

Лекции по Линейной Алгебре

Дима Трушин

2021 — 2022

Содержание

1 Системы линейных уравнений	3
1.1 Системы линейных уравнений и связанная с ними терминология	3
1.2 Матрицы связанные со СЛУ	3
1.3 Элементарные преобразования	4
1.4 Алгоритм Гаусса	4
2 Матрицы	7
2.1 Определение матриц	7
2.2 Операции над матрицами	7
2.3 Специальные виды матриц	8
2.4 Свойства операций	8
2.5 Связь с системами линейных уравнений	9
2.6 Дефекты матричных операций	10
2.7 Деление	10
2.8 Матрицы элементарных преобразований	12
2.9 Невырожденные матрицы	12
2.10 Блочное умножение матриц	14
2.11 Блочные элементарные преобразования	15
2.12 Массовое решение систем	16
2.13 Классификация СЛУ	18
2.14 Полиномиальное исчисление от матриц	21
3 Перестановки	26
3.1 Отображения множеств	26
3.2 Перестановки	26
3.3 Операция на перестановках	27
3.4 Переименование элементов	28
3.5 Циклы	28
3.6 Знак перестановки	30
3.7 Подсчет знака	32
3.8 Возведение в степень	33
3.9 Произведение циклов	33
4 Определитель	36
4.1 Философия	36
4.2 Три разных определения	37
4.3 Явные формулы для определителя	38
4.4 Свойства определителя	39
4.5 Полилинейность и кососимметричность определителя	40
4.6 Полилинейные кососимметрические отображения	41
4.7 Мультипликативные отображения	43
4.8 Миноры и алгебраические дополнения	46
4.9 Формулы Крамера	48
4.10 Характеристический многочлен	49

4.11	Теорема Гамильтона-Кэли	52
5	Комплексные числа	54
5.1	Идея	54
5.2	Абстрактное определение комплексных чисел	56
5.3	Две модели комплексных чисел	56
5.4	Простейшие свойства и операции	58
5.5	Геометрическая модель	58
5.6	Основная теорема алгебры	60
5.7	Многочлены	62
6	Векторные пространства	65
6.1	Идея и определение	65
6.2	Подпространство	66
6.3	Линейные комбинации	67
6.4	Базис	68
6.5	Удобный формализм	70
6.6	Размерность	70
6.7	Конкретные векторные пространства	71
6.8	Подпространства в F^n	72

1 Системы линейных уравнений

1.1 Системы линейных уравнений и связанная с ними терминология

Наша задача научиться решать Системы Линейных Уравнений (СЛУ), то есть находить все их решения или доказывать, что решений нет. Общий вид СЛУ и ее однородная версия (ОСЛУ):

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1 \\ \dots \\ a_{m1}x_1 + \dots + a_{mn}x_n = b_m \end{cases} \quad \begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = 0 \\ \dots \\ a_{m1}x_1 + \dots + a_{mn}x_n = 0 \end{cases}$$

Коэффициенты Где живут коэффициенты a_{ij} и b_j ? Варианты:

- Вещественные числа \mathbb{R}
- Комплексные числа \mathbb{C}
- Рациональные числа \mathbb{Q}

Для решения СЛУ **НЕ** имеет значения откуда берутся коэффициенты, так как решения будут лежать там же. Потому мы будем работать с числами из \mathbb{R} .

Решение Решением системы линейных уравнений называется набор чисел (c_1, \dots, c_n) , $c_i \in \mathbb{R}$ такой, что при подстановке c_i вместо x_i , все уравнения системы превращаются в верные равенства. Введем обозначение $\mathbb{R}^n = \mathbb{R} \times \dots \times \mathbb{R} = \{(c_1, \dots, c_n) \mid c_i \in \mathbb{R}\}$. То есть элемент \mathbb{R}^n – это набор из n вещественных чисел. Потому любое решение $c = (c_1, \dots, c_n)$ является элементом \mathbb{R}^n .

1.2 Матрицы связанные со СЛУ

Для каждой СЛУ введем следующие обозначения:

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad (A|b) = \left(\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & b_m \end{array} \right)$$

Названия:

- A – матрица системы
- b – вектор правой части
- $(A|b)$ – расширенная матрица системы
- x – вектор решений

Будем кратко записывать СЛУ и ее однородную версию так: $Ax = b$ и $Ax = 0$. Также для краткости будем обозначать системы буквами Σ .

При решении системы линейных уравнений приходится много раз переписывать кучу данных, чтобы сократить эти записи целесообразно сократить количество записываемой на бумаге информации. Расширенная матрица системы $(A|b)$ является необходимым минимумом такой информации. Потому сейчас к такой записи можно относиться как к удобному способу компактно записать систему.

Количество решений Случай одного уравнения и одной неизвестной $ax = b$, где $a, b \in \mathbb{R}$:

- При $a \neq 0$ – одно решение $x = b/a$.
- При $a = 0$, $b \neq 0$ – нет решений.
- При $a = 0$, $b = 0$ – любое число является решением, т.е. бесконечное число решений.

Что значит решить систему Решить систему значит описать множество ее решений, то есть либо доказать, что система не имеет решений вовсе, либо описать все наборы, которые являются решениями. Если система не имеет решений, она называется несовместной, в противном случае – совместной.

Эквивалентные системы Пусть даны две системы линейных уравнений с одинаковым числом неизвестных (но быть может разным числом уравнений) Σ_1 и Σ_2 . Будем говорить, что эти системы эквивалентны и писать $\Sigma_1 \sim \Sigma_2$, если множества решений этих систем совпадают. Если $E_i \subseteq \mathbb{R}^n$ – множество решений i -ой системы, то системы эквивалентны, если $E_1 = E_2$.

Вот полезный пример эквивалентных систем:

$$\begin{cases} x + y = 1 \\ x - y = 0 \end{cases} \sim \begin{cases} 2x = 1 \\ 2y = 1 \end{cases}$$

Как решать систему Пусть нам надо решить систему Σ . Идея состоит в том, чтобы постепенно менять ее на эквивалентную до тех пор, пока она не упростится до такого состояния, что все ее решения становятся легко описываемые.

$$\Sigma = \Sigma_1 \mapsto \Sigma_2 \mapsto \dots \mapsto \Sigma_n \leftarrow \text{легко решается}$$

Теперь надо объяснить две вещи: (1) какого сорта преобразования над системами мы будем делать и (2) к какому замечательному виду мы их приводим и как в нем выглядят все решения. Ответам на эти два вопроса и будет посвящена оставшаяся часть лекции.

1.3 Элементарные преобразования

Мы разделим все преобразования на три типа¹:

$$\begin{aligned} \text{I тип: } & \left(\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ a_{i1} & \dots & a_{in} & b_i \\ a_{j1} & \dots & a_{jn} & b_j \\ a_{m1} & \dots & a_{mn} & b_m \end{array} \right) \mapsto \left(\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ a_{i1} & \dots & a_{in} & b_i \\ a_{j1} + \lambda a_{i1} & \dots & a_{jn} + \lambda a_{in} & b_j + \lambda b_i \\ a_{m1} & \dots & a_{mn} & b_m \end{array} \right) \quad i \neq j \\ \\ \text{II тип: } & \left(\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ a_{i1} & \dots & a_{in} & b_i \\ a_{j1} & \dots & a_{jn} & b_j \\ a_{m1} & \dots & a_{mn} & b_m \end{array} \right) \mapsto \left(\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ a_{j1} & \dots & a_{jn} & b_j \\ a_{i1} & \dots & a_{in} & b_i \\ a_{m1} & \dots & a_{mn} & b_m \end{array} \right) \\ \\ \text{III тип: } & \left(\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ a_{i1} & \dots & a_{in} & b_i \\ a_{m1} & \dots & a_{mn} & b_m \end{array} \right) \mapsto \left(\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ \lambda a_{i1} & \dots & \lambda a_{in} & \lambda b_i \\ a_{m1} & \dots & a_{mn} & b_m \end{array} \right) \quad \lambda \neq 0 \end{aligned}$$

Поясним словами, что делают преобразования:

1. Прибавляем к j -ой строке i -ю, умноженную на константу $\lambda \in \mathbb{R}$.
2. Меняем местами i -ю и j -ю строки.
3. Умножаем i -ю строку на ненулевую константу $\lambda \neq 0$, $\lambda \in \mathbb{R}$.

