

ЭКЗАМЕН ПО АЛГЕБРЕ

Лектор: Гайфуллин С. А. • Автор: Пшеничный Никита*, группа 109

I курс • Осенний семестр 2023 г.

Аннотация

При подготовке этого файла я использовал: курс лекций С. А. Гайфуллина, записи лекций Ю. Г. Прохорова на *teach-in*, книгу «Курс алгебры» Э. Б. Винберга и курс семинаров А. А. Клячко.

Экзаменационные вопросы

- | | |
|--|----|
| 1 Системы линейных уравнений. Матрица коэффициентов и расширенная матрица коэффициентов. Элементарные преобразования. Эквивалентные системы. Элементарные преобразования переводят СЛУ в эквивалентную | 3 |
| 2 Экзотические уравнения. Свободные и главные переменные. Ступенчатый и улучшенный ступенчатый вид матрицы. Метод Гаусса решения СЛУ | 4 |
| 3 Единственность улучшенного ступенчатого вида матрицы. Понятие ранга матрицы (через ступенчатый вид) и его корректность | 6 |
| 4 Векторное пространство. Простейшие свойства из аксиом. Подпространство. Критерий того, что подмножество является подпространством | 7 |
| 5 Понятие линейной зависимости системы векторов. Три свойства линейной зависимости | 10 |
| 6 Однородные системы с количеством неизвестных большим количества уравнений. Основная лемма о линейной зависимости | 11 |
| 7 Решения однородной системы образуют подпространство. Линейная оболочка: определение и доказательство того, что это подпространство | 11 |
| 8 Базис системы векторов: эквивалентность 4 определений. Стандартный базис в \mathbb{R}^n . Дополнение линейно независимой системы до базиса. Выбор базиса из полной системы | 13 |
| 9 Ранг системы векторов и размерность векторного пространства. Связь ранга системы и размерности линейной оболочки. Строчный, столбцовый и ступенчатый ранги матрицы, их совпадение | 15 |
| 10 Свойства ранга матрицы. Теорема Кронекера — Капелли. Критерий определённости системы | 16 |
| 11 Фундаментальная система решений и алгоритм её поиска. Размерность пространства решений однородной СЛУ. Структура решений неоднородной СЛУ | 17 |
| 12 Линейное отображение. Его матрица в фиксированных базисах. Образ заданного вектора. Изоморфизм. Любое конечномерное пространство изоморфно пространству строк | 18 |
| 13 Операции над линейными отображениями и над матрицами, связь между ними. Матричная запись СЛУ | 19 |
| 14 Свойства операций над матрицами. Связь с транспонированием | 20 |
| 15 Вывод обобщённой ассоциативности для ассоциативной операции | 21 |

*Telegram: @pshenikita

16	Верхние оценки на ранг суммы и произведения матриц	21
17	Правая и левая обратные матрицы. Критерий существования. Обратная матрица, её единственность и критерий существования	23
18	Элементарные матрицы. Умножение на элементарные матрицы слева и справа. Матрица, обратная к произведению. Обратная к транспонированной матрице	24
19	Алгоритм поиска обратной матрицы. Разложение невырожденной матрицы в произведение элементарных	25
20	Подстановки и перестановки. Их количество. Произведение подстановок, его свойства. Разложение подстановки на произведение независимых циклов	26
21	Инверсии. Чётность перестановки и подстановки. Знак подстановки, изменение чётности при умножении на транспозицию. Разложение подстановки на транспозиции. Знак произведения подстановок	28
22	Чётность цикла. Чётность произвольной подстановки через декремент	29
23	Формула определителя квадратной матрицы. Определитель транспонированной матрицы. Линейность и кососимметричность определителя как функции от строк и столбцов матрицы	29
24	Определитель матрицы с нулевой строкой/столбцом. Определитель матрицы с пропорциональными строками. Изменение определителя при элементарных преобразованиях строк/столбцов. Определитель треугольной матрицы. Алгоритм вычисления определителя с помощью элементарных преобразований. Эквивалентные условия невырожденности матрицы. Определитель матрицы с углом нулей	30

1 Системы линейных уравнений. Матрица коэффициентов и расширенная матрица коэффициентов. Элементарные преобразования. Эквивалентные системы. Элементарные преобразования переводят СЛУ в эквивалентную

Определение 1.1. Матрицей размера $m \times n$ над полем \mathcal{K} называется прямоугольная таблица из элементов поля \mathcal{K} , имеющая m строк и n столбцов:

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

Определение 1.2. Линейным уравнением с неизвестными x_1, x_2, \dots, x_n над полем \mathcal{K} называется уравнение вида

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b,$$

где коэффициенты a_1, a_2, \dots, a_n и свободный член b являются элементами поля \mathcal{K} .

Система m линейных уравнений с n неизвестными в общем виде пишется так:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2, \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m, \end{cases} \quad (*)$$

Определение 1.3. Матрица

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

называется матрицей коэффициентов, а матрица

$$\tilde{A} := \left(\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array} \right)$$

— расширенной матрицей коэффициентов системы (*).

Определение 1.4. Решение системы — это элемент поля \mathcal{K}^n , который при подстановке вместо (x_1, \dots, x_n) обращает каждое уравнение в верное равенство. Система уравнений называется **совместной**, если она имеет хотя бы одно решение, и **несовместной** в противном случае. Совместная система называется **определённой**, если её решение единственно.

Определение 1.5. Элементарными преобразованиями системы линейных уравнений называются преобразования следующих трёх типов:

1. прибавление к одному уравнению другого, умноженного на число;
2. перестановка двух уравнений;
3. умножение одного уравнения на число, отличное от нуля.

Элементарными преобразованиями строк матрицы называются преобразования следующих трёх типов:

1. прибавления к одной строке другой, умноженной на число;

2. перестановка двух строк;
3. умножение одной строки на число, отличное от нуля.

Определение 1.6. Две СЛУ называются **эквивалентными**, если множества их решений совпадают. Обозначение для расширенных матриц: $\tilde{A} \sim \tilde{B}$.

Теорема 1.1. Если одну систему можно перевести в другую элементарными преобразованиями, то они эквивалентны.

Докажем сначала вспомогательное утверждение:

Лемма 1.1. Преобразование, обратное к элементарному, тоже элементарное.

Доказательство. Докажем для каждого преобразования:

1. («прибавить i -ое уравнение к j -му с коэффициентом λ ») $^{-1}$ = («прибавить i -ое к j -му с коэффициентом $-\lambda$ »)
2. Преобразование второго типа обратное к самому себе
3. («умножить i -ое уравнение на $c \neq 0$ ») $^{-1}$ = («умножить i -ое уравнение на $c^{-1} \neq 0$ »)

■

Теперь докажем теорему:

Доказательство. Докажем, что каждое решение первой системы является решением второй. Это очевидно для преобразований второго и третьего типа, докажем и для первого:

$$(a_{j1} + \lambda a_{i1})x_1 + \dots + (a_{jn} + \lambda a_{in})x_n = \underbrace{a_{j1}x_1 + \dots + a_{jn}x_n}_{=0} + \lambda \underbrace{(a_{i1}x_1 + \dots + a_{in}x_n)}_{=0} = 0.$$

Далее, из леммы 1.1 обратное к элементарному преобразование тоже элементарное. Поэтому всякое решение второй системы является решением первой. Значит, множества решений этих систем совпадают, т. е. они эквивалентны. ■

Примечание. Обратное утверждение неверно — если СЛУ эквивалентны, то они не всегда переводятся друг в друга элементарными преобразованиями. Контрпример — две системы с пустыми множествами решений:

$$A = \left(\begin{array}{cc|c} 0 & 1 & 1 \\ 0 & 0 & 1 \end{array} \right) \equiv B = \left(\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 0 & 1 \end{array} \right).$$

Никаким элементарным преобразованием строк нельзя занулить первый столбец матрицы B .

2 Экзотические уравнения. Свободные и главные переменные. Ступенчатый и улучшенный ступенчатый вид матрицы. Метод Гаусса решения СЛУ

Определение 2.1. **Лидером** (ведущим элементом) ненулевой строки $(a_1, a_2, \dots, a_n) \in \mathcal{K}^n$ её первый ненулевой элемент.

Определение 2.2. Матрица называется **ступенчатой**, если номера ведущих элементов её ненулевых строк образуют строго возрастающую последовательность, а нулевые строки расположены в конце:

$$\left(\begin{array}{ccccc} * & * & * & * & * \\ & * & * & * & * \\ & & * & * & * \\ 0 & & & * & * \\ & & & & * \end{array} \right)$$

Матрица называется улучшенной ступенчатой, если она ступенчатая, её ведущие элементы равны 1, а элементы над ними равны 0:

$$\begin{pmatrix} 1 & 0 & * & 0 & 0 \\ & 1 & * & 0 & 0 \\ & & & 1 & 0 \\ & & 0 & & 1 \end{pmatrix}$$

Теорема 2.1. Всякую матрицу путём элементарных преобразований строк можно привести к ступенчатому виду.

Доказательство. Если данная матрица нулевая, то она уже ступенчатая. Если она ненулевая, то пусть j_1 — номер её первого ненулевого столбца. Переставив, если нужно, строки, добьёмся того, чтобы $a_{1j_1} \neq 0$. После этого прибавим к каждой строке, начиная со второй, первую строку, умноженную на подходящее число, с таким расчётом, чтобы все элементы j_1 -го столбца, кроме первого, стали равными нулю. Теперь рассмотрим матрицу без первой строки и первый j_1 столбцов. Приведём её таким же методом к ступенчатому виду. Продолжая процесс таким же образом, мы получим ступенчатую матрицу. ■

Процесс, проводимый нами в доказательстве последней теоремы, называется *прямым ходом метода Гаусса*.

Примечание. Для приведения матрицы к ступенчатому виду достаточно преобразований первого типа. Действительно, преобразования второго типа нужны были нам лишь для того, чтобы поднять на первую строчку ненулевой элемент. Однако, эту задачу можно выполнить преобразованием первого типа. Пусть $a_{i_1j_1} \neq 0$. Тогда прибавим i_1 строку расширенной матрицы к первой. Теперь получаем $a_{0j_1} = a_{i_1j_1} \neq 0$. А далее действуем так же.

Теперь приведём расширенную матрицу коэффициентов СЛУ к улучшенному ступенчатому виду. По теореме 1.1 множество её решений не изменилось, а решать её в таком виде куда проще.

Определение 2.3. Пусть j_1, j_2, \dots, j_r — номера ведущих коэффициентов ненулевых уравнений системы. Неизвестные $x_{j_1}, x_{j_2}, \dots, x_{j_r}$ назовём **главными**, а остальные — **свободными**.

Определение 2.4. Уравнения вида

$$0 \cdot x_1 + 0 \cdot x_2 + \dots + 0 \cdot x_n = b,$$

где $b \neq 0$ назовём **экзотическими**.

Теорема 2.2. Для каждого набора значений свободных переменных существует единственный набор значений главных переменных, который дополняет данный набор до решения совместной системы.

Доказательство. Идём по строкам ступенчатой расширенной матрицы коэффициентов СЛУ снизу вверх. Рассмотрим первую встреченную нами ненулевую строку, её номер i_r . В соответствующем уравнении ровно одна главная переменная — x_{j_r} . Её можно выразить через свободные переменные и свободный член уравнения единственным образом. Теперь возьмём следующую строку. Её номер i_{r-1} , и в ней ровно две главные неизвестные — x_{j_r} и $x_{j_{r-1}}$. Выразим $x_{j_{r-1}}$ через x_{j_r} , свободные переменные и свободный член. А теперь подставим выражения x_{j_r} через свободные переменные, полученное на предыдущем шаге. Получается, $x_{j_{r-1}}$ тоже выражается через свободный член и свободные переменные единственным образом. Продолжив процесс, получим выражения для всех главных переменных через свободные. ■

Процесс, проводимый нами в доказательстве последней теоремы, называется *обратным ходом метода Гаусса*.

Примечание. Как следствие, любая СЛУ над бесконечным полем имеет либо ни одного, либо одно, либо бесконечно много решений. А над конечным — либо ни одного, либо одно, либо $|\mathcal{K}|^{n-r}$, где r — количество ступенек в ступенчатой матрице (иными словами, $n - r$ — количество свободных переменных). Доказательство того, что это число r определено корректно, будет позднее.

3 Единственность улучшенного ступенчатого вида матрицы. Понятие ранга матрицы (через ступенчатый вид) и его корректность

Теорема 3.1. Каждая матрица имеет единственный улучшенный ступенчатый вид.

