatorname{rk} A + \operatorname{rk} B$.

□

***Определение* 2.13.** $\mathcal{A}\colon K^n \to K^n$ — линейный оператор.

$\mathcal{A}$ называется элементарным, если $\mathcal{A}$ — обратим и $\exists i_0, j_0 : (\mathcal{A}(x))_i = x_i, i \neq i_0$. А $(\mathcal{A}(x))_{i_0} = x_{i_0} + kx_{j_0}$,

Соответствующая матрица — матрица элементарного преобразования.

Разберем случаи:

1. $i_0 \neq j_0 :\quad \forall k \in K$ формула задает обратимое преобразование.

   $$t_{i_0,j_0}(k) \text{ — трансвекция: } \begin{pmatrix} x_1 \\ \vdots \\ x_{i_0} \\ \vdots \\ x_n \end{pmatrix} \to \begin{pmatrix} x_1 \\ \vdots \\ x_{i_0} + k \cdot x_{j_0} \\ \vdots \\ x_n \end{pmatrix}$$

   Обратная матрица к трансвекции $t_{i_0,j_0}(k)$: $t^{-1}_{i_0,j_0}(k) = t_{i_0,j_0}(-k)$

   Матрица трансвекции — единичная матрица, но на позиции $(a)_{i_0,j_0}$ стоит k.

2. $i_0 = j_0 :\quad (Ax)_{i=0} = (k+1) \cdot x_{i_0} = l \cdot x_{i_0}\quad (l := k+1)$ — обратимо, если $l \neq 0$ (в общем случае $l \in K^*$). $m_{i_0}(l)$ — дилатация, $m^{-1}_{i_0}(l) = m_{i_0}(\frac{1}{l}) = m_{i_0}(\frac{1}{k+1})$.

   Матрица дилатации — единичная матрица, но на $(a)_{i_0 j_0} = l = k+1$.

Утверждение 2.12.

1. $T_{ij}(a) \cdot A$ получится из A прибавлением к i-ой строке j-ой строки, умноженной на a.
2. $M_i(a) \cdot A$ тоже самое, но умножением i-ой строки на a.
3. $A \cdot M_i(a)$ тоже самое, но со столбцом.
4. $A \cdot T_{ij}(a)$, прибавлением к j-му столбцу i-го столбца, умноженного на a.

Доказательство. $1, 2$ следует из того что $T_{ij}(a) \left(\, c_1 \mid c_2 \mid \ldots \mid c_n \,\right) = \left(\, T_{ij}(a)c_1 \mid T_{ij}(a)c_2 \mid \ldots \mid T_{ij}c_n \,\right)$ и тоже для m_i.

А для столбцов $1, 2$ — это определения элементарного преобразования $3, 4$. Ну там можно транспонировать: $(A \cdot T_{i,j}(a))^T = (T_{i,j}(a))^T \cdot A^T = T_{j,i}(a) \cdot A^T$ — прибавляем к j-ой строке A^T i-ую строку. Транспонировав обратно, получим заявленное □

Замечание. E — элементарная матрица $\implies$ $\operatorname{rk}(EA) = \operatorname{rk}(A) = \operatorname{rk}(AE)$, по свойству $2'$ ранга, так как E — обратима $\iff$ элементарные преобразования матрицы не меняют их ранга.

Следствие. Алгоритмическое определение ранга: приведем A элементарными преобразованиями к виду трапеции (результат Гаусса). Тогда количество ненулевых строчек — ранг матрицы.

Замечание. Элементарное преобразование 3-го типа. $S_{ij}\colon \begin{pmatrix} x_1 \\ \vdots \\ x_i \\ \vdots \\ x_j \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_j \\ \vdots \\ x_i \\ \vdots \\ x_n \end{pmatrix}$ Матрица E, где вместо единиц на s_{ii} и s_{jj} стоят единицы на s_{ij} и s_{ji}. Умножение слева на S_{ij} меняет местами строки i, j, а справа — столбцы.

$S_{ij} = m_j(-1)t_{ij}(1)t_{ji}(-1)t_{ij}(1)$.

Теорема 2.13. A — матрица:

1. $\exists e_1, \dots, e_k$ — элементарные, такие что $e_k \cdot \ldots \cdot e_1 \cdot A$ — трапециевидная.
2. $A \in GL_n(K) \implies \exists e_1, \dots, e_k$ — элементарные, такие, что $e_k \cdot \ldots \cdot e_1 \cdot A = E$.

2') $A \in GL_n(K), \exists e_1, \dots, e_k \quad A = e_k \cdot \ldots \cdot e_1$.

3. $\exists e_1, \dots, e_k$ — элементарные $\exists f_1, \dots, f_l$ — элементарные, такие что $e_k \dots e_1 \cdot A \cdot f_l \dots f_1 = \left|\begin{array}{c|c} E_r & 0 \\ \hline 0 & 0 \end{array}\right|$.

Доказательство. 2° Понятно, что $e_1, e_2, \dots, e_k$ — обратимы. Тогда A — обратима $\iff e_k \dots e_2 e_1 A =$ треугольная матрица (результат Гаусса). Дальше её можно превратить в единичную

2° $\to$ 2'°: $A \in GL_n(K) \exists A^{-1} \in GL_n(K)$ по пункту 2 $\exists e_1, \dots, e_k\colon e_k \cdot \ldots \cdot e_2 \cdot e_1 A^{-1} = E$.

2° $\implies$ 3°: Знаем, что $\exists$ обратимые C, D: $CAD = \left|\begin{array}{c|c} E_r & 0 \\ \hline 0 & 0 \end{array}\right|$. По пункту 2 C, D представимы элементарными преобразованиями.

1° $A \in M_{m,n}(K)$. Индукция по n.

База: $n = 1$. Упражнение или смотри дальше (на то, что происходит в индукционном переходе).
Переход: $n \to n+1$. $A = (a_{ij})_{\substack{i=1..m \\ j=1..n+1}}$. Рассмотрим случаи:

1. $a_{11} \neq 0$, применим $t_{21}(-\frac{a_{21}}{a_{11}}), t_{31}(-\frac{a_{31}}{a_{11}}), \dots, t_{m_1}(-\frac{a_{m_1}}{a_{11}})$. После домножения получим: первую строчку, в последующих в первом столбце ноль, а дальше получилась матрица с размерностью меньшей на 1.

   По индукционному переходу $\exists e_1, \dots, e_k$ — элементарные, $e_1 \dots e_k A =$ трапециевидная матрица. e_i можно дополнить до нашей матрицы: $\begin{array}{c|c} 1 & 0 \\ \hline 0 & e_i \end{array}$.
2. $a_{11} = 0$, но $\exists k\colon a_{k_1} \neq 0$. Поменяем две строчки местами.
3. Весь первый столбец — нули. Забьем на него и делаем шаг индукции как в п.1.

Утверждение 2.14. Треугольная матрица обратима $\implies$ все $a_i \neq 0$ (на диагонали не нули).

Доказательство. Пусть не так. Рассмотрим такой минимальный i, что $a_i = 0$. Посмотрим на столбцы. Тогда $c_1, c_2, \ldots, c_i \in \langle e_1, \ldots, e_{i-1}\rangle \implies c_1, c_2, \ldots, c_i$ — ЛЗ. $c_1, \ldots, c_n$ — ЛЗ и $\operatorname{rank} < n \implies$ A — необратима. □

Итого, пусть у нас есть треугольная матрица. Применим $t_{1,n}(-\frac{a_{1n}}{a_{nn}})t_{2n}(-\frac{a_{2n}}{a_{nn}})\ldots t_{n-1,n}(-\frac{a_{n-1,n}}{a_{n,n}})$ (методом Гаусса убиваем все ненулевые элементы в последнем столбце). Теперь у нас в последнем столбце везде нули, кроме последней строчки. Повторяем процесс для всех столбцов, итого получаем матрицу, где на диагонали остались a_{ii}, а всё остальное - нули. □

Утверждение 2.15 (Алгоритм поиска обратной матрицы)**.** Для того, чтобы найти обратную матрицу нужно взять матрицу $\left(A \mid E \right)$ и привести левую матрицу к единичной. Тогда справа будет обратная.

***Определение* 2.14.** $A = (a_{ij}) \in M_n(K)$ называется верхнетреугольной, если $a_{ij} = 0 \quad \forall i > j$.

$A = (a_{ij}) \in M_n(K)$ называется нижнетреугольной, если $a_{ij} = 0 \quad \forall j > i$.

Утверждение 2.16.

1. $LT_n(K), UT_n(K)$ (множество нижне/верхнетреугольных) — подкольца в $M_n(K)$.
2. $LT_n \cap UT_n$ — кольцо диагональных матриц $\cong \underbrace{K \times K \times \ldots \times K}_{n\text{раз}}$

Доказательство.

2. Сложение — очев. Умножение — очев (записать руками и удостовериться).
1. Очев/упражнение (очев).

□

Замечание. $A \in M_n(K) \implies \exists \mathcal{A} : K^n \to K^n (X \mapsto A \cdot X)$, тогда

$A \in UT_n(K) \iff \forall i \in 1 : n \quad \mathcal{A}(e_i) \in \langle e_1, \ldots, e_i\rangle$. $\langle e_1\rangle \leqslant \langle e_1, e_2\rangle \leqslant \ldots \leqslant \langle e_1, \ldots, e_n\rangle$.

***Определение* 2.15.** A — нильпотентна, если $\exists k\colon A^k = 0$.

Утверждение 2.17. $A \in UT_n(K)$. A — нильп. $\iff a_{ii} = 0$.

Доказательство. $\begin{pmatrix} a_{11} & & * \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix}^n = \begin{pmatrix} a_{11}^n & & * \\ & \ddots & \\ 0 & & a_{nn}^n \end{pmatrix}$

Тогда $\implies \exists a_{ii} \neq 0 \implies A^n \neq 0$.

В обратную сторону: $\mathcal{A}(e_i) \in \langle e_1, \ldots, e_i\rangle, a_{ii} = 0$. Откуда получаем $Ae_i = b_1e_1 + b_2e_2 + \ldots + b_{i-1}e_{i-1} + 0$.

Значит $\mathcal{A}(e_i) \in \langle e_1, \ldots, e_{i-1}\rangle \quad \forall i$. Тогда $\mathcal{A}^2(e_i) \in \langle e_1, \ldots, e_{i-2}\rangle$. Это значит, что $\mathcal{A}^i(e_i) \in \langle\rangle \implies \mathcal{A}^i(e_i) = 0$. □

Замечание. $A^k = 0 \iff \exists$ замена базиса такая, что $A \in M_n(K)$ перейдет в верхнетреугольный вид.

В методе Гаусса у нас есть набор преобразований $e_k \ldots e_2e_1A \in UT_n(K)$. Вспомним, что e_i либо перестановка строк, либо $t_{ij}(a)$, где $i > j$.

Пусть перестановок нет. Тогда $e_k = t_{i_kj_k}(a) \in LT_n(K) \implies e_k \ldots e_1 \in LT_n(K)$, где $i_k > j_k$.

Тогда $LA = U$, $L \in LT_n, U \in UT_n$, то есть $A = L^{-1}U$, $L^{-1} \in LT_n$, $U \in UT_n$ ($L^{-1} \in LT_n$, так как L^{-1} — композиция $t^{-1}_{i_k,j_k}(a) = t_{i_k,j_k}(-a)$, где $i_k > j_k$). Получили LU разложение.

В общем случае сделаем в начале сделаем перестановки строк $P = s_{i_1,j_1}s_{i_2,j_2}\dots s_{i_k,j_k}$. Тогда PA - матрица, для которой $\exists LU$ - разложение. Тогда $PA = LU \implies A = P^{-1}LU$ - LPU-разложение на матрицу перестановки, нижне- и верхне-треугольную.

Теорема 2.18. Следующие условия равносильны ($A \in M_n(K)$):

1. $\exists A^{-1}(A \in GL(K) = M_n(K)^*)$.
2. $A = e_1 \dots e_k$, e_i — элементарные матрицы.
3. $\operatorname{rk} A = n$.
4. $\mathcal{A} \colon X \mapsto A \cdot X$ — инъективный линейный оператор: $K^n \to K^n$.
5. Тоже самое, но сюръективный.
6. Если рассмотреть матрицу как систему, то для любого вектора правой части есть единственное решение $AX = B \iff A^{-1}B = X$.

Доказательство. Уже доказывали $\square$

3. Явные формулы в линейной алгебре (Теория определителей)

Мотивация: Решим систему $\begin{cases} ax+by=e \\ cx+dy=f \end{cases}$. Получим решения $\begin{cases} x=\frac{ed-bf}{ad-bc} \\ y=\frac{af-ec}{ad-bc} \end{cases}$.

В чем смысл $ad-bc$. Возьмем вектора $\begin{pmatrix} a \\ c \end{pmatrix}$ и $\begin{pmatrix} b \\ d \end{pmatrix}$. Тогда площадь параллелограмма, натянутого на эти вектора $S=|ad-bc|$ и $ad-bc$.

Пусть $\widehat{S}(\Phi)$ — ориентированная площадь, $|\widehat{S}(\Phi)|=S(\Phi)$. $\widehat{S}(\Phi)>0$, если поворот от первого вектора ко второму против часовой стрелки.

Свойства. 1. $\widehat{S}(V_1,V_2)=-\widehat{S}(V_2,V_1)$.

2. $\widehat{S}(kv_1,v_2)=k\widehat{S}(v_1,v_2)$.

3. $S(v_1,v_2'+v_2'')=S(v1,v_2')+S(v_1,v_2'')$

Общий случай.

***Определение* 3.1.** $V_1,V_2,\ldots,V_n$, V — векторные пространства над K.

Отображение $\mathcal{A}\colon V_1\times V_2\times\ldots\times V_n\to V$ называется полилинейным, если $\forall i\forall v_i\in V_i\mathcal{A}_{v_1,\ldots,v_n}: V_i\to V(v_i\mapsto\mathcal{A}(v_1,v_2,\cdots,v_{i-1},v_i,\cdots,v_n))$ (на всех позициях, кроме $i-$й, стоят зафиксированные переменные) — линейно. То есть, если закрепить все переменные, кроме одной, то отображение будет линейно.

Будем изучать $V=K^n,\omega\colon(K^n)^m\to K$.

Лемма. $e_1,\ldots,e_n$ — базис K^n. $\omega\colon(K^n)^m\to K$ — полилинейно, тогда $\omega(v_1,v_2,\ldots,v_m)=\sum\limits_{\{i_1,\ldots,i_m\}\in\{1..n\}^n}a_{i_11}\cdot a_{i_22}\ldots a_{i_mm}\omega(e_{i_1},e_{i_2},\ldots,e_{i_m})$.

Доказательство. $\omega(v_1,v_2,\ldots,v_m)=\omega(\sum a_{j_1}e_j,\sum a_{j_2}e_j,\ldots)=\sum\limits_{j=1}^n a_{j_1}\cdot\omega(e_j,\sum\ldots)$ и дальше по линейности. □

***Определение* 3.2.** Кососимметрической n-формой называется полилинейное отображение $\omega:(K^n)^n\to K$, такое что $(\exists i,j\colon v_i=v_j\implies\omega(v_1,\ldots,v_n)=0)$.

Утверждение 3.1. 1. ω — кососимметрична $\implies\forall i\neq j:\omega(v_1,v_2,\ldots,v_i,\ldots,v_j,\ldots,v_n)=-\omega(v_1,\ldots,v_j,\ldots,v_i,\ldots v_n)$.

2. $\operatorname{char}k\neq 2\implies$ верно и обратное. То есть, если выполняется равенство то и ω — кососимметричная.

Доказательство. 1. фиксируем все, кроме v_i. Тогда $f(x,y)=\omega(v_1,..,v_{i-1},x,v_{i+1},\ldots,y,\ldots,v_n)$. f — полилинейно. Надо доказать, что $f(x,y)=0\iff f(x,y)=-f(y,x)\forall x,y$. $\Leftarrow-\operatorname{char}k\neq 2,\Rightarrow$ всегда.

$\Rightarrow f(x+y,x+y)=0\implies f(x,x)+f(x,y)+f(y,x)+f(y,y)=0\implies f(x,y)=-f(y,x)$

$\Leftarrow\operatorname{char}k\neq 2, f(x,x)=-f(x,x)\implies 2f(x,x)=0\implies f(x,x)=0$

□

Утверждение 3.2. $\exists$ не более одной кососимметричной n-формы с точностью до линейного множителя.

Доказательство. ω определено однозначено значениями

1. На базисе: $\omega(e_{i_1}, e_{i_2}, \dots, e_{e_n}) = \widetilde{\omega}(e_{i_1}, e_{i_2}, \dots, e_{i_n})$. Из леммы известно, что тогда $\omega = \widetilde{\omega}$.
2. ω — кососимметрична, среди $i_1, \dots, i_n$ есть одинаковые. Тогда $\omega(e_{i_1}, \dots) = 0$.
3. Осталось изучить перестановки e. Пусть π перестановка. Тогда $e_{\pi(1)}, e_{\pi(2)}, \dots$ — правильный порядок. Каждая перестановка двух элементов меняет знак у ω. То есть $\omega(e_{\pi(1)}, e_{\pi(2)}, \dots) = (-1)^k \omega(e_1, e_2, \dots, e_n)$, где k — количество сделанных ходов.

Из 1,2,3 следует, что $\omega(e_1, e_2, \dots, e_n) = \widetilde{\omega}(e_1, \dots, e_n)$ и они кососимметричны, то они равны.

Тогда потребуем, чтобы ω была кососимметричной n-формой, $\omega(e_1, e_2, \dots, e_n) = 1$, где $e_1, e_2, \dots, e_n$ базис в K^n. Тогда таких функция $\leqslant 1$. □

***Определение* 3.3.** Такие функции называются определителем порядка n.

***Определение* 3.4.** S_n — группа перестановок: $S_n = \{f\colon \{1, 2, \dots, n\} \to \{1, 2, \dots, n\} \mid f \text{ — биекция}\}$. С операцией $\cdot$ — композиция.

***Определение* 3.5.** $t_{ij} \in S_n$ — транспозиция. $t_{ij}(i) = j, t_{ij}(j) = i, t_{ij}(k) = k$, при $i \neq j$.

Утверждение 3.3. $\langle \{t_{ij}\}_{\substack{i=1..n \\ j=1..n}} \rangle = S_n$.

Доказательство. Индукция по n.

- База $n = 2$: $S_2 = \langle id, t_{12} \rangle$.
- Переход. $n \to n+1$. Пусть $\pi \in S_{n+1}$. $\exists i : \pi(i) = n+1$. Рассмотрим $t_{i,n+1}$, то есть $t_{i,n+1}(i) = n+1$ и $t_{i,n+1}(n+1) = i$. $\pi \circ t_{i,n+1}(n+1) = \pi(i) = n+1$.