1.4 Алгоритм Гаусса

Этот метод заключается в приведении СЛУ к некоторому «ступенчатому виду», где множество решений очевидно.² Разберем типичный ход алгоритма Гаусса на примере 3 уравнений и 4 неизвестных.³

¹Стоит отметить, что нумерация типов преобразования не является общепринятой и отличается от учебника к учебнику.

²Данный метод является самым быстрым возможным как для написания программ, так и для ручного вычисления. При вычислениях руками, однако, полезно местами пользоваться «локальными оптимизациями», то есть, если вы видите, что какая-то хитрая комбинация строк сильно упростит вид системы, то сделайте ее.

³При переходе от одной матрицы к другой я новым коэффициентам даю старые имена, чтобы не захламлять текст новыми обозначениями.

Прямой ход алгоритма Гаусса

$$\begin{aligned}
 &\left(\begin{array}{cccc|c} a_{11} & a_{12} & a_{13} & a_{14} & b_1 \\ a_{21} & a_{22} & a_{23} & a_{24} & b_2 \\ a_{31} & a_{32} & a_{33} & a_{34} & b_3 \end{array}\right) \quad \begin{array}{l} \text{2-я строка} \\ \text{3-я строка} \end{array} \quad \begin{array}{l} - \frac{a_{21}}{a_{11}} \cdot \text{1-я строка} \\ - \frac{a_{31}}{a_{11}} \cdot \text{1-я строка} \end{array} \\
 &\left(\begin{array}{cccc|c} a_{11} & a_{12} & a_{13} & a_{14} & b_1 \\ 0 & a_{22} & a_{23} & a_{24} & b_2 \\ a_{31} & a_{32} & a_{33} & a_{34} & b_3 \end{array}\right) \quad \begin{array}{l} \text{3-я строка} \\ \text{3-я строка} \end{array} \quad \begin{array}{l} - \frac{a_{31}}{a_{11}} \cdot \text{1-я строка} \\ - \frac{a_{32}}{a_{22}} \cdot \text{2-я строка} \end{array} \\
 &\left(\begin{array}{cccc|c} a_{11} & a_{12} & a_{13} & a_{14} & b_1 \\ 0 & a_{22} & a_{23} & a_{24} & b_2 \\ 0 & a_{32} & a_{33} & a_{34} & b_3 \end{array}\right) \\
 &\left(\begin{array}{cccc|c} a_{11} & a_{12} & a_{13} & a_{14} & b_1 \\ 0 & a_{22} & a_{23} & a_{24} & b_2 \\ 0 & 0 & a_{33} & a_{34} & b_3 \end{array}\right)
 \end{aligned}$$

В результате данного хода какие-то коэффициенты, например a_{33} , могли занулиться, потому возможны следующие принципиально другие случаи⁴

$$\left(\begin{array}{cccc|c} \underline{a_{11}} & a_{12} & a_{13} & a_{14} & b_1 \\ 0 & \underline{a_{22}} & a_{23} & a_{24} & b_2 \\ 0 & 0 & 0 & \underline{a_{34}} & b_3 \end{array}\right) \quad \left(\begin{array}{cccc|c} \underline{a_{11}} & a_{12} & a_{13} & a_{14} & b_1 \\ 0 & 0 & \underline{a_{23}} & a_{24} & b_2 \\ 0 & 0 & 0 & \underline{a_{34}} & b_3 \end{array}\right) \quad \left(\begin{array}{cccc|c} \underline{a_{11}} & a_{12} & a_{13} & a_{14} & b_1 \\ 0 & \underline{a_{22}} & a_{23} & a_{24} & b_2 \\ 0 & 0 & 0 & 0 & \underline{b_3} \end{array}\right) \quad \left(\begin{array}{cccc|c} \underline{a_{11}} & a_{12} & a_{13} & a_{14} & b_1 \\ 0 & \underline{a_{22}} & a_{23} & a_{24} & b_2 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Главные и неглавные переменные Подчеркнутые элементы считаются не равными нулю. В ступенчатом виде все переменные (и соответственно коэффициенты перед ними) делятся на главные и неглавные. Главные коэффициенты – это первые ненулевые коэффициенты в строке (подчеркнутые). Переменные при них называются главными, остальные ненулевые коэффициенты и переменные – неглавные.

Обратный ход алгоритма Гаусса Разберем типичный обратный ход алгоритма Гаусса. Подчеркнутые элементы считаются не равными нулю.

$$\begin{aligned}
 &\left(\begin{array}{cccc|c} \underline{a_{11}} & a_{12} & a_{13} & a_{14} & b_1 \\ 0 & \underline{a_{22}} & a_{23} & a_{24} & b_2 \\ 0 & 0 & \underline{a_{33}} & a_{34} & b_3 \end{array}\right) \quad \begin{array}{l} \text{разделить } i\text{-ю строку на } a_{ii} \\ \text{2-я строка} \end{array} \\
 &\left(\begin{array}{cccc|c} 1 & a_{12} & a_{13} & a_{14} & b_1 \\ 0 & 1 & a_{23} & a_{24} & b_2 \\ 0 & 0 & 1 & a_{34} & b_3 \end{array}\right) \quad \begin{array}{l} \text{2-я строка} \\ \text{1-я строка} \end{array} \quad \begin{array}{l} - a_{23} \cdot \text{3-я строка} \\ - a_{13} \cdot \text{3-я строка} \end{array} \\
 &\left(\begin{array}{cccc|c} 1 & a_{12} & a_{13} & a_{14} & b_1 \\ 0 & 1 & 0 & a_{24} & b_2 \\ 0 & 0 & 1 & a_{34} & b_3 \end{array}\right) \\
 &\left(\begin{array}{cccc|c} 1 & a_{12} & 0 & a_{14} & b_1 \\ 0 & 1 & 0 & a_{24} & b_2 \\ 0 & 0 & 1 & a_{34} & b_3 \end{array}\right) \quad \begin{array}{l} \text{1-я строка} \\ \text{1-я строка} \end{array} \quad \begin{array}{l} - a_{12} \cdot \text{2-я строка} \\ - a_{12} \cdot \text{2-я строка} \end{array} \\
 &\left(\begin{array}{cccc|c} 1 & 0 & 0 & a_{14} & b_1 \\ 0 & 1 & 0 & a_{24} & b_2 \\ 0 & 0 & 1 & a_{34} & b_3 \end{array}\right)
 \end{aligned}$$

В специальных случаях приведенных выше, получим

$$\left(\begin{array}{cccc|c} 1 & 0 & a_{13} & 0 & b_1 \\ 0 & 1 & a_{23} & 0 & b_2 \\ 0 & 0 & 0 & 1 & b_3 \end{array}\right) \quad \left(\begin{array}{cccc|c} 1 & a_{12} & 0 & 0 & b_1 \\ 0 & 0 & 1 & 0 & b_2 \\ 0 & 0 & 0 & 1 & b_3 \end{array}\right) \quad \left(\begin{array}{cccc|c} 1 & 0 & a_{13} & a_{14} & 0 \\ 0 & 1 & a_{23} & a_{24} & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right) \quad \left(\begin{array}{cccc|c} 1 & 0 & a_{13} & a_{14} & b_1 \\ 0 & 1 & a_{23} & a_{24} & b_2 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Полученный в результате обратного хода вид расширенной матрицы называется улучшенным ступенчатым видом, т.е., это ступенчатый вид, где все коэффициенты при главных неизвестных – единицы, и все коэффициенты над ними равны нулю.

⁴Это не полный список всех случаев.