Доказательство. Рассмотрим матрицу A . Допустим, она может быть приведена элементарными преобразованиями к двум улучшенным ступенчатым видам B и C . Наша цель — доказать, что $B = C$. Рассмотрим однородную систему уравнений с матрицей коэффициентов A . Расширенная матрица коэффициентов $\tilde{A} = (A \mid 0)$ приводится теми же элементарными преобразованиями к виду ступенчатым видам $\tilde{B} = (B \mid 0)$ и $\tilde{C} = (C \mid 0)$. Это означает, что однородные системы с матрицами коэффициентов B и C эквивалентны. Пусть $B \neq C$. Отбросим нулевые строки в матрицах \tilde{B} и \tilde{C} , при этом системы останутся эквивалентными. Будем идти по строкам матриц \tilde{B} и \tilde{C} , пока не дойдём до места, где будет различие. Попадаем в один из трёх случаев:

1. *Строки с первой по $(k-1)$ -ую снизу в матрицах \tilde{B} и \tilde{C} совпадают, а лидеры k -ой строки снизу в матрицах \tilde{B} и \tilde{C} имеют различные позиции.* Пусть лидеры стоят в столбцах p и q соответственно. Не ограничивая общности, можем считать, что $p < q$. Из того, что строки ниже, чем k -ые снизу у матриц \tilde{B} и \tilde{C} совпадают, следует, что разделение переменных x_i при $i > q$ на главные и свободные в системах \tilde{B} и \tilde{C} одинаково. Положим все свободные переменные с номерами $> q$ равными нулю. В системе $(C \mid 0)$ переменная x_q главная и, следовательно (т.к. система однородная) при указанном задании переменных она также обязательно равна нулю. В системе $(B \mid 0)$ переменная x_q свободная, а потому при указанном задании переменных она может принимать значение 1. Таким образом, нашли решение одной системы, которое не является решением другой. Противоречие с эквивалентностью систем $(B \mid 0)$ и $(C \mid 0)$.
2. *Строки с первой по $(k-1)$ -ую снизу в матрицах \tilde{B} и \tilde{C} совпадают, лидеры k -ой строки снизу у этих матриц имеют одинаковые позиции p , но есть номер $s > p$ такой, что в s -ом столбце в рассматриваемой строке у матриц \tilde{B} и \tilde{C} стоят различные числа.* Пусть эти числа b и c соответственно. Не ограничивая общности, $b \neq 0$. Тогда x_s — свободная переменная для системы $(B \mid 0)$, т.к. в столбцах, соответствующих главным переменным стоят нули за счёт улучшенного ступенчатого вида. А значит, x_s — свободная переменная и для $(C \mid 0)$. Положим все свободные переменные, кроме x_s , равными нулю, а $x_s = 1$. Тогда из системы $(B \mid 0)$ получаем, что $x_s = -b$, а из системы $(C \mid 0)$ — что $x_s = -c$, но $b \neq c$. Противоречие.
3. *Проходя снизу вверх по ненулевым строкам матриц \tilde{B} и \tilde{C} , мы всё время видели, что очередные строки совпадают, но строки в одной из матриц закончились, а в другой — нет.* Пусть строки закончились в матрице \tilde{B} , тогда в матрице \tilde{C} есть ещё одна нулевая строка. Из того, что строки ниже, чем данная, у матриц \tilde{B} и \tilde{C} совпадают, следует, что разделение переменных x_i при $i > q$ на главные и свободные в соответствующих системах одинаково. Но в системе $(B \mid 0)$ переменная x_q свободная (нет строки, где лидер имеет позицию q), а в системе $(C \mid 0)$ — свободная. Далее можем поступить так же, как и в первом случае.

■

Примечание. Отсюда следует, что количество ненулевых строк в любом ступенчатом виде данной матрицы одинаково. Действительно, ведь для любого ступенчатого вида можно построить улучшенный ступенчатый с таким же количеством ненулевых строк — достаточно каждую ненулевую строку разделить на её ведущий элемент, а затем вычесть её из всех строк выше с подходящим коэффициентом. А ступенчатый вид единственный.

Определение 3.1 (Ступенчатый ранг матрицы). Количество ненулевых строк в ступенчатом виде данной матрицы A называется **рангом матрицы A** и обозначается $\text{rk } A$.

4 Векторное пространство. Простейшие свойства из аксиом. Подпространство. Критерий того, что подмножество является подпространством

Определение 4.1. Векторным пространством над полем \mathcal{K} называется такое множество V с операциями сложения и умножения на элементы поля \mathcal{K} , обладающими следующими свойствами:

- $$\left. \begin{array}{l} 1. \forall a, b, c \in V (a + b) + c = a + (b + c) \\ 2. \exists \mathbf{0} \in V : \forall v \in V v + \mathbf{0} = v \\ 3. \forall v \in V \exists (-v) \in V : (-v) + v = \mathbf{0}. \\ 4. \forall a, b \in V a + b = b + a \end{array} \right\} V \text{ — абелева группа по } +$$
- $$\begin{array}{l} 5. \forall \lambda \in \mathbb{R}, u, v \in V \lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v \\ 6. \forall \lambda, \mu \in \mathbb{R}, v \in V (\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v \\ 7. \forall \lambda, \mu \in \mathbb{R}, v \in V (\lambda \mu) \cdot v = \lambda \cdot (\mu \cdot v) \\ 8. \forall v \in V 1 \cdot v = v \end{array}$$

Определение 4.2. Векторные пространства U и V над полем \mathcal{K} называются **изоморфными**, если существует линейное биективное отображение $\varphi : U \rightarrow V$. Само отображение φ называется при этом **изоморфизмом** пространств V и U .

Примечание. Докажем, что аксиома 4 выводится через остальные. Сделаем это в несколько шагов (над знаками равенства указан номер аксиомы или пункта доказательства, благодаря которой сделан переход):

$$1^*. 0 \cdot v = (0 + 0) \cdot v \stackrel{6}{=} 0 \cdot v + 0 \cdot v \Rightarrow \boxed{0 \cdot v = \mathbf{0}}$$

$$2^*. (-1) \cdot v + v \stackrel{8}{=} (-1 \cdot v) + 1 \cdot v \stackrel{6}{=} (-1 + 1) \cdot v = 0 \cdot v \stackrel{1^*}{=} \mathbf{0} \Rightarrow \boxed{(-1) \cdot v = -v}$$

$$3^*. v - v \stackrel{8, 2^*}{=} 1 \cdot v + (-1) \cdot v \stackrel{6}{=} (1 - 1) \cdot v = 0 \cdot v = \mathbf{0} \Rightarrow \boxed{v - v = \mathbf{0}}$$

Теперь выведем 4 аксиому из остальных:

$$\begin{aligned} u + v &\stackrel{2}{=} (u + v) + \mathbf{0} \stackrel{3}{=} (u + v) + (-(v + u) + (v + u)) \stackrel{1}{=} ((u + v) - (v + u)) + (v + u) = \\ &= (u + \underbrace{v - v}_{=0} - u) + (v + u) \stackrel{3^*}{=} (\underbrace{u - u}_{=0}) + (v + u) = v + u. \end{aligned}$$

Антон Александрович сказал, что остальные не выводятся. Но мы с Костей Зюбиным не смогли доказать это для 5-ой аксиомы. Доказательство независимости от остальных для каждой аксиомы проводится так: нужно привести пример такой структуры, в которой выполняются все аксиомы, кроме выбранной.

- **1 аксиома.** Рассмотрим множество $M = \{e, a, b\}$ с операцией $*$, заданной следующей таблицей:

$*$	e	a	b
e	e	a	b
a	a	a	e
b	b	e	b

Заметим, что операция $*$ коммутативна, в M существует нейтральный элемент e по $*$ и каждый элемент имеет обратный по $*$. Однако эта операция не ассоциативна:

$$(b * a) * a = e * a = a, \quad b * (a * a) = b * a = e.$$

Теперь возьмём алгебраическую систему $V = (\mathbb{R} \times M, +, \star)$ с операциями, определёнными по следующим правилам:

$$u + v = (a, x) + (b, y) := (a + b, x * y), \quad \lambda \star v = \lambda \star (a, x) := (\lambda a, x).$$

Аксиома 1 не выполнена, т. к. $*$ неассоциативна. Выполнение аксиом 2-4 следует из того, что они выполняются для $+$ над \mathbb{R} и $*$ над M . Проверим выполнение остальных аксиом:

$$\begin{aligned} 5: & \quad \lambda \star (a + b, x * y) = (\lambda(a + b), x * y) = (\lambda a + \lambda b, x * y) = (\lambda a, x) + (\lambda b, y) = \lambda \star ((a, x) + (b, y)) \\ 6: & \quad (\lambda + \mu) \cdot (a, x) = ((\lambda + \mu)a, x) = (\lambda a + \mu a, x * x) = (\lambda a, x) + (\mu a, x) = \lambda \star (a, x) + \mu \star (a, x) \\ 7: & \quad (\lambda \mu) \star (a, x) = (\lambda \mu a, x) = \lambda \star (\mu a, x) \\ 8: & \quad 1 \star (a, x) = (1 \cdot a, x) = (a, x) \end{aligned}$$

- **2 аксиома.** Без второй аксиомы нельзя ввести третью, поэтому её удаление не имеет смысла.
- **3 аксиома.** Рассмотрим алгебраическую систему $V = (\mathbb{R} \cup \{\infty\}, +, \cdot)$. Доопределим сложение и умножение для ∞ следующим образом:

$$\infty + a = a + \infty := \infty, \quad \lambda \cdot \infty := \infty.$$

Выполнение аксиом 1, 2 и 4 сразу вытекает из определения. Аксиома 3 не выполнена, т. к. у ∞ нет обратного по $+$. Выполнение аксиом 5-8 проверяется перебором нескольких случаев.

- **6 аксиома.** Рассмотрим алгебраическую систему $V = (\mathbb{R}, +, \star)$, в которой сложение определено так же, как в действительных числах, а умножение так:

$$\lambda \star v := v.$$

Аксиомы 1-4 выполнены, т. к. они выполнены для \mathbb{R} и $+$. Выполнение аксиом 5, 7 и 8 сразу вытекает из определения. Аксиома 6 не выполнена:

$$u + u = 1 \star u + 1 \star u, \quad (1 + 1) \star u = u.$$

- **7 аксиома.** Рассмотрим \mathbb{R} как векторное пространство над полем \mathbb{Q} с базисом $M \supset \{1, \sqrt{2}\}$. Пусть отображение $f : \mathbb{R} \rightarrow \mathbb{R}$ задаётся своими значениями на числах из M , а для других чисел определяется соотношением

$$f(q_1 v_1 + q_2 v_2 + \dots + q_n v_n) = q_1 f(v_1) + q_2 f(v_2) + \dots + q_n f(v_n),$$

где v_i — некоторые векторы из базиса M . Такое отображение является линейным, сохраняющим все рациональные числа.

Теперь возьмём алгебраическую систему $V = (\mathbb{R}, +, \star)$, в которой сложение $+$ определено естественным образом, а умножение \star определяется через f и естественное умножение \cdot :

$$\lambda \star u := f(\lambda) \cdot u.$$

Аксиомы 1-4 выполнены, т. к. они выполнены для \mathbb{R} и $+$. Выполнение аксиомы 5 проверяется непосредственно. Аксиома 6 выполнена, т. к. отображение f линейно. Проверим, что аксиома 7 не выполнена:

$$\sqrt{2} \star (\sqrt{2} \star u) = \sqrt{2} \star u = u, \quad (\sqrt{2} \star \sqrt{2}) \star u = 2u.$$

Выполнение аксиомы 8 вытекает из определения.

- **8 аксиома.** Рассмотрим алгебраическую систему $V = (\mathbb{R}, +, \star)$, в которой сложение определено естественным образом, а умножение так:

$$\lambda \star u := 0.$$

Аксиомы 1-4 выполнены, т. к. они выполнены для \mathbb{R} и $+$. Выполнение аксиом 5, 6 и 7 проверяется непосредственно. Аксиома 8 не выполнена.

Теорема 4.1. Множество строк \mathcal{K}^n является векторным пространством.

Доказательство. Легко видеть, что для него выполняется каждая из аксиом. ■

Теорема 4.2 (Свойства векторного пространства).

1. В любом векторном пространстве нулевой вектор единственный
2. Для любого вектора v противоположный вектор $-v$ единственный
3. Для любого вектора выполнено $0 \cdot v = 0$
4. Для любого числа λ выполнено $\lambda \cdot 0 = 0$
5. Для любого вектора v выполнено $(-1) \cdot v = -v$
6. Для любого вектора v выполнено $-(-v) = v$
7. Для любых векторов u и v $-(u + v) = (-u) + (-v)$
8. $\lambda v = 0 \Rightarrow (\lambda = 0) \wedge (v = 0)$

Доказательство.

1. Пусть есть два нулевых вектора — 0_1 и 0_2 . Тогда $0_1 + 0_2 = 0_1$ с одной стороны (т.к. 0_2 нулевой) и $0_1 + 0_2 = 0_2$ (т.к. 0_1 нулевой). Отсюда $0_1 = 0_2$.
2. Пусть таких векторов два: $(-v)_1$ и $(-v)_2$. Тогда имеем

$$(-v)_1 = \underbrace{(-v)_1 + v}_{=0} + (-v)_2 = (-v)_2.$$

3. Доказывалось ранее.
4. $\lambda \cdot 0 = \lambda \cdot (0 + 0) = \lambda \cdot 0 + \lambda \cdot 0$. Вычитая $\lambda \cdot 0$ из обеих частей равенства, получаем требуемое.
5. Доказывалось ранее.
6. $-(-v) + (-v) = (-1) \cdot (-v) + (-1) \cdot v = (-1) \cdot \underbrace{(-v + v)}_{=0} = 0$
7. $-(u + v) = (-1) \cdot (u + v) = (-1)u + (-1)v = (-u) + (-v)$.
8. Допустим, $\lambda \neq 0$. Тогда существует число $1/\lambda \neq 0$. Имеем

$$0 = \frac{1}{\lambda} 0 = \frac{1}{\lambda} (\lambda v) = \left(\frac{1}{\lambda} \cdot \lambda \right) v = v.$$

■

Определение 4.3. Подмножество U векторного пространства V над полем \mathcal{K} называется **подпространством** в V , если оно является векторным пространством над полем \mathcal{K} .

Теорема 4.3 (Критерий подпространства). Подмножество U векторного пространства V над полем \mathcal{K} является подпространством тогда и только тогда, когда:

1. $\forall u_1, u_2 \in U \ (u_1 + u_2) \in U$
2. $\forall u \in U, \lambda \in \mathcal{K} \ \lambda u \in U$

Доказательство. \Rightarrow . Пусть U — подпространство в V . Тогда сумма двух его элементов лежит снова в U и умножение любого элемента на число лежит в U .