  Тогда сузим π до n. Получим $\widetilde{\pi} = \{1 \dots n\} \to \{1 \dots n\}, \widetilde{\pi} \in S_n$. По и.п. $\widetilde{\pi} = t_{i_1,j_1} \circ t_{i_2,j_2} \circ \dots \circ t_{i_k,j_k} = \pi \circ t_{i,n+1}$ Тогда заметим, что

$$\pi = \underbrace{t_{i_1,j_1} \circ t_{i_2,j_2} \circ \dots}_{\text{образующие для} \widetilde{\pi}} \circ (t_{i,n+1})^{-1}.$$

□

***Определение* 3.6.** Перестановка π называется четной (нечетной), если выполнено одно из равносильных условий:

1. $\pi = t_{i_1,j_1} \dots t_{i_{2k},j_{2k}}$ (соответственно $2k+1$).
2. $\#\{(i,j) \mid {\substack{i \in \{1..n\} \\ j \in \{1..n\}}} \wedge \begin{cases} i < j \\ \pi(i) > \pi(j) \end{cases} \}$ — четно/нечетно соответственно.
3. $\prod\limits_{i<j} \frac{\pi(i) - \pi(j)}{i - j} = 1$ (соответственно -1).

Следствие. 1. корректно (то есть четность чила множителей не зависит от разложения).

Доказательство. Докажем, что $1 \iff 2$.

Количество из определения 2 называется число инверсий. Надо доказать, что $\pi = \prod_{l=1}^{k} t_{i_l,j_l} \implies$ количество инверсий $\equiv k \pmod 2$.

Индукция по k:

- База. $k = 0, \pi = \mathrm{id}$. 0 инверсий.
- Переход: надо доказать, что $\pi \in S_n \forall i, j$ четности числа инверсий для π и $t_{ij}\pi$ — разные.

  Какие пары поменяли статус при применении t_{ij}: $(\pi(i), t_l), (\pi(j), t_l), (\pi(i), \pi(j))$. Первого типа — k, второго — k, третьего — 1. А значит четность изменилась.

□

***Определение* 3.7.** $A \in M_n(K)$. Определителем A называется число

$$detA = |A| = \sum_{\pi \in S_n} \varepsilon(\pi) a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}$$

, где $\varepsilon(\pi) = 1$ — π четна, -1 иначе.

Замечание. t_{12}. $\pi \leftrightarrow t_{12} \circ \pi$ — биекция между четными и нечетными.

Утверждение 3.4. Функция $\omega\colon (K^n)^n \to K$, $\omega(c_1, \dots, c_n) = \det(C_1 \mid C_2 \mid \dots \mid C_n)$ — полилинейная кососимметрическая форма.

Доказательство. Полилинейность — очев.

Кососимметричность: $\omega(c_1, \dots, c_i, \dots, c_j, \dots) = 0$, если $c_i = c_j$. Докажем, что все слагаемые в формуле разбиваются на пары вида $(x, -x)$ для det.

Рассмотрим $\varepsilon(\pi) a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}$. Здесь a_{ki} и a_{lj}.

Тогда пусть $\pi(k) = i, \pi(l) = j$.

Рассмотрим $\varepsilon(t_{ij}\pi)$. Здесь все будет так же, за исключением $a_{ki} = a_{kj}, a_{li} = a_{lj}, \varepsilon(t_{ij}\pi) = -\varepsilon(\pi) \implies A + B = 0$. □

Теорема 3.5. $\det(A) = \det(A^T)$.

Следствие. Любое свойство det про столбцы $\rightsquigarrow$ такое же свойство про строки.

Доказательство.

$$\begin{aligned}
\det A &= \sum_{\pi \in S_n} a_{1\pi(1)} \dots a_{n\pi(n)} \cdot \varepsilon(\pi). \\
\det A^T &= \sum_{\pi \in S_n} a_{\pi(1)1} a_{\pi(2)2} \dots a_{\pi(n)n} \cdot \varepsilon(\pi) = \\
&= \sum_{\pi \in S_n} a_{\pi(1),\pi^{-1}(\pi(1))} a_{\pi(2),\pi^{-1}(\pi(2))} \dots a_{\pi(n),\pi^{-1}(\pi(n))} \varepsilon(\pi) \\
&\overset{(*)}{=} \sum_{\sigma \in S_n} a_{1\sigma(1)} \dots a_{n,\sigma(n)} \varepsilon(\sigma) = \det A
\end{aligned}$$

Здесь $\sigma = \pi^{-1}$. $\varepsilon(\pi) = \varepsilon(\sigma)$ так как количество транспозиций у них равно. □

Теорема 3.6. $A \in M_n(K)$.

1. $\det(t_{ij}(a)A) = \det(At_{ij}(a)) = \det A$.
2. $\det(m_i(a)A) = \det(A \cdot m_i(a)) = a \det A$
3. $\det(s_{ij}A) = \det(As_{ij}) = -\det A$.

Доказательство. 3. кососимметричность. (Второе определение).

2. Линейность по i-ой строке (столбцу).
1. $\det(t_{ij}A) = \det(A)$. Пусть r_i — i-ая строка.

   Тогда $\det\begin{pmatrix} A_1 \\ \hline r_i + r_j \cdot a \\ \hline B_1 \end{pmatrix} = \det\begin{pmatrix} A_1 \\ \hline r_i \\ \hline B_1 \end{pmatrix} + \det\begin{pmatrix} A_1 \\ \hline r_j \cdot a \\ \hline B_1 \end{pmatrix} = \det\begin{pmatrix} A_1 \\ \hline r_i \\ \hline B_1 \end{pmatrix} + a \cdot \det\begin{pmatrix} A_1 \\ \hline r_j \\ \hline \vdots \\ r_j \\ \hline \vdots \end{pmatrix} =$

   $\det A$. Последний переход за счет определения кососимметрической формы.

□

Замечание. Определитель — сумма произведения элементов A по ладейной расстановке.

Умеем приводить матрицу к треугольному виду. Тогда заметим, что единственная ненулевая перестановка — id. А значит det треугольной матрицы — произведение элементов матрицы на диагонали. А дальше надо домножить на -1 в степени количества перестановок.

Теорема 3.7. A — обратима $\iff \det A \neq 0$.

Доказательство. A — обратима $\iff e_1 \dots e_k A =$ треугольная матрица B — обратима.

$\det B \neq 0 \iff$ все $a_i \neq 0$.

B — обратима $\iff a_i \neq 0$ (доказывали). □

Теорема 3.8. $A, B \in M_n(K)$. Тогда

1. $\det(AB) = \det(A) \cdot \det(B)$
2. если $\exists A^{-1}$, то $\det(A^{-1}) = \frac{1}{\det A}$.
3. $\det E = 1$.

То есть $\det\colon GL(n, k) \to K^*$ — гомоморфизм групп (единственный нетривиальный).

Доказательство. 3. E — частный случай треугольной. Очев

2. Следует из 1 и 3: $1 = \det E = \det(A \cdot A^{-1}) = \det(A) \cdot \det(A^{-1})$.
1. Представим B как набор столбцов c_1 — переменная, а $A = \text{const}$.

   $A \cdot B = (A \cdot C_1 \mid A \cdot C_2 \mid \dots \mid A \cdot C_n)$. $B \mapsto \det(AB)$ — кососимметрическая полилинейная форма от $C_1, C_2, \dots, C_n$. Воспользуемся кососимметричностью: $C_i = C_j \implies AC_i = A \cdot C_j$ — два одинаковых столбца в $AB \implies \det AB = 0$.

   $B' = (C_1' \mid C_2 \mid \dots \mid C_n), B'' = (C_1'' \mid C_2 \mid \dots \mid C_n)$. Тогда $AB = (A(C_1' + C_1'') \mid C_2 \mid \dots) = (AC_1' + AC_2'' \mid \dots)$.

$AB' = (AC_1' \mid AC_2' \mid \cdots \mid AC_n'), AB'' = (AC_1'' \mid AC_2'' \mid \cdots \mid AC_n'').B \mapsto \det(AB), B \mapsto \det(B)$ - полилинейные кососимметрические $\implies$ по единственности $\exists c : \det(AB) = c \cdot \det(B) \forall B$

Подставим $B = E : \det(A) = c \cdot \det(E) = c$. Итого $\det(AB) = \det(A) \cdot \det(B)$

□

Теорема 3.9 (Определитель блочной матрицы)**.** 1. $A = \left(\begin{array}{c|c} A_1 & * \\ \hline 0 & A_2 \end{array}\right) \implies \det A = \det(A_1)\det(A_2)$.

2. Если блоков k, то $\det A = \prod \det(A_i)$. (A_i — квадратные блоки).

Доказательство. Второй пункт из первого по индукции (упражнение).

1. $\det \left(\begin{array}{c|c} E_x & * \\ \hline 0 & E_y \end{array}\right) = 1$. Так как треугольная матрица.
2. Зафиксируем B. $\det \left(\begin{array}{c|c} A_1 & B \\ \hline 0 & E \end{array}\right) = c_b \det(A_1)$ — полилинейная и кососимметричная относительно столбцов A_1.

   Поставим $A_1 = E \implies c_b = 1$ по пункту 1.
3. fix B, A_1 $\det \left(\begin{array}{c|c} A_1 & b \\ \hline 0 & A_2 \end{array}\right) = c_{A_1,B} \cdot \det(A_2)$. Подставляем $A_2 = E$: $\det A_1 = \det \left(\begin{array}{c|c} A_1 & B \\ \hline 0 & E \end{array}\right) = c_{A_1,B} \cdot 1 \implies c_{A_1,B} = \det A_1$. А значит $\det \left(\begin{array}{c|c} A_1 & b \\ \hline 0 & A_2 \end{array}\right) = \det A_1 \det A_2$.

□

Теорема 3.10 (Разложение по строкам/столбцам)**.** $A = (a_{ij})$. $A_{ij} = \det$ матрицы, полученной удалением i-ой строки и j-го столбца.

Тогда $\forall i \det A = \sum\limits_{j=1}^{n} (-1)^{i+j} a_{ij} A_{ij}$ — разложение по строке.

Сила в том, что определитель n-го порядка можно свести к det $(n-1)$-го порядка.

Доказательство. Для строк. Пусть $r_i = (a_{i1}, a_{i2}, \ldots, a_{in}) = \sum a_{ik} f_k$, где f_k — строка с 1 на k-й позиции.

По полилинейности $\det A = \sum a_{ik} \det A_k$. $A_k = \begin{pmatrix} r_1 \\ r_2 \\ r_{i-1} \\ 0 \ \ldots \ 1 \ 0 \ \ldots \ 0 \\ \vdots \\ r_n \end{pmatrix}$.

Тогда $\det A_k = (-1)^{i+k} \cdot \det B$. Где B мы просто перенесли i-ую строку и k-й столбец на первые места. Тогда получилась блочная матрица. $= A_{ik} \cdot (-1)^{i+k}$. □

Следствие. $\sum_{i=1}^{n} (-1)^{i+j} a_{ij} \cdot A_{kj} = 0$ $(k \neq i)$.

Доказательство. Эта сумма по предыдущей теореме равна $\pm \det$ матрицы вида $k \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix}$ (как наша матрица A, но на k-й строке опять стоит какая-то r_i). Если распишем разложеие по $k-$й строке определителя такой матрицы, то получим 0. □

***Определение* 3.8.** $(-1)^{i+j}A_{ij}$ — алгебраическое дополнение элемента a_{ij}

***Определение* 3.9.** Пусть $A \in M_n(K)$

$\operatorname{Adj} A = ((-1)^{i+j}A_{ji})$ — присоединенная матрица/

Теорема 3.11. $A \cdot \operatorname{Adj}(A) = \operatorname{Adj}(A) \cdot A = (\det A) \cdot E$.

В частности, если A — обратима ($\det A \neq 0$), $A^{-1} = \frac{1}{\det A} \operatorname{Adj} A$.

Доказательство. $\operatorname{Adj}(A) = (b_{ij})$, $A \cdot \operatorname{Adj}(A) = (c_{ij})$.

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{n} a_{ik} \cdot (-1)^{k+j}A_{jk} = \sum_{k=1}^{n}(-1)^{k+j}a_{ik}A_jk = \left[\begin{array}{ll} 0, & i \neq k \\ \det A, & i = k \end{array}\right. .$$

Итого: $c_{ij} = \delta_{ij} \det A \implies (c_{ij}) = \det A \cdot E$, где $\delta ij = \begin{array}{l} 0, i \neq j \\ 1, i = j \end{array}$. ☐

Замечание. Теперь СЛУ $AX = B$, A — обратима, тогда $X = A^{-1}B = \frac{\operatorname{Adj} A}{\det A} \cdot B$

Теорема 3.12. Формула Крамера. Пусть дана СЛУ $A \cdot X = B$, $A \in M_n(K), B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$, $\det A = \Delta \neq 0$.

$\Delta_i = -\det$ матрицы, полученной из A заменой i-го столбца на B.

Тогда решение: $x_i = \frac{\Delta_i}{\Delta} \quad \forall i = 1..n$.

Доказательство. $\det A \neq 0 \iff A$ — обратима $\iff \forall B \exists! X \colon AX = B, X = A^{-1}B$.

$$A^{-1} = (b_{ij}).\ A^{-1}\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Тогда $x_i = \sum_{k=1}^{n} b_{ik}b_k = \sum_{k=1}^{n} \frac{1}{\det A}(-1)^{i+k}A_{ki}b_k = \frac{1}{\Delta}\sum_{k=1}^{n}(-1)^{i+k}A_{ki}b_k = \frac{1}{\Delta}\det(c_1 \mid c_2 \mid \ldots \mid B \mid c_n) = \frac{\Delta_i}{\Delta}$ ☐

***Определение* 3.10.** $A \in M_{m,n}(K)$: отображение $I \times J \to K$, $|I| = m, |J| = n$.

Минором порядка S называется $\det(A\Big|_{I' \times J'})$, где $I' \subset I, J' \subset J, |I'| = |J'| = S$.

У матрица A есть $\binom{m}{S} \cdot \binom{n}{S}$ миноров порядка S.

***Определение* 3.11.** Минорный ранг A — наибольший порядок ненулевого минора в A.

Замечание. Из разложения по строке следует: все миноры порядка $S+1$ нулевые ранга $\leqslant S$.

Следствие. Множество матриц $\in M_{m,n}(K)$ ранга $\leqslant S$ — поверхность в $(m-n)$—мерном пространстве, заданная системой полиномиальных уравнений.

Упражнение. Сколько миноров надо протестировать, чтобы убедиться, что все $= 0$? А чтобы убедиться, что все > 0?

Теорема 3.13. $A \in M_{n,m}(K) \operatorname{rk} A = k$. Докажем, что минорный тоже K.

Доказательство.

1. Рассмотрим любой минор порядка $> k$. Выберем столбцы $c_{i_1}, \ldots, c_{i_S}$ — соответствующие столбцы $\implies$ они ЛЗ. Пусть c'_{i_1}, c'_{i_S} — столбцы подматрицы $\implies$ они ЛЗ.

Тогда по определению det подматрицы равен нулю.

2. $\exists c_{i_1}, \ldots, c_{i_k}$ — ЛНЗ столбцы размера k, $\operatorname{rk} \widetilde{A} = k, m \geqslant k$. И ЛНЗ строки $r_{j_1}, \ldots, r_{j_k}$ в $\widetilde{A}$, где $\widetilde{A}$ — матрица из выбранных столбцов.

   Тогда получили квадратную матрицу размера и ранга $k \implies \operatorname{rk} A \neq 0$.

$\square$

4. Локализация и поле дробно-рациональных функций

В $\mathbb{Z}$ — почти все элементы необратимы. Но можно перейти к $\mathbb{Q}$ — все ненулевые элементы $\mathbb{Z}$ стали обратимы.

А мы хотим обобщить данную операцию на большое количество колец. То есть, пусть R — кольцо, $M \subset R$. Вопрос: можно ли сделать S — кольцо, такое что $R \subset S$ — подкольцо в S, причем любой элемент из M из S обратим.

Заметим, что если $0 \in M$, то это плохо. Или в $\mathbb{Z}/4\mathbb{Z}$ если сделать 2 обратимым, то $2 \cdot 2 = 0$ — обратим.

***Определение* 4.1.** R — коммутативное кольцо. $M \subset R$ называется мультипликативной системой, если:

1. $m_1, m_2 \in M \implies m_1 m_2 \in M$.
2. $0 \notin M$.

Пример. R — область целостности. $M = R \setminus \{0\}$ — мультипликативная система.

***Определение* 4.2.** $M = R \setminus \{0\}$, R — область целостности, R_m — поле частных кольца R (и это будет поле).

Теорема 4.1. M — мультипликативная система в коммутативном кольце R. Тогда $\exists$ Кольцо R_M и инъективный гомоморфизм колец $i\colon R \to R_M$ (вложение), такие что:

1. $i(x) \in R_M^* \quad \forall x \in M$,
2. Универсальное свойство: $\forall$кольцо $S, \forall$гомоморфизм$f\colon R \to S$, такой что $f(x) \in S^* \quad x \in M$ $\exists! g\colon R_m \to S$, такой что $f = g \circ i$

Замечание. R — коммутативное кольцо. Тогда $\exists K : R$ — подкольцо $K \iff R$ — область целостности.

Доказательство теоремы. Будем считать, что R — область целостности, $M = R \setminus \{0\}$.

Будем вводить дроби. Для начала рассмотрим $\widetilde{K} = R \times (R \setminus \{0\})$. Зададим на нем отношение эквивалентности: $(a, b) \sim (c, d) \iff ad = bc$. Проверим данное утверждение:

- $(a, b) \sim (a, b) \Leftarrow ab = ab$.
- $(a, b) \sim (c, d) \implies (c, d) \sim (a, b)$ по коммутативности.
- $(a, b) \sim (c, d) \sim (e, f)$. Так как $ad = bc \wedge cf = ed \implies a \cdot cf = ade = bce \iff acf = bce \xRightarrow{R\text{ — о.ц.}} af = be \iff (a, b) \sim (e, f)$.

Обозначим $K = \widetilde{K}/\sim$. Зададим $+, \cdot\colon K \times K \to K$: $(a, b) + (c, d) = (ad + bc, bd), (a, b) \cdot (c, d) = (ac, bd)$.

Тогда $i\colon \begin{matrix} R \to K \\ a \mapsto (a, 1) \end{matrix}$, $a = \frac{a}{1}$. Надо проверить: определение и корректность, $(K, +, \cdot)$ — поле, u — инъективный гомоморфизм колец, универсальное свойство.