Удобный формализм Пока мы подробно не говорили о матрицах, введем некие удобные обозначения, которые упростят запись решений СЛУ.

$$a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{R}^n \text{ и } b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \mathbb{R}^n. \text{ Тогда } a + b = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix} \in \mathbb{R}^n \text{ и } \lambda a = \begin{pmatrix} \lambda a_1 \\ \vdots \\ \lambda a_n \end{pmatrix} \in \mathbb{R}^n \text{ для любого } \lambda \in \mathbb{R}.$$

Получение решений В системе ниже, выберем переменную x_4 как параметр

$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & a_{14} & b_1 \\ 0 & 1 & 0 & a_{24} & b_2 \\ 0 & 0 & 1 & a_{34} & b_3 \end{array} \right)$$

Тогда решения имеют вид⁵

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} - x_4 \begin{pmatrix} a_{14} \\ a_{24} \\ a_{34} \end{pmatrix}$$

Специальные случаи:

$$\begin{array}{ll} \left(\begin{array}{cccc|c} 1 & 0 & a_{13} & 0 & b_1 \\ 0 & 1 & a_{23} & 0 & b_2 \\ 0 & 0 & 0 & 1 & b_3 \end{array} \right) & \text{Решения: } \begin{pmatrix} x_1 \\ x_2 \\ x_4 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} - x_3 \begin{pmatrix} a_{13} \\ a_{23} \\ 0 \end{pmatrix} \\ \left(\begin{array}{cccc|c} 1 & a_{12} & 0 & 0 & b_1 \\ 0 & 0 & 1 & 0 & b_2 \\ 0 & 0 & 0 & 1 & b_3 \end{array} \right) & \text{Решения: } \begin{pmatrix} x_1 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} - x_2 \begin{pmatrix} a_{12} \\ 0 \\ 0 \end{pmatrix} \\ \left(\begin{array}{cccc|c} 1 & 0 & a_{13} & a_{14} & 0 \\ 0 & 1 & a_{23} & a_{24} & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array} \right) & \text{Решения: Нет решений, т.к. последнее уравнение } 0 = 1 \\ \left(\begin{array}{cccc|c} 1 & 0 & a_{13} & a_{14} & b_1 \\ 0 & 1 & a_{23} & a_{24} & b_2 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right) & \text{Решения: } \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} - x_3 \begin{pmatrix} a_{13} \\ a_{23} \end{pmatrix} - x_4 \begin{pmatrix} a_{14} \\ a_{24} \end{pmatrix} \end{array}$$

Количество решений в ступенчатом виде Если во время прямого хода алгоритма Гаусса в расширенной матрице системы вам встретилась строка вида $(0 \dots 0 \mid b)$, где b – произвольное ненулевое число, то данная система решений не имеет. В этом случае нет необходимости переходить к обратному ходу. Если же таких строк не встретилось, то система обязательно имеет решения. При этом, если есть свободные переменные, то решений бесконечное число, а если их нет, то решение единственное.

Технические рекомендации Работая с целочисленными матрицами, старайтесь во время прямого хода алгоритма Гаусса не выходить за рамки целых чисел.

- Используйте элементарные преобразования I типа только с целым параметром.
- Полезно не злоупотреблять умножением на ненулевое целое, умножайте только на ± 1 . Иначе придется работать с большими числами.

На этапе обратного хода алгоритма Гаусса избавиться от деления уже не возможно.

⁵Операция умножения матрицы на число покомпонентная (умножаем каждый элемент на число). Сумма и разность двух матриц покомпонентная (складываем или вычитаем числа на одних и тех же позициях).

2 Матрицы

2.1 Определение матриц

Матрица – это прямоугольная таблица чисел

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}, \text{ где } a_{ij} \in \mathbb{R}$$

Множество всех матриц с m строками и n столбцами обозначается $M_{m \times n}(\mathbb{R})$. Множество квадратных матриц размера n будем обозначать $M_n(\mathbb{R})$. Матрицы с одним столбцом или одной строкой называются векторами (вектор-столбцами и вектор-строками соответственно). Множество всех векторов с n координатами обозначается через \mathbb{R}^n . Мы по умолчанию считаем, что наши вектора – вектор-столбцы.⁶

2.2 Операции над матрицами

Сложение Пусть $A, B \in M_{m \times n}(\mathbb{R})$. Тогда сумма $A + B$ определяется покомпонентно, т.е. $C = A + B$, то $c_{ij} = a_{ij} + b_{ij}$ или

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & \dots & a_{1n} + b_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & \dots & a_{mn} + b_{mn} \end{pmatrix}$$

Складывать можно только матрицы одинакового размера.⁷

Умножение на скаляр Если $\lambda \in \mathbb{R}$ и $A \in M_{m \times n}(\mathbb{R})$, то λA определяется так: $\lambda A = C$, где $c_{ij} = \lambda a_{ij}$ или

$$\lambda \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} \lambda a_{11} & \dots & \lambda a_{1n} \\ \vdots & \ddots & \vdots \\ \lambda a_{m1} & \dots & \lambda a_{mn} \end{pmatrix}$$

Умножение матриц Пусть $A \in M_{m \times n}(\mathbb{R})$ и $B \in M_{n \times k}(\mathbb{R})$, то произведение $AB \in M_{m \times k}(\mathbb{R})$ определяется так: $AB = C$, где $c_{ij} = \sum_{t=1}^n a_{it}b_{tj}$ или

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} b_{11} & \dots & b_{1k} \\ \vdots & \ddots & \vdots \\ b_{n1} & \dots & b_{nk} \end{pmatrix} = \begin{pmatrix} \sum_{t=1}^n a_{1t}b_{t1} & \dots & \sum_{t=1}^n a_{1t}b_{tk} \\ \vdots & \ddots & \vdots \\ \sum_{t=1}^n a_{mt}b_{t1} & \dots & \sum_{t=1}^n a_{mt}b_{tk} \end{pmatrix}$$

На умножение матриц можно смотреть следующим образом. Чтобы получить коэффициент c_{ij} надо, из матрицы A взять i -ю строку (она имеет длину n), а из матрицы B взять j -ый столбец (он тоже имеет длину n). Тогда их надо скалярно перемножить и результат подставить в c_{ij} .

Транспонирование Пусть A – матрица вида

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \text{ или } \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} \text{ или } \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

Определим транспонированную матрицу $A^t = (a'_{ij})$ так: $a'_{ij} = a_{ji}$. Наглядно, транспонированная матрица для приведенных выше

$$\begin{pmatrix} a_{11} & \dots & a_{m1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \dots & a_{mn} \end{pmatrix} \text{ или } \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \\ a_{13} & a_{23} \end{pmatrix} \text{ или } (x_1 \ x_2 \ x_3)$$

⁶Важно, directX и OpenGL используют вектор-строки! Потому часть инженерной литературы на английском связанной с трехмерной графикой оперирует со строками. Это важно учитывать, так как нужно вносить поправки в соответствующие формулы.

⁷Можно по аналогии определить и вычитание матриц, но в этом нет необходимости. Например, потому что вычитание можно определить как $A + (-1)B$, где $(-1)B$ – умножение на скаляр. Либо можно определить аксиоматически, как это сделано ниже в следующем разделе.

След матрицы Пусть $A \in M_n(\mathbb{R})$, тогда определим след матрицы A , как сумму ее диагональных элементов: $\text{tr } A = \sum_{i=1}^n a_{ii}$.

2.3 Специальные виды матриц

Ниже мы перечислим названия некоторых специальных классов матриц:

- $A = \begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_n \end{pmatrix}$ – диагональная матрица. Все ненулевые элементы стоят на главной диагонали, то есть в позиции, где номер строки равен номеру столбца.
- $A = \begin{pmatrix} \lambda & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda \end{pmatrix}$ – скалярная матрица. Диагональная матрица с одинаковыми элементами на диагонали.