\Leftarrow . Наоборот, пусть выполнены условия теоремы. Тогда выполнение аксиом 1, 4-8 сразу следует из того, что они выполнены над V . Чтобы доказать справедливость аксиомы 2, нужно, чтобы $0 \in V$. Это так в силу того, что $U \ni 0 \cdot u = 0$. А для выполнения аксиомы 3 требуется, что $\forall u \in U \ (-u) \in U$. Это выполнится, т.к. $U \ni (-1) \cdot u = -u$. ■

5 Понятие линейной зависимости системы векторов. Три свойства линейной зависимости

Определение 5.1. Пусть v_1, \dots, v_k — векторы из векторного пространства V , а $\lambda_1, \dots, \lambda_k$ — элементы поля \mathcal{K} . Тогда **линейной комбинацией** векторов v_1, \dots, v_k с коэффициентами $\lambda_1, \dots, \lambda_k$ — это выражение

$$\lambda_1 v_1 + \dots + \lambda_k v_k.$$

При $\lambda_1 = \dots = \lambda_k = 0$ линейная комбинация называется **тривиальной**.

Определение 5.2. Конечная система векторов называется **линейно зависимой**, если существует нетривиальная нулевая линейная комбинация. Бесконечная система векторов называется **линейно зависимой**, если в ней можно выделить конечную линейно зависимую подсистему. Система векторов называется **линейно независимой**, если она не линейно зависима.

Теорема 5.1 (Три свойства линейной зависимости).

1. Пусть \mathcal{S} и \mathcal{S}' — две системы векторов, причём $\mathcal{S} \subseteq \mathcal{S}'$. Тогда если \mathcal{S} линейно зависима, то и \mathcal{S}' линейно зависима.
2. Система V линейно зависима тогда и только тогда, когда в ней есть вектор v , который линейно выражается через остальные.
3. Пусть система V линейно независима, а система $V \cup \{u\}$ линейно зависима. Тогда существует единственный набор элементов поля \mathcal{K} : μ_1, \dots, μ_k такой, что $u = \mu_1 v_1 + \dots + \mu_k v_k$, где $\{v_1, \dots, v_k\} \subseteq V$ (равенство достигается для конечной системы).

Примечание. Свойство 2, как видно, из формулировки, является критерием линейной зависимости.

Доказательство. Докажем сначала для конечных систем:

1. $\mathcal{S} = \{v_1, \dots, v_k\}$ линейно зависима, поэтому в ней есть вектор u , выражающийся линейно через некоторые векторы v_1, \dots, v_k . Однако заметим, что $\{u, v_1, \dots, v_k\} \subseteq \mathcal{S} \subseteq \mathcal{S}'$. Поэтому u выражается через векторы системы \mathcal{S}' : коэффициенты при v_1, \dots, v_k не меняем, а коэффициенты при остальных векторах выбираем нулевыми.
2. $V = \{v_1, \dots, v_k\}$ линейно зависима, значит, существует нетривиальная линейная комбинация, такая что

$$\lambda_1 v_1 + \dots + \lambda_k v_k = 0, \quad (\lambda_1, \dots, \lambda_k) \neq (0, \dots, 0).$$

Существует j такой, что $\lambda_j \neq 0$, поэтому можно выразить v_j :

$$v_j = \sum_{i \neq j} \left(-\frac{\lambda_i}{\lambda_j} \right) v_i.$$

Обратно, пусть существует вектор $v_j = \sum_{i \neq j} \lambda_i v_i$. Тогда

$$\lambda_1 v_1 + \dots + (-1)v_j + \dots + \lambda_k v_k = 0.$$

Эта линейная комбинация нетривиальная, т.к. $-1 \neq 0$.

3. Существует нетривиальная линейная комбинация

$$\lambda_1 v_1 + \dots + \lambda_k v_k + \mu u = 0 \tag{*}$$

При этом $\mu \neq 0$, т.к. иначе останется линейная комбинация $\lambda_1 v_1 + \dots + \lambda_k v_k = 0$, а она обязательно тривиальная (т.к. система $\{v_1, \dots, v_k\}$ линейно независима), а поэтому и комбинация (*) тривиальная. Итак, $\mu \neq 0$, поэтому можно так же, как в пункте 2, выразить его через остальные:

$$u = \sum_i \left(-\frac{\lambda_i}{\mu} \right) v_i.$$

А теперь — для бесконечных:

1. \mathcal{S} линейно зависима, а значит, в ней можно выделить конечную линейно зависимую подсистему. А из того, что $\mathcal{S}' \supseteq \mathcal{S}$, в \mathcal{S}' можно выделить эту же линейно зависимую подсистему.
2. Выделим в V конечную линейно зависимую систему и применим утверждение теоремы для неё.
3. Выделим в $V \cup \{u\}$ линейно зависимую подсистему и применим утверждение теоремы для неё.

■

6 Однородные системы с количеством неизвестных большим количеством уравнений. Основная лемма о линейной зависимости

Определение 6.1. СЛУ называется однородной, если свободные члены во всех уравнениях равны нулю.

Примечание. Однородные СЛУ всегда совместны, в качестве решения подходит строка $(0, \dots, 0) \in \mathcal{K}^n$.

Лемма 6.1. Если в однородной системе неизвестных больше, чем уравнений, то она имеет ненулевое решение.

Доказательство. Количество главных переменных равно количеству лидеров, а оно, в свою очередь, не превышает количества уравнений (строк матрицы коэффициентов), а оно меньше количества неизвестных. Значит, количество главных переменных меньше количества всех переменных, значит, среди переменных есть свободные, т. е. решений этой системы бесконечно много. Среди них можно выбрать ненулевое. ■

Лемма 6.2 (Основная лемма о линейной зависимости). Пусть $\{v_1, \dots, v_n\}$ и $\{u_1, \dots, u_m\}$ — две системы векторов из V . Допустим, что каждый вектор v_i линейно выражается через систему векторов $\{u_1, \dots, u_m\}$ и при этом $n > m$. Тогда система $\{v_1, \dots, v_n\}$ линейно зависима.

Доказательство. Из условия, существуют такие λ_{ij} , что

$$v_i = \sum_{j=1}^m \lambda_{ij} u_j.$$

Составим линейную комбинацию

$$\sum_{i=1}^n \mu_i v_i = \sum_{i=1}^n \left(\mu_i \sum_{j=1}^m \lambda_{ij} u_j \right) = \sum_{i=1}^n \sum_{j=1}^m (\mu_i \lambda_{ij} u_j) = \sum_{j=1}^m \sum_{i=1}^n (\mu_i \lambda_{ij} u_j) = \sum_{j=1}^m \left(\sum_{i=1}^n \mu_i \lambda_{ij} \right) u_j.$$

Эта линейная комбинация (уж точно) равна нулю, если $\sum_{i=1}^n \mu_i \lambda_{ij} = 0 \forall j$. Докажем, что мы можем подобрать подходящие μ_i . Имеем однородную СЛУ с переменными μ_i (n штук) и коэффициентами λ_{ij} (m штук), причём $n > m$, значит (по предыдущей лемме), у этой системы есть ненулевое решение. Итак, существуют такие коэффициенты μ_i , не все равные нулю, что $\mu_1 v_1 + \dots + \mu_n v_n = 0$. ■

7 Решения однородной системы образуют подпространство. Линейная оболочка: определение и доказательство того, что это подпространство

Теорема 7.1. Совокупность всех решений системы однородных линейных уравнений с n неизвестными является подпространством пространства \mathcal{K}^n .

Доказательство. Рассмотрим произвольную систему однородных линейных уравнений:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = 0, \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0, \end{cases}$$

Очевидно, что нулевая строка является её решением и что произведение любого решения на число также является решением. Докажем, что сумма решений (u_1, \dots, u_n) и (v_1, \dots, v_n) является решением. Подставляя её компоненты в i -ое уравнение системы, получаем:

$$a_{i1}(u_1 + v_1) + \dots + a_{in}(u_n + v_n) = \underbrace{a_{i1}u_1 + \dots + a_{in}u_n}_{=0} + \underbrace{a_{i1}v_1 + \dots + a_{in}v_n}_{=0} = 0.$$

■

Теорема 7.2. Совокупность всех решений произвольной совместной системы линейных уравнений есть сумма какого-либо одного её решения и подпространства решений системы однородных линейных уравнений с той же матрицей коэффициентов.

Доказательство. Пусть $u \in \mathcal{K}^n$ — какое-либо фиксированное решение системы

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2, \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m, \end{cases} \quad (*)$$

Аналогично предыдущему доказывается, что сумма решения u и произвольного решения однородной системы является решением системы (*). Обратно, если u' — любое решение системы (*), то $v = u' - u$ — решение однородной системы. ■

Примечание (из Винберга). Неопределённые системы линейных уравнений могут иметь различную «степень неопределённости», каковой естественно считать число свободных неизвестных в общем решении системы. Однако одна и та же система линейных уравнений может допускать различные общие решения, в которых разные неизвестные играют роль свободных, и закономерен вопрос, будет ли число свободных неизвестных всегда одним и тем же. Положительный ответ на этот вопрос даётся с помощью понятия размерности векторного пространства.

Определение 7.1. Пусть $S \subset V$ (V — векторное пространство). Совокупность всевозможных линейных комбинаций векторов из S называется **линейной оболочкой** множества S и обозначается через $\langle S \rangle$. Говорят, что пространство V **порождается** множеством S , если $\langle S \rangle = V$.

Определение 7.2. Пространство называется **конечномерным**, если оно порождается конечным количеством векторов и **бесконечномерным**, если оно порождается бесконечным количеством векторов.

Примечание. Я не заметил важной ремаки в конспектах Сергей Александровича — в курсе мы считаем вообще все пространства конечномерными. С бесконечномерными возникают большие проблемы — у нас даже нет определения линейной зависимости для бесконечного количества векторов. В дальнейшем мы будем доказывать утверждения для конечных систем, подразумевая, что для бесконечных они тоже верны (чаще всего достаточно убрать верхний предел суммирования). Цитата из Винберга по этому поводу: «Понятия базиса и размерности могут быть перенесены на бесконечномерные векторные пространства. Чтобы это сделать, надо определить, что такое линейная комбинация бесконечной системы векторов. В чисто алгебраической ситуации нет иного выхода, кроме как ограничиться рассмотрением линейных комбинаций, в которых лишь конечное число коэффициентов отлично от нуля». И далее следует определение линейной комбинации для бесконечной системы векторов как выражение вида $\sum_{i \in I} \lambda_i a_i$, в котором лишь конечное число

коэффициентов λ_i отлично от нуля, так что сумма фактически является конечной и, таким образом, имеет смысл. Потом можно определить и линейную зависимость, и базис, и т. д. Но понятно, что так решается проблема только для счётных множеств. Что делать с несчётными, неясно совсем.

Теорема 7.3. Пусть $S \subset V$ (V — векторное пространство). Тогда линейная оболочка $\langle S \rangle$ является подпространством в V .

Доказательство. По теореме 4.2 достаточно проверить, что линейная оболочка замкнута относительно операций сложения векторов и умножения вектора на число. Это сразу следует из определения. ■

Утверждение (упражнение из Винберга). $\langle S \rangle$ — это наименьшее подпространство в V , содержащее S .

Доказательство. Предположим, что из $\langle S \rangle$ можно убрать элемент $v' = \lambda_1 v_1 + \dots + \lambda_k v_k$. Но мы можем сконструировать v' из v_1, \dots, v_k с помощью операций умножения на число и сложения векторов, поэтому (из теоремы 4.2) он должен лежать в подпространстве. Противоречие. Значит, никакой элемент $\langle S \rangle$ нельзя убрать, чтобы оно осталось подпространством. ■

8 Базис системы векторов: эквивалентность 4 определений. Стандартный базис в \mathbb{R}^n . Дополнение линейно независимой системы до базиса. Выбор базиса из полной системы

Определение 8.1. Подсистема $L \subseteq S$ называется **полной**, если любой вектор из S является линейной комбинацией векторов из L .

Утверждение. $L \subseteq S$ полна тогда и только тогда, когда $\langle L \rangle = \langle S \rangle$.

Доказательство. \Rightarrow . Заметим, что $\langle L \rangle \subseteq \langle S \rangle$ (просто потому что $L \subseteq S$). Любой вектор из S является линейной комбинацией векторов из L , а значит, линейные комбинации векторов из S также являются линейными комбинациями векторов из L . А это значит, что $\langle S \rangle \subseteq \langle L \rangle$. Отсюда получаем $\langle L \rangle = \langle S \rangle$.

\Leftarrow . Каждый вектор из S принадлежит линейной оболочке S (просто потому что $S \subseteq \langle S \rangle$). А т. к. $\langle S \rangle = \langle L \rangle$, то этот вектор принадлежит линейной оболочке L , т. е. линейно выражается через векторы из L . ■

Теорема 8.1. Пусть B — подсистема векторов в системе S . Тогда следующие условия эквивалентны:

1. B — максимальная по включению линейно независимая подсистема векторов из S ;
2. B — полная линейно независимая подсистема векторов из S ;
3. B — минимальная по включению полная подсистема векторов из S ;
4. Каждый вектор из S линейно выражается через векторы из B , причём единственным образом.

Определение 8.2. Подсистема подмножества векторного пространства, удовлетворяющая условиям предыдущей теоремы, называется **базисом** этого подмножества.

Доказательство. Докажем, что из каждого следующего пункта следует предыдущий:

$1 \Rightarrow 2$. Пусть B — базис. Тогда B линейно независима, нужно лишь доказать, что B — полная подсистема. Возьмём $v \in S \setminus B$. Тогда система $B \cup \{v\}$ линейно зависима по определению базиса. По свойству линейной зависимости, вектор v является линейной комбинацией векторов из B . Значит, система B полна по определению.