Проверим определение: $(a,b)\sim(a_1,b_1)$. Тогда проверим, что $(a_1d+b_1c,b_1d)\sim(ad+bc,bd) \iff (a_1d+b_1c)bd=b_1d(ad+bc) \iff a_1bd^2+babcd=ab_1d^2+b_1cd \iff a_1b=ab_1$.

Умножение — определение.

Проверим свойства сложения: ассоциативность $(\overline{(a,b)}+\overline{(c,d)})+\overline{e,f}=\overline{(ad+bc,bd)}+\overline{(e,f)}=\overline{(adf+bcf+bde,bdf)}$. При этом $\overline{(a,b)}+(\overline{(c,d)}+\overline{(e,f)})=\overline{(a,b)}+\overline{(df+de,df)}=\overline{(adf+bcf+bde,bdf)}$

$0_K\coloneqq(0,1),(0,1)+(a,b)=(0\cdot b+a\cdot 1,1\cdot b)=(a,b)$.

$-(a,b)=(-a,b)$ — упражнение.

Ассоциативность умножение — очевидно.

Коммутативность умножения тоже.

$1_K=\overline{(1,1)}\ (1,1)\cdot(a,b)=(1\cdot a,1\cdot b)=(a,b)$. $(a+b)c=ac+bc$: $(\overline{(a,d)}+\overline{(b,e)})\overline{(c,f)}=\overline{(ae+bd,cd)}\cdot\overline{(c,f)}=\overline{(aec+bdc,edf)}$. В другое сторону лень.

$\overline{(a,b)}\cdot\overline{(b,a)}=\overline{(ab,ab)}=\overline{(1,1)}=1$. Если $a,b\neq 0, a\neq 0 \implies \overline{(a,b)}$ — обратим. $a=0\implies\overline{(0,b)}=\overline{(0,1)}=0$. Значит K — поле.

Проверим, что i — гомоморфизм: $i(a)=\overline{(a,1)},i(b)=\overline{(b,1)},i(a+b)=\overline{(a+b,1)}$.

Будем обозначить $\overline{(a,b)}\eqqcolon\frac{a}{b}=i(a)\cdot i(b)^{-1}$.

Проверим универсальное свойство. $f:R\to S$ — гомоморфизм. $f(r)\in S^*\quad\forall r\neq 0$. $f(r)=g\circ i(r)\iff f(r)=g(\frac{r}{1})$.

$g(r)\cdot g(\frac{1}{r})=g(1)=1=f(r)\cdot f(r)^{-1}\implies g(\frac{1}{r})=f(r)^{-1}\implies g(\frac{r_1}{r})\cdot g(\frac{1}{r})=f(r)\cdot f(r_1)^{-1}$.

g — определено однозначно: $g(\frac{a}{b})=f(a)\cdot f(b)^{-1}$.

Корректность $\frac{a'}{b'}=\frac{a}{b}\iff a'b=b'a\implies f(a'b)=f(b'a)\iff f(a')\cdot f(b)=f(b')\cdot f(a)\iff f(a)f(b)^{-1}=f(a')\cdot f(b')^{-1}$— g не зависит от выбора представителя. □

Пример. Поле частных — полная локализация. R — ОГИ. $p\in R$ — простое. $M=\{x\in R\mid x\not\vdots\, p\}$ — мультипликативная система. R_M — локальное кольцо (остался один просто элемент).

Пример. $R=\mathbb{Z}$: поле частных — $\mathbb{Q}$.

$R=K[X]$, K — Поле частных называется $K(x)$, поле дробнорациональных функций.

Замечание. $Q\in K(x)$, $\exists!$(с точностью до ассоциированности)f,g: $Q=\frac{f}{g},(f,g)=1$.

Доказательство. $Q=\frac{\widetilde{f}}{\widetilde{g}}\exists(\widetilde{f},\widetilde{f})=d,\widetilde{f}=df,\widetilde{g}=dg$, $(df,dg)\sim(f,g)$.

Пусть $\frac{f}{g}=\frac{f_1}{g_1},(f_1,g_1)=1\implies fg_1=gf_1,dg_1\vdots g\wedge(f,g)=1\implies g_1\vdots g$. Аналогично $g\vdots g_1,f\vdots f_1,f_1\vdots f$. $f=cf_1,g=cg_1,\deg(c)=0$. □

$K(x)^*$ устроена понятно: $\frac{f}{g}=\frac{\prod p_i^{a_i}}{\prod q_i^{b_o}}=a\prod\varphi_i^{c_i}$. где φ_i — унитальные неприводимые $\in K[x],c_i\in\mathbb{Z}$.

Что со сложением: найдем БАЗИС $K(x)$ над K: $P\cup F$. $P=\{1,x,x^2,\ldots\}$ — базис $K[x]$. $F=\{\frac{p}{q^l}\mid p,q$ — унитальные $\wedge\ l$—неприводимый $\wedge\deg p<\deg q\}$ — простейшие дроби.

Теорема 4.2. $P\cup F$ — базис.

Доказательство. Шаг 1. $Q\in K(x)\implies\exists!R\in K[x]:Q=R+\frac{f}{g},f,g\in K[x],\deg f<\deg g$. $Q\eqqcolon R+\frac{f}{g},Q=\frac{R}{1}+\frac{f}{g}=\frac{Rg+f}{g}$ правильная дробь.

Пусть $Q_0=\frac{f_0}{g_0}$. Положим $g=g_0$, $f_0=R\cdot g_0+f$ (теорема о делении с остатком). Откуда и получаем $Q=R+\frac{f}{g}$.

Единственность: $R + \frac{f}{g} = R' + \frac{f'}{g'}$. $R - R' = \frac{f'}{g'} - \frac{f}{g} = \frac{f'g - g'f}{gg'}$.

$(R - R')gg' = f'g - g'f$. Если $R - R' \neq 0 \implies \deg(R - R')gg' \geqslant \deg gg' = \deg g + \deg g'$, но $\deg f'g = \deg f' + \deg g < \deg g' + \deg g$. Для $\deg fg'$ — тоже самое.

То есть $\deg(f'g + fg') < \deg g + \deg'$. Противоречие.

Осталось доказать: $\forall$ правильная дробь однозначно представляется как сумма простейших.

***Определение* 4.3.** Правильная дробь называется примарной, если она представима в виде $\frac{f}{p^k}$, p — неприводимая, $\deg f < \deg p^k$.

Шаг 2. Любая правильная дробь — сумма многочлена и примарных.

Пусть правильная дробь $Q = \frac{p}{q_1^{a_1} q_2^{a_2} \ldots q_k^{a_k}}$, где q_i – неприводимы (неразложимы).

Докажем по индукции:

- База: $k = 1$. Очев. Сразу примарная
- Переход: $k \to k + 1$. Пусть $q := \prod\limits_{i=1}^{k} q_i^{a_i}$. Но вспомним, что q_i - неприводимы, значит q и q_{k+1} взаимопросты, тогда $\exists f, g \in K[x] : fq + gq_{k+1}^{a_{k+1}} = 1$. Ну тогда $Q = \frac{p}{q \cdot q_{k+1}^{a_{k+1}}} = \frac{p\left(fq + gq_{k+1}^{a_{k+1}}\right)}{q \cdot q_{k+1}^{a_{k+1}}} = \frac{pf}{q_{k+1}^{a_{k+1}}} + \frac{pg}{q}$. Ну понятно, если надо, то поделим с остатком и вынесем многочлен. Первая дробь тогда примарна по определению. Вторая дробь раскладывается на примарные по индукционному предположению.

Шаг 3. Любая примарная дробь — сумма многочлена и простейших дробей.

Пусть $\frac{f}{p^k}$ — примарная, p — неразложимая. $\frac{f}{p^k} = F + \frac{h}{p^k}, F \in K[x], \frac{h}{p^k}$ — правильная примарная.

$\exists h_0, h_1, h_2, \ldots, h_{k-1} \in K[x] \colon \deg h_i < \deg p$ и $f = h_0 + h_1 + h_2 p^2 + \ldots + h_{k_1} p^{k-1}$. Обозначим это утверждение звездочкой.

Тогда $\frac{h}{p^k} = \frac{h_0}{p^k} + \frac{h_1}{p^{k-1}} + \ldots + \frac{h_{k-1}}{p}$. Так как $\deg h_i < \deg P$, то данные дроби простейшие.

Доказательство звездочки: индукция по k.

- База. $k = 1$: $h = h_0$.
- Переход: $k \to k + 1$: Поделим с остатком $h = p \cdot q + r, \deg r < \deg p$. Положим $h_0 = r$. $h = h_0 + p \cdot q$ и $\deg q = \deg h - \deg p < \deg p^{k+1} - \deg p = \deg p^k$. Тогда по индукции $q = h_1 + h_2 \cdot p + \ldots + h_k \cdot p^{k+1}$.

□

Давайте найдем явную формулу для $Q = \frac{f}{g}$, где $g = (x - a_1) \cdot \ldots \cdot (x - a_n)$ и $\deg f < \deg g$.

Напишем Лагранжа для задачи $(a_1, f(a_1)), \ldots, (a_n, f(a_n))$. $f = \sum\limits_{i=1}^{n} \frac{f(a_i) \prod\limits_{i \neq j} (x - a_j)}{\prod\limits_{j \neq i} (a_i - a_j)} = \sum\limits_{i=1}^{n} f(a_i) \frac{\frac{g}{x - a_i}}{g'(a_i)}$.

Откуда получаем, что $\frac{f}{g} = \sum \frac{f(a_i)}{g'(a_i)} \cdot \frac{1}{x - a_i}$

5. Теория групп

Теория групп = теория неабелевых групп, теория абелевых групп $\approx$ линейная алгебра.

Например, $G = \langle x_1, x_2, \ldots, x_n\rangle$. Тогда $G \cong$ произведению циклических групп.

Или $G = \langle a, b\rangle$, G — абелева, тогда $G = \{a^k b^l \mid k, l \in \mathbb{Z}\}$.

***Определение* 5.1.** V — конечное множество, $|V| = n$. $S(V) = \{f\colon V \to V (f \text{ — биекция})\}$.

Если $V = 1..n \implies S(V) = S_n$.

***Определение* 5.2.** K — поле, $n \in \mathbb{N}$, тогда $GL(n, K)$ — обратимые матрицы порядка $n = \{A\colon V \to V \mid \begin{matrix} A \text{ — биективное отображение} \\ V \text{ — } n\text{-мерное пространство} \end{matrix} \}$

Замечание. S_n вкладывается в $GL(n, K)$.

Доказательство. π — перестановка, $V = \langle e_1, e_2, \ldots, e_n\rangle$. $A_\pi(e_i) = e_{\pi(i)}$. Тогда $\pi \to A_\pi$ — инъективный гомоморфизм. □

Теорема 5.1 (Теорема Кэли)**.** Любая конечная группа изоморфна подгруппе в S_n при некотором n.

Доказательство. Положим $n = |G|$. G — конечная группа, то есть $G = \{g_1, \ldots, g_n\}$. Тогда $g \in G \quad m_g\colon G \to G \quad m_g(g_i) = gg_i$ — биекция.

То есть $g \cdot g_i = g_{\pi_g(i)}, \pi_g \in S_n$ — перестановка.

Теперь зададим гомоморфизм: $i\colon \begin{matrix} G \to S_n \\ g \to \pi_g \end{matrix}$. i — инъективно: $\pi_g = \pi_{g'} \implies g \cdot e_G = g' \cdot e_G \implies g = g'$.

Покажем, что i — гомоморфизм: надо проверить $\pi_{g_1 g_2} = \pi_{g_1} \cdot \pi_{g_2}$.

$\pi_{hf} = \pi_h \cdot \pi_f. \quad g_{\pi_h(\pi_f(i))} = h \cdot g_{\pi_f(i)} = h(fg_i) = (hf)g_i = g_{\pi_{hf}(i)}$. □

Замечание. Заметим, что в доказательстве теоремы Кэли мы находим не обязательно минимальное регулярное представление. Например, для S_4 минимальное представление равно S_4, а у нас S_{24}.

5.1. Смежные классы и теорема Лагранжа

Пусть есть группа G и $H \leqslant G$ — подгруппа.

***Определение* 5.3.** Левый смежный класс по подгруппе H, это $gH = \{g \cdot h \mid h \in H\}$.

***Определение* 5.4.** Правый смежный класс по подгруппе H — $H \cdot g = \{h \cdot g \mid h \in H\}$

Вообще говоря $gH \neq Hg$ (если H — неабелева).

Пример. Пусть $g \in H \implies gH = Hg = H$.

Свойства смежных классов. 1. $g_1 H = g_2 H \iff g_2^{-1} g_1 \in H \iff g_1^{-1} g_2 \in H$.

2. $\forall 2$ смежных класса не пересекаются или совпадают.

Доказательство. 1. $g_1H = g_2H \iff \{g_1h\} = \{g_2h\} \iff \{g_2^{-1}g_1h\} = \{h\} = H$.

$\Leftarrow$: $g_2^{-1}g_1 \in H \implies \{g_2^{-1}g_1h\} = H$.

$\Rightarrow$: $\{g_2^{-1}g_1h\} = H$, подставим $h = e \implies g_2^{-1}g_1 \in H$.

Аналогично для $g_1g_2^{-1}$. Получили классы эквивалентности: $g_1 \underset{H}{\sim} g_2 \iff g_1H = g_2H$.

2. Докажем отношение эквивалентности: $g_1 \underset{H}{\sim} g_2 \iff g_1 \in g_2H$.

$\Rightarrow$. $g_1H = g_2H$. Подставим $h = e$.

$\Leftarrow$. $g_1 = g_2 \cdot h_0, h_0 \in H$. $\{g_1h \mid h \in H\} = \{(g_2h_0)h \mid h \in H\} = \{g_2(h_0h) \mid h \in H\} = \{g_2\widetilde{h} \mid \widetilde{h} \in H\} = g_2H$.

$\square$

Замечание. Схожие утверждения верны и для правых классов.

Итого: $\forall$ подгруппа H задает 2 разбиения G на смежные классы.

Пример. $G = (\mathbb{Z}, +), H = \langle a \rangle = \{ka \mid k \in \mathbb{Z}\}$

$l = \{l + ka \mid k \in \mathbb{Z}\} = \overline{l_a}$ — a классов вычетов.

***Определение* 5.5.** G — группа, H — подгруппа, такая что $\exists k$ левых смежных классов, k называется индексом H в G. Обозначение: $|G : H| = k$

Упражнение. $gH \longleftrightarrow Hg^{-1}$ — биекция между левыми и правыми смежными классами.

Теорема 5.2 (Теорема Лагранжа)**.** $|G| = n, |H| = k,\ H \leqslant G$.

Тогда $|G : H| = \frac{n}{k}$. В частности $|G| \vdots |H|$. Порядок группы делится на порядок подгруппы.

Доказательство. Вспомним доказательство частного случая с первого модуля (порядок группы делится на порядок элемента). Мы фиксировали a и разбивали все элементы на циклы длины $\operatorname{ord}_G a$ вида $x \to ax \to a^2x \to \dots a^{\operatorname{ord}_G(a)-1}x \to x$. В новых терминах получившиеся циклы — классы смежности a по подгруппе H. $\forall g \in G\colon |gH| = |H| = \operatorname{ord} a = k \Rightarrow |G : H| = \frac{n}{k}$ $\square$

***Определение* 5.6.** G/H — множество левых смежных классов.

$H \setminus G$ — множество правых смежных классов.

5.2. Группа перестановок

***Определение* 5.7.** $\pi \in S_n$ называется циклом, если $\exists i_1, \dots, i_k \in \{1..n\}$, такое что $\pi(i_l) = i_{l+1}$и $\pi(i_k) = i_1$ и $\pi(j) = j$ для остальных.

***Определение* 5.8.** Циклы называются независимыми, если их множества подвижных точек не пересекаются.

Замечание. $\pi_1, \pi_2, \dots, \pi_n$ — попарно независимые циклы $\implies$ их произведение не зависит от порядка множителей.

Теорема 5.3. $\pi \in S_n$. π — единственным образом (с точностью до порядка) представима как произведение независимых циклов.

Доказательство. Будем доказывать для $S_n \cong S(M)$.

- База, $n = 1$.

- Переход: $1, \dots, n-1 \to n$.

  Рассмотрим $\pi \in S(M), a \in M$. Рассмотрим $\pi(a), \pi(\pi(a)), \dots$. Рассмотрим минимальное k, такое что $\pi^k(a) = \pi^l(a)$ для какого-то $0 \leqslant l < k$./

  Если $l \neq 0$, так как π — биекция, то $\pi^{k-1}(a) = \pi^{l-1}(a)$. Противоречие.

  Если $l = 0$, то получили цикл. $N = \{\pi^i(a) \mid i < k\}$. Пусть $\pi_0(x) = \pi(x)$, если $x \in N$ или x иначе. По индукционному предположению существуют циклы.

Единственность: ему лень :(□

***Определение* 5.9.** π — цикл на $i_1, i_2, \dots, i_k$. $\pi = (i_1 i_2 .. i_k)$

Тогда $\pi \in S_n$ — произвольная перестановка, $\pi = (i_1 \dots i_k)(j_1 \dots j_l)(s_1 \dots s_m)$

Теорема 5.4. (ij) — транспозиция. $\langle (ij) \rangle = S_n$.

Доказательство. Очев + доказывали □

Теорема 5.5. $\langle (ijk) \rangle = A_n$ — группа четных перестановок.

Доказательство. $(ijk) = (ij)(jk) \implies (ijk) \in A_n \implies \langle (ijk) \rangle \leqslant A_n$.

Обратно: пусть $\pi \in A_n$. $\pi = t_1 t_2 \dots t_{2k}$, t_i — транспозиции. Достаточно доказать, что $\forall$ транспозиций t_i, t_j $t_i \cdot t_j \in \langle (ijk) \rangle$.

Пусть $t_i = (ab), t_j = (cd)$. Тогда рассмотрим 3 случая:

1. $t_i = t_j \implies t_i \circ t_j = t_i^2 = \mathrm{id} \in \langle (ijk) \rangle$.
2. $b = c$, $a \neq d$. Очев.
3. a, b, c, d различны. Легко показать, что $(ab)(cd) = (cad)(abc) \in \langle (ijk) \rangle$.

□

***Определение* 5.10.** $a \underset{H}{\equiv} b \Leftarrow a \in bH$ (далее $\equiv$ вместо $\sim$).

Пример. $H = \{n\mathbb{Z} \mid x \in \mathbb{Z}\}$ — подгруппа.