2.4 Свойства операций

Все операции на матрицах обладают «естественными свойствами» и согласованы друг с другом. Вот перечень базовых свойств операций над матрицами:⁸

1. **Ассоциативность сложения** $(A + B) + C = A + (B + C)$ для любых $A, B, C \in M_{m,n}(\mathbb{R})$
2. **Существование нейтрального элемента для сложения** Существует единственная матрица 0 обладающая следующим свойством $A + 0 = 0 + A = A$ для всех $A \in M_{m,n}(\mathbb{R})$. Такая матрица целиком заполнена нулями.
3. **Коммутативность сложения** $A + B = B + A$ для любых $A, B \in M_{m,n}(\mathbb{R})$.
4. **Наличие обратного по сложению** Для любой матрицы $A \in M_{m,n}(\mathbb{R})$ существует матрица $-A$ такая, что $A + (-A) = (-A) + A = 0$. Такая матрица единственная и состоит из элементов $-a_{ij}$.
5. **Ассоциативность умножения** Для любых матриц $A \in M_{m,n}(\mathbb{R})$, $B \in M_{n,k}(\mathbb{R})$ и $C \in M_{k,t}(\mathbb{R})$ верно $(AB)C = A(BC)$.
6. **Существование нейтрального элемента для умножения** Для каждого k существует единственная матрица $E \in M_k(\mathbb{R})$ такая, что для любой $A \in M_{m,n}(\mathbb{R})$ верно $EA = AE = A$. У такой матрицы $E_{ii} = 1$, а $E_{ij} = 0$. Когда нет путаницы, матрицу E обозначают через 1 .
7. **Дистрибутивность умножения относительно сложения** Для любых матриц $A, B \in M_{m,n}(\mathbb{R})$ и $C \in M_{n,k}(\mathbb{R})$ верно $(A + B)C = AC + BC$. Аналогично, для любых $A \in M_{m,n}(\mathbb{R})$ и $B, C \in M_{n,k}(\mathbb{R})$ верно $A(B + C) = AB + AC$.
8. **Умножение на числа ассоциативно** Для любых $\lambda, \mu \in \mathbb{R}$ и любой матрицы $A \in M_{m,n}(\mathbb{R})$ верно $\lambda(\mu A) = (\lambda\mu)A$. Аналогично для любого $\lambda \in \mathbb{R}$ и любых $A \in M_{m,n}(\mathbb{R})$ и $B \in M_{n,k}(\mathbb{R})$ верно $\lambda(AB) = (\lambda A)B$.
9. **Умножение на числа дистрибутивно относительно сложения матриц и сложения чисел** Для любых $\lambda, \mu \in \mathbb{R}$ и $A \in M_{m,n}(\mathbb{R})$ верно $(\lambda + \mu)A = \lambda A + \mu A$. Аналогично, для любого $\lambda \in \mathbb{R}$ и $A, B \in M_{m,n}(\mathbb{R})$ верно $\lambda(A + B) = \lambda A + \lambda B$.
10. **Умножение на скаляр нетривиально** Если $1 \in \mathbb{R}$, то для любой матрицы $A \in M_{m,n}(\mathbb{R})$ верно $1A = A$.
11. **Умножение на скаляр согласовано с умножением матриц** Для любого $\lambda \in \mathbb{R}$ и любых $A \in M_{m,n}(\mathbb{R})$ и $B \in M_{n,k}(\mathbb{R})$ верно $\lambda(AB) = (\lambda A)B = A(\lambda B)$.
12. **Транспонирование согласовано с суммой** Для любых матриц $A, B \in M_{m,n}(\mathbb{R})$ верно $(A + B)^t = A^t + B^t$.

⁸Все эти свойства объединяет то, что они являются аксиомами в различных определениях для алгебраических структур. Позже мы столкнемся с такими структурами.

13. **Транспонирование согласовано с умножением на скаляр** Для любой матрицы $A \in M_{m,n}(\mathbb{R})$ и любого $\lambda \in \mathbb{R}$ верно $(\lambda A)^t = \lambda A^t$.
14. **Транспонирование согласовано с умножением** Для любых матриц $A, B \in M_{m,n}(\mathbb{R})$ верно $(AB)^t = B^t A^t$.

К этим свойствам надо относиться так. Доказывая что-то про матрицы, можно лезть внутрь определений операций над ними, а можно пользоваться свойствами операций. Так вот, список выше – это минимальный набор свойств операций, из которых можно вытащить базовую информацию про эти операции и при этом не лезть внутрь определений.

Нулевые строки и столбцы Пусть в матрице $A \in M_{m,k}(\mathbb{R})$ i -я строка полностью состоит из нулей и нам дана матрица $B \in M_{k,n}(\mathbb{R})$. Тогда в произведении AB i -я строка тоже будет нулевой. Изобразим это ниже графически

$$AB = \begin{pmatrix} * & * & \dots & * \\ * & * & \dots & * \\ 0 & 0 & \dots & 0 \\ * & * & \dots & * \end{pmatrix} \begin{pmatrix} * & * & \dots & * \\ * & * & \dots & * \\ * & * & \dots & * \\ * & * & \dots & * \end{pmatrix} = \begin{pmatrix} * & * & \dots & * \\ * & * & \dots & * \\ 0 & 0 & \dots & 0 \\ * & * & \dots & * \end{pmatrix}$$

Действительно, i -я строка произведения зависит от i -ой строки левого множителя (матрицы A) и всех столбцов B . Но умножая нулевую строку A на что угодно, получим нули в i -ой строке результата. Аналогичное утверждение верно для столбцов в матрице B , а именно. Пусть в матрице $B \in M_{k,n}(\mathbb{R})$ i -ый столбец полностью состоит из нулей и нам дана матрица $A \in M_{m,k}(\mathbb{R})$. Тогда в произведении AB i -ый столбец тоже будет нулевой.

$$AB = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ \vdots & \vdots & \vdots & \vdots \\ * & * & * & * \end{pmatrix} \begin{pmatrix} * & * & 0 & * \\ * & * & 0 & * \\ \vdots & \vdots & \vdots & \vdots \\ * & * & 0 & * \end{pmatrix} = \begin{pmatrix} * & * & 0 & * \\ * & * & 0 & * \\ \vdots & \vdots & \vdots & \vdots \\ * & * & 0 & * \end{pmatrix}$$

2.5 Связь с системами линейных уравнений

Пусть нам дана система линейных уравнений соответствующая матрицам

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad (A|b) = \left(\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & b_m \end{array} \right)$$

Мы кратко записывали такую систему $Ax = b$, а ее однородную версию через $Ax = 0$. Но теперь, когда мы знаем умножение матриц, видно, что Ax – это произведение матрицы A , на вектор неизвестных x .

Главные бонус от матриц и операций над ними заключается вот в чем. У нас исходно была большая и неуклюжая система линейных уравнений, в которой участвовали очень знакомые и простые для использования числа. Теперь же мы заменили много линейных уравнений с кучей неизвестных на одно линейное матричное уравнение $Ax = b$. Однако, теперь вместо приятных в использовании чисел у нас встретились более сложные объекты – матрицы. Потому к матрицам надо относиться как к более продвинутой версии чисел.

Линейная структура Пусть у нас дана система $Ax = b$ как выше. Тогда $y \in \mathbb{R}^n$ является решением этой системы, если выполнено матричное равенство $Ay = b$. Аналогично и для однородной системы. Теперь заметим следующее:

1. Если $y_1, y_2 \in \mathbb{R}^n$ – решения системы $Ax = 0$, то $y_1 + y_2$ тоже является решением системы $Ax = 0$. Действительно, надо показать, что $A(y_1 + y_2) = 0$. Но $A(y_1 + y_2) = Ay_1 + Ay_2 = 0 + 0 = 0$.
2. Если $y \in \mathbb{R}^n$ – решение системы $Ax = 0$ и $\lambda \in \mathbb{R}$, то λy – тоже решение $Ax = 0$. Действительно, $A(\lambda y) = \lambda Ay = 0$.