$2 \Rightarrow 3$. По условию система B полная. Допустим, что для некоторого $v \in B$ система $B \setminus \{v\}$ также является полной. То есть, найдутся такие $e_1, \dots, e_k \in B$ и $\lambda_1, \dots, \lambda_k \in \mathcal{K}$, что $v = \sum_{i=1}^k \lambda_i e_i$. Но тогда B линейно зависима (по критерию линейной зависимости).

$3 \Rightarrow 4$. Пусть B — минимальная по включению полная подсистема. Тогда по определению полной подсистемы каждый вектор из S линейно выражается через B . Допустим, что есть вектор $v \in S$, такой что он выражается двумя различными способами

$$v = \sum_{i=1}^n \lambda_i e_i = \sum_{i=1}^n \mu_i e_i, \quad e_i \in B, \lambda_i, \mu_i \in \mathcal{K}.$$

Получаем $0 = \sum_{i=1}^n (\lambda_i - \mu_i) e_i$ — нетривиальная линейная комбинация. По критерию линейной зависимости, найдётся e_j , который выражается через остальные. Тогда система $B \setminus \{e_j\}$ полная. Получили противоречие с её минимальностью.

$4 \Rightarrow 1$. Допустим, что B линейно зависима. Тогда по критерию линейной зависимости существует $v \in B$, такой что

$$v = \sum_{i=1}^n \lambda_i e_i, \quad e_i \in B \setminus \{v\}, \lambda_i \in \mathcal{K}.$$

Получаем два линейных выражения v через B (второе имеет вид $v = 1 \cdot v$). Противоречие, значит, B линейно независима. Докажем теперь, что она максимальна по включению. Рассмотрим $u \in S \setminus B$. По условию, вектор u линейно выражается через B . Тогда по критерию линейной зависимости $B \cup \{u\}$ линейно зависима. ■

Определение 8.3. Пусть $\{e_1, \dots, e_k\}$ — базис векторного пространства V и $v = v_1 e_1 + v_2 e_2 + \dots + v_k e_k$. Тогда

столбец $\begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix}$ называется **координатами** вектора v в базисе $\{e_1, \dots, e_k\}$. Так как $V \sim K^k$, то можно писать

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix}.$$

Определение 8.4. Размерностью конечномерного векторного пространства V называется число векторов $\dim V$ в его базисе.

Теорема 8.2. Определение выше корректно. Иными словами, все базисы конечномерного векторного пространства V содержат одно и то же число векторов.

Доказательство. Если бы в пространстве V существовали два базиса из разного числа векторов, то тот из них, в котором больше векторов, был бы линейно зависим по основной лемме. ■

Утверждение (задача из Винберга). Число базисов n -мерного векторного пространства над полем из q элементов равно

$$\prod_{k=0}^{n-1} (q^n - q^k).$$

Доказательство. Всего у нас в таком пространстве q^n векторов. Нам нужно выбрать среди них q линейно независимых, они и будут базисом. Для выбора первого вектора есть $q^n - 1$ возможностей, нам подходят все, кроме нулевого. Для выбора второго — $q^n - q$, нам подходят все, кроме коллинеарных первому, а таких q . И так далее посчитаем искомую величину для $k - 1$ векторов. Теперь, чтобы посчитать количество способов выбрать k -ый линейно независимых вектор, посчитаем количество способов выбрать k -ый линейно зависимый вектор и вычтем из общего количества векторов. Итак, мы знаем, что система из $k - 1$ выбранных векторов линейно независима, а из k — линейно зависима. Отсюда (по третьему свойству линейной зависимости) k -ый вектор выражается через остальные единственным образом. А коэффициентов в этом выражении можно выбрать q^{k-1} штук (по q для каждого из $k - 1$ векторов). Итак, количество возможностей выбрать k -ый вектор линейно независимым равняется $q^n - q^{k-1}$. Теперь считаем ответ по правилу произведения (эти выборы не зависят друг от друга) и получаем требуемое. ■

Определение 8.5. Стандартным базисом в K^n называется базис, состоящий из строк единичной матрицы размера $n \times n$.

Примечание. Можете посмотреть интересные задачи 5-9 в Винберге, мне лень оформлять их решения.

Теорема 8.3. В конечномерном пространстве любую линейно независимую систему можно дополнить до базиса.

Доказательство. Пусть $\{e_1, \dots, e_k\}$ — конечная подсистема в V . Тогда, если эта система максимальная по включению, то она базис. Иначе существует $e_{k+1} \in V$ такой, что система $\{e_1, \dots, e_k, e_{k+1}\}$ линейно независима. Продолжая процесс далее, получим базис (в силу конечномерности пространства V). ■

Теорема 8.4. Из любой конечной полной подсистемы S (в которой есть ненулевой вектор) можно выбрать базис S .

Доказательство. Воспользуемся тем, что базис — минимальная по включению полная подсистема. Пусть нам дана полная конечная подсистема $\{v_1, \dots, v_n\}$. Если её можно уменьшить (выкинуть один из векторов) так, чтобы система осталась полной, то сделаем это. Иначе она уже базис. А т.к. система конечна, мы не можем бесконечно её уменьшать. Поэтому через конечное число шагов дойдём до непустой (т.к. в S был ненулевой вектор) минимальной по включению полной системы, т.е. до базиса. ■

Теорема 8.5 (Свойство монотонности размерности). Всякое подпространство U конечномерного векторного пространства V также конечномерно, причём $\dim U \leq \dim V$. Более того, если $U \neq V$, то $\dim U < \dim V$.

Доказательство. Пусть $\{e_1, \dots, e_k\}$ — базис подпространства U , т.е. максимальная по включению линейно независимая система векторов из этого подпространства. Тогда $\dim U = k$. Линейно независимую систему $\{e_1, \dots, e_k\}$ можно дополнить до базиса всего пространства V . Следовательно, если $U \neq V$, то $\dim V > k$. ■

Лемма 8.1. Всякое векторное пространство V над полем \mathcal{K} изоморфно пространству $\mathcal{K}^{\dim V}$.

Доказательство. Пусть $\{e_1, \dots, e_n\}$ — базис пространства V ($n := \dim V$). Рассмотрим отображение

$$\varphi : V \rightarrow K^n,$$

ставящее в соответствие каждому вектору строку из его коэффициентов в линейном разложении в базисе $\{e_1, \dots, e_n\}$. Иными словами,

$$\sum_{i=1}^n x_i e_i \mapsto (x_1, \dots, x_n).$$

Очевидно, что оно биективно (т.к. каждый вектор линейно выражается через базисные единственным образом). Легко убедиться и в том, что такое отображение линейно. А значит, это изоморфизм. ■

Теорема 8.6 (из Винберга). Конечномерные векторные пространства над одним и тем же полем изоморфны тогда и только тогда, когда они имеют одинаковую размерность.

Доказательство. Если $f : V \rightarrow U$ — изоморфизм векторных пространств и $\{e_1, \dots, e_k\}$ — базис пространства V , то $\{f(e_1), \dots, f(e_k)\}$ — базис пространства U (образ базиса является базисом образа) в силу линейности функции f :

$$f\left(\sum_i \lambda_i e_i\right) = \sum_i \lambda_i f(e_i).$$

Так что, $\dim U = \dim V$. Обратно, согласно предыдущей лемме, всякое n -мерное пространство изоморфно \mathcal{K}^n , а значит, они изоморфны между собой. ■

9 Ранг системы векторов и размерность векторного пространства. Связь ранга системы и размерности линейной оболочки. Строчный, столбцовый и ступенчатый ранги матрицы, их совпадение

Определение размерности векторного пространства было дано ранее (определение 8.3).

Определение 9.1. Рангом системы векторов называется размерность её линейной оболочки.

Ранее доказывалось (теорема 8.2), что это определение корректно.

Определение 9.2. Системы векторов $\{a_1, \dots, a_n\}$ и $\{b_1, \dots, b_m\}$ называются **эквивалентными**, если каждый из векторов b_j линейно выражается через a_1, \dots, a_n и, наоборот, каждый из векторов a_i линейно выражается через b_1, \dots, b_m .

Лемма 9.1. Ранги эквивалентных систем векторов равны.

Доказательство. Каждый вектор из $\{a_1, \dots, a_n\}$ линейно выражается через векторы из $\{b_1, \dots, b_m\}$, значит, линейные комбинации вида $\sum_i \lambda_i a_i$ тоже линейно выражаются через векторы из $\{b_1, \dots, b_m\}$. Отсюда $\langle a_1, \dots, a_n \rangle \subseteq \langle b_1, \dots, b_m \rangle$. Аналогично доказывается обратное, а отсюда

$$\langle a_1, \dots, a_n \rangle = \langle b_1, \dots, b_m \rangle$$

А из равенства линейных оболочек очевидно вытекает равенство их размерностей. ■

Определение 9.3. Строчным рангом матрицы A называется ранг системы её строк, столбцовым рангом — ранг системы её столбцов.

Теорема 9.1. Строчный, столбцовый и ступенчатый ранги совпадают.

Сначала докажем две вспомогательные леммы.

Лемма 9.2. Каждый вид ранга не меняется при элементарных преобразованиях строк.

Доказательство. Докажем утверждение отдельно для каждого вида ранга:

- **Строчный ранг.** Пусть мы пришли элементарным преобразованием от матрицы A к матрице A' . Очевидно, что системы строк этих матриц эквивалентны. А потому их ранги равны.
- **Столбцовый ранг.** Докажем, что линейные зависимости между столбцами матрицы не меняются при элементарных преобразованиях строк. Линейная зависимость между какими-то столбцами матрицы может пониматься как линейная зависимость между всеми её столбцами, в которую остальные столбцы входят с нулевыми коэффициентами. Следовательно, если какие-то столбцы матрицы линейно зависимы, то они останутся линейно зависимыми после любых элементарных преобразований строк. Так как элементарные преобразования обратимы, то и наоборот: если какие-то столбцы линейно независимы, то они и останутся линейно независимыми. Значит, если какие-то столбцы матрицы составляют максимальную линейно независимую систему её столбцов, то после любых элементарных преобразований строк столбцы с теми же номерами будут составлять максимальную линейно независимую систему столбцов полученной матрицы, и поэтому ранг матрицы не изменится.
- **Ступенчатый ранг.** Утверждение для него сразу следует из единственности улучшенного ступенчатого вида. ■

Лемма 9.3. В ступенчатом виде все виды ранга совпадают.

Доказательство. Докажем, что ненулевые строки образуют базис системы строк (т.е. просто, что они линейно независимы). Пусть лидеры имеют номера j_1, \dots, j_r . Уберём из системы ненулевых строк строку с номером i . Тогда из улучшенного ступенчатого вида матрицы, у оставшихся векторов j_i -ая координата равна 0, а значит, никакой их линейной комбинацией нельзя получить i -ую строку. Таким образом, система ненулевых строк — линейно независима и максимальна по включению (остальные строки нулевые), а значит, является базисом.

Теперь докажем, что столбцы с номерами j_1, j_2, \dots, j_r образуют базис системы столбцов. Действительно, эта система полна и минимальна по включению, то есть, базис.

Ступенчатый ранг матрицы равен количеству её ненулевых строк, что, в свою очередь, равно строчному рангу. Также, ступенчатый ранг равен количеству главных переменных, а это, как мы показали, и есть столбцовый ранг. ■

Теперь совсем легко доказать теорему 9.1:

Доказательство. Приведём матрицу к улучшенному ступенчатому виду, каждый вид ранга при этом не изменится. А в улучшенном ступенчатом виде все ранги совпадают. ■

10 Свойства ранга матрицы. Теорема Кронекера — Капелли. Критерий определённости системы

Определение 10.1. Пусть A — матрица $m \times n$. Матрица $B = A^T$ размера $n \times m$ называется **транспонированной** к матрице A , если

$$b_{ij} = a_{ji}.$$

Примечание. Ясно, что $(A^T)^T = A$.

Теорема 10.1 (Свойства ранга матрицы). Пусть A — матрица $m \times n$. Тогда

1. $\text{rk } A \leq \min\{m, n\}$
2. $\text{rk } A = \text{rk } A^T$
3. Если к матрице добавить k столбцов (строк), то ранг не уменьшится и увеличится не более, чем на k

Доказательство.

1. $\text{rk } A$ равен рангу системы S строк матрицы A , т. е. $\dim\langle S \rangle$. Система S , очевидно, полна в $\langle S \rangle$, а значит, из неё можно выделить базис, в нём будет не больше векторов, чем в исходной системе, т. е. не больше m . Аналогично доказывается $\text{rk } A \leq n$.
2. Ранг системы строк A равен рангу системы столбцов A^T (это одна и та же система).
3. Базис системы строк (столбцов) матрицы A — это линейно независимая система. Значит, в новой матрице её можно дополнить до базиса. Другие строки матрицы A в него уже не попадут (они образуют линейно зависимую систему со старым базисом), поэтому в него могут добавиться только новые строки.

■

Теорема 10.2 (Кронекер — Капелли). СЛУ совместна тогда и только тогда, когда ранг матрицы её коэффициентов равен рангу расширенной матрицы её коэффициентов.

Доказательство. Приведём расширенную матрицу коэффициентов к улучшенному ступенчатому виду (ранг и совместность СЛУ при этом не меняются).

⇒. Если СЛУ совместна, то в ней нет экзотических уравнений, т. е. нет лидеров в последнем столбце матрицы. А, как мы доказывали ранее, базис системы столбцов состоит из тех столбцов, в которых есть лидеры. Поэтому последний столбец расширенной матрицы выражается линейно через базис системы столбцов матрицы коэффициентов. Значит, их ранги равны.