$b \cdot H = b + H$ — класс вычетов по модулю n. $a \in bH$ $a = b \cdot h, h \in H \iff b^{-1}a \in H$.

$a \underset{H}{\equiv} b$, если $a \in Hb$ $(ab^{-1} \in H)$.

5.3. Факторгруппа

***Определение* 5.11.** $H \leqslant G$ называется нормальной ($H \trianglelefteq G$), если выполнено любое из трех равносильных утверждений:

1. $a \underset{H}{\equiv} b, c \underset{H}{\equiv} d \implies ac \underset{H}{\equiv} bd \quad \forall a, b, c, d \in G$.
2. $\forall a \in G \colon aH = Ha$.
3. $\forall h \in H, g \in G \colon g^{-1}hg \in H$.

***Определение* 5.12.** $g^{-1}hg$ и h называются сопряженными посредством h.

Доказательство. Направления доказательства $3 \implies 1$.

$a \equiv b \implies a = bh_1, c \equiv d \implies c = dh_2$, где $h_1, h_2 \in H \implies ac = bh_1dh_2 = bdd^{-1}h_1dh_2 = bd{\cdot}h_3{\cdot}h_2$, $h_3, h_2 \in H \implies \in bdH$. ☐

Замечание. Сопряженность — отношение эквивалентности. $G = \bigsqcup\limits_i C_i$, C_i — класс сопряженности.

***Определение* 5.13.** $H \trianglelefteq G$. Факторгруппой G/H называется множество классов смежности со следующей операцией $(a \cdot H)(b \cdot H) = ab \cdot H$.

Обозначение: $\overline{a_H}$, $\overline{a_H} \cdot \overline{b_H} := \overline{ab}_H$. Заметим, что первое определение нормальности показывает корректность данной операции.

Пример. $G = S_n$. $H \trianglelefteq S_n \implies \left[\begin{array}{l} H = \{e\} \\ H = S_n \\ H = A_n \end{array}\right.$

$G/G = \{\overline{e}\}$, $G/\{e\} \cong G$.

S_n/A_n: $e \cdot A_n = A_n$, $(12) \cdot A_n = S_n \setminus A_n$.

Напоминание: (K — поле) $GL_n(K)$ — обратимые матрицы размера n, $SL_n(K) = \{A \in M_n(K) \mid \det A = 1\}$.

Утверждение 5.6. $SL_n(K) \trianglelefteq Gl_n(K)$.

$GL_n(K)/SL_n(K)$. $A \cdot SL_n(K) = \{B \mid \det B = \det A\}$.

Поэтому $GL_n(K)/SL_n(K) \cong K^*$.

Утверждение 5.7. T — множество диагональных матриц, причем $a^n = 1$. Тогда $T \trianglelefteq SL_n(K), SL_n(K)/$ $PSL_n(K)$ — projective special group.

Пример. $f = \{\dfrac{ax+b}{cx+d} \mid ad - bc \neq 0\}$ — группа дробно-линейных преобразований над K. $f \rightsquigarrow = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = A$, $f_1 \rightsquigarrow \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = A_1$, $f \circ f_1 \rightsquigarrow A \cdot A_1$. То есть группа дробно-линейных преобразований — $PGL_2(n)$.

5.4. Теорема о гомоморфизме

Пусть G_1, G_2 — группы. $f\colon G_1 \to G_2$ — гомоморфизм, если $f(g_1g_2) = f(g_1)f(g_2)$. Изоморфизм $\iff$ гомоморфизм + биекция. f — автоморфизм $\iff$ изоморфизм и $G_1 = G_2$.

Замечание. G — абелева, $f(g) = g^{-1}$ — автоморфизм.

$g_0 \in G$ — фиксированно, $f_2(g) = g_0^{-1}gg_0$ — автоморфизм сопряжения.

$\ker f = \{g \in G \mid f(g) = e_{G_2}\}$ — ядро гомоморфизма. $\operatorname{Im} f = \{f(g) \mid g \in G\}$ — образ гомоморфизма.

Лемма. $f\colon G_1 \to G_2$, $\operatorname{Im} f \leqslant G_2, \ker f \trianglelefteq G_1$.

Доказательство. $f(g_1) = e, f(g_2) = e$. $f(g_1g_2) = f(g_1)f(g_2) = e$. $f(e_{G_1}) = e_{G_2}, f(e) = f(e \cdot e) = f(e) \cdot f(e)$.

$h \in \ker f \Rightarrow f(g^{-1}hg) = f(g^{-1})f(h)f(g) = f(g^{-1})f(g) = e$.

P.S. Тут не хватает ещё проверок, но они тривиальны ☐

Теорема 5.8. $f\colon G_1 \to G_2 \implies G_1/\ker f \cong \operatorname{Im} f$.

Доказательство. Возьмем $a \in \operatorname{Im} f$. Рассмотрим $f^{-1}(a) = \{b \mid f(b) = a\}$. Возьмем $b_0 \in f^{-1}(a)$, тогда $b \in f^{-1}(a) \iff f(b) = f(b_0) \iff f(bb_0^{-1}) = e \iff bb_0^{-1} \in \ker f \iff b \in b_0 \cdot \ker f$.

$f^{-1}(a) = b_0 \ker f$.

Построим $\widetilde{f}\colon G_1/\ker f \to \operatorname{Im} f$. $\widetilde{f}(b \ker f) = f(b)$.

1. $\widetilde{f}$ корректно. $c \in b \ker f \implies f(c) = f(bh) = f(b)f(h) = f(b)$.
2. $\widetilde{f}$ — гомоморфизм: $\widetilde{f}(\overline{a} \cdot \overline{b}) = \widetilde{f}(\overline{ab}) = f(ab) = f(a)f(b) = \widetilde{f}(\overline{a})\widetilde{f}(\overline{b})$.
3. $\widetilde{f}$ — сюръективно. $a \in \operatorname{Im} f \implies a = f(b) \implies a = \widetilde{f}(\overline{b})$.
4. $\widetilde{f}$ — инъективно. $\widetilde{f}(\overline{b}) = e \iff f(b) = e \iff b \in \ker f \iff \overline{b} = \overline{e}$.

□

Пример. $G = \mathbb{R}^*, H = \mathbb{R}^*_+$. $G/H \cong \{1, -1\} \cong \mathbb{Z}/2\mathbb{Z}$. $f\colon G \to G$, $f(x) = \frac{x}{|x|} = \operatorname{sgn}(x)$.

Пример. $G = D_4$ — группа самосовмещений квадрата. $|D_4| = 8$. Есть 1, 3 поворота и 4 оси симетрии.

$|G/H| = 4, G/G = F_2^2$. Первый бит — поворот на $\frac{\pi}{2}$ и зеркаливание.

Пример. G_1/G_2 — группы. $G = G_1 \times G_2$, $\widetilde{G_1} = \{(g_1, 3) \mid g_1 \in G_1\} \cong G_1$.

$G/G_1 \cong G_2$. $f\colon G_1 \times G_2 \to G_2$, $(g_1, g_2) \to g_2$, $\ker f = \widetilde{G_1}, \operatorname{Im} f = G_2 \implies G/G_1 = G_2$.

Пусть G — большая группа. Возьмем $H \trianglelefteq G$, заменим G на $(H, G/H)$. Например, может оказаться, что $G \cong H \times G/H$.

Пример, $H \cong \mathbb{Z}/2\mathbb{Z}, G/H \cong \mathbb{Z}/2\mathbb{Z}$, то тогда либо $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ и $G \cong \mathbb{Z}/4\mathbb{Z}$.

***Определение* 5.14.** G — называется простой, если у нее нет нетривиальных нормальных подгрупп.

Теорема 5.9. A_n — проста ($n \geqslant 5$).

Теорема 5.10. $PSL_n(K)$ проста для большинства n.

Теорема 5.11.

$$G \text{ — конечная простая} \implies \left[\begin{array}{ll} G \cong \mathbb{Z}/p\mathbb{Z} & p \text{ — простое} \\ G \cong A_n & n \geqslant 5 \\ G \cong PSL_n(K) & K \text{ — конечное поле} \\ \text{еще несколько матричных групп} & \\ \text{еще 26 исключительных простых групп} & \end{array}\right.$$

5.5. Действие групп

***Определение* 5.15.** G — группа, M — множество.

Действие G на M — отображение из $G \times M \to M$. $(g, m) \to g \cdot m$, такая что

1. $(g_1 g_2)m = g_1(g_2 m)$ и $em = m$.

***Определение* 5.16** (Альтернативное определение)**.** G действует на M, если задан гомоморфизм $f\colon G \to S(M)$.

Замечание. Построим $f_g\colon M \to M, m \mapsto g \cdot m$. Это биекция.

Говорят g действует на M. M — G-множество. $G \curvearrowright M$.

Пример.

1. $I_n = \{1..n\}$, $G = S_n$. $G \curvearrowright I_n$.
2. $I_n \times I_n \quad S_n \curvearrowright I_n \times I_n \quad \pi(x, y) = (\pi(x), \pi(y))$
3. $M = 2^{I_n}$. $S_n \curvearrowright 2^{I_n}$. $\pi \cdot \{x_1, \ldots, x_n\} = \{\pi(x_1), \ldots, \pi(x_n)\}$.
4. K — поле. K^* действует на K гомоморфизмами.

   ВАЖНО!!!!!!! $a \cdot b = ab$.
5. $(\langle g \rangle) C_n \curvearrowright \mathbb{C}$ $g \cdot z = e^{\frac{2\pi i}{n}} \cdot z$ — поворот на $\frac{2\pi}{n}$. $g^k z = e^{\frac{2\pi i k}{n}} z$.
6. $S_3 \curvearrowright \mathbb{C}$. (123) — умножение на $-\frac{1}{2} + \frac{\sqrt{3}}{2} i$. $(12) \cdot z = \overline{z}$.

***Определение* 5.17.** G точно действует на M, если $G \to S(M)$ — инъективно.

Неточное действие: $G \curvearrowright M$ $g \cdot m := m$ — тривиальное действие.

$S_3 \curvearrowright M$ изометриями (точно). Не $\exists$ точного действия на $S_4 \curvearrowright M$.

Пример Примеры из теории групп. Действие сдвигами $G \curvearrowright G\colon a \cdot b = a \cdot b$.

$H \leqslant G$. $G \curvearrowright G/H$, $g_1(g_2 H) = (g_1 g_2) H$. $\forall$ действие на чтобы то не было сводится к тому, что выше.

$G \curvearrowright G$ сопряжениями: $a \cdot b = aba^{-1}$. Действие автоморфизмами $g_1(b) = aba^{-1}$.

5.6. Орбиты и стабилизаторы

***Определение* 5.18.** $G \curvearrowright M$. $m_1 \sim m_2 \Leftarrow \exists g\colon g m_1 = m_2$.

Утверждение 5.12. $\sim$ — отношение эквивалентности.

***Определение* 5.19.** Класс эквивалентности $\sim$ называется орбитой действия.

***Определение* 5.20.** Орбита элемента — $G \cdot m = \{g \cdot m \mid g \in G\}$.

Замечание. M — дизъюнктное объединение орбит. $M = \bigcup\limits_{i \in I} O_i$ — орбиты.

тогда O_i — G-множества. $x \in O_i, g \in G \implies gx \in O_i$ — транзитивные множества.

***Определение* 5.21.** Множество называется транзитивным, если $\forall m_1, m_2 \in M \exists g \in G : g m_1 = m_2$.

***Определение* 5.22.** $\mathrm{Iso}(2)$ — группа изометрий плоскости. Транизитивно: на точки/прямые, не транзитивно на отрезки.

***Определение* 5.23.** $G \curvearrowright M$, $m \in M$. Стабилизатор $G_m = \{g \in G \mid gm = m\}$.

Пример. $S_4 \curvearrowright 2^{I_4}$. $m = \{1, 2\}, G \cdot m = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\}, G_m = \langle (34), (12) \rangle$.

Теорема 5.13.

1. $G_m \leqslant G$.
2. $m \in M,\ n = g_0 m \in Gm,\ m = g_1 n$. Тогда $\exists$ биекция $Gm \leftrightarrow G/G_m$, причем $\{g \mid gm = n\} = g_0 G_m$, $\{g \mid gn = m\} = G_m g_1$.

3. $|Gm| \cdot |G_m| = |G|$.

Доказательство. 1. Очев.

2. $g_0 G_m \subset \{g \mid gm = n\}$ — ясно. $\supset$: пусть $gm = n$. $g_0^{-1}gm = g_0^{-1}n = m \implies g_0^{-1}g \in G_m \implies g \in g_0G_m$.

3. из 2) биекция: элементы орбиты $M \leftrightarrow$ смежные классы $\implies |Gm| = |G : G_m| \implies |Gm| \cdot |G_m| = |G : G_m||G_m| = |G|$.

$\square$

Пример. $Iso(2)$ — движения плоскости. $S(K) = \{g \in Iso(2) \mid g(k) = k\}$, k — квадрат.

$g \in S(k)$ — переставляет A, B, C, D. Такая перестановка однозначно задает g. $G\cdot A = \{A, B, C, D\}, |GA$
4. $|G| = |G \cdot A| \cdot |G_A| = 4 \cdot |G_A| = 4 \cdot |(G_A)_B| = 8$.

$G_A \curvearrowright \{B, C, D\}$. $G_A \cdot B = \{B, D\}$.

5.7. Лемма Бернсайда

***Определение* 5.24.** $Fix(g) = \{m \in M \mid gm = m\}$ — фиксатор (множество неподвижных точек).

Теорема 5.14 (Лемма Бернсайда)**.** G — конечная, $G \curvearrowright M$. Тогда количество орбит действия равно среднему арифметическому размера фиксатора.

$$\frac{\sum_{g\in G} |Fix(G)|}{|G|} = \text{количество орбит.}$$

Доказательство. Рассмотрим $NotMove = \{(g, m) \mid g \in G, m \in M, gm = m\}$. Тогда $\sum\limits_{m\in M} |G_m| = |NotMove| = \sum_{g\in G} |Fix(g)|$. Тогда:

$$\frac{\sum_{g\in G} |Fix(g)|}{G} = \frac{\sum_{m\in M} |G_m|}{|G|} = \sum_{m\in M} \frac{|G_m|}{|G|} = \sum_{m\in M} \frac{1}{|Gm|}.$$

Тогда, если рассмотреть орбиту длины k, то она дает вклад $\underbrace{\frac{1}{k} + \frac{1}{k} + \ldots + \frac{1}{k}}_{k} = 1 \implies$ сумма количества орбит.

$\square$

Пример. Подсчет числа структур с точностью до изоморфизма.

Закрепленное ожерелье: $F : \mathbb{Z}/12\mathbb{Z} \to \{B, W\}$. Таких 2^{12}. $F_1 \sim F_2 \Leftarrow F_1(x) = F_2(x + x_0)$ при некотором x_0.

Пусть O — множество закрепленных ожерелий. $\mathbb{Z}/12\mathbb{Z} \curvearrowright O$. Каково число орбит? Оно равно $\frac{|Fix(0)|+|Fix(1)|+\ldots}{12} =$.

$|Fix(0)| = 2^{12}, |Fix(1)| = |Fix(11)| = |Fix(5)| = Fix(7) = 2^1, |Fix(2)| = |Fix(10)| = 2^2, |Fix(3)| = |Fix(9)| = 2^3, |Fix(4)| = 2^4 = |Fix(8)|, |Fix(6)| = 2^6$.

5.8. Применения теории конечных групп действий

$|G| = n$. Верно ли, что в G есть элемент порядка d, $n \,\vdots\, d$? Нет, иначе бы в группе всегда был элемент порядка n, а значит любая группа была бы циклической, что неверно. Но если $d = p$, то ок.

Верно ли, что в G есть подгруппа порядка d? Нет, например, в A_4 нет подгруппы порядка 6. Но если $d = p^k$, то ок.

Теорема 5.15 (Теорема Коши)**.** $|G| \vdots p, p$ — простое $\Rightarrow \exists g \in G \colon \operatorname{ord} g = p$

Доказательство. Рассмотрим $M = \{(g_1, \ldots, g_p) \mid g_i \in G, g_1 g_2 \ldots g_p = e\}$. $|M| = |G|^{p-1} \vdots p$, поскольку мы можем выбрать первые $p-1$ элементов произвольным образом а последним взять обратный к произведению. C_p — циклическая группа порядка p, $C_p \curvearrowright M : t(g_1, g_2, \ldots, g_p) = (g_2, \ldots, g_p, g_1) \in M, \quad t^k(g_1, g_2, \ldots, g_p) = (g_{k+1}, g_{k+2}, \ldots, g_p, g_1, g_2, \ldots, g_k) \in M$.

Пусть $x \in M$. $|C_p \cdot x| = \frac{|C_p|}{|C_{p_x}|} = \left[\begin{array}{l} 1 \\ p \end{array}\right.$ $(|C_p| = p$ — простое). $|M| = \sum$ длина орбиты $= 1 + 1 + \ldots + 1 + p + \ldots + p = a \cdot 1 + b \cdot p \vdots p \Rightarrow a \vdots p$. Длина орбиты равна 1 только у элементов из $\{(g, g, \ldots, g) \mid g^p = e\}, \quad \{g \mid g^p = e\} = \{e\} \cup \{g \mid \operatorname{ord} g = p\}$. Поскольку длина орбиты $(e, e, \ldots, e)$ равна 1, то $a \neq 0 \Rightarrow a \geq p$. Т.е. существует ненулевое делящееся на p количество решений уравнения $x^p = e$, а значит существуют элементы порядка p □

Теорема 5.16 (Первая теорема Силова)**.** Пусть $|G| = p^n \cdot d, d \not\vdots\, p$.

Тогда $\exists H \leqslant G \colon |H| = p^n$.

Доказательство. $M = \{x \subset G \mid |x| = p^n\}$. $G \curvearrowright M$ (сдвигами). $|M| = \binom{p^n d}{p^n} = \frac{(p^n d)!}{(p^n)!(p^n(d-1))!} \not\vdots\, p \implies$ длина хотя бы одной орбиты не делится на $p \implies \exists O \colon |O| \not\vdots\, p$. $O = Gx$, $|O| = \frac{|G|}{|G_x|} = \frac{p^n d}{|G_x|} \not\vdots\, p \implies |G_x| \vdots p^n$, но $|G_x| \leqslant^{(*)} p^n \implies |G_x| = p^n$.

(*) $x = \{a_1, \ldots, a_{p^n}\}$. $g \in G_x \Rightarrow g a_1 = a_i$. Выбор i однозначно определяет $g = a_i a_1^{-1} \implies$ всего $\leqslant p^n$ вариантов. □

ТУТ НАЧИНАЕТСЯ ЧЕТВЁРТЫЙ МОДУЛЬ

Мы помним, что $G \curvearrowright G$ сдвигами, а следовательно $G \mapsto S_n$, $n = |G|$.