Теперь сравним решения систем $Ax = b$ и $Ax = 0$. Прежде всего заметим, что однородная система всегда имеет решение $x = 0$. И вообще говоря, может так оказаться, что $Ax = b$ не имеет решений. Например, $(A|b) = (0|1)$. Однако, если $Ax = b$ совместна, то обе системы имеют «одинаковое число» решений.

Утверждение. Пусть система $Ax = b$ имеет хотя бы одно решение $z \in \mathbb{R}^n$ и пусть $E_b \subseteq \mathbb{R}^n$ – множество решений $Ax = b$ и $E_0 \subseteq \mathbb{R}^n$ – множество решений $Ax = 0$. Тогда $E_b = z + E_0 = \{z + y \mid y \in E_0\}$.

Доказательство. Для доказательства $z + E_0 \subseteq E_b$ надо заметить, что если $y \in E_0$, то $z + y \in E_b$. Для обратного включения проверяется, что если $z' \in E_b$, то $z' - z \in E_0$. \square

2.6 Дефекты матричных операций

Матрицы как новые числа Рассмотрим множество квадратных матриц с введенными выше операциями: $(M_n(\mathbb{R}), +, -, \cdot, {}^t)$. Про это множество стоит думать как про новый вид чисел со своими операциями. Принципиальное отличие – нельзя делить на любую ненулевую матрицу, как это можно было делать с числами. Однако, это не единственное отличие.

Аномалии матричных операций Матричные операции обладают несколькими аномалиями по сравнению со свойствами операций над обычными числами.

1. Существование вычитания следует из «хорошести» операции сложения. Она позволяет определить вычитание без проблем. Однако, операция умножения уже хуже, чем на обычных числах, потому не получится определить на матрицах операцию деления.
2. Умножение матриц НЕ коммутативно. Действительно

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{но} \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

3. В матрицах есть «делители нуля», т.е. существуют две ненулевые матрицы A и B такие, что $AB = 0$.⁹
Пример:

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

4. В матрицах есть «нильпотенты», то есть можно найти такую ненулевую матрицу A , что $A^n = 0$. Пример,

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

2.7 Деление

Что значит деление в числах? Предположим, что у нас есть два числа $a, b \in \mathbb{R}$. Тогда деление $a/b = a \cdot b^{-1}$ – это просто умножение на обратный элемент, а обратный элемент b^{-1} определяется свойством $bb^{-1} = 1$. Данное наблюдение дает ключ к распространению деления и обращения на случай матриц. А именно, вместо деления, мы будем рассматривать обратные матрицы и умножение на них. Вот неочевидное преимущество такого подхода. Из-за некоммутативности матричного умножения, нам пришлось бы вводить два вида деления: левое и правое. А значит, пришлось бы изучать свойства двух операций и их согласованность. Вместо этого, намного проще изучать обратные матрицы и умножать на них слева и справа с помощью обычного умножения.

Односторонняя обратимость Пусть $A \in M_{m,n}(\mathbb{R})$, будем говорить, что $B \in M_{n,m}(\mathbb{R})$ является левым обратным к A , если $BA = E \in M_n(\mathbb{R})$. Аналогично, $B \in M_{n,m}(\mathbb{R})$ – правый обратный к A , если $AB = E \in M_m(\mathbb{R})$. Надо иметь в виду, что вообще говоря левые и правые обратные между собой никак не связаны и их может быть много. Например, пусть $A = (1, 0) \in M_{1,2}(\mathbb{R})$. Тогда у такой матрицы нет левого обратного, а любая матрица вида $(1, a)^t$ является правым обратным. Если для матрицы A существует левый обратный, то она называется обратимой слева. Аналогично, при существовании правого обратного – обратимой справа.

⁹На самом деле, это очень «хорошая» аномалия, так как она связана с тем, что ОСЛУ имеют решения. Действительно, вопрос решения ОСЛУ $Ax = 0$ – это в точности вопрос существования правых делителей нуля для A в множестве \mathbb{R}^n .

Обратимые матрицы Матрица $A \in M_n(\mathbb{R})$ называется обратимой, если к ней существует левый и правый обратный.¹⁰

Утверждение. Пусть матрица $A \in M_n(\mathbb{R})$ обратима. Тогда левый обратный и правый обратный единственны и совпадают друг с другом.

Доказательство. Пусть $L \in M_n(\mathbb{R})$ – произвольный левый обратный к A , а $R \in M_n(\mathbb{R})$ – произвольный правый обратный. Тогда рассмотрим выражение LAR , расставляя по разному скобки имеем:

$$R = ER = (LA)R = L(AR) = LE = L$$

Теперь, если L и L' – два разных левых обратных. Зафиксируем произвольный правый обратный R . Из выше сказанного следует, что $L = R$ и $L' = R$. Значит все левые обратные равны между собой. Аналогично для правых. \square

Значит, если матрица A обратима, то существует единственная матрица B , удовлетворяющая свойствам $AB = BA = E$. Такую матрицу B обозначают A^{-1} и называют обратной к матрице A .

Утверждение. Пусть $A, B \in M_n(\mathbb{R})$ – обратимые матрицы. Тогда

1. AB тоже обратима и при этом $(AB)^{-1} = B^{-1}A^{-1}$.
2. A^t также будет обратима и $(A^t)^{-1} = (A^{-1})^t$ и обозначается A^{-t} .

Доказательство. 1) Действительно, надо проверить, что для AB существует двусторонняя обратная. Заметим, что $B^{-1}A^{-1}$ является таковой:

$$ABB^{-1}A^{-1} = E \quad \text{и} \quad B^{-1}A^{-1}AB = E$$

В частности, последнее означает, что $(AB)^{-1} = B^{-1}A^{-1}$.

2) Пусть матрица A обратима, тогда

$$AA^{-1} = E \quad \text{и} \quad A^{-1}A = E$$

Транспонируем оба равенства, получим

$$(A^{-1})^t A^t = E \quad \text{и} \quad A^t (A^{-1})^t = E$$

Это означает, что A^t обратима и при этом $(A^t)^{-1} = (A^{-1})^t$. \square

Обратимые преобразования над СЛУ Пусть у нас есть $A \in M_{m,n}(\mathbb{R})$ и $b \in \mathbb{R}^m$, которые задают систему линейных уравнений $Ax = b$, где $x \in \mathbb{R}^n$. Возьмем произвольную обратимую матрицу $C \in M_m(\mathbb{R})$. Тогда система $Ax = b$ эквивалентна системе $CAx = Cb$. Действительно, если для некоторого $y \in \mathbb{R}^n$ имеем $Ay = b$, то, умножая обе части на C слева, получим $CAy = Cb$, значит y решение второй системы. Наоборот, пусть $CAy = Cb$, тогда, умножая обе части на C^{-1} слева, получим $Ay = b$, значит y решение первой системы.

Сказанное выше значит, что мы можем менять СЛУ на эквивалентные с помощью умножения слева на любую обратимую матрицу. Мы уже знаем, что есть другая процедура преобразования СЛУ с таким же свойством – применение элементарных преобразований. Возникает резонный вопрос: какая процедура лучше? Оказывается, что между ними нет разницы в том смысле, что умножение на обратимую матрицу всегда совпадает с некоторой последовательностью элементарных преобразований и наоборот любое элементарное преобразование можно выразить с помощью умножения на обратимую матрицу. Этому свойству и будет посвящен остаток лекции.

¹⁰Можно было бы определить обратимую матрицу и в неквадратном случае. Однако, можно показать, что не бывает обратимых неквадратных матриц.