⇐. Если ранг матрицы коэффициентов равен рангу расширенной матрицы, то последний столбец расширенной матрицы линейно выражается через базис системы столбцов матрицы коэффициентов (иначе нужно было бы добавить его в базис и ранг расширенной матрицы был бы больше на 1). А значит, экзотических уравнений нет, и система совместна.

■

Теорема 10.3 (Критерий определённости системы). Совместная система линейных уравнений является определённой тогда и только тогда, когда ранг матрицы её коэффициентов равен числу неизвестных.

Доказательство. Ранг матрицы коэффициентов равен количеству ненулевых строк в ступенчатом виде, т. е. количеству главных переменных. Условие теоремы равносильно тому, что главных переменных столько же, сколько всех переменных, т. е. тому, что система определена.

■

11 Фундаментальная система решений и алгоритм её поиска. Размерность пространства решений однородной СЛУ. Структура решений неоднородной СЛУ

Определение 11.1. Фундаментальная система решений — это базиса подпространства решений однородной СЛУ.

Примечание. Доказательство следующей теоремы даёт практический способ построения ФСР.

Теорема 11.1. Размерность пространства решений системы однородных линейных уравнений с n неизвестными и матрицей коэффициентов A равна $n - \text{rk } A$.

Доказательство. Рассмотрим систему уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = 0, \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0, \end{cases}$$

С помощью элементарных преобразований приведём её к ступенчатому виду. Число ненулевых уравнений в этом ступенчатом виде равно $r = \text{rk } A$. Поэтому общее решение будет содержать r главных неизвестных и

с точностью до перенумерации неизвестных будет иметь вид

$$\begin{cases} x_1 = c_{11}x_{r+1} + c_{12}x_{r+2} + \dots + c_{1,n-r}x_n, \\ x_2 = c_{21}x_{r+1} + c_{22}x_{r+2} + \dots + c_{2,n-r}x_n, \\ \dots \\ x_r = c_{r1}x_{r+1} + c_{r2}x_{r+2} + \dots + c_{r,n-r}x_n. \end{cases}$$

Придавая поочерёдно одному из свободных неизвестных $x_{r+1}, x_{r+2}, \dots, x_n$ значение 1, а остальным — 0, получим следующие решения системы:

$$\begin{aligned} u_1 &= (c_{11}, c_{21}, \dots, c_{r1}, 1, 0, \dots, 0), \\ u_2 &= (c_{12}, c_{22}, \dots, c_{r2}, 0, 1, \dots, 0), \\ &\dots \\ u_{n-r} &= (c_{1,n-r}, c_{2,n-r}, \dots, c_{r,n-r}, 0, 0, \dots, 0, 1). \end{aligned}$$

Ранг системы векторов $\{u_1, u_2, \dots, u_{n-r}\}$ равен рангу матрицы

$$\left(\begin{array}{cccc|cccc} c_{11} & c_{21} & \dots & c_{r1} & 1 & 0 & \dots & 0 \\ c_{12} & c_{22} & \dots & c_{r2} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{1,n-r} & c_{2,n-r} & \dots & c_{r,n-r} & 0 & 0 & \dots & 1 \end{array} \right)$$

Элементарные преобразования столбцов (как и элементарные преобразования строк) сохраняют ранг матрицы. Заметим, что поменяв местами «блоки», отделённые друг от друга чертой, мы приведём матрицу к улучшенному ступенчатому виду. Как можно видеть, все её строки в улучшенном ступенчатом виде ненулевые, а потому, во-первых, ранг этой матрицы равен количеству строк, т.е. $n - r$, а во-вторых, система $\{u_1, \dots, u_{n-r}\}$ линейно независима. Также, эта система полна, т.к. любая линейная комбинация вида

$$\lambda_1 u_1 + \dots + \lambda_{n-r} u_{n-r}$$

является решением, в котором свободные неизвестные имеют значения $\lambda_1, \dots, \lambda_{n-r}$. ■

Структура решений неоднородной СЛУ — это теорема 7.2.

12 Линейное отображение. Его матрица в фиксированных базисах. Образ заданного вектора. Изоморфизм. Любое конечномерное пространство изоморфно пространству строк

Определение 12.1. Отображение $\varphi : U \rightarrow V$ (U и V — векторные пространства) называется **линейным**, если $\varphi(u_1 + u_2) = \varphi(u_1) + \varphi(u_2)$ и $\varphi(\lambda u) = \lambda \varphi(u)$.

Определение 12.2. Фиксируем базис $e = \{e_1, \dots, e_n\}$ в U и базис $f = \{f_1, \dots, f_m\}$. Матрица $A(\varphi, e, f) = (a_{ij})$, по столбцам которой стоят координаты образов базисных векторов из e в базисе f , называется **матрицей линейного отображения** φ .

Примечание. Размеры матрицы линейного отображения — $m \times n$.

Утверждение. $\varphi(v) = A \cdot v$, где A — матрица линейного отображения φ .

Доказательство. С одной стороны,

$$\varphi(v) = \varphi\left(\sum_i^k v_i e_i\right) = \sum_i^k v_i \varphi(e_i).$$

А с другой стороны,

$$A \cdot v = \begin{pmatrix} f(e_1) & f(e_2) & \dots & f(e_k) \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix} = \sum_i^k v_i \varphi(e_i).$$

Отсюда сразу следует $\varphi(v) = A \cdot v$. ■

Про изоморфизмы было написано ранее: см. определение 4.2 и лемму 8.1.

13 Операции над линейными отображениями и над матрицами, связь между ними. Матричная запись СЛУ

Примечание. Здесь векторные пространства U, V, W взяты над одним полем \mathcal{K} и, говоря «число», имеем в виду произвольный элемент \mathcal{K} .

Определение 13.1 (Операции над линейными отображениями). Пусть $\varphi : U \rightarrow V, \psi : U \rightarrow V, \xi : V \rightarrow W$. Определим следующие операции над ними:

1. **Сумма.** $(\varphi + \psi)(u) := \varphi(u) + \psi(u)$. Проверим, что $\varphi + \psi$ линейно:

$$\begin{aligned} (\varphi + \psi)(u_1 + u_2) &= \varphi(u_1 + u_2) + \psi(u_1 + u_2) = \varphi(u_1) + \varphi(u_2) + \psi(u_1) + \psi(u_2) = (\varphi + \psi)(u_1) + (\varphi + \psi)(u_2), \\ (\varphi + \psi)(\lambda u) &= \varphi(\lambda u) + \psi(\lambda u) = \lambda(\varphi(u) + \psi(u)) = \lambda \cdot (\varphi + \psi)(u). \end{aligned}$$

2. **Умножение на число.** $(c\varphi)(u) = c \cdot \varphi(u)$. Нетрудно проверить, что $c\varphi$ линейно.
3. **Композиция.** $(\xi \circ \varphi)(u) = \xi(\varphi(u))$. Проверим линейность:

$$\begin{aligned} (\xi \circ \varphi)(u_1 + u_2) &= \xi(\varphi(u_1 + u_2)) = \xi(\varphi(u_1) + \varphi(u_2)) = \xi(\varphi(u_1)) + \xi(\varphi(u_2)) = (\xi \circ \varphi)(u_1) + (\xi \circ \varphi)(u_2), \\ (\xi \circ \varphi)(\lambda u) &= \xi(\varphi(\lambda u)) = \xi(\lambda \varphi(u)) = \lambda \xi(\varphi(u)) = \lambda(\xi \circ \varphi)(u). \end{aligned}$$

Определение 13.2 (Операции над матрицами). Пусть A, B и C — матрицы линейных преобразований φ, ψ и ξ соответственно в фиксированных базисах $e = \{e_1, \dots, e_n\}$ в U , $f = \{f_1, \dots, f_m\}$ в V , $s = \{s_1, \dots, s_k\}$ в W . Определим следующие операции над ними:

1. **Суммой матриц A и B** называется матрица преобразования $\varphi + \psi$. Обозначается $A + B$. Заметим, что суммировать можно лишь матрицы одинакового размера.
2. **Произведением числа λ и матрицы A** называется матрица преобразования $\lambda\varphi$. Обозначается λA .
3. **Произведением матриц C и A** называется матрица преобразования $\xi \circ \varphi$. Обозначается CA . Заметим, что умножать можно лишь матрицы размеров $k \times m$ и $m \times n$.

Утверждение. Формулы для операций над матрицами $A(\varphi, e, f) = (a_{ij})$ и $B(\psi, e, f) = (b_{ij})$ и $C(\xi, f, s) = (c_{ij})$ (обозначения — из предыдущих определений) пишутся так:

1. $(A + B)_{ij} = (a_{ij} + b_{ij})$ (при этом A и B $m \times n$);
2. $(\lambda A)_{ij} = (\lambda a_{ij})$;
3. $(CA)_{ij} = \sum_{t=1}^m c_{it} \cdot a_{tj}$ (при этом A и C $m \times n$ и $k \times m$);

Доказательство. Столбца матрицы линейного преобразования — это образы базисных векторов, поэтому чтобы понять, как выглядит матрица преобразования, достаточно посмотреть на то, куда переходит базис. Разберём отдельно все операции:

1. Сложение:

$$(\varphi + \psi)(e_j) = \varphi(e_j) + \psi(e_j) = \sum_{i=1}^m a_{ij} f_i + \sum_{i=1}^m b_{ij} f_i = \sum_{i=1}^m (a_{ij} + b_{ij}) f_i.$$

Коэффициенты при f_i и стоят в новой матрице на месте (i, j) . Таким образом, $(A + B)_{ij} = (a_{ij} + b_{ij})$.

2. Умножение на число:

$$(\lambda\varphi)(e_j) = \lambda \left(\sum_{i=1}^m a_{ij} f_i \right) = \sum_{i=1}^m (\lambda a_{ij}) f_i,$$

отсюда $(\lambda A)_{ij} = (\lambda a_{ij})$.

3. Произведение:

$$(\xi \circ \varphi)(e_j) = \xi \left(\sum_{t=1}^m a_{tj} f_t \right) = \sum_{t=1}^m a_{tj} \xi(f_t) = \sum_{t=1}^m a_{tj} \left(\sum_{i=1}^k c_{it} s_i \right) = \sum_{t=1}^m \sum_{i=1}^k a_{tj} c_{it} s_i = \sum_{i=1}^k \left(\sum_{t=1}^m c_{it} a_{tj} \right) s_i,$$

$$\text{отсюда } (CA)_{ij} = \sum_{t=1}^m c_{it} \cdot a_{tj}.$$

■

Теперь СЛУ с матрицей коэффициентов A , неизвестными $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ и свободными членами $B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$

можно записать так:

$$AX = B.$$

Теорема 13.1. Соответствие $\varphi \rightarrow A(\varphi, e, f)$ задаёт биекцию между линейными отображениями $U \rightarrow V$ и матрицами $m \times n$.

Доказательство. В курсе аналитической геометрии мы доказывали (см. билет про скалярное произведение в моём файле) теорему о том, что $f(*) = (u, *)$ — общий вид линейной функции. Причём, в доказательстве мы предъявляли вектор $u = (\varphi(e_1), \dots, \varphi(e_n))$. Отсюда сразу следует утверждение теоремы, ведь есть расписать координаты векторов $\varphi(e_i)$ в базисе f по столбцам, u станет в точности матрицей линейного преобразования φ в фиксированных базисах e и f . ■

14 Свойства операций над матрицами. Связь с транспонированием

Легко видеть, что биекция, существование которой доказывается в теореме 13.1, является линейным отображением (из определения операций над матрицами). Также легко видеть, что множество линейных отображений — это векторное пространство. А значит, и множество матриц фиксированного размера является векторным пространством. При этом, $\dim_{m \times n} \text{Mat} = mn$.

Теорема 14.1 (Свойства умножения матриц).

1. $(AB)C = A(BC)$
2. $A(B + C) = AB + AC$
3. $(A + B)C = AC + BC$
4. $\lambda(AB) = (\lambda A)B = A(\lambda B)$

Доказательство. В силу теоремы 13.1 нам достаточно показать эти свойства для соответствующих операций над линейными отображениями.

1. Пусть $\varphi : W \rightarrow L$, $\psi : V \rightarrow W$, $\xi : U \rightarrow V$. Тогда

$$((\varphi \circ \psi) \circ \xi)(u) = (\varphi \circ \psi)(\xi(u)) = \varphi(\psi(\xi(u))) = \varphi((\psi \circ \xi)(u)) = (\varphi \circ (\psi \circ \xi))(u),$$

$$\text{отсюда } (\varphi \circ \psi) \circ \xi = \varphi \circ (\psi \circ \xi).$$

2. Пусть $\varphi : V \rightarrow W$, $\psi : V \rightarrow W$ и $\xi : U \rightarrow V$. Тогда

$$((\varphi + \psi) \circ \xi)(u) = (\varphi + \psi)(\xi(u)) = \varphi(\xi(u)) + \psi(\xi(u)) = (\varphi \circ \xi)(u) + (\psi \circ \xi)(u).$$

3. Аналогично предыдущему пункту.

4. Пусть $\varphi : V \rightarrow W$, $\psi : U \rightarrow V$. Тогда

$$(\lambda(\varphi \circ \psi))(u) = \lambda\varphi(\psi(u)) = (\lambda\varphi \circ \psi)(u) = (\varphi \circ \lambda\psi)(u).$$

■

Теорема 14.2 (Связь с транспонированием).