А еще мы помним, что можно взять $H \trianglelefteq G$ и из этого можно сделать дерево (разбивая так все группы, не являющиеся простыми) из $H, G \setminus H$. Листьями этого дерева будут простые группы.

Теорема 5.17 (Жордана-Гёльдера)**.** Пусть имеется набор $H_1, \ldots, H_n$ — простые подгруппы (подфакторы) G, тогда он зависит (с точностью до изоморфизма H_i-ых) только от исходной группы G. То есть не имеет значения как мы раскладываем на простые группы.

Доказательство. Дана без доказательства □

***Определение* 5.25.** Разрешимая группа — конечная группа, все простые подфакторы которой — $\mathbb{Z}/p_i\mathbb{Z}$

Это простейший случай, и в таких группах доказательства чаще всего являются индукцией по количеству факторов(покоординатная индукция), а вычисления можно делать в них покоординатно.

Следующие по сложности варианты подфакторов — A_n — чётные перестановки, но ладно.

***Определение* 5.26.** Группа перестановок — подгруппа S_n. $\pi_1, \pi_2, \ldots, \pi_k \in S_n$. $G = \langle \pi_i \rangle$.

Мы хотим:

1. $|G| =?$ (узнать порядок порождённой группы, сколько перестановок получается из исходного набора).

2. membership test: если $\pi \in S_n$, то верно ли, что $\pi \in G$. Если да, то какое разложение по базису? То есть $\pi = \prod {\pi_{i_k}}^{\pm 1}$ (элементы в разложении могут повторяться).

Идея:

1. $G \curvearrowright \{1, 2, \dots, n\}$. Тогда (т.к. мы знаем, что порядок группы есть мощность орбиты элемента на порядок стабилизатора этого элемента, и затем так можно и стабилизатор разбивать далее): $|G| = |G \cdot 1| \cdot |G_1| = |G \cdot 1| \cdot |(G_1) \cdot 2| \cdot |G_{1,2}| \cdot \ldots = \prod |G_{1,2,\dots,k} \cdot (k+1)|$

   $|G \cdot 1|$ можно посчитать, нарисовав графы перестановок всех π_i и посмотреть компоненту связности единицы.

   Но как с $|(G_1) \cdot 2|$ быть? Нужно знать системы образующих для $(G_1), (G_{12}), (G_{123})$ и прочих, но окуда брать эти системы?

Лемма (Лемма Шрайера)**.** Пусть G — конечная группа, $H \leqslant G$, причем $G = \langle g_1, \dots, g_n \rangle$

$G/H = \{x_1 H, x_2 H, \dots, x_k H\}$ смежные классы, а $x_1, x_2, \dots, x_k$ — система представителей смежных классов, при этом $x_1 = e$.

Положим $\overline{g} = x_i$, если $gH = x_i H$, т.е. для каждого элемента g, элемент $\overline{g}$ — представитель класса смежности g.

Тогда $H = \langle (\overline{g_l x_i})^{-1} g_l x_i \rangle_{\substack{i=1..k \\ l=1..n}}$

Доказательство. Нужно доказать, что сами перечисленные элементы лежат в H, и что любой элемент из H представим в указанном виде.

Пусть $a \coloneqq g_l x_i, b \coloneqq \overline{g_l x_i}$. $b^{-1} a \in H$, так как $bH = aH$, окей, значит перечисленные элементы действительно лежат в H.

Осталось доказать, что любой элемент выражается через эти комбинации.

Пусть $h \in H$. $h = g_{i_1} \cdot g_{i_2} \dots g_{i_s}$

Определим $x_{i_s} = x_1 = e$. Сначала запишем ржаку:

$$x_{i_0}^{-1} h = x_{i_0}^{-1} g_{i_1} x_{i_1} \cdots g_{i_{s-2}} x_{i_{s-2}} \cdot x_{i_{s-2}}^{-1} g_{i_{s-1}} x_{i_{s-1}} \cdot x_{i_{s-1}}^{-1} g_{i_s} x_{i_s}$$

Что это? Запишем для каждого $l = 1..s$ $\quad x_{i_{(l-1)}}^{-1} g_{i_l} x_{i_l}$ ($x_{i_0}, \dots, x_{i_{s-1}}$ произвольные). Заметим, что $x_{i_0}^{-1} h = x_{i_0}^{-1} g_{i_1} x_{i_1} \dots x_{i_{(s-1)}}^{-1} g_{i_s} x_{i_s}$ (Это исходное представление h через g_i, поскольку x_{i_l} посередине посокращались, $x_{i_s} = e$ по определению, осталось только $x_{i_0}^{-1}$ слева).

Тогда по очереди для $l = (s-1)..0$ определим $x_{i_l} = \overline{g_{i_{l+1}} x_{i_{l+1}}} \Rightarrow x_{i_{(l-1)}}^{-1} g_{i_l} x_{i_l}$ — элемент нашей системы образующих. $\Rightarrow x_{i_0}^{-1} h =$ произведение наших образующих $\in H$. $h \in H \Rightarrow x_{i_0} \in H \Rightarrow x_{i_0} = e \Rightarrow h =$ произведение наших образующих. Ура, доказали! $\square$

я хочу к маме :(я тоже :(Если разобраться, то всё довольно несложно!

А теперь применим полученную лемму к нашему частному случаю.

Упражнение Частный случай (не упражнение). $G \curvearrowright M$, $m \in M$. $G = \langle g_1, \dots, g_n \rangle$.

$G \cdot m = \{m_1 = m, m_2, \dots, m_k\}$, $\forall i \exists x_i \colon x_i m = m_i$.

$H = G_m$, тогда $G/H = \{x_1 H, x_2 H, \dots, x_k H\}$. Тогда по лемме Шрайера можно найти систему образующих для G_m (стабилизатора).

Построим *сильную базу* для G (последовательно набирая образующие стабилизаторов): $G \cdot 1 = \{i_{11}, i_{12}, \dots, i_{1k_1}\}$, $x_{1l} \cdot 1 = i_{1l}$.

Нашли по Шрайеру образующие для G_1. $G_1 \cdot 2 = \{i_{21}, i_{22}, \ldots, i_{2k_2}\}, x_{2l} \cdot 2 = i_{2l}$ и так далее. $\{x_{ij}\}_{\substack{i=1..n-1 \\ j=1..k_i}}$ — *сильная база* для G.

Теперь ответим на два главных вопроса:

1. $|G| = |G_1| \cdot |G_1 \cdot 2| \cdot |G_{12} \cdot 3| \cdot \ldots = k_1 \cdot k_2 \cdots k_{n-1} \leqslant n! \quad (k_1 \leqslant n, k_2 \leqslant n-1, \ldots)$ (конкретно тут n — число слоёв в нашей сильной базе).

2. membership test: $g \in S_n$

   $g(1) = a_1 = x_{1a_1}(1)($ x_{1a_1} — элемент, который переводит 1 в $a_1), x_{1a_1} \in G$. $x_{1a_1}^{-1} g \in (S_n)_1$.

   $x_{1a_1}^{-1} g(2) = a_2 = x_{2a_2}(2), x_{2a_2} \in G_1, x_{2a_2}^{-1} x_{1a_1}^{-1} g \in (S_n)_{12}$. И так далее...

   В конце, если $x_{n-1a_{n-1}}^{-1} x_{n-2a_{n-2}}^{-1} \ldots x_{1a_1}^{-1} g = id$.

   Тогда $g = x_{1a_1} x_{2a_2} ... x_{(n-1)a_{n-1}}$.

   Если на каком-то шаге k не нашлось такого x_{ka_k}, то membership test провален

   Если же дошли до конца, то получили $x_{n-1a_{n-1}}^{-1} x_{n-2a_{n-2}}^{-1} \cdots x_{1a_1}^{-1} g = 1$, а значит

$$g = x_{1a_1} x_{2a_2} \cdots x_{n-1a_{n-1}}$$

***Определение* 5.27.** Построение сильной базы и то, как мы проверяем membership test есть алгоритм Шрайера—Симса

Замечание. Размер сильной базы — не более чем квадратичен от n $(k_1 + \ldots + k_{n-1} \leqslant n + (n - 1) + \ldots)$.

Вопрос: $G \leqslant S_n$. Вопрос такой: при каких $k\colon \forall G \leqslant S_n \exists$ система образующих размера $\leqslant k$? $k = k(n)$.

Упражнение. $S_n = \langle (12), (123..n) \rangle$

Пример. $n = 2m$. $G = \langle (12), (34), \ldots, (2m-1\ 2m) \rangle \cong (\mathbb{Z}/2\mathbb{Z})^m$.

$|G| = 2^m$, $\forall g \in G \setminus \{e\} \operatorname{ord} g = 2$, $\quad g_1, \ldots, g_k \in G$. $|\langle g_1, \ldots, g_k \rangle| = 2^k \implies \forall$ с.о. (система образующих) имеет $\geqslant m = \frac{n}{2}$ элементов.

Так мы показали, что $k(n) \geqslant \frac{n}{2}$ (если возвращаться к исходному вопросу.) Это, вероятно, и есть доказательство точности оценки.

Теорема 5.18. $G \leqslant S_n \implies G$ имеет систему образующих из $\leqslant \left[\frac{n}{2}\right]$ элементов.

Доказательство. Я запрещаю вам доказывать данную теорему.

Ну т.е. теорема доказывается как-то сложно, как-то с перебором и вообще со ссылкой на теорему о классификации конечных простых групп. Так что дана без доказательства. □

Теорема 5.19. $G \leqslant S_n \implies G = \langle g_1, \ldots, g_k \rangle$, $k < n$.

Доказательство. $G = \langle g_1, \ldots, g_k \rangle$. Построим ориентированный граф Γ. Вершины — числа от 1 до n, а рёбра породим следующим образом:

$g_l \rightsquigarrow$ ребро $i \to j$, если $g_l(i) = j$ и при этом $\forall k < i$ $g_l(k) = k$. Заметим, что все рёбра ведут от меньшего к большему. Т.е. нашли первую по номеру не неподвижную точку, смотрим, куда она переходит и рисуем ребро.

Утверждение: можно выбрать образующие так, что Γ — без циклов (как неориентированный граф) ($\implies$ меньше n ребер).

Докажем это утверждение. Пусть нам последовательно кидают перестановки $h_1, h_2, \ldots \in G$, а мы в online строим систему образующих для них так, чтобы в соответствующем графе не было циклов. Формально говоря, по $h_1, h_2, \dots \in G$ $\forall k$ строим $g_{k,1}, \ldots, g_{k,i_k}$, такой что $\langle g_{k,1}, \ldots, g_{k,i_k} \rangle = \langle h_1, \ldots, h_k \rangle$ и граф Γ — ацикличен. (тут i_k является, по сути, размером системы образующих на шаге k. Почему i? Хороший вопрос.)

Индукция по k. База — очев. Переход $g_{k1}, g_{k2}, \ldots, g_{ki_k} \rightsquigarrow$ ацикличная.

Добавляем h_{k+1} и добавляем ребро в $\Gamma \rightsquigarrow \Gamma'$. $g_{k+1,i} = g_{k,i}, g_{k+1,i_k+1} = h_{k+1}$ (прим. редакции: дальше вместо k должно быть $k+1$, но нам пофиг)

1. Γ' — ацикличный $\implies$ ок.

2. Пусть получился цикл (неориентированный) на вершинах $S_1, \ldots, S_m$, $\quad S_{i+1} = g_{k,r_i}^{\pm 1}(S_i)$ (± 1 зависит от ориентации ребра), не умаляя общности положим $S_1 = \min S_i \implies S_2 = g_{k,r_1}(S_1)$ (т.к $S_1 < S_2$).

   Заменим g_{k,r_1} на $g_{k,r_m}^{\pm 1} \ldots g_{k,r_2}^{\pm 1} g_{k,r_1} = \widetilde{g}_{k,r_1}$. При этой замене порождённая группа не изменилась (т.к. g_{k,r_1} и $\widetilde{g}_{k,r_1}$ выражаются друг через друга и остальные g_{k,r_i}). Тогда $\widetilde{g}_{k,r_1}(S_1) = S_1$ по построению и $\widetilde{g}_{k,r_1}(x) = x \quad \forall x < S_1$ в силу выбора S_1. Избавились от цикла. Если появился новый (а мог появиться только один) — починим его и т.д.

   Процесс остановится, так как выполняется полуинвариант: в результате замен растёт сумма номеров минимальных подвижных точек, т.к. при замене у нас у $\widetilde{g}_{k,r1}$ номер наименьшей неподвижной точки увеличился как минимум на один.

Всё, доказательство закончилось! Мы успешно разбили циклы и получили граф без циклов! А значит мы умеем выбирать образующие так, что Γ не содержит циклов! $\square$

Я потерялся очень сильно я не знаю как жить дальше.

Больше не теряйся <3

В целом, разобраться можно, но обозначения ржачные...

5.9. Центр и коммутант

***Определение* 5.28.** G — группа, центр G $Z(G) = \{a \mid ag = ga \ \forall g \in G\}$.

***Определение* 5.29.** $a, b \in G$ коммутатор a и b — $[a, b] = a^{-1}b^{-1}ab = (ba)^{-1}ab = \frac{ab}{ba}$ (своего рода). Т.е. «насколько отличаются произведения в разном порядке»

***Определение* 5.30.** Пусть $H_1, H_2 \leqslant G$. Тогда коммутант $[H_1, H_2] = \langle [h_1, h_2] \mid h_1 \in H_1, h_2 \in H_2 \rangle$. Важно! Это подгруппа, порождённая всеми попарными коммутаторами, а не просто множество из них. Бывают случаи, когда все попарные коммутаторы не совпадают с порождённой группой.

***Определение* 5.31.** Коммутант G — $[G, G]$.

Теорема 5.20 (Свойства центра и коммутанта)**.** Набор всяких тривиальных и не очень свойств

0_1. G — абелева $\iff Z(G) = G$.

0_2. G — абелева $\iff [G, G] = \{e\}$.

1_1. $Z(g) \trianglelefteq G$.

1_2. $[G, G] \trianglelefteq G$.

2_1. $Z(G)$ — абелева группа.

2_2. $G/[G,G]$ — абелева.

3. $H \trianglelefteq G$, G/H — абелева $\implies$ $H \geqslant [G,G]$ (универсальное свойство коммутанта). (Расшифровка: если H нормальная подгруппа в G, и G фактор по H — абелева, то H содержит коммутант G в качестве подгруппы)

Альтернативный способ записать третье свойство: пусть A — абелева группа, тогда любой гомоморфизм $f : G \to A$ пропускается через $G/[G,G]$. Это несколько похооже на другие универсальные свойства, которые у нас были.

Доказательство. Первые два свойства очевидны. Далее:

1_1. Нам нужно проверить замкнутость относительно умножения, наличие единицы и наличие обратного. $e \in Z(G)$ очевидно. $a, b \in Z(G), \forall c \in G \quad ac = ca, bc = cb \implies (ab)c = a(bc) = a(cb) = (ac)b = (ca)b = c(ab) \implies ab \in Z(G)$.

$a \in Z(G)$, хотим проверить, что $a^{-1} \in Z(G). a^{-1}b = (b^{-1}a)^{-1} = (ab^{-1})^{-1} = ba^{-1} \implies a^{-1} \in Z(G)$. Проверили, что $Z(G)$ — подгруппа. Нормальность проверяется легко через сопряжения: $g^{-1}hg = g^{-1}gh = h$.

1_2. $[G,G] \leqslant G$ — по определению, остаётся проверить нормальность.

Пусть $x \in [G,G]$, разберём случаи:

(a) x — отдельный коммутант, т.е. $x = [a,b] = a^{-1}b^{-1}ab$. Рассмотрим $g^{-1}xg = g^{-1}a^{-1}b^{-1}abg = g^{-1}a^{-1}gg^{-1}b^{-1}gg^{-1}agg^{-1}bg$ (просто вставили gg^{-1} и $g^{-1}g$ несколько раз) $= (g^{-1}ag)^{-1}(g^{-1}bg)^{-1}(g^{-1}ag)^{1}(g^{-1}bg)^{1} = [a', b']$, где $a' = g^{-1}ag, b' = g^{-1}bg$. Т.е. сопряжённый к коммутанту — тоже коммутант.

Заметка: обратный к коммутанту — коммутант: $[a,b]^{-1} = (a^{-1}b^{-1}ab)^{-1} = b^{-1}a^{-1}ba = [b,a] \implies \forall$ элемент $[G,G]$ — произведение коммутаторов, на обратные можем забивать.

(b) $x \in [G,G]$, тогда $x = [a_1,b_1][a_2,b_2]\ldots[a_n,b_n]$, $g^{-1}xg = g^{-1}[a_1,b_1]gg^{-1}[a_2,b_2]g\ldots g^{-1}[a_n,b_n]g =$ (по той же схеме, что в первом пункте) $= [a_1', b_1'][a_2', b_2']\ldots[a_n', b_n'] \in [G,G]$.

Ура, сопряжённый к любому из $[G,G]$ лежит в $[G,G]$, а значит мы нормальны.

2_1. Очев по определению центра. Элементы центра это те, которые «абелевы со всеми», а значит и с другими элементами центра.

2_2. Возьмём из $G/[G,G]$ два класса — $\overline{a}$ и $\overline{b}$. Заметим, что $\overline{a} \cdot \overline{b} = \overline{ab} \quad \underbrace{\overline{b^{-1}a^{-1}}\overline{ba}}_{\in[G,G] \implies \overline{b^{-1}a^{-1}ba} = e} = \overline{ba}$

(схлопнули bb^{-1} и aa^{-1}).

3. G/H — абелева $\forall a, b \in G \quad \overline{a_H}\overline{b_H} = \overline{b_H}\overline{a_H}$. $\overline{a_H}^{-1}\overline{b_H}^{-1}\overline{a_H}\overline{b_H} = \overline{e_H} \implies \overline{a^{-1}b^{-1}ab} = \overline{e_H} \implies a^{-1}b^{-1}ab \in H$, т.е. $[a,b] \in H \implies [G,G] \leqslant H$.

3 Alt Несложное упражнение на языке стрелочек.

$\square$

Тут нужна картинка, но я краб

А я — рак

Теорема 5.21. A — конечно абелевая $\implies A \cong \mathbb{Z}/p_1^{\alpha_1} \times \mathbb{Z}/p_2^{\alpha_2} \times \ldots \times \mathbb{Z}/p_k^{\alpha_k}$.