2.8 Матрицы элементарных преобразований

Тип I Пусть $S_{ij}(\lambda) \in M_n(\mathbb{R})$ – матрица, полученная из единичной вписыванием в ячейку i, j числа λ (при этом $i \neq j$, то есть ячейка берется не на диагонали). Эта матрица имеет следующий вид:

$$i \quad \begin{matrix} & & j & \\ \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \lambda & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} \end{matrix}$$

Тогда прямая проверка показывает, умножение $A \in M_{nm}(\mathbb{R})$ на $S_{ij}(\lambda)$ слева прибавляет j строку умноженную на λ к i строке матрицы A , а умножение $B \in M_{mn}(\mathbb{R})$ на $S_{ij}(\lambda)$ справа прибавляет i столбец умноженный на λ к j столбцу матрицы B . Заметим, что $S_{ij}(\lambda)^{-1} = S_{ij}(-\lambda)$.

Тип II Пусть $T_{ij} \in M_n(\mathbb{R})$ – матрица, полученная из единичной перестановкой i и j столбцов (или что то же самое – строк). Эта матрица имеет следующий вид

$$\begin{matrix} & i & & j \\ i & \begin{pmatrix} 1 & & & \\ & 0 & & 1 \\ & & \ddots & \\ & 1 & & 0 \\ & & & 1 \end{pmatrix} & & \\ j & & & \end{matrix}$$

Тогда прямая проверка показывает, умножение $A \in M_{nm}(\mathbb{R})$ на T_{ij} слева переставляет i и j строки матрицы A , а умножение $B \in M_{mn}(\mathbb{R})$ на T_{ij} справа переставляет i и j столбцы матрицы B . Заметим, что $T_{ij}^{-1} = T_{ij}$.

Тип III Пусть $D_i(\lambda) \in M_n(\mathbb{R})$ – матрица, полученная из единичной умножением i строки на $\lambda \in \mathbb{R} \setminus 0$ (или что то же самое – столбца). Эта матрица имеет следующий вид

$$i \quad \begin{matrix} & & i & \\ \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \lambda & \\ & & & \ddots \\ & & & & 1 \end{pmatrix} \end{matrix}$$

Тогда прямая проверка показывает, умножение $A \in M_{nm}(\mathbb{R})$ на $D_i(\lambda)$ слева умножает i строку A на λ , а умножение $B \in M_{mn}(\mathbb{R})$ на $D_i(\lambda)$ справа умножает i столбец матрицы B на λ . Заметим, что $D_i(\lambda)^{-1} = D_i(\lambda^{-1})$.

2.9 Невырожденные матрицы

Начнем с полезного утверждения.

Утверждение 1. Пусть $A \in M_n(\mathbb{R})$ – произвольная квадратная матрица. Тогда следующие условия эквивалентны:

1. Систем $Ax = 0$ имеет только нулевое решение.
2. Система $A^t y = 0$ имеет только нулевое решение.
3. Матрица A представляется в виде $A = U_1 \cdot \dots \cdot U_k$, где U_i – матрицы элементарных преобразований.
4. Матрица A обратима.
5. Матрица A обратима слева, т.е. существует L такая, что $LA = E$.

6. Матрица A обратима справа, т.е. существует R такая, что $AR = E$.

Определение 2. Пусть $A \in M_n(\mathbb{R})$ – произвольная квадратная матрица. Будем говорить, что A невырождена¹¹, если удовлетворяет любому из перечисленных в предыдущем утверждении условий.

Доказательство Утверждения 1. (1) \Rightarrow (3). Приведем A к улучшенному ступенчатому виду с помощью Гаусса. Так как $Ax = 0$ имеет только нулевое решение, то ступенчатый вид – это единичная матрица E . Пусть S_1, \dots, S_k – матрицы элементарных преобразований, которые мы совершили во время Гаусса. Это значит, что мы произвели следующие манипуляции

$$A \mapsto S_1 A \mapsto S_2 S_1 A \mapsto \dots \mapsto (S_k \dots S_1 A) = E$$

То есть $A = S_1^{-1} \dots S_k^{-1}$. Заметим, что S_i^{-1} – это матрица обратного элементарного преобразования к S_i . Обозначим $U_i = S_i^{-1}$ и получим требуемое.

(2) \Rightarrow (3). Проведем предыдущее рассуждение для матрицы A^t вместо A . Получим, что $A^t = U_1 \dots U_k$. Тогда $A = U_k^t \dots U_1^t$. Теперь осталось заметить, что U_i^t тоже является матрицей элементарного преобразования.

(3) \Rightarrow (4). Мы имеем $A = U_1 \dots U_k$, причем каждая из U_i обратима. Так как произведение обратимых обратима, то A также обратима.

(4) \Rightarrow (5) и (4) \Rightarrow (6) очевидно, так это переход от более сильного условия к более слабому.

(5) \Rightarrow (1). Пусть A обратима слева и нам надо решить систему $Ax = 0$. Умножим ее слева на левый обратный к A , получим $x = 0$, что и требовалось.

(6) \Rightarrow (2). Пусть A обратима справа и нам надо решить систему $A^t y = 0$. Умножим эту систему слева на R^t , где R – правый обратный к A . Тогда $R^t A^t x = 0$. Но $R^t A^t x = (AR)^t x = Ex = x = 0$, что и требовалось. \square

В силу этого утверждения, мы не будем различать невырожденные и обратимые матрицы между собой.

Делители нуля Пусть $A \in M_n(\mathbb{R})$ – некоторая ненулевая матрица и пусть $B \in M_{nm}(\mathbb{R})$. Матрица B называется правым делителем нуля для A , если $AB = 0$. Условие (1) предыдущего утверждения эквивалентно отсутствию правых делителей нуля. Условие (1) не сильнее, значит надо показать, что оно влечет отсутствие делителей нуля. Если B – правый делитель нуля для A , то любой столбец b матрицы B удовлетворяет условию $Ab = 0$, а значит нулевой.

Аналогично определяются левые делители нуля для A и показывается, что их отсутствие равносильно условию (2) предыдущего результата.

Элементарные преобразования и обратимость Пусть $A \in M_{mn}(\mathbb{R})$ и $b \in \mathbb{R}^m$. Тогда у нас есть две процедуры преобразования СЛУ $Ax = b$:

1. Применение элементарных преобразований к строкам системы.
2. Умножение обеих частей равенства на обратимую матрицу: $Ax = b$ меняем на $CAx = Cb$, где $C \in M_n(\mathbb{R})$ – обратимая.

Так как любое элементарное преобразование сводится к умножению слева на обратимую матрицу, то мы видим, что первый вид модификации систем является частным случаем второго. В обратную сторону, из доказанного утверждения следует, что любая обратимая матрица может быть расписана как произведение матриц элементарных преобразований. Значит, умножить на обратимую матрицу слева – это все равно что сделать последовательность элементарных преобразований.

Главный плюс элементарных преобразований – у них простые матрицы, а минус – их нужно много, очень много, чтобы преобразовать одну систему в другую. С обратимыми матрицами все наоборот: сами матрицы устроены непонятно как, но зато нужно всего одно умножение матриц, чтобы перевести систему из одной в другую. Именно на это надо обращать внимание при выборе подхода по преобразованию систем.

¹¹Классически невырожденные матрицы определяются совсем по-другому, однако, все эти определения между собой эквивалентны. Будьте готовы к тому, что в литературе вы увидите совсем другое определение.

Насыщенность обратимых Я хочу продемонстрировать еще одно полезное следствие из Утверждения 1. Предположим у нас есть две матрицы $A, B \in M_n(\mathbb{R})$. Тогда AB обратима тогда и только тогда, когда A и B обратимы. Действительно, справа налево мы уже знаем, обратимость обеих матриц A и B влечет обратимость произведения, мы даже знаем, что при этом $(AB)^{-1} = B^{-1}A^{-1}$. Надо лишь показать в обратную сторону. Предположим, что AB обратима, это значит, что для некоторой матрицы $D \in M_n(\mathbb{R})$ выполнено

$$ABD = E \quad \text{и} \quad DAB = E$$

Тогда первое равенство говорит, что BD является правым обратным к A . А в силу эквивалентности пунктов (4) и (6) Утверждения 1 это означает, что A обратима. Аналогично, DA является левым обратным к B и в силу эквивалентности пунктов (4) и (5) Утверждения 1, матрица B обратима. Так что произведение матриц обратимо тогда и только тогда, когда каждый сомножитель обратим.