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

Доказательство. Эти свойства докажем, расписав их по формулам, которые мы вывели ранее:

1. $(A + B)_{ij}^T = (A + B)_{ji} = a_{ji} + b_{ji} = (A^T + B^T)_{ij}$.
2. $(\lambda A)_{ij}^T = (\lambda A)_{ji} = (\lambda a_{ij})^T = \lambda a_{ji} = (\lambda A^T)_{ij}$.
3. $(AB)_{ij}^T = (AB)_{ji} = \sum_{t=1}^m b_{jt} a_{ti} = (B^T A^T)_{ij}$.

■

15 Вывод обобщённой ассоциативности для ассоциативной операции

Примечание. Здесь для удобства часто будем называть операцию умножением.

Определение 15.1. Ассоциативная операция называется **обобщённо ассоциативной**, если произведение любого количества сомножителей не зависит от расстановки скобок в этом произведении.

Определение 15.2. Назовём **стандартной** такую расстановку скобок, в которой операции выполняются слева направо.

Теорема 15.1. Ассоциативная операция всегда обобщённо ассоциативна.

Доказательство. Доказательство проведём индукцией по количеству множителей k :

База индукции ($k = 3$). Верно в силу ассоциативности.

Шаг индукции. Пусть для $k < n$ утверждение верно. Докажем его для $k = n$. Докажем, что для произвольной расстановки скобок результат будет таким же, как и для стандартной. Рассмотрим некоторую расстановку скобок в произведении $x_1 * \dots * x_n$. Пусть последнее умножение перемножает скобки A и B . Рассмотрим два случая:

1. $B = x_n$. Тогда для количество множителей в скобке A равно $n - 1 < n$, а потому по предположению индукции можем стандартно расставить скобки в ней. Но тогда и во всё выражении они будут расставлены стандартно и теорема доказана.
2. $B \neq x_n$. Внутри B по предположению индукции расстановку скобок можно принять стандартной, а потому $B = C * x_n$. А отсюда

$$A * B = A * (C * x_n) = (A * C) * x_n$$

из ассоциативности, и мы попали в предыдущий случай.

■

16 Верхние оценки на ранг суммы и произведения матриц

Антон Александрович задавал нам на дом вывести и нижние оценки, поэтому они здесь будут.

Утверждение. $|\text{rk } A - \text{rk } B| \leq \text{rk } (A + B) \leq \text{rk } A + \text{rk } B$.

Доказательство. Сначала докажем оценку сверху. Строки матрицы $A + B$ — это линейные комбинации строк матриц A и B . А значит, базис строк $A + B$ — линейно независимая система, линейно выражающаяся через базисы строк A и B . А значит, по основной лемме о линейной зависимости $\text{rk}(A + B) \leq \text{rk} A + \text{rk} B$.

Оценка снизу равносильна системе

$$\begin{cases} \text{rk} A - \text{rk} B \leq \text{rk}(A + B), \\ \text{rk} B - \text{rk} A \leq \text{rk}(A + B) \end{cases}$$

Докажем первое из неравенств системы, второе доказывается аналогично. Итак, из оценки сверху:

$$\text{rk}(A + B) + \text{rk} B = \text{rk}(A + B) + \text{rk}(-B) \leq \text{rk} A.$$

Перенеся слагаемые в нужные стороны, получим то, что хотели. ■

Примечание. $\text{rk} A = \text{rk}(\lambda A)$ ($\lambda \neq 0$), т. к. по сути умножение матрицы на ненулевое число — это умножение каждой из её строк на это число, а это преобразование является элементарным.

Утверждение. $\text{rk} A + \text{rk} B - n \leq \text{rk} AB \leq \min\{\text{rk} A, \text{rk} B\}$, где $A_{m \times n}$ и $B_{n \times k}$.

Лемма 16.1. Столбцы AB — линейные комбинации столбцов A с коэффициентами из столбцов B . Строки BA — это линейные комбинации строк B с коэффициентами из строк A .

Примечание. Далее за $X^{(i)}$ будем обозначать i -ый столбец матрицы X , а за $X_{(i)}$ — её i -ую строку.

Доказательство. Докажем утверждение непосредственным умножением:

$$(AB)^{(j)} = \begin{pmatrix} \sum_{t=1}^n a_{1t} b_{tj} \\ \sum_{t=1}^n a_{2t} b_{tj} \\ \vdots \\ \sum_{t=1}^n a_{mt} b_{tj} \end{pmatrix} = \sum_{t=1}^n b_{tj} A^{(t)}.$$

Второе утверждение доказывается аналогично. ■

Теперь докажем оценки на ранг произведения:

Доказательство. Сначала докажем верхнюю оценку. Система столбцов матрицы AB линейно выражается через столбцы A , поэтому (из основной леммы о линейной зависимости) $\text{rk} AB \leq \text{rk} A$. Аналогично, $\text{rk} AB \leq \text{rk} B$. Отсюда сразу следует требуемое. Теперь докажем и нижнюю оценку. Для этого рассмотрим матрицу

$$\begin{pmatrix} E & 0 \\ \begin{smallmatrix} n \times n & n \times k \\ 0 & AB \end{smallmatrix} \\ \begin{smallmatrix} m \times n & m \times k \end{smallmatrix} \end{pmatrix}$$

размера $(m + n) \times (n + k)$. Как нетрудно заметить, её ранг равен $\text{rk} AB + \text{rk} E$. Из леммы 16.1, можно производить элементарные преобразования не над отдельными её строками, а над блоками из матриц (Антон Александрович называл их «гиперстроками»), ведь такие преобразования можно разбить на цепочки преобразований обычных строк. Итак, элементарными преобразованиями (которые, как известно, не меняют ранг) переведём нашу матрицу в такую:

$$\begin{pmatrix} E & 0 \\ 0 & AB \end{pmatrix} \rightsquigarrow \begin{pmatrix} E & 0 \\ A & AB \end{pmatrix} \rightsquigarrow \begin{pmatrix} E & -B \\ A & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} E & B \\ A & 0 \end{pmatrix}$$

Теперь докажем, что $\text{rk} \begin{pmatrix} E & B \\ A & 0 \end{pmatrix} \geq \text{rk} A + \text{rk} B$. Приведём нашу блочную матрицу к улучшенному ступенчатому виду. Для этого можно брать строки единичной матрицы и вычитать их из строк матрицы A ,

обнуляя их. Это возможно, т. к. строки матрицы E образуют стандартный базис в \mathcal{K}^n , а потому строки A точно выражаются как линейные комбинации строк E . Что же будет при этом происходить со вторым «гиперстолбцом»? Там мы просто каждый раз будем из нулевой матрицы вычитать B с каким-то коэффициентом. А потому результат будем λB . Итак, улучшенный ступенчатый вид нашей матрицы:

$$\begin{pmatrix} E & B \\ 0 & \lambda B \end{pmatrix}.$$

Её ранг равен количеству ненулевых строк, т. е. $n + \text{rk } B$. А из неравенства $\text{rk } A \geq n$ получаем то, что хотели. Итак,

$$\text{rk } AB + n = \text{rk } AB + \text{rk } E = \text{rk } \begin{pmatrix} E & 0 \\ 0 & AB \end{pmatrix} \geq \text{rk } A + \text{rk } B.$$

Перенеся слагаемые в нужные стороны, получим то, что хотели. ■

17 Правая и левая обратные матрицы. Критерий существования. Обратная матрица, её единственность и критерий существования

Определение 17.1. Пусть A — матрица $m \times n$. Матрица B размера $n \times m$ называется **левой обратной** к матрице A , если $BA = E$ и **правой обратной** к матрице A , если $AB = E$.

Определение 17.2. Пусть A — матрица $n \times n$. Матрица B размера $n \times n$ называется **обратной** к матрице A , если $AB = BA = E$. Обозначается A^{-1} .

Теорема 17.1 (Критерий существования левой/правой обратной). Левая обратная к матрице A существует тогда и только тогда, когда $\text{rk } A = n$. Если $m = n$ и левая обратная к матрице A существует, то она единственна. Те же утверждения для правой обратной.

Доказательство. Рассмотрим матрицу BA . Если $\text{rk } A < n$, то $\text{rk } AB \leq \text{rk } A < n$, но $\text{rk } E = n$, а значит, $AB \neq E$. Противоречие.

Пусть теперь $\text{rk } A = n$. Тогда строки A — полная система в \mathcal{K}^n , т. к. базис системы строк A является базисом пространства \mathcal{K}^n (в этом базисе все векторы линейно независимы и их количество правильное). Строки матрицы BA — это линейные комбинации строк A с коэффициентами из строк B . Причём, т. к. система строк A полна, то существуют коэффициенты (строки матрицы B), линейная комбинация строк A с которыми даст строки единичной матрицы. Иными словами, существует такая матрица B , что $BA = E$.

А если $m = n$ и $\text{rk } A = n$, то вся система строк является базисом \mathcal{K}^n , а разложение по базису каждого вектора единственно. Поэтому существует единственный набор коэффициентов, линейная комбинация строк A с которыми даст строки единичной матрицы. Иными словами, существует единственная матрица B , такая что $BA = E$. Для правой обратной аналогично. ■

Примечание. Отсюда следует, что к матрице A существует и левая, и правая обратные (причём, единственные) тогда и только тогда, когда $\text{rk } A = m = n$, т. е. матрица A квадратная и её ранг равен размеру. Теперь легко видеть, что если B — левая обратная к A , а C — правая, то $B = C$:

$$B = B(AC) = (BA)C = C.$$

Отсюда получаем следующую теорему:

Теорема 17.2. К матрице A существует (и притом, только одна) обратная матрица тогда и только тогда, когда она квадратная и её ранг равен размеру.

Теорема 17.3. Одно из равенств $AB = E$ или $BA = E$ влечёт другое.

Доказательство. Пусть выполнено $AB = E$. Тогда B — правая обратная к A . Так как правая обратная существует, то $\text{rk } A = n$. А отсюда следует, что и левая обратная существует. Выше обсуждалось, что эти матрицы обязаны быть равны. ■

Утверждение (Задача Антона Александровича). A^{-1} (если существует) является многочленом от A .

Доказательство. Рассмотрим матрицы $A^{n^2}, A^{n^2-1}, \dots, A^2, A, E$. Их всего $n^2 + 1$ штук. А размерность пространства $\text{Mat}_{n \times n} \ni A$ равна n^2 . Значит, эти матрицы линейно зависимы. Иными словами, существует их нетривиальная нулевая линейная комбинация. Пусть её коэффициенты — $\lambda_1, \lambda_2, \dots, \lambda_{n^2+1}$. Тогда рассмотрим многочлен

$$\lambda_1 X^{n^2} + \lambda_2 X^{n^2-1} + \dots + \lambda_{n^2} X + \lambda_{n^2+1} E.$$

Из определения коэффициентов λ_i , A является корнем этого многочлена. Значит, множество многочленов, аннулирующих A непусто. Выберем из него многочлен наименьшей степени, пусть это

$$f(X) = \mu_1 X^k + \mu_2 X^{k+1} + \dots + \mu_k X + \mu_{k+1} E.$$

Предположим, что $\mu_{k+1} = 0$. Тогда имеем

$$\mu_1 A^k + \mu_2 A^{k+1} + \dots + \mu_k A = 0.$$

Домножим на A^{-1} справа и получим многочлен степени $k-1$, аннулирующий матрицу A . Противоречие с тем, что минимальная степень многочлена с таким свойством — k .

Итак, $\mu_{k+1} \neq 0$. Тогда домножим равенство

$$\mu_1 A^k + \mu_2 A^{k+1} + \dots + \mu_k A + \mu_{k+1} E = 0$$

справа на A^{-1} и выразим её:

$$A^{-1} = \sum_{i=1}^k \left(-\frac{\mu_i}{\mu_{k+1}} \right) A^{k-i}.$$

■

Определение 17.3. Матрица называется **вырожденной (обратимой)**, если у неё нет обратной.

Примечание. В решении теоретических задач часто полезно помнить, что улучшенный ступенчатый вид матрицы — это E тогда и только тогда, когда она невырождена.

18 Элементарные матрицы. Умножение на элементарные матрицы слева и справа. Матрица, обратная к произведению. Обратная к транспонированной матрице

Определение 18.1. Непосредственным вычислением проверяется, что элементарные преобразования строк какой-либо матрицы A равносильные её умножению слева на **элементарные матрицы** следующих трёх типов:

$$E + cE_{ij} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & \cdots & c \\ & & & \ddots & \vdots \\ & & & & 1 \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}, \quad P_{ij} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 0 & \cdots & 1 \\ & & \vdots & \ddots & \vdots \\ & & 1 & \cdots & 0 \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}, \quad Q_i(c) = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & c & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix},$$

где $i \neq j$ и $c \neq 0$, а все элементы этих матриц, не выписанные явно, такие же, как у единичной матрицы.

Умножение на элементарные матрицы справа дают нам элементарные преобразования столбцов. Так, умножение матрицы A слева на $E + cE_{ij}$ ($i \neq j$) приводит к тому, что к i -ой строке прибавляется j -ая строка, умноженная на c . А если умножить ту же матрицу на A справа, то к j -му столбцу прибавляется i -ый столбец, умноженный на c .

Примечание. Из Винберга. Метод Гаусса в матричной интерпретации состоит в последовательном умножении уравнения

$$AX = B$$

слева на элементарные матрицы, имеющем целью приведения матрицы A к улучшенному ступенчатому виду. Используя вместо элементарных матриц какие-либо другие матрицы, можно получить другие методы решения систем линейных уравнений, которые, быть может, не столь просты в теоретическом отношении, но, скажем, более надёжны при приближённых вычислениях (в случае $\mathcal{K} = \mathbb{R}$). Таков, например, метод вращений, при котором в качестве элементарных берутся матрицы вида

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & \cos \alpha & \cdots & -\sin \alpha & \\ & & \vdots & \ddots & \vdots & \\ & & \sin \alpha & \cdots & \cos \alpha & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}.$$

Утверждение.