Доказательство. Нет. □

Пример. S_n, $n \geqslant 5$. $[S_n, S_n] = A_n$, $S_n/A_n = C_2$, $[A_n, A_n] = A_n$ — совершенная группа.

$Z(S_n) = \{e\} = Z(A_n) = \{e\}$.

$n = 4$. $[S_4, S_4] = A_4$. $[A_4, A_4] = D_4 = \langle(12), (34), (13), (24)\rangle$. $[D_4, D_4] = \{e\}$.

Пример. G — конечная $\to G_1 = G/Z(G) \to G_2 = G_1/Z(G_1) \to \ldots G_k = G_{k-1}/Z(G_{k-1})$.

Либо. $G \to G_1 = [G, G] \to G_2 = [G, G_1] \to G_i = [G, G_{i-1}]$.

Либо $G_{k+1} = [G_k, G_k]$.

Утверждение 5.22. 1. Первая цепочка приходит к $\{e\} \iff$ вторая цепочка приходит к $\{e\}$.

2. Вторая цепочка приходит к $\{e\} \implies$ третья цепочка приходит к $\{e\}$.

Если существует k, такое $G_k = \{e\}$(первый и второй случаи), то G называется нильпотентной группой. Если существует k, такое $G_k = \{e\}$(третий случай), то G называется разрешимой группой.

Пример. S_4 — разрешима, но не нильпотентна.

Пример. Рассмотрим нижнетреугольные матрицы $\leqslant GL_n(K)$ — нильпотентная подгруппа.

$Z(GL_n(K)) = \{k \cdot E\}$ — скалярные матрицы (то есть единичная + диагональные). $GL_n/Z(GL_n) = PGL_n$, $Z(PGL_n) = \{e\}$.

$[GL_n, GL_n] = SL_n(K), [SL_n, SL_n] = SL_n(K)$.

Теорема 5.23. G — конечна. Тогда

Следующие условия равносильны:

1. G — разрешима (то есть разлагается на простые абелевы группы).
2. Все простые подфакторы G — это $\mathbb{Z}/p_i\mathbb{Z}$.

Доказательство. $1 \implies 2$. G раскладывается на $G/[G, G]$ (абелева) и $G_1 = [G, G]$, далее G_1 раскладывается на $G_1/[G_1, G_1]$ и $G_2 = [G_1, G_1]$, и так далее... В свою очередь все $G_i/[G_i, G_i]$ раскладываются на подфакторы — $\mathbb{Z}/p_j\mathbb{Z}$.

$2 \implies 1$. Пусть G неразрешима. Тогда $\exists i : [G_i, G_i] = G_i \neq \{e\}$. Все подфакторы G абелевы $\iff$ все подфакторы G_i абелевы. $G_i = H$.

Разложим H на $H_1 = [H, H]$ и $H_2 = H/[H, H]$. H_2 разложим ещё на H_3 и H_2/H_3, и так далее... Спускаемся по дереву, в ветке с H_2: если $[H, H] = H$, то $[H/U, H/U] = H/U$, то есть всегда будет $U : [U, U] = U \implies$ никогда не будет абелевой группы. □

Теорема 5.24. G — конечная, тогда $|G| = p^n \implies G$ — нильпотентна.

Доказательство. $G \to G/Z(G) = G/Z(G) = G_1 \rightsquigarrow G_1/Z(G_1) = G_2 \rightsquigarrow \ldots$, $G_i = p^{\alpha_i} \quad \forall i$. Достаточно доказать: $G_i \neq \{e\} G_{i+1} \neq G_i$, то есть $Z(G_i) \neq \{e\}$.

То есть Th $\Leftarrow$ лемма. □

Лемма. $|G| = p^n$, p — простое $\implies Z(G) \neq \{e\}$.

Доказательство. Пусть $G \curvearrowright G$ сопряжениями. $g \cdot m = gmg^{-1}$. O_i — орбита, $O_1 = G \cdot e = \{e\}$. $|O_1| + |O_2| + \ldots = p^n \implies \exists i \neq 1 : |O_i| = 1$, так как любая орбита имеет порядок либо 1, либо степень p. Тут важно пояснить, что если $gxg^{-1} = x$, то $gx = xg$, а если орбита $= 1$, то это выполняется для всех $g \implies x \in Z(G)$.

Теперь пусть $|G| = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. По первой теореме Силова $\exists |G_1| = p_1^{\alpha_1}, |G_2| = p_2^{\alpha_2}, \ldots$. □

Теорема 5.25. $|G| = p^2 \implies G$ — абелева.

Доказательство. $|G| = p^2$, $\exists g \colon \operatorname{ord} g = p^2 \implies G$ — циклическая $\cong \mathbb{Z}/p^2\mathbb{Z} \ldots$

Иначе $\forall g \neq e \operatorname{ord} g = p$. Тогда либо $Z(G) = G$ (тогда G — абелева), либо $|Z(G)| = p$ (такого быть не может). Тогда $Z(G) = \langle a \rangle, \operatorname{ord} a = p, b \notin Z(G), \operatorname{ord} b = p$. $\langle a, b \rangle = p^2 \implies \langle a, b \rangle = G \implies G$ — абелева. □

Замечание. G — абелева $\implies G \cong \mathbb{Z}/p^2\mathbb{Z}$ или $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Пример. $|G| = p^3$. Пусть $H \trianglelefteq G$. $H = \langle x, y \mid x^p = y^p = e, xy = yx \rangle \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

$\exists z \in G \setminus H, \operatorname{ord} z = p$, $\langle x, y, z \rangle = G = \{x^k y^l z^m\}$.

$H \trianglelefteq G \implies g^{-1} x^k y^l g = x^{k'} y^{l'}$.

Тогда $z^{-1} h z = f(h) \in H$, знание f однозначно задает G. $z^{-1} h z = f(h), hz = zf(h)$.

Наблюдение: $H \trianglelefteq G, g \in G$. $f_g(h) = g^{-1} h g$ — автоморфизм H. $(f_g(h))^{-1} = f_{g^{-1}}(h)$.

***Определение* 5.32.** $Aut(G)$ — группа автоморфизмов H (относительно композиции).

Утверждение 5.26. G — группа. $G_1, G_2 \leqslant G$. $f \colon G_1 \times G_2 \to G$ и $(g_1, g_2) \to g_1 g_2$.

f — изоморфно (тогда $\implies G \cong G_1 \times G_2$) $\iff$

1. $G_1 + G_2 = G$.
2. $G_1 \cap G_2 = \{e\}$.
3. $g_1 g_2 = g_2 g_1 \quad \forall g_1 \in G_1, g_2 \in G_2$.

Упражнение. Пусть знаем $1, 2$ — выполнены, тогда $3 \iff G_1 \trianglelefteq G, G_2 \trianglelefteq G$.

***Определение* 5.33.** Если все то же, что и выше, но только одна из G_1, G_2 нормальна, то G называется внутренним полупрямым произведением G_1 и G_2.

$g = g_1 g_2$ и G — нормальная, $(g_1 g_2) \cdot (g_1' g_2') = g_1 g_1' (g_1')^{-1} g_2 g_1' g_2' = (g_1 g_1')((g_1')^{-1} g_2 g_1') g_2' = \underbrace{(g_1 g_1')}_{\in G_1} \underbrace{(f_{g_1'}(g_2) g_2')}_{\in G_2}$.

Полупрямое произведение задаётся G_1, G_2 и гомоморфизмом $G_1 \to Aut(G_2)$.

6. Пространства с операторами

***Определение* 6.1.** Линейный оператор — линейное отображение (линейный эндоморфизм) $\mathcal{A}\colon V \to V$.

Кольцо операторов — $End(V)$ $\quad(+,\cdot)$ с единицей, алгебра над V.

***Определение* 6.2.** Алгебра над K — кольцо $(A,+,\cdot)$ являющееся векторным пространством над K.

Причем $\forall a, b \in A, k \in K : k(ab) = a(kb) = (ka)b$.

Замечание. A — алгебра с 1 $\implies$ задан гомоморфизм колец $i\colon K \to A$ $(k \rightsquigarrow k \cdot 1)$.

Обратно: задан $i\colon K \to A$ $\operatorname{Im} i \subset Z(a) \implies A$ превращается в алгебру над K.

Пример. $K[x]$ — алгебра над K.

Пример. $K \subset F$ — поля. F — алгебра над K. $\mathbb{C}$ — алгебра над $\mathbb{R}$.

Пример. $A = End(V) \cong M_n(K), n = \dim V$.

Замечание Напоминание. $\mathcal{A}\colon V \to V$, $e_1, \ldots, e_n$ — базис.

$\mathcal{A}(e_i) = \sum a_{ij} e_j \implies (a_{ji})$ — матрица $\mathcal{A}$ в базисе $\{e_i\}$. $A = [\mathcal{A}]$.

Вопросы:

1. Классификация эндоморфизмов. $B = C^{-1}AC \iff B, A$ — матрица одного оператора в разных базисах. Классификация — определение классов сопряжения в $M_n(K)$.
2. Распознавание типов отображений. $\mathcal{A}$ — оператор $\rightsquigarrow$ находим базис, $e_1, \ldots, e_n$ — базис, A — очень простая.

   $\mathcal{A} \in End(V)$, $K[t]$. $A \in M_n(K)$. Тогда $\exists!$ гомоморфизм $P = \sum a_i t^i \to \sum a_i A^i$, $t_A : K[t] \to M_n(K), t \mapsto A$.

   Если зафиксировать $\mathcal{A} \in End(V) \rightsquigarrow V, K[t]$.

   То есть теперь мы можем сделать $t \cdot V \coloneqq A(V)$. В итоге, $(V, \mathcal{A}) \sim K[t]$ — модуль + ОГИ.

Пример. V_1, V_2 — векторные пространства над K.

$\mathcal{A}_1 \oplus \mathcal{A}_2 \colon V_1 \oplus V_2 \to V_1 \oplus V_2, \mathcal{A}(v_1, v_2) = (\mathcal{A}_1(v_1), \mathcal{A}_2(v_2))$, e_i — базис $V_1 \rightsquigarrow A_1$, l_i — базис $V_2 \rightsquigarrow A_2$.

$\mathcal{A}_i \in End(V_i)$, тогда $(\mathcal{A}_1 \oplus \mathcal{A}_2)_{\{e_i\} \cup \{l_i\}} = \left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right)$.

***Определение* 6.3.** $\mathcal{A} \in End(V)$. $U \leqslant V$ — называется инвариантивным ($\mathcal{A}$-инвариантивным), если $\mathcal{A}(U) \subset U$.

Пусть $V \cong V_1 \oplus V_2$, V_1, V_2 — инвариативные подпространства. Тогда $[A]$ имеет вид $\left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right)$ в базисе объединения базисов V_1 и V_2.

Утверждение 6.1. $\mathcal{A} \in End(V), U \leqslant V$ — инвариантно.

Тогда, в базисе U $(u_1, u_2, \ldots, u_k)$ + как-то дополненном до V $[\mathcal{A}]$ имеет вид $\left(\begin{array}{c|c} A_1 & B \\ \hline 0 & A_2 \end{array}\right)$, где $A_1 = [\mathcal{A}\big|_u]_{u_1, u_2, \ldots, u_k}$.

Что такое A_2? $\mathcal{A}(u_{k+1}) = \underbrace{\sum_{i=1}^{k} b_i u_i}_{\in U} + \underbrace{\sum_{i=k+1}^{n} a_i u_i}_{u_0} \equiv \sum_{k=1}^{n} a_i u_i \pmod U$.

Множество классов — пространство V/U (потому что можно говорить, что $v_1 \equiv v_2 \pmod U$, если $v_1 - v_2 \leqslant U$).

$A_2 = [\mathcal{A}\Big|_{V/U}]_{u_{k+1},\ldots,u_n}$ — на базисе дополнения U до базиса V.

Пример. Картинка.

Теперь $\mathcal{A} : V \to V$, U — инвариативно относительно $\mathcal{A} \implies$ корректна задана $\mathcal{A}\Big|_{V/U} = End(V/U)$.

$\mathcal{A}(\overline{v}) := \overline{\mathcal{A}(v)}$. Это легко проверяется по определению: $\overline{v} = \overline{v'} \iff v - v' \in U \implies \mathcal{A}(v - v') \in U \iff \mathcal{A}(v) - \mathcal{A}(v') \in U \implies \overline{\mathcal{A}(v)} = \overline{\mathcal{A}(v')}$ в V/U.

U — инвариантное подпространство, $\dim U = 1, U = \langle u\rangle, Au \subset \langle u\rangle$, то есть $\mathcal{A}u = \lambda u$.

***Определение* 6.4.** Собственный вектор оператора $\mathcal{A}$ называется $v \in V \setminus \{0\} \colon \mathcal{A}(v) = \lambda v$.

А λ называется собственным числом оператора $\mathcal{A}$.

v — собственный вектор $\implies \langle v\rangle$ — инвариативное подпространство — неподвижная прямая.

V — конечномерное пространство. $\mathcal{A} \in End(V)$. A — его матрица, $\lambda \in K$.

Тогда λ — собственное число $\mathcal{A} \iff \exists V \neq 0 \colon \mathcal{A}(v) = \lambda V \iff \mathcal{A}(v) - \lambda V = \iff \mathcal{A}(v) - \lambda Id(v) = 0 \iff (\mathcal{A} - \lambda \cdot Id)(v) = 0 \iff \ker(\mathcal{A} - A \cdot id) \neq 0 \iff \ker(A - \lambda E) \neq 0 \iff \det(A - \lambda E) = 0$.

Рассмотрим $\det(A - tE) = \det \begin{pmatrix} a_{11}t & \ldots & a_{ij} \\ & \ddots & \\ a_{ij} & & a_{nn}t \end{pmatrix} \in K[t]$.

Теорема 6.2. λ — собственное число $\mathcal{A} \iff \lambda$ — корень многочлена $\chi_A(t) = \det(A - tE)$.

***Определение* 6.5.** $\chi_A(t)$ — характеристический многочлен оператора A (и матрицы).

Утверждение 6.3. $\chi_A(t)$ не зависит от базиса A.

Доказательство. A, A' — матрицы $\mathcal{A}$ в разных базисах. $A' = C^{-1}AC \implies \chi_A(t) = \det(C^{-1}AC - tE) = \det(C^{-1}AC - C^{-1}tEC) = \det(C^{-1}(A - tE)\cdot C) = \det(C^{-1})\cdot\det(A - tE)\cdot\det(C) = \det(A - tE) = \chi_A(t)$. □

Следствие из Th. $\mathcal{A} \in End(V)$, $\dim V = n \implies \mathcal{A}$ имеет $\leqslant n$ собственных чисел.

Лемма. Собственные вектора, соответствующие различным собственным числам ЛНЗ.

Доказательство. $v_1, v_2, \ldots, v_k$ $\mathcal{A}(v_i) = \lambda_i v_i$. $\lambda_i \neq \lambda_j$ при $i \neq j$. Хотим показать ЛНЗ.

Индукция по k. База: $k = 0$ — верно.

Переход от k к $k + 1$.

$v_1, \ldots, v_{k+1}$ — собственные вектора $\lambda_1, \ldots, \lambda_{k+1}$ — собственные числа. Пусть $v_1, \ldots, v_{k+1}$ — ЛЗ. То есть есть набор a_i: $\sum a_i v_i = 0$. Применим $\mathcal{A} \implies \sum a_i \lambda_i v_i = 0$, с другой стороны умножим комбинацию на λ_{k+1} и вычтем одно из другого.

Получим $\sum\limits_{i=1}^{k} a_i \underbrace{(\lambda_i - \lambda_{i+1})}_{\neq 0} v_i = 0 \implies a_1, \ldots, a_k = 0 \implies a_{k+1} = 0.$ □

Следствие. $\mathcal{A} \in End(V)$, $n = \dim V$. Пусть $\chi_A(t) = (-1)^n \prod (t - a_i), a_i \neq a_j$.

Тогда существует базис V, состоящих из собственных векторов $\mathcal{A}$.

В этом базиса матрица A — диагональная.

Доказательство. По предыдущей теореме $\forall a_i \exists$ собственный вектор $v_i \colon \mathcal{A}(v_i) = A_i v_i$. По лемме $v_1, v_2, \ldots, v_n$ — базис.

$$\mathcal{A}(v_i) = 0 \cdot v_1 + 0 \cdot v_2 + \ldots + \lambda_i \cdot v_i + \ldots + 0 \cdot v_n \implies i\text{-ый столбец выглядит как } \begin{pmatrix} 0 \\ \ldots \\ \lambda_i \\ \ldots \\ 0 \end{pmatrix} \implies$$

получили диагональную матрицу с $A_{ii} = \lambda_i$. □

***Определение* 6.6.** Такие операторы называются диагонализируемыми.

Как работать в общем случае? Идея: придумать $f \in K[x] \colon f(\mathcal{A}) = 0$.

***Определение* 6.7.** $Tr(A) = \sum\limits_{i=1}^{n} a_{ii}$. $A = (a_{ij})$. $Tr(A) = \pm$(коэффициент при t^{n-1} у $\chi_A(t)$) $\implies$ $Tr(A)$ не зависит от выбора базиса.

Теорема 6.4 (Кэли-Гамильтона)**.** Пусть $\mathcal{A} \in End(V)$. Тогда $\chi_A(\mathcal{A}) = 0$.

То есть $\mathcal{A}^n + a_{n-1}\mathcal{A}^{n-1} + \ldots + a_1 \mathcal{A} + a_0 Id = 0$.

Пример. Матрица 2x2. $A^2 = Tr(A) \cdot A - \det A$.

Доказательство. Пусть у нас есть поле $K \rightsquigarrow \overline{K}$ — алгебраическое замыкание. То есть любой многочлен представим как произведение $(x - a_i)$, где a_i — корень многочлена.

Тогда $\xi_A(x) = \prod (x - a_i), a_i \in \overline{K}$. Тогда $a_1, a_2, \ldots, a_n$ — собственные числа.

Индукция по $n = \dim V$. При $n = 1$ это база: матрица $\big(a\big) = aE, x_0 = t - a \rightsquigarrow A - aE = 0$ — верно.

Переход от $n - 1$ к n. a_1 — собственное число $\mathcal{A} \implies \exists x : \mathcal{A}x = a_1 x$, $\langle x \rangle$ — инвариантное пространство. Тогда матрица в базисе $x_1 \equiv x, x_2, \ldots$. Получим матрицу вида $\left(\begin{array}{c|c} a_1 & * \\ \hline 0 & \widetilde{A} \end{array}\right)$. Тогда $\widetilde{A}$ — матрица $A\Big|_{v/\langle x \rangle}$.