2.10 Блочное умножение матриц

Формулы блочного умножения Пусть даны две матрицы, которые разбиты на блоки как показано ниже:

$$\begin{matrix} & \begin{matrix} k & s \end{matrix} \\ \begin{matrix} m \\ n \end{matrix} & \begin{pmatrix} A & B \\ C & D \end{pmatrix} \end{matrix} \quad \begin{matrix} & \begin{matrix} u & v \end{matrix} \\ \begin{matrix} k \\ s \end{matrix} & \begin{pmatrix} X & Y \\ W & Z \end{pmatrix} \end{matrix}$$

Числа m, n, k, s, u, v – размеры соответствующих блоков. Наша цель понять, что эти матрицы можно перемножать блочно. А именно, увидеть, что результат умножения этих матриц имеет вид

$$\begin{matrix} & \begin{matrix} u & v \end{matrix} \\ \begin{matrix} m \\ n \end{matrix} & \begin{pmatrix} AX + BW & AY + BZ \\ CX + DW & CY + DZ \end{pmatrix} \end{matrix}$$

Делается это таким трюком. В начале заметим, что

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

После чего методом «пристального взгляда» перемножаем матрицы с большим количеством нулей (попробуйте проделать это!).

На этот факт можно смотреть вот как. Матрица – это прямоугольная таблица заполненная числами. А можно составлять прямоугольные таблицы заполненные другими объектами, например матрицами. Тогда они складываются и перемножаются так же как и обычные матрицы из чисел. Единственное надо учесть, что в блочном умножении есть разница между $AX + BW$ и $XA + BW$, так как A, B, X и W не числа, а матрицы, то их нельзя переставлять местами, порядок теперь важен.

Вот полезный пример. Пусть дана матрица из $M_{n+1}(\mathbb{R})$ вида

$$\begin{pmatrix} A & v \\ 0 & \lambda \end{pmatrix}, \quad \text{где } A \in M_n(\mathbb{R}), \quad v \in \mathbb{R}^n, \quad \lambda \in \mathbb{R}$$

Тогда

$$\begin{pmatrix} A & v \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} A & v \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} A^2 & Av + v\lambda \\ 0 & \lambda^2 \end{pmatrix} = \begin{pmatrix} A^2 & Av + \lambda v \\ 0 & \lambda^2 \end{pmatrix} = \begin{pmatrix} A^2 & (A + \lambda E)v \\ 0 & \lambda^2 \end{pmatrix}$$

Предпоследнее равенство верно, так как не важно с какой стороны умножать v на скаляр λ .

Вот еще один полезный пример блочного умножения. Пусть $x_1, \dots, x_m \in \mathbb{R}^n$ и $y_1, \dots, y_m \in \mathbb{R}^n$ – столбцы. Составим из этих столбцов матрицы $X = (x_1 | \dots | x_m)$ и $Y = (y_1 | \dots | y_m)$.¹² Заметим, что $X, Y \in M_{n \times m}(\mathbb{R})$. Тогда

$$XY^t = (x_1 | \dots | x_m)(y_1 | \dots | y_m)^t = \sum_{i=1}^m x_i y_i^t$$

¹² Данная запись означает, что мы берем столбцы x_i и записываем их подряд в одну большую таблицу.

2.11 Блочные элементарные преобразования

Преобразования первого типа Пусть у нас дана матрица

$$\begin{matrix} & k & s \\ m & \begin{pmatrix} A & B \end{pmatrix} \\ n & \begin{pmatrix} C & D \end{pmatrix} \end{matrix}$$

Я хочу взять первую «строку» из матриц (A, B) умножить ее на некую матрицу R слева и прибавить результат к «строке» (C, D) . Для этого матрица R должна иметь n строк и m столбцов. То есть процедура будет выглядеть следующим образом

$$\begin{matrix} & k & s \\ m & \begin{pmatrix} A & B \end{pmatrix} \\ n & \begin{pmatrix} C & D \end{pmatrix} \end{matrix} \mapsto \begin{matrix} & k & s \\ m & \begin{pmatrix} A & B \end{pmatrix} \\ n & \begin{pmatrix} C + RA & D + RB \end{pmatrix} \end{matrix}$$

Оказывается, что такая процедура является умножением на обратимую матрицу слева, а именно

$$\begin{matrix} m & n \\ n & \end{matrix} \begin{pmatrix} E & 0 \\ R & E \end{pmatrix} \begin{matrix} k & s \\ m & n \end{matrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{matrix} k & s \\ m & n \end{matrix} \begin{pmatrix} A & B \\ C + RA & D + RB \end{pmatrix}$$

Заметим, что

$$\begin{pmatrix} E & 0 \\ R & E \end{pmatrix}^{-1} = \begin{pmatrix} E & 0 \\ -R & E \end{pmatrix}$$

В частности из этого наблюдения следует, что блочные элементарные преобразования строк не меняют множества решений соответствующей системы.

Аналогично можно делать блочные элементарные преобразования столбцов. А именно

$$\begin{matrix} m & k & s \\ n & \begin{pmatrix} A & B \\ C & D \end{pmatrix} \end{matrix} \mapsto \begin{matrix} m & k & s \\ n & \begin{pmatrix} A & B + AT \\ C & D + CT \end{pmatrix} \end{matrix}$$

где T матрица с k строками и s столбцами. Как и в случае преобразований со строками, эта процедура сводится к операции умножения на обратимую матрицу справа

$$\begin{matrix} m & k & s \\ n & \begin{pmatrix} A & B \\ C & D \end{pmatrix} \end{matrix} \begin{matrix} k & s \\ s & \end{matrix} \begin{pmatrix} E & T \\ 0 & E \end{pmatrix} = \begin{matrix} k & s \\ m & n \end{matrix} \begin{pmatrix} A & B + AT \\ C & D + CT \end{pmatrix}$$

Как и раньше

$$\begin{pmatrix} E & T \\ 0 & E \end{pmatrix}^{-1} = \begin{pmatrix} E & -T \\ 0 & E \end{pmatrix}$$

Замечание Обратите внимание, что при блочных преобразованиях строк умножение на матрицу-коэффициент R происходит слева, а при преобразованиях столбцов умножение на матрицу-коэффициент T происходит справа.

Преобразования второго типа Преобразование вида

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \mapsto \begin{pmatrix} C & D \\ A & B \end{pmatrix}$$

сводится к умножению на обратимую блочную матрицу слева

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

А преобразование

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \mapsto \begin{pmatrix} B & A \\ D & C \end{pmatrix}$$

сводится к умножению на обратимую блочную матрицу справа

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

При этом

$$\begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix}$$

Преобразования третьего типа Если $R \in M_m(\mathbb{R})$ – обратимая матрица, то

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \mapsto \begin{pmatrix} RA & RB \\ C & D \end{pmatrix}$$

является преобразованием умножения на обратимую матрицу слева, а именно

$$\begin{pmatrix} R & 0 \\ 0 & E \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} RA & RB \\ C & D \end{pmatrix}$$

при этом

$$\begin{pmatrix} R & 0 \\ 0 & E \end{pmatrix}^{-1} = \begin{pmatrix} R & 0 \\ 0 & E \end{pmatrix}$$

Аналогично, для обратимой матрицы $T \in M_k(\mathbb{R})$, преобразование

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \mapsto \begin{pmatrix} AT & B \\ CT & D \end{pmatrix}$$

является преобразованием умножения на обратимую матрицу справа, а именно

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} T & 0 \\ 0 & E \end{pmatrix} = \begin{pmatrix} AT & B \\ CT & D \end{pmatrix}$$

Как и раньше, при работе со строками умножение на матрицу-коэффициент происходит слева, а при работе со столбцами – справа.