1. $(AB)^{-1} = B^{-1}A^{-1}$;
2. $(A^T)^{-1} = (A^{-1})^T$.

Доказательство. Нужно просто перемножить и удостовериться, что получается E :

1. $(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}B = E$;
2. $(A^{-1})^T A^T = (AA^{-1})^T = E^T = E$.

Как следствие, если A и B обратимы, то и AB тоже. ■

19 Алгоритм поиска обратной матрицы. Разложение невырожденной матрицы в произведение элементарных

Чтобы найти обратную матрицу, нам нужно решить матричное уравнение

$$AX = E.$$

Для этого нам нужно решить n систем уравнений с одной и той же матрицей коэффициентов A , столбцы свободных членов которых составляют матрицу E . Эти системы можно решать одновременно методом Гаусса. После приведения матрицы коэффициентов к единичной матрице (что возможно в силу её невырожденности) преобразованные столбцы свободных членов составят искомую матрицу A^{-1} .

$$(A \mid E) \rightsquigarrow \dots \rightsquigarrow (E \mid A^{-1}).$$

A , как уже обсуждалось, метод Гаусса заключается в домножении матрицу на элементарные слева. А т. к. улучшенный ступенчатый вид невырожденной матрицы единичный, то получаем

$$A = U_1 A_1 = U_2 U_1 A_2 = \dots = U_N \dots U_1 E = U_N \dots U_1,$$

где U_i — элементарные матрицы.

Александр Александрович Гайфуллин рассказал полезный трюк. Часто приходится решать матричные уравнения типа

$$AX = B.$$

Решением является $A^{-1}B$. Однако искать обратную к A , а затем умножать её на B может быть затруднительно. Можно поступить тем же способом, которым мы пользовались ранее, заменив единичную матрицу на B (ведь по сути ничего не меняется, нам всё ещё нужно решить n СЛУ с n неизвестными):

$$(A \mid B) \rightsquigarrow \dots \rightsquigarrow (E \mid A^{-1}B).$$

Ещё это можно объяснить следующим образом (так это делал Сергей Александрович): элементарные преобразования строк — это умножения слева на элементарные матрицы. Мы делаем над обеими частями матрицы $(A \mid B)$ одни и те же элементарные преобразования, в результате слева получаем $U_N \dots U_1 \cdot A = E$, значит, $U_N \dots U_1 = A^{-1}$, а справа $U_N \dots U_1 B = A^{-1}B$.

20 Подстановки и перестановки. Их количество. Произведение подстановок, его свойства. Разложение подстановки на произведение независимых циклов

Определение 20.1. Зафиксируем множество $\Omega_n = \{1, 2, \dots, n\}$. **Подстановкой** будем называть биекцию $\sigma : \Omega_n \rightarrow \Omega_n$, а **перестановкой** — упорядоченный набор элементов Ω_n . Обозначать подстановки будем так:

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

Примечание. Между перестановками и подстановками можно установить биекцию, поэтому эти понятия взаимозаменяемы.

Определение 20.2. Произведением подстановок называется их композиция.

Теорема 20.1. Перестановки порядка n образуют группу. Она обозначается S_n .

Доказательство. Проверим выполнение всех аксиом:

1. Ассоциативность выполняется, т. к. она выполняется для всех отображений
2. Тожественная подстановка

$$\varepsilon = \begin{pmatrix} 1 & \dots & i & \dots & n \\ 1 & \dots & i & \dots & n \end{pmatrix}$$

является нейтральным элементом.

3. Если поменять местами две строки в записи перестановки σ , то мы получим такую, которая в композиции с σ даст тождественную. Это и есть обратная подстановка.

■

Утверждение. $|S_n| = n!$

Доказательство. Нам нужно выбрать n элементов из множества $\{1, 2, \dots, n\}$. У нас есть n способов выбрать первый элемент, затем $n - 1$ способов выбрать второй элемент и т. д. Таким образом, количество способов выбрать уникальную подстановку равно

$$n \cdot (n - 1) \cdot \dots \cdot 1 = n!$$

■

Примечание. Из лекций Ю. Г. Прохорова. В общем случае перестановки не коммутируют. Однако есть условие, при котором это свойство всё-таки выполняется.

Определение 20.3. Пусть $\sigma \in S_n$. Элемент $i \in \Omega_n$ называется **неподвижным**, если $\sigma(i) = i$.

Всё множество Ω_n разбивается на два подмножества:

$$\Omega_n = F(\sigma) \sqcup M(\sigma),$$

где $F(\sigma)$ — множество неподвижных элементов, а $M(\sigma)$ — подвижных.

Лемма 20.1. $i \in M(\sigma) \Rightarrow \sigma(i) \in M(\sigma)$.

Доказательство. Действительно, пусть $i \in M(\sigma)$ (обозначим $\sigma(i) = j$) и $\sigma(i) \in F(\sigma)$. Тогда

$$\sigma(i) = \sigma(\sigma(i)) = \sigma(j),$$

при этом $i \neq j$, однако σ — биекция. Противоречие. ■

Теорема 20.2. Если $M(\sigma_1) \cap M(\sigma_2) = \emptyset$, то $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.

Доказательство. Множества $F(\sigma_1)$ и $M(\sigma_1)$ не пересекаются и полностью покрывают собой множество Ω_n . То же верно и для множеств $F(\sigma_2)$ и $M(\sigma_2)$. Из этого следует, что $M(\sigma_2) \subseteq F(\sigma_1)$ и $M(\sigma_1) \subseteq F(\sigma_2)$ (чтобы убедиться в этом, можно нарисовать картинку).

Не ограничивая общности, пусть $i \in M(\sigma_1)$. Тогда $i \notin M(\sigma_2)$ и, как следствие, $i \in F(\sigma_2)$. А по предыдущей лемме, $\sigma_1(i) \in M(\sigma_1)$ и аналогично получаем $\sigma_1(i) \in F(\sigma_2)$. Итак,

$$(\sigma_1 \circ \sigma_2)(i) = \sigma_1(\sigma_2(i)) = \sigma_1(i), \quad (\sigma_2 \circ \sigma_1)(i) = \sigma_2(\sigma_1(i)) = \sigma_1(i).$$

Таким образом, значения $\sigma_1 \circ \sigma_2$ и $\sigma_2 \circ \sigma_1$ совпадают в каждой точке, а значит, они равны. ■

Определение 20.4. Подстановка $\sigma \in S_n$ называется **циклом**, если существуют числа $i_1, \dots, i_k \in \Omega_n$, такие что $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$. Остальные элементы отображаются сами в себя. При этом, k называется **длиной цикла**. Сокращённая запись цикла — $[i_1, i_2, \dots, i_k]$.

Определение 20.5. Циклы σ_1 и σ_2 называются **независимыми**, если

$$M(\sigma_1) \cap M(\sigma_2) = \emptyset.$$

Примечание. Такие циклы, как уже доказано, коммутируют.

Теорема 20.3. $\forall \sigma \in S_n$ существуют независимые циклы $\sigma_1, \dots, \sigma_k$ такие, что

$$\sigma = \sigma_1 \cdot \dots \cdot \sigma_k.$$

при этом такое разложение единственно с точностью до порядка множителей.

Доказательство. Доказательство проведём индукцией по $|M(\sigma)|$. База индукции очевидна, докажем шаг. Рассмотрим какой-то $i \in \Omega_n$ и введём следующие обозначения:

$$i_0 := i, \quad i_1 := \sigma(i), \quad i_2 := \sigma^2(i), \quad \dots, \quad i_k := \sigma^k(i).$$

Иными словами, $i_k = \sigma(i_{k-1})$. Элементов i_j бесконечно много, однако множество Ω_n , в которое они все входят, конечно. А потому последовательность должна с какого-то момента заиклиться, при этом наименьший положительный период r не превосходит n . Итак, имеем

$$\sigma^t(i) = \sigma^{t+r}(i), \quad \varepsilon(i) = \sigma^r(i), \tag{*}$$

отсюда $\sigma^r(i) = i$, причём r — минимальное положительное число с таким свойством. Утверждается, что тогда числа i_0, i_1, \dots, i_{r-1} попарно различны. Действительно, если это не так, то, произведя заново выкладку (*), придём к противоречию с минимальностью r . Теперь рассмотрим перестановку

$$\hat{\sigma} = [i_0, \dots, i_{r-1}]^{-1} \circ \sigma.$$

Заметим, что

$$\begin{aligned} \hat{\sigma}(i_0) &= [i_{r-1}, \dots, i_0](\sigma(i_0)) = [i_{r-1}, \dots, i_0](i_1) = i_0, \\ \hat{\sigma}(i_1) &= [i_{r-1}, \dots, i_0](\sigma(i_1)) = [i_{r-1}, \dots, i_0](i_2) = i_1, \\ &\vdots \\ \hat{\sigma}(i_{r-1}) &= [i_{r-1}, \dots, i_0](\sigma(i_{r-1})) = [i_{r-1}, \dots, i_0](i_0) = i_{r-1}. \end{aligned}$$

Значит, $i_1, \dots, i_{r-1} \in F(\hat{\sigma})$. Заметим при этом, что образы остальных элементов такие же, ведь цикл $[i_{r-1}, \dots, i_0]$ никуда их не переставляет: $\hat{\sigma}(j) = \sigma(j)$ при $j \notin \{i_0, \dots, i_{r-1}\}$. Проанализируем, что мы получили. У подстановки σ элементы i_0, \dots, i_{r-1} были подвижными, т.к., из уже доказанного, числа $\{i_0, \dots, i_{r-1}\}$ попарно различны. А у новой подстановки $\hat{\sigma}$ эти элементы стали неподвижными, а остальные — какими были, такими и остались. Значит, $|M(\hat{\sigma})| < |M(\sigma)|$, пока σ не тождественна. Значит, по предположению индукции, для $\hat{\sigma}$ существует разложение на независимые циклы. А в произведении с циклом $[i_{r-1}, \dots, i_0]$ они дадут σ . ■

21 Инверсии. Чётность перестановки и подстановки. Знак подстановки, изменение чётности при умножении на транспозицию. Разложение подстановки на транспозиции. Знак произведения подстановок

Определение 21.1. В подстановке σ положение двух элементов $\sigma(i)$ и $\sigma(j)$ ($i < j$) называется **порядком**, если $\sigma(i) < \sigma(j)$ и **инверсией**, если $\sigma(i) > \sigma(j)$.

Определение 21.2. **Чётностью подстановки** называется чётность общего числа инверсий в ней. **Знак подстановки** $\operatorname{sgn} \sigma := (-1)^{\text{чётность } \sigma}$.

Примечание. Определения для перестановок даются так же, как для соответствующих им подстановок.

Лемма 21.1. При умножении подстановки σ на транспозицию $[i, j]$ слева меняет местами числа i и j , а справа — меняет местами числа $\sigma(i)$ и $\sigma(j)$.

Доказательство. Если $\sigma(x) \notin \{i, j\}$, то $([i, j] \circ \sigma)(x) = \sigma(x)$. Если же $\sigma(x) = i$, то $([i, j] \circ \sigma)(x) = j$ и наоборот. Это доказывает первое утверждение.

Если $x \notin \{i, j\}$, то $[i, j](x) = x$. Теперь $(\sigma \circ [i, j])(i) = \sigma(j)$, а $(\sigma \circ [i, j])(j) = \sigma(i)$. ■

Теорема 21.1. Чётность подстановки меняется при умножении на транспозицию.

Доказательство. При транспозиции соседних элементов меняется взаимное расположение только этих элементов, так что число инверсий изменяется (увеличивается или уменьшается) на 1; следовательно, чётность меняется. Теперь заметим, что

$$[i, j] = [i, i+1] \circ [i+1, i+2] \circ \dots \circ [j-1, j] \circ [j-2, j-1] \circ \dots \circ [i, i+1].$$

То есть, транспозиция несоседних элементов раскладывается в произведение $2(j-i)+1$ соседних элементов. При каждой из них меняется чётность подстановки, а всего их нечётное количество, поэтому в итоге чётность изменится. ■

Теорема 21.2. Любая подстановка раскладывается в произведение транспозиций.

Доказательство. Любая подстановка раскладывается в произведение независимых циклов. А каждый цикл раскладывается в произведение транспозиций:

$$[i_1, i_2, \dots, i_k] = [i_2 \circ i_1] \circ [i_3 \circ i_2] \circ \dots \circ [i_k, i_{k-1}].$$

Примечание. Из двух предыдущих теорем следует, что если $\sigma = \sigma_1 \cdot \dots \cdot \sigma_N$ — разложение подстановки в произведение транспозиций, то $\operatorname{sgn} \sigma = (-1)^N$. А для цикла (разложение на транспозиции которого приводилось выше) $\operatorname{sgn} [i_1, \dots, i_k] = (-1)^{k-1}$.

Утверждение (Задача из Кострикина). Доказать, что любая чётная подстановка представима в виде произведения циклов длины 3.

Доказательство. Чётная подстановка раскладывается в произведения чётного числа транспозиций. Осталось заметить, что

$$[i_1, i_2] \circ [i_3, i_4] = [i_1, i_2] \circ \underbrace{[i_1, i_3] \circ [i_1, i_3]}_{\varepsilon} \circ [i_3, i_4] = [i_1, i_2, i_3] \circ [i_1, i_3, i_4].$$

Теорема 21.3. $\operatorname{sgn} (\sigma \circ \delta) = \operatorname{sgn} \sigma \cdot \operatorname{sgn} \delta$.