Тогда $\xi_{\mathcal{A}} = (a_1 - t) \cdot \xi_{\widetilde{A}}(t)$. Значит $\implies \xi_{\overline{A}}(t) = \prod\limits_{i=2}^{n} (t - a_i) \implies (\prod_{i=2}^{n} (t - a_i))(\widetilde{A}) = 0$.

А значит, $(\prod\limits_{i=2}^{n} (t - a_i)) A(v) = kx$. А значит, $(A - a_1 Id)(kx) = k(\mathcal{A}x - a_1 x) = 0$. □

Возьмем характеристический многочлен матрицы $\xi(t) = \prod_{i=1}^{k} p_1^{a_1}(t)$, p_i — неразложимые.

Тогда пусть $v_i = \{v \in V \mid p_i^{a_i}(\mathcal{A})(v) = 0\}$ — аннуляторное пространство. Пусть $p_i^{a_i} = t - a$. Тогда $v_i = \{v \mid \mathcal{A}(v) = a \cdot v\}$ — собственное подпространство соответствующее a.

Замечание. Это подпространство. (очев)

Теорема 6.5. $V = V_1 \oplus V_2 \oplus \ldots \oplus V_k$.

Доказательство. $(*)$. Пусть $A \in End(U)$, тогда $\forall P : P(\mathcal{A}) = 0 \wedge P = P_1 \cdot P_2, (P_1, P_2) = 1 \implies A = \ker(P_1(\mathcal{A})) \oplus \ker(P_2(\mathcal{A}))$. $\xi(\mathcal{A}) = 0$, $\xi(t_1) = p_1^{a_1} \cdot (p_2^{a_2} \cdot \ldots \cdot p_n^{a_n})$.

Тогда $V = \underbrace{\ker p_1^{a_1}}_{V_1} \oplus \underbrace{\ker(p_2^{a_2} \cdot \ldots \cdot p_n^{a_n})}_{V_1'}$.

Тогда $\mathcal{A}\Big|_{V_i'} = \mathcal{A}'$, V_i — инвариантные пространства. Осталось $p_2^{a_2}(p_3^{a_3} \cdot \ldots p_n^{a_n})$. Теперь раскладываем его, ну и поехали дальше.

Теперь докажем утверждение со звездочкой.

$(P_1, P_2) = 1 \implies \exists f, g \in K[x] \colon P_1 \cdot f + P_2 \cdot g = 1$. Тогда $P_1(\mathcal{A})f(\mathcal{A}) + P_2(\mathcal{A}) \cdot g(\mathcal{A}) = id$. А значит для любого $u \in U \colon (P_1(\mathcal{A})f(\mathcal{A}))(u) + (P_1(\mathcal{A}) \cdot g(\mathcal{A}))(u) = u$. Обозначим первое слагаемое за u_2, а второе за u_1. Тогда $P_2(\mathcal{A})u_2 = P_2(\mathcal{A}) \cdot P_1(\mathcal{A})f(\mathcal{A})u_2 = P(\mathcal{A})(f\mathcal{A}(u_2)) = 0 \implies u_2 \in \ker P_2(\mathcal{A})$.

Значит $u = u_1 + u_2$, лежащие в $\ker(P_1(\mathcal{A}))$ и $\ker(P_2(\mathcal{A}))$.

При этом $\ker(P_1(\mathcal{A})) \cap \ker(P_2(\mathcal{A})) = \{0\}$, т.к если $u_1 = u_2 = 0$, то $u = 0$. $\square$

Перейдем теперь в $\mathbb{C}$. $p_i = (t - a_i)$. $v_i = \ker(\mathcal{A} - a_i E)^{b_i}$ — корневые подпространства. $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$, V_i — инвариантные подпространства. $p(\mathcal{A})(v) = 0$. $V \to \mathcal{A}v$. $p(\mathcal{A}) \cdot = (\mathcal{A} \cdot p(\mathcal{A})v = \mathcal{A}(P(A(V))) = 0)$.

Продолжим изучать операторы $\mathcal{A}$: $(\mathcal{A} - aId)^k = 0$. Пусть $\mathcal{B} = \mathcal{A} - aId \implies \mathcal{B}^b = 0$.

$\mathcal{B} \rightsquigarrow B$ — очень простая матрица в хорошем базисе.

6.1. Жорданов базис нильпотенотного оператора

***Определение* 6.8.** $\mathcal{A} \in End(V)$ — нильпотентный, если $\exists k \colon \mathcal{A}^k = 0$.

Замечание. $\mathcal{A}$ — диагонализуемая нильпотентная $\implies \mathcal{A} = 0$.

Пример Жордановка цепочка. $V = \langle v_1, v_2, \ldots, v_n \rangle$. $\mathcal{A} \in End(v) \colon \mathcal{A}(v_i) = v_{i+1}, \mathcal{A}(v_n) = 0$.

То есть $v_1 \overset{\mathcal{A}}{\Longrightarrow} v_1 \overset{\mathcal{A}}{\Longrightarrow} \ldots \overset{\mathcal{A}}{\Longrightarrow} v_n \overset{\mathcal{A}}{\Longrightarrow} 0$. Например, $V = K[x]_n$, $\mathcal{A}(f) = f'$.

Теорема 6.6. У любого нильпонетного оператора есть базис из жордановых цепочек (непересекающийся)

Замечание. Для любой жордановой цепочки $\mathcal{A}$ в таком базисе будет как все нули + единицы на диагонали снизу от главной.

Для нильпотентного — набор таких блоков.

Доказательство. Любой нельпотентный оператор можно представить как какую-то диаграмму Юнга.

Пусть $\mathcal{B}$ — нильпотентна, k — минимальное, такое что $B^k = 0$.

Пусть $S_0 = \ker B$. Построим $S_0 \supset S_1 \supset S_2 \supset \ldots \supset S_{k-1}$, $S_i = (\ker B) \cap (\operatorname{Im} B^i)$. $S_k = (\ker B) \cap \operatorname{Im} B^k = 0$.

Если мы доказали существование, то покажем, что $\sum \dim(s_i) = \dim V$.

Причем скажем, что $s_i = \ker(B\Big|_{\operatorname{Im} B^i}) \implies \dim s_i = \dim(\operatorname{Im} B^i) - \dim(\operatorname{Im}(B\Big|_{\operatorname{Im} B^i})) = \dim(\operatorname{Im}(B^i)) - \dim(\operatorname{Im}(B^{i+1}))$. Сложим $\dim s_i$. Получим $\dim \operatorname{Im} B^0 - \dim \operatorname{Im} B^k = \dim V$.

[Здесь далее $v_{i,j}^k$ обозначает элемент, находящий в i-ой жордановой цепочке длины k, причем он j-я степень прообраза]. Выведем базис $s_{k-1} \colon v_{1,1}^{k-1}, v_{2,1}^{k-1}, \ldots, v_{s_{k-1}}^{k-1} \in \operatorname{Im}(B^{k-1}) \implies \exists v_{1,k-1}^{k-1}, v_{2,k-1}^{k-1} \colon B^{k-1}(v_{i,k-1}^{k-1}) = v_{i,1}^{k-1}$.

Тогда $v_{i,j}^{k-1} = B^{k-1-j}(V_{i,k-1}^{k-1})$ — построили a_{k-1} жордановых цепочек длины $k-1$.

Дополним до базиса $s_{k-2}\colon v_{1,1}^{k-2}, \dots, v_{a_{k-2},1}^{k-2} \in S_{k-2}$ и аналогично.

Построили $\{v_{i,j}^{k-2}\}_{\substack{i=1..k-2\\ j=1..k-2}}$.

Сколько мы построили векторов? $(\dim s_{k-1})k + (\dim s_{k-2} - \dim s_{k-1})(k-1) + \ldots + \dim s_0 - \dim s_1 = \dim s_{k-1} + \dim s_{k-2} + \ldots \overset{(*)}{=} \dim V$. $(*)$ — по лемме.

Осталось доказать: $\{v_{i,j}^k\}$ — ЛНЗ $\implies$ $\{v_{i,j}^k\}$ — базис.

Пусть $\sum_{\substack{l=0..k-1\\ j=1..l+1\\ i=1..a_l}} a_{i,j}^l v_{i,j}^l = 0$. Пусть $L = \max\{j \mid \exists i, l\colon a_{ij}^l \neq 0\}$. Применим B^{l-1}: $\sum a_{i,L}^l v_{i,1}^l = 0$, а это базис ядра $\mathcal{B} \implies a_{i,L}^l = 0$. Противоречие. □

Хотим теперь возвести матрицу в степень, то есть $A \rightsquigarrow A^N$. Давайте посмотрим на $f(n) = \max(a_{ij}^n)$. Для довольно случайно матрицы эта функция будет расти довольно экспоненциально $f(n) \sim a^n$. Но a тоже имеет значение.

Будем считать, что $A \in M_n(\mathbb{C})$. Тогда $\exists C\colon C^{-1}AC = I$ — блочная жорданова матричка. Тогда заметим, что $A^n = (CIC^{-1})(CIC^{-1})\ldots = CI^nC^{-1}$. Теперь научимся считать возводить в степень жорданову матрицу.

Для этого заметим, что нам достаточно умножать только жордановы блоки. $(J_\alpha(\lambda))^n = (\lambda E_\alpha + J_\alpha(0))^n = \sum\limits_{k=0}^{n} \binom{n}{k} \lambda^{n-k} J_\alpha(0)^k$. Тогда если посмотреть на блок, то заметим, что блок из единиц двигается. Ну тогда все понятно.
Для тех, кому не понятно:
Матрица $J_\alpha(0))^n$ будет на $(k+1)$-й диагонали иметь единицы, всё остальное нули.
А у матрицы $J_\alpha(\lambda))^n$ на главной диагонали λ^n, на следующей $\binom{n}{1}\lambda^{n-1}$ и так далее.

Тогда заметим, что $f(n) \sim \mathcal{O}^*(\lambda^n)$ для блока, а для всей матрицы надо взять максимум по λ.

Когда $\{A^n\}$ ограничена ограничена? Когда $|\lambda| \geqslant 1$ и все блоки с $\lambda = 1$ размера 1.

Когда $A^n \to 0$? Когда $|\lambda| \leqslant 1$.

6.2. Когда мы в $\mathbb{C}$

Рассмотрим несколько случаев:

1. $K = \mathbb{R}$. Перейдем в $\mathbb{C}$. Пусть $v_1, v_2 \ldots, v_n$ — базис из собственных векторов, $\lambda_1, \ldots, \lambda_n$ — собственные числа.

   $x \mapsto Ax$. $v_i \in \mathbb{C}^n$. Наблюденме: $Av_i = \lambda_i v_i$, $\lambda_i \notin \mathbb{R}$. Сопряжение: $A \cdot \overline{v_i} = \overline{\lambda_i} \cdot \overline{v_i}$.

   Тогда заметим, что $v_i, \overline{v_i} \to \left(v_i + \overline{v_i}, \frac{v_i - \overline{v_i}}{2}\right)$, где числа из пары $\in \mathbb{R}$.

   Тогда заметим, что $A(v_i + \overline{v_i}) = Av_i + A\overline{v_i} = \lambda v_i + \overline{\lambda}\overline{v_i}$, тоже самое для $\frac{v_i - \overline{v_i}}{2}$, $\langle v_i + \overline{v_i}, v_i - \overline{v_i}\rangle$ — инвариантное подпространство.

   Тогда $A \in M_n(K)$ диагонализуема как матрица над $\mathbb{C} \implies \exists$ базис в $\mathbb{R}^n$ в котором матрица состоит из блоков вида $\begin{pmatrix} a_i & b_i \\ -b_i & a_i \end{pmatrix}$.

   А если матрица не диагонализуема, то матрица будет состоять из таких блоков B_i (аналогично Жордановым):

$$\begin{pmatrix} a_i & b_i & 0 & 0 \\ -b_i & a_i & 1 & 0 \\ 0 & 0 & a_i & b_i \\ 0 & 0 & -b_i & a_i \end{pmatrix}$$

6.3. Циклические пространства и фробениусова форма

$\mathcal{A}\colon V \to V$, поле по K.

Выберем $v \in V, v \neq 0$

Рассмотрим последовательность $\langle v, \mathcal{A}v, \mathcal{A}^2v, \ldots, \mathcal{A}^kv\rangle$ — не ЛНЗ. $\exists\{a_i\}, A^k(v) = A^k(v) = \sum\limits_{i=1}^{k} a_iA^i(V) \wedge$ $\{v, v, \mathcal{A}v, \mathcal{A}^2v, \ldots, \mathcal{A}^kv\}$ — не ЛНЗ.

Утверждение 6.7. $\langle v\rangle_{K[t]} = \langle v, \mathcal{A}v, \ldots, \mathcal{A}^{k-1}\rangle$. Найдем $\min k$, такое, $\exists\{a_i\} \in K$, такие, что $A\Big|_{\langle v\rangle_{K[t]}} = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{k-1} \end{pmatrix}$.

$\langle v\rangle_{K[t]}$ — циклическое подпространство.

$A(b_0 + b_1Av + \ldots + A^{k-1}v) = b_0Av + \ldots + b_{k-2}A^{k-1}(v)$.

Утверждение 6.8. $\chi_{\mathcal{A}\big|_{\langle v\rangle}} = t^k - a_{k-1}t^{k-1} .. - a_0$.

Утверждение 6.9. $\forall$ пространство раскладывается в прямую сумму циклических подпространств (относительно $\mathcal{A}$).
На матричном языке — любая матрица подобна матрице, состоящей из нескольких блоков, как выше (фробениусова форма).

7. Евклидовы и унарные пространства

***Определение* 7.1.** Евклидовым пространством называется пара $(V, (\ ,\ ))$, так что V — векторное пространство над $\mathbb{R}$.

$(\ ,\ )\, V \times V \to \mathbb{R}$, такой что $(\ ,\ )$ билинейна, $(\ ,\ )$ — симметрична и $\forall v \in V : (v, v) \geqslant 0 \wedge (v, v) = 0 \iff v = 0$.

Будем называть $(\ ,\ )$ скалярным произведением.

Пример. $V = \mathbb{R}^n$. Тогда формула известна. Очев, что все очев.

Пример. $V = C[0, 1], (f, g) = \int\limits_0^1 f(x)g(x)\mathrm{d}x$.

***Определение* 7.2.** V — евклидово $v \in V$, норма V — $\|v\| = \sqrt{(v, v)}$.

$v_1, v_2 \in V, d(v_1, v_2) = \|v_1 - v_2\|$.

Утверждение 7.1. d — метрика.

Утверждение 7.2. V — евклидово. $v_1, v_2 \in V \implies |(v_1, v_2)|^2 \leqslant \|v_1\| \cdot \|v_2\|$.

***Определение* 7.3.** V — евклидово. Тогда $\langle v_1, v_2\rangle$ — это $\alpha \in [0; \pi]$, такой, что $\cos\alpha = \frac{(v_1,v_2)}{\|v_1\|\cdot\|v_2\|}$.

***Определение* 7.4.** Если $(v_1, v_2) = 0$, то будем называть v_1, v_2 ортогональными.

***Определение* 7.5.** V — евклидово пространство, $v_1, \ldots, v_n$ — базис. Тогда матрица $a_{ij} = (v_i, v_j)$ — матрица Грама.

Возьмем $u_1, u_2 \in V$, с координатами x_i, y_i в базисе $\{v_i\}$. Тогда скалярное $(u_1, u_2) = X^T G Y$, где G — матрица Грама.

Если матрица Грама равна E, то у нас ортонормированный базис и $X^T G Y = X^T Y = x_1y_1 + x_2y_2 + \ldots + x_ny_n$.

***Определение* 7.6.** Пусть $v_1, \ldots, v_n$ — базис. Тогда он ортонормирован, если $\forall i, j : (v_i, v_j) = \delta_{ij}$.

Теорема 7.3 (оротогонализация Грама Шмидта)**.** V — евклидово пространство, $v_1, v_2, \ldots, v_n$ — базис. Тогда $\exists$ ортонормированный базис (ОНБ) $e_1, \ldots, e_n$, причем $\forall i : \langle v_1, \ldots, v_i\rangle \overset{(*)}{=} \langle e_1, \ldots, e_i\rangle$.

Доказательство. Докажем, что $\exists$ базис со $(*)$ по индукции.

База: $e_1 = \frac{v_1}{\|v_1\|}$. $\langle e_1\rangle = \langle v_1\rangle$, $(e_1, e_1) = \frac{1}{\|v_1\|^2}(v_1, v_1) = 1$.

Переход $l \to l{+}1$. Строим $\widetilde{e_{l+1}} = a_1e_1{+}a_2e_2{+}\ldots{+}v_{l+1}, a_i \in \mathbb{R}$. $\langle e_1, \ldots, e_l, \widetilde{e_{l+1}}\rangle = \langle e_1, e_2, \ldots, e_l, v_{l+1}\rangle = \langle v_1, v_2., \ldots, v_{l+1}\rangle$.

Проверим ортогональность. $\forall a_i : (a_1e_1 + \ldots + a_le_l + v_{l+1}, e_i) = 0$i

Это следует из того, что можно раскрыть сумму $\sum\limits_{j=1}^{l} a_j(e_j, e_i) + (v_{l+1}, e_i) = 0 \implies a_i(e_i, e_j) + (v_{l+1}, e_i) = 0$. Тут почти все равно нулю, кроме $(e_i, e_i) = 1$. Тогда $a_i = -\frac{(v_{l+1},e_i)}{(e_i,e_i)} = -(v_{l+1}, e_i)$. □

Замечание. Пусть $e_1, e_2, \ldots, e_n$ — ОНБ,$v \in V$. $x_1, \ldots, x_n$ — координаты v. Тогда $v{\cdot}e_i = (\sum x_ie_i, e_i) = \sum x_j(e_j, e_i) = x_i$.

С предыдущей лекции нам известно, что скалярное произведение — симметрическая билинейная форма над $\mathbb{R}$.

Пример. $\mathbb{R}^2, f(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}) = x_1y_1 - x_2y_2$ или $(x_1 - x_2)(y_1 - y_2)$ или $x_1y_2 - x_2y_1$.

Это все симметрические билинейные формы.

Или $V = 2^M$ и $f(x, y) = |X \cap Y| \pmod 2$, если явно записывать, то $f(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}) = x_1y_1 + \ldots + x_ny_n$.

***Определение* 7.7.** Симметрическая билинейная форма на V (над K) называется невырожденной если $(\forall y \in V : f(x, y) = 0) \implies x = 0$.

***Определение* 7.8.** V — векторное пространство, то $V^* = Hom(V, K)$ — множество линейных отображений (функционалов $V \to K$).