Доказательство. Разложим подстановки в условии в произведения подстановок:

$$\sigma = \sigma_1 \circ \dots \circ \sigma_N, \quad \delta = \delta_1 \circ \dots \circ \delta_M,$$

Тогда

$$\operatorname{sgn}(\sigma \circ \delta) = \operatorname{sgn}(\sigma_1 \circ \dots \circ \sigma_N \circ \delta_1 \circ \dots \circ \delta_M) = (-1)^{N+M} = (-1)^N \cdot (-1)^M = \operatorname{sgn} \sigma \cdot \operatorname{sgn} \delta.$$

■

Примечание. Как следствие, $\operatorname{sgn} \sigma^{-1} = \operatorname{sgn} \sigma$, т. к.

$$1 = \operatorname{sgn} \varepsilon = \operatorname{sgn}(\sigma \circ \sigma^{-1}) = \operatorname{sgn} \sigma \cdot \operatorname{sgn} \sigma^{-1}$$

и $\operatorname{sgn}(\sigma \circ \delta) = \operatorname{sgn}(\delta \circ \sigma)$. Отсюда же можно извлечь ещё одно полезное следствие:

Теорема 21.4. При $n > 1$ число чётных подстановок равно числу нечётных.

Доказательство. Докажем, что отображение $\sigma \mapsto [1, 2] \circ \sigma$ является биекцией из множества чётных подстановок в множество нечётных. Из уже доказанного, если σ чётная, то $[1, 2] \circ \sigma$ нечётная. Докажем же, что φ — биекция. Во-первых, φ — сюръекция, действительно, каждая нечётная подстановка σ является образом чётной подстановки $[1, 2] \circ \sigma$. Во-вторых, φ — инъекция, так как, очевидно, $\sigma \neq \delta \Rightarrow [1, 2] \circ \sigma \neq [1, 2] \circ \delta$. ■

Примечание. Множество чётных подстановок порядка n обозначается A_n . Из уже доказанного, легко увидеть, что они образуют группу по операции композиции.

22 Чётность цикла. Чётность произвольной подстановки через декремент

Чётность цикла была раньше.

Определение 22.1. Декремент подстановки σ — это число $d(\sigma)$, равное n за вычетом количества независимых циклов в разложении σ .

Теорема 22.1. $\operatorname{sgn} \sigma = (-1)^{d(\sigma)}$.

Доказательство. Пусть k_1, \dots, k_m — длины независимых циклов в разложении σ . Тогда

$$\operatorname{sgn} \sigma = \prod_{i=1}^m (-1)^{k_i-1} = (-1)^{\sum_{i=1}^m (k_i-1)} = (-1)^{n-m} = (-1)^{d(\sigma)}.$$

■

23 Формула определителя квадратной матрицы. Определитель транспонированной матрицы. Линейность и кососимметричность определителя как функции от строк и столбцов матрицы

Определение 23.1. Определителем квадратной матрицы $A = (a_{ij})$ порядка n называется число

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

Теорема 23.1. $\det A^T = \det A$.

Примечание. Как следствие, любое свойство определителя матрицы по отношению к её строкам верно также и для её столбцов.

Доказательство. Заметим, что т. к. S_n — группа, то если σ пробегает S_n то и σ^{-1} пробегает S_n .

$$\det A^T = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot a_{\sigma(1)1} \dots a_{\sigma(n)n} = \{\delta := \sigma^{-1}\} = \sum_{\delta \in S_n} \operatorname{sgn} \delta \cdot a_{1\delta(1)} \dots a_{n\delta(n)} = \det A.$$

■

Теорема 23.2. Определитель является полилинейной кососимметричной функцией строк матрицы.

Доказательство. Линейность определителя по каждой из строк матрицы вытекает из того, что для любого i его можно представить в виде

$$\det A = \sum_j a_{ij} u_j,$$

где u_1, \dots, u_n не зависят от элементов i -ой строки матрицы (видно из формулы определителя).

Для проверки кососимметричности посмотрим, что происходит при перестановке i -ой и j -ой строк матрицы. Из доказательства теоремы 21.4 видно, что отображение $\varphi : \sigma \in S_n \mapsto \sigma \circ [i, j] \in S_n$ биективно, при этом $\operatorname{sgn} \sigma = -\operatorname{sgn} \varphi(\sigma)$ и $\varphi(\sigma) = \varphi^{-1}(\sigma)$. Поэтому подстановки можно разбить на такие пары $(\sigma, \varphi(\sigma))$ (как следствие, если σ пробегает S_n , то и $\varphi(\sigma)$ её пробегает). Обозначим за $A_{(i) \leftrightarrow (j)}$ матрицу, у которой переставлены местами строки с номерами i и j . Тогда

$$\begin{aligned} \det A_{(i) \leftrightarrow (j)} &= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot a_{1\sigma(1)} \dots a_{i\sigma(j)} \dots a_{j\sigma(i)} \dots a_{n\sigma(n)} = \\ &= \{\delta := \varphi(\sigma)\} = \sum_{\delta \in S_n} (-\operatorname{sgn} \delta) \cdot a_{1\delta(1)} \dots a_{i\delta(i)} \dots a_{j\delta(j)} \dots a_{n\delta(n)} = -\det A. \end{aligned}$$

■

24 Определитель матрицы с нулевой строкой/столбцом. Определитель матрицы с пропорциональными строками. Изменение определителя при элементарных преобразованиях строк/столбцов. Определитель треугольной матрицы. Алгоритм вычисления определителя с помощью элементарных преобразований. Эквивалентные условия невырожденности матрицы. Определитель матрицы с углом нулей

Лемма 24.1. Определитель матрицы со строкой нулей равен нулю.

Доказательство. Пусть i -ая строка матрицы нулевая. В каждом слагаемом из формулы определителя присутствует множитель $a_{i\sigma(i)} = 0$. Поэтому каждое слагаемое равно нулю, поэтому нулю равна вся сумма, т. е. определитель. ■

Теорема 24.1 (Изменения определителя при элементарных преобразованиях). При элементарных преобразованиях

- 1-го типа определитель не изменяется;
- 2-го типа определитель умножается на -1 ;
- 3-го типа умножается на ненулевую константу.

Доказательство. Докажем через определение, а потом обсудим, почему лучше делать так, а не как рассказывал Сергей Александрович на лекциях.

1. Пусть к i -ой строке прибавили j -ую с коэффициентом λ . Тогда определитель новой матрицы равен

$$\sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot a_{1\sigma(1)} \dots (a_{i\sigma(i)} + \lambda a_{j\sigma(i)}) \dots a_{n\sigma(n)} = \det A + \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot a_{1\sigma(1)} \dots a_{j\sigma(i)} \dots a_{j\sigma(j)} \dots a_{n\sigma(n)}.$$

Посмотрим на образовавшуюся сумму. Как мы уже знаем, каждой подстановке σ можно биективно сопоставить подстановку $\delta = \sigma \circ [i, j]$ (при этом $\sigma(i) = \delta(j)$, $\sigma(j) = \delta(i)$, а остальные элементы переходят туда же, куда и раньше). Поэтому возникает биекция между слагаемыми нашей суммы:

$$\operatorname{sgn} \sigma \cdot a_{1\sigma(1)} \dots a_{j\sigma(i)} \dots a_{j\sigma(j)} \dots a_{n\sigma(n)} \mapsto -\operatorname{sgn} \sigma a_{1\delta(1)} \dots a_{j\delta(j)} \dots a_{i\delta(i)} \dots a_{n\delta(n)}.$$

Они отличаются только знаком, поэтому в сумме дают 0. А значит, и вся сумма равна 0 и остаётся только $\det A$.

2. Это буквально кососимметричность.
3. Пусть i -ую строку матрицы умножили на $c \neq 0$. Тогда в каждом слагаемом формулы определителя новой матрицы будет присутствовать ровно один множитель из i -ой строки, $c \cdot a_{i\sigma(i)}$. Поэтому, вынеся из каждого слагаемого константу c , получим, что определитель новой матрицы равен $c \cdot \det A$.

■

Примечание. На лекциях Сергей Александрович давал другое доказательство того, что определитель не изменяется при элементарных преобразованиях первого типа. Сначала доказывалась лемма, что определитель с двумя одинаковыми строками равен нулю. Доказательство было такое: если поменять эти строки местами, то из кососимметричности знак определителя изменится, а сама матрица при этом не поменяется. Поэтому $\det A = -\det A$, а отсюда $\det A = 0$. Проблема вот в чём: это доказательство не работает для матриц над полем с характеристикой 2, потому что над этим полем равенство $2 \cdot \det A = 0$ не влечёт $\det A = 0$, т. к. 2 — это и есть 0 (примером такого поля служит \mathbb{Z}_2). Мне на это указал принимающий на коллоквиуме, и я придумал доказательство выше.

Теорема 24.2. Определитель треугольной матрицы равен произведению элементов на её главной диагонали.

Лемма 24.2. Для любой нетождественной подстановки $\sigma \in S_n$ существует $i \in \Omega_n$ такой, что $i > \sigma(i)$.

Доказательство. Докажем утверждение индукцией по n .

База индукции ($n = 2$). Единственная нетождественная подстановка порядка 2 — это $[1, 2]$. При этом, $2 > [1, 2](2) = 1$.

Шаг. Пусть утверждение верно для любого $n < m$. Пусть $\sigma \in S_m$ — нетождественная подстановка. Если $\sigma(m) = m$, то можно рассмотреть её без последнего элемента. Так как если $i \neq m$, то $i \in \Omega_{m-1}$ и $\sigma(i) \in \Omega_{m-1}$, то имеем подстановку $\sigma' \in S_{m-1}$ такую, что $\sigma'(j) = \sigma(j)$ для каждого $j \in \Omega_{m-1}$. Если для неё не существует такого i , что $i > \sigma'(i)$, то по предположению индукции она тождественная. Но тогда и σ тождественная.

А если $\sigma(m) \neq m$, то $\sigma(m) = i \in \Omega_{m-1}$, а значит $m > \sigma(m)$.

■

Теперь докажем теорему 24.2:

Доказательство. Докажем теорему для нижнетреугольных матриц, к случаю верхнетреугольных матриц утверждение будет сводиться транспозицией. Итак, формула для определителя:

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

Тожественная подстановка σ соответствует слагаемому $a_{11} \dots a_{nn}$ (т. е. как раз произведению элементов на главной диагонали). А для любой другой подстановки найдётся i такое, что $i > \sigma(i)$, иными словами $a_{i\sigma(i)}$ будет находится выше главной диагонали, а потому $a_{i\sigma(i)} = 0$, а значит, занулятся всё слагаемое.

■

Алгоритм вычисления определителя с помощью элементарных преобразований. Пусть мы хотим найти определитель матрицы A . Для этого будем приводить её к ступенчатому виду элементарными преобразованиями. При этом, следить за тем, преобразований каких типов мы применяем и домножать результат на c^{-1} , если применяем преобразование 3-го типа с константой c и на -1 , если применяем преобразование 2-го типа (из линейности). А ступенчатый вид — это треугольная матрица, для неё определитель — это произведение диагональных элементов.

Теорема 24.3 (Эквивалентные условия невырожденности матрицы). Следующие условия эквивалентны:

1. К матрице A существует обратная.

2. $\operatorname{rk} A = n$.
3. $\det A \neq 0$.

Доказательство. Равносильность между первым и вторым пунктами уже была доказана. Докажем равносильность между вторым и третьим пунктами.

\Rightarrow . Если $\operatorname{rk} A = n$, то улучшенный ступенчатый вид матрицы A единичный, поэтому, находя определитель с помощью элементарных преобразований, не получим ни одного нулевого множителя. А значит, $\det A \neq 0$.

\Leftarrow . Находя $\det A$ с помощью элементарных преобразований, получаем $\det A = \lambda \det \tilde{A}$, где \tilde{A} — улучшенный ступенчатый вид матрицы A , а $\lambda \neq 0$. $\det A \neq 0 \Rightarrow \det \tilde{A} \neq 0$. А \tilde{A} — треугольная матрица, и её определитель равен произведению элементов на главной диагонали. Оно ненулевое, значит, $\tilde{A} = E$. Отсюда следует невырожденность матрицы и $\operatorname{rk} A = n$. ■

Теорема 24.4 (Об определителе матрицы с углом нулей). Пусть матрица A имеет вид

$$A = \begin{pmatrix} B & D \\ 0 & C \end{pmatrix},$$

где B и C — квадратные матрицы. Тогда

$$\det A = \det B \cdot \det C.$$

Доказательство. При фиксированных B и D определитель матрицы A является полилинейной и кососимметричной её последних строк и, тем самым, кососимметричной и полилинейной функцией строк матрицы C . Согласно теореме 25.1, получаем

$$\det A = \det \begin{pmatrix} B & D \\ 0 & E \end{pmatrix} \cdot \det C.$$

Первый множитель, в свою очередь, является полилинейной и кососимметричной функцией первых столбцов матрицы, а потому (по той же теореме) получаем

$$\det A = \det \begin{pmatrix} B & D \\ 0 & E \end{pmatrix} \cdot \det C = \det \begin{pmatrix} E & D \\ 0 & E \end{pmatrix} \cdot \det B \cdot \det C,$$

но матрица $\begin{pmatrix} E & D \\ 0 & E \end{pmatrix}$ треугольная с единицами на главной диагонали, поэтому её определитель равен 1. ■

Утверждение (Задача Антона Александровича). Если матрицы A и C коммутируют, то

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - CB).$$

Примечание. Все такие задачи решаются через определитель теорему об определителе матрицы с углом нулей — нужно создать этот угол нулей путём элементарных преобразований над «гиперстроками»/«гиперстолбцами».

Доказательство. ■