Пусть f — билинейная форма $\implies \exists F\colon V \to V^*, x \mapsto f_x\colon f_x(g) = f(x, y)$.

f — невырождена $\implies F$ — изоморфизм.

Пусть f — билинейная форма $\rightsquigarrow \Gamma_f = (a_{ij}), a_{ij} = f(e_i, e_j)$, где $\{e_i\}$ — базис. Тогда $f(\sum x_ie_i, \sum y_ie_i) = \sum a_{ij}x_iy_{hj} = X^T\Gamma_fY$.

Перейдем теперь к $K = \mathbb{C}$. $f(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}) = \sum x_i\overline{y}_i$, $f(x, x) > 0$.

***Определение* 7.9.** Унитарным пространством называется пара $(V, (-,-))$, где V — векторное пространство над $\mathbb{C}$, $(-,-)\colon V \times V \to \mathbb{C}$, такое, что

1. $(x_1 + x_2, y) = (x_1, y) + (x_2, y)$ или $(x, y_1 + y_2) = (x, y_1) + (x, y_2)$.
2. $(ax, y) = a(x, y), (x, ay) = \overline{a}(x, y)$.
3. $f(x, y) = \overline{f(y, x)}$.
4. $f(x, x) \in \mathbb{R}_+$, при $x \neq 0$.

Длина, КБШ, метрика — все тоже самое.
С углами сложнее (это останется тайной).
Отрогонализация Грама-Шмидта работает, в частности, $\forall$ унитарном пространстве есть ортонормированный базис. При этом $f(X, Y) = X^T\Gamma_f\overline{Y}$.

7.1. Ортогональное дополнение

***Определение* 7.10.** V — эвклидово/унитарное пространство: $U \leqslant V$. Ортогональное дополнение U — это $U^\perp = \{v \in V \mid (u, v) = 0 \forall u \in U\}$.

Утверждение 7.4. $U^\perp$ — подпространство в V.

Доказательство. Упражнение. □

Теорема 7.5.

1. $\dim U^\perp = \dim V - \dim U$.
2. $U^{\perp\perp} = U$.

3. $V = U \oplus U^\perp$ — любой элемент из V представим в виде пары из U и $U^\perp$.

Доказательство.

1. $\dim V = n, \dim U = K$. Возьмем базис $e_1, \dots, e_k$, дополним через $e_{k+1}, \dots, e_n$ до ОНБ (до любого, а далее Грам-Шмидт).

   Заметим, что $x = \sum x_i e_i \in U^\perp \iff (\sum\limits_{i=1}^{n} x_i e_i, e_j) = 0 \forall j = 1,..,k \wedge e_j \in U^\perp \iff x_j = 0 \forall j = 1..k \iff x = \sum\limits_{k+1}^{n} x_i e_i \iff x \in \langle e_{k+1}, \dots, e_n \rangle$.

   Итого, $\dim U^\perp = n - k = \dim V - \dim U$.

   Тогда $U^{\perp\perp} = \langle e_{k+1}, \dots, e_n \rangle^\perp = \langle e_1, \dots, e_k \rangle = U$.

   Ну и понятно, как раскладывается вектор из V.

□

***Определение* 7.11.** $v = u + u^\perp, u \in U, u^\perp \in U^\perp$, u — проекция v на U, $u^\perp$ — ортогональная составляющая.

$\|u^\perp\|$ — расстояние от v до u.

Утверждение 7.6 (Матрица Грама при замене базиса). f — билинейная полуторномерная форма. Γ_f — матрица Грама в базисе $e_1, \dots, e_n$.

Возьмем другой базис, C — матрица перехода.

$X \rightsquigarrow CX = \widetilde{X}$. Пусть $D = C^{-1}$. Тогда $X = D\widetilde{X}$.

$f(x, y) = X^T \Gamma Y = (\widetilde{X} D)^T \Gamma (D\widetilde{Y}) = \widetilde{X}^T (D^T \Gamma D) \widetilde{Y} \implies D^T \Gamma D = \widetilde{\Gamma}$ — матрица Грама в новом базисе.

7.2. Соответствиемежду формами/матрицами

Билинейная полуторная форма $\implies A \in M_n(K)$.

Симметрическая билинейная форма $\iff A = A^T$ — симм. матрица. ($A = \Gamma_f$).

Полуторная форма $\iff a_{ij} = \overline{a_{ji}} \iff \overline{A^T} = A$, $A^* := \overline{A^T}$ матричное сопряжение.

$A = A^*$ — эрмитова матрица.

f — симметрическая билинейная/полуторная форма.

Переформулировка: дана $f(X, X) = \sum a_{ij} x_i x_j$ — квадратичная форма.

Как понять: верно ли, что $q(x) > 0\ \forall x \neq 0$.

f – положительно определена $\implies$ f — скалярное произведение $\implies$ $\exists$ ОНБ: $\exists C$: $\det C^T AC = \det(C^T) \det(C) \det(A) = (\det C)^2 \det A = 1 = \det E \implies \det A > 0$

Теорема 7.7 (Критерий Сильвестра). f — симметричная билинейная, $A \in M_n(\mathbb{R})$ — матрица Грама f в базисе $e_1, \dots, e_n$.

Тогда f — положительно определена $\iff \forall i = 1..n\ \triangle_i > 0$, где $\triangle_i := \det(a_{jk})_{\substack{j=1..i \\ k=1..i}}$.

Доказательство. Необходимость. $I = \{i_1, i_2, \dots, i_k\}$ — номера строк/столбцов.
A_I — подматрица со строками/столбцами из I. A_I — матрица Грама. $f\Big|_{\langle e_{i_1}, \dots, e_{i_k} \rangle}$ — положительно определена.

Достаточность. Пусть $\Delta_i > 0$. Докажем индукцией по k: $f\Big|_{\langle e_1,\dots,e_k\rangle}$ — положительно определена $\implies$ при $k = n$ то , что надо.

База: $f\Big|_{\langle e_1\rangle}$ $f(ae_1, ae_1) = a^2(e_1, e_1) = a^2 a_{11} > 0$.

Переход: $k \to k+1$. $f\Big|_{\langle e_1,\dots,e_k\rangle}$ — положительно определена, $(\langle e_1, \dots, e_k\rangle, f)$ — евклидово пространство. $\implies$ $\exists$ ОНБ, $\widetilde{e_1}, \dots, \widetilde{e_k}$. Матрица Грама $f\Big|_{\langle e_1,\dots,e_{k+1}\rangle}$ в базисе $\widetilde{e_1}, \dots, \widetilde{e_k}, e_{k+1} = \left(\begin{array}{ccc|c} 1 & \dots & 0 & a_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & a_k \\ \hline a_1 & \dots & a_k & a \end{array}\right)$. $\widetilde{e}_{k+1} = e_{k+1} - \sum\limits_{i=1}^{k} a_i \widetilde{e_i}$. Теперь $(\widetilde{e}_{k+1}, \widetilde{e_i}) = (e_{k+1} - \sum a_i \widetilde{e_i}, \widetilde{e_i}) = (e_{k+1}, \widetilde{e_i}) - \sum\limits_{j=1}^{k} a_j (\widetilde{e_j}, \widetilde{e_i}) = a_i - a_i = 0$.

Тогда $\widetilde{A} = \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & b \end{pmatrix}$, $\det \widetilde{A} = \det(C^T) \cdot \Delta_{k+1} \det C > 0 \implies b > 0 \implies f$ имеет ОНБ в $\langle e_1, \dots, e_{k+1}\rangle \implies f$ — положительно определена на $\langle e_1, \dots, e_{k+1}\rangle$.

*. $f(\sum c_i \widetilde{e_i}, \sum c_i \widetilde{e_i}) = \sum_{i=1}^{k} c_i^2 + c_{k+1}^2 b > 0$ $\square$

8. Операторы в евклидовых и унитарных пространствах

8.1. Самосопряженные операторы

***Определение* 8.1.** V — евклидово/унитарное пространство, $\mathcal{A} \in End(V)$.

$\mathcal{B}$ — сопряженный оператор, если $(\mathcal{A}x, y) = (x, \mathcal{B}y) \forall x, y \in V$.

Теорема 8.1. $\exists \wedge \exists!$ сопряженный оператор $\mathcal{A}^*$. $\mathcal{A} = \mathcal{A}^*$ — называется самосопряженным.

Теорема 8.2. $\mathcal{A}$ — самосопряжен $\iff$ у $\mathcal{A}$ есть ОНБ из собственных векторов и все с.ч вещественны.

$\mathcal{A}$ — самосопряжен $\iff [\mathcal{A}]_{\text{ОНБ}} = A$ такова, что $A^T = \overline{A}$, $A = (\delta_{ij})$, $\overline{A} = (\overline{\delta_{ij}})$.

Доказательство. $\mathcal{A}$ — самосопряжен $\iff \forall i, j : (\mathcal{A}e_i, e_j) = (e_i, \mathcal{A}e_j) \iff (\sum\limits_{k=1}^{n} a_{ik}e_k, e_j) = (e_i, \sum\limits_{k=1}^{n} a_{jk}e_k) \iff -(a_{ij}e_j, e_J) = (e_i, a_{ji}e_i) \iff a_{ij}(e_j, e_i) = \overline{a_{ji}}(e_i, e_i) \iff a_{ij} = \overline{a_{ji}}$.

$\mathcal{A}$ — самосопряжена $\implies \forall\lambda$ — собственное число $\lambda \in \mathbb{R}$, потому что, если взять собственный вектор $x, \mathcal{A}x = \lambda x$, получим, что $(\mathcal{A}x, x) = (x, \mathcal{A}x) \implies (\lambda x, x) = (x, \lambda x) \implies \lambda(x, x) = \overline{\lambda}(x, x) \implies \lambda = \overline{\lambda}$

В том числе для $A \in M_n(\mathbb{R}), A = A^T$ — все корни $\chi_A(t)$ — вещественны. □

Утверждение 8.3. $\mathcal{A}$ — самосопряженный оператор, $\mathcal{A} \in End(V)$, $U \leqslant V$ — инвариантное подпространство относительно $\mathcal{A}$, тогда $U^\perp$ — инвариантное подпространство.

Доказательство. $v \in U^\perp$, то есть $(u, v) = 0 \ \forall u \in U$, $\mathcal{A}v \colon \ (um\mathcal{A}V) = (\mathcal{A}u, v) = 0 \implies \mathcal{A}v \in u^\perp$. □

Доказтельство теоремы.... $\Leftarrow$. Пусть у $\mathcal{A}\exists$ ОНБ из собственных векторов с вещественными собственными числами. То есть в некотором ОНБ $[\mathcal{A}]$ диагонализуема и $\lambda_i \in \mathbb{R}$. $A^T = \overline{A}(= A)$.

$\Rightarrow$. База $n = 1$.

Переход $n \to n+1$. $\mathcal{A}$ — самосопряженная, $v_1, \ldots, v_n$ — ОНБ. $[\mathcal{A}]_{\{v_i\}} = A, A^T = \overline{A}, \exists\lambda_1 \in \mathbb{R}$ — собственное число A.

$\exists v \in V : \mathcal{A}v = \lambda_1 v$, $\langle v \rangle$ — инвариантное подпространство $\implies \langle v \rangle^\perp$ — инвариантное подпространство, $\dim\langle v \rangle^\perp = n + 1 - 1 = n$. $\mathcal{A}\Big|_{\langle v \rangle^\perp} : \langle v \rangle^\perp \to \langle v \rangle^\perp$.

$\mathcal{A}\Big|_{\langle v \rangle^\perp}$ — самосопряженнная по предположению. $\exists e_1, \ldots, e_n$ – ОНБ из собственных векторов $\mathcal{A}$ с вещественными собственными числами.

$e_{n+1} := \frac{v}{\|v\|}, \|e_{n+1}\| = 1$ и $\langle e_{n+1}, e_i \rangle = 0 \implies e_1, \ldots, e_{n+1}$. □

8.2. Оценка квадратичной формы

Хотим посмотреть на $q(x_1, \ldots, x_n) = \sum\limits_{i,j=1} a_{ij}x_i x_j$.

Ищем A: $q(x_1, \ldots, x_n) \leqslant A(x_1^2 + \ldots + x_n^2)$, причем A — минимально.

Заметим, что $\sum a_{ij}x_ix_j = (AX, X)$, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $A = (a_{ij})$.

$X = \sum c_i v_i \implies (AX, X) = (\sum c_i\lambda_i v_i, \sum c_i v_i) = \sum \lambda_i c_i^2$.

Возьмем $A = \max\{\lambda_i, 0\} \implies \sum \lambda_i c_i \leqslant A \sum c_i^2$. Следовательно, $q(x_1, \ldots, x_n) \leqslant \lambda_{\max}(\sum x_i^2)$, λ_{max} — максимальное собственное число. Аналогично, $\geqslant \lambda_{min}(\sum x_i^2)$.

8.3. Ортогональные и унитарные операторы

***Определение* 8.2.** $\mathcal{A} \in End(V)$, V — евклидово/унитарно.

Тогда $\mathcal{A}$ называется ортогональным/унитарным оператором, если выполняется одно из равносильных свойств:

1. $(\mathcal{A}X, \mathcal{A}Y) = (x, y)\ \forall x, y \in V$,
2. $\|\mathcal{A}x\| = \|X\|, \forall X \in V$,
3. $\mathcal{A}$ — обратим и $(\mathcal{A}X, Y) = (X, \mathcal{A}^{-1}Y)$,
4. В $\forall$ ОНБ $\overline{A}^T = A^{-1}$,
5. ОНБ $\rightsquigarrow$ ОНБ $\forall$ ОНБ,
6. $\exists$ ОНБ, такой что $\rightsquigarrow$ ОНБ.

Доказательство. $1 \implies 2, 3 (x = y)$.

$4 \iff 3$: очевидно как факт 1 про самосопряжение. $1 \implies 5, 6$ — очев $(x, y) \implies (\mathcal{A}x, \mathcal{A}y)$
$6 \implies 1$: $\mathcal{A}e_i = f_i, \{e_i\}, \{f_i\}$ — ОНБ, $x = \sum x_i e_i, y = \sum y_i f_i$. ... □

Замечание. $\mathcal{A}$ — самосопряженный $\implies$ есть ОН собственный базис ($\lambda \in \mathbb{R}$).

$A = \overline{A}^T$ — матрица $\mathcal{A}$ в ОНБ. $\exists C: C^{-1}AC = C^TAC$. RHS сохраняется при применении $\mathcal{A} \implies$ LHS — тоже.

А значит любую квадратичную форму можно привести к виду $\sum \lambda_i x_i^2$.

Свойство. $\mathcal{A}$ — ортогональный/унитарный оператор. λ — собственное число, ($A \in M_n(\mathbb{C}) \implies \overline{A}^T = A^{-1}$).

λ — собственное число $\implies |\lambda| = 1$, $Av = \lambda v \implies (Av, v) = (v, A^{-1}v) \iff \lambda(v, v) = (v, \frac{1}{\lambda}v) = \frac{1}{\overline{\lambda}}(v, v) \implies \lambda\overline{\lambda} = 1$.
В частности $|\det A| = 1$

***Определение* 8.3.** Собственный ортогональный оператор — такой, что $\det A = 1$ (сохр-й ориентацию).

Замечание. Ортогональные/унитарные операторы — группа по умножению. Группы O_n, SO_n, Un_n, SO_n

Пример. $O_1 = \{\pm 1\}$, $SO_1 = \{1\}$, U_1 — группа углов.

$SU_1 = \{1\}$, SO_2 — группа углов.

Теорема 8.4. V — унитарное пространство, $\mathcal{A} \in End(V)$ — унитарный оператор $\iff \exists$ ОНБ из собственных векторов собственными числами $\{\lambda_i\}, |\lambda_i| = 1 \quad \forall i$.

Лемма. $U \leqslant V$ — инвариантное $\implies U^\perp$ — инвариантное.

Доказательство. $v \in u^\perp$ рассмотрим $\mathcal{A}v$: $\forall u \in U: (u, \mathcal{A}v) = (\mathcal{A}^{-1}u, \mathcal{A}^{-1}\mathcal{A}v) = (\mathcal{A}^{-1}u, v) = 0$. □

Доказательство. см евклидов случай. □

Теорема 8.5. V — евклидово пространство. $\mathcal{A} \in End(V)$ — ортогонально $\iff \exists$ ОНБ $e_1, \ldots, e_n$ такой что, A — блочная матрица из блоков $(n = 2)$ $\begin{pmatrix} \cos\alpha & -\sin\alpha \\ +\sin\alpha & \cos\alpha \end{pmatrix}$ и возможно блоков размера 1 из $\{-1, 1\}$.
То есть $\forall$ ортогональное преобразование — это композиция поворотов в нескольких попарно ортогональных плоскостях и зеркальных симметрий.

Доказательство. $\mathcal{A} \rightsquigarrow A$, $A^T = A^{-1}$. $A \in M_n(\mathbb{R}) \subset M_n(\mathbb{C})$. $\overline{A}^T = A^{-1}$ — унитарный оператор $\mathbb{C}^n \to \mathbb{C}^n \implies \exists$ ОНБ из собственных векторов $e_1, \ldots, e_n$. $V = \omega_1 \oplus \omega_{-1} (\omega_{\lambda_i} \bigoplus\limits_{\lambda_i \neq \pm 1} \omega_{\overline{\lambda_i}})$.

$\omega_i = \langle e_{i_1}, \ldots, e_{i_k} \rangle, \mathrm{rk}_{\mathbb{C}}(A - E) = n - k, \mathrm{rk}_{\mathbb{R}}(A - E) = n - k \implies \exists$ базис $\widetilde{e_{i_1}}, \ldots, \widetilde{e_{i_k}} \in \mathbb{R}^n$. Ортонормируем его по Граму-Шмидту: $\widetilde{\widetilde{e_{i_k}}}$. Точно так же для ω_{-1}.

Все новые вектора ортогональны, так как $\omega_1 \perp \omega_{-1}$. $x_i \neq 1, -1, \omega_{x_i} = \langle e_{j_1}, \ldots, e_{j_k} \rangle$.

$\begin{pmatrix} a + bi \\ c + di \end{pmatrix} e_{jl} = r_{jl} + i s_{jl}$. $A(\overline{e}_{jl}) = \overline{\lambda_i} \overline{e}_{jl} \implies \dim w_{\lambda_i} = \dim w_{\overline{\lambda_i}}$.
$\lambda_i = \cos\alpha_i + i \sin\alpha_i$
А дальше посмотрите запись, у меня лапки.
«Опять немножечко скомкано получилось, кое-какие детали замяты, но что-то мне надоело ..., будем считать, что доказали.» — Михаил Антипов. □