2.12 Массовое решение систем

Пусть нам надо решить сразу несколько систем $Ax_1 = b_1, \dots, Ax_k = b_k$, где $A \in M_{m \times n}(\mathbb{R})$, $b_i \in \mathbb{R}^m$ и $x_i \in \mathbb{R}^n$. Определим матрицы $X = (x_1 | \dots | x_k) \in M_{n \times k}(\mathbb{R})$ и $B = (b_1 | \dots | b_k) \in M_{m \times k}(\mathbb{R})$ составленные из столбцов x_i и b_i соответственно. Тогда по формулам блочного умножения матриц

$$AX = A(x_1 | \dots | x_k) = (Ax_1 | \dots | Ax_k) = (b_1 | \dots | b_k) = B$$

То есть массовое решение системы уравнений равносильно решению матричного уравнения $AX = B$.

Решение матричных уравнений

Дано $A \in M_{m \times n}(\mathbb{R})$, $B \in M_{m \times k}(\mathbb{R})$.

Задача Найти $X \in M_{n \times k}(\mathbb{R})$ такую, что $AX = B$.

Алгоритм

1. Составить расширенную матрицу $(A|B)$. Например, если $A \in M_{3 \times 3}(\mathbb{R})$, а $B \in M_{3 \times 2}(\mathbb{R})$, то получим

$$(A|B) = \left(\begin{array}{ccc|cc} a_{11} & a_{12} & a_{13} & b_{11} & b_{12} \\ a_{21} & a_{22} & a_{23} & b_{21} & b_{22} \\ a_{31} & a_{32} & a_{33} & b_{31} & b_{32} \end{array} \right)$$

2. Привести расширенную матрицу $(A|B)$ к улучшенному ступенчатому виду. В примере выше, может получиться

$$\left(\begin{array}{ccc|cc} 1 & a_{12} & 0 & b_{11} & 0 \\ 0 & 0 & 1 & b_{21} & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array} \right) \text{ или } \left(\begin{array}{ccc|cc} 1 & 0 & a_{13} & b_{11} & b_{12} \\ 0 & 1 & a_{23} & b_{21} & b_{22} \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

3. Для каждого столбца матрицы X выразить его главные переменные через свободные и записать ответ в виде матрицы. Если для какого-то столбца решений нет, то нет решений и у матричного уравнения $AX = B$. В примере выше, в первом случае нет решения для второго столбца, потому что решений нет в этом случае. Во втором случае,

$$X = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -a_{13} \\ -a_{23} \\ 1 \end{pmatrix} \begin{pmatrix} t & u \end{pmatrix}, \text{ где } t, u \in \mathbb{R}$$

Если нужно решить матричное уравнение $XA = B$ для матриц соответствующего размера, то можно его транспонировать и свести задачу к рассмотренной. А именно, это уравнение равносильно уравнению $A^t X^t = B^t$. Тогда его можно решать относительно X^t , а потом транспонировать ответ.

Нахождение обратной матрицы методом Гаусса

Дано Матрица $A \in M_n(\mathbb{R})$.

Задача Понять обратима ли матрица A и если она обратима, то найти ее обратную A^{-1} .

Алгоритм

1. Нам надо по сути решить систему $AX = E$, где E – единичная матрица. Потому составим расширенную матрицу системы $(A|E)$.
2. Приведем эту матрицу к улучшенному ступенчатому виду.
3. В результате возможны 2 случая:
 - (а) После приведения получили матрицу $(E|B)$. Тогда A обратима и $A^{-1} = B$.
 - (б) После приведения получили матрицу $(D|B)$ и у матрицы D есть свободные позиции. Тогда матрица A не обратима.

Заметим, что если в процессе алгоритма, мы слева от черты в расширенной матрице нашли свободную переменную, то на этом можно остановиться – матрица A необратима.

Корректность алгоритма Давайте я поясню почему алгоритм работает корректно. Пусть у нас есть система $AX = B$ с краткой записью $(A|B)$. Если мы применим элементарное преобразование строк к краткой записи, то это будет означать умножение на матрицу элементарного преобразования слева, то есть при переходе $(A|B) \mapsto (UA|UB)$ мы меняем систему $AX = B$ на $UAX = UB$. А значит, если матрица X была решением $AX = B$, то мы имеем верное равенство двух матриц $AX = B$. Если две одинаковые матрицы слева домножить на одну и ту же матрицу, то результат получится равным, то есть отсюда следует, что $UAX = UB$. То есть любое решение системы $AX = B$ превращается в решение системы $UAX = UB$. Так как матрица элементарного преобразования U обратима, то мы можем домножить второе на U^{-1} , а значит работает рассуждение в обратную сторону и все решения второй являются решениями первой.

Теперь мы знаем, что меняя по алгоритму систему, мы не меняем множество решений. Кроме того, по алгоритму, у нас в результате работы бывают две ситуации, либо мы приходим к ситуации $(E|B)$ либо к $(D|B)$ и в D есть свободная позиция. Давайте разберем их отдельно.

1. Пусть мы привели систему к виду $(E|B)$. Эта запись соответствует системе $EX = B$, то есть $X = B$. Более того, полученная система эквивалентна исходной $AX = B$. Теперь мы видим, что у системы $X = B$ единственное решение B , а это значит что и у системы $AX = B$ единственное решение B (так как они эквивалентны). А значит в этом случае B – это правая обратная к A , а следовательно и просто обратная.

2. Теперь предположим, что мы получим $(D|B)$, где у D есть свободная переменная. Так как мы переходили от $(A|E)$ к $(D|B)$ элементарными преобразованиями строк, то для некоторой обратимой матрицы $C \in M_n(\mathbb{R})$ выполнено $D = CA$. Так как у матрицы D есть свободная позиция и она квадратная ¹³ То обязательно найдется нулевая строка. А раз так, то матрица D не может быть обратима справа. Действительно, тогда в произведении DR для любой $R \in M_n(\mathbb{R})$ будет иметь нулевую строку там же, где нулевая строка у D . А значит, не может быть E . Раз матрица D не обратима, то и матрица A не обратима, иначе D была бы обратима, как произведение обратимых матриц.

2.13 Классификация СЛУ

Единственность улучшенного ступенчатого вида Давайте в начале ответим на очень важный вопрос: а единственный ли у матрицы улучшенный ступенчатый вид? Очевидно, что ступенчатый вид не единственный. Однако, улучшенный ступенчатый вид окажется однозначно определенным. Это означает, что у ступенчатого вида однозначно определена его форма (количество и длины ступенек). В частности у любой СЛУ однозначно определены главные и свободные переменные. Все это не бросается сразу в глаза и требует доказательства. Давайте начнем с простого наблюдения.

Утверждение 3. Пусть $A \in M_{mn}(\mathbb{R})$ и $B \in M_{kn}(\mathbb{R})$ – матрицы в ступенчатом виде, причем B получена из A выкидыванием одного ненулевого уравнения. Тогда системы $Ax = 0$ и $Bx = 0$ не эквивалентны. ¹⁴

Доказательство. Пусть для определенности A и B имеют следующий вид (все незаполненные места предполагаются нулями):

$$A = \begin{pmatrix} & & & k & & & & \\ * & * & * & * & * & * & * & * \\ & & * & * & * & * & * & * \\ & & & & * & * & * & * \\ & & & & & * & * & \end{pmatrix} \quad B = \begin{pmatrix} & & & k & & & & \\ * & * & * & * & * & * & * & * \\ & & & & & & & \\ & & & & & * & * & * \\ & & & & & & * & * \end{pmatrix}$$

И пусть уравнение, которым они различаются начинается с k -ой позиции, т.е. x_k – главная переменная в A , но неглавная в B .

Пусть $E_A, E_B \subseteq \mathbb{R}^n$ – множества решений систем $Ax = 0$ и $Bx = 0$, соответственно. Так как в A уравнений больше, чем в B , то $E_A \subseteq E_B$.

Чтобы показать неравенство, предположим, что наоборот $E_A = E_B$. Рассмотрим следующие подмножества в них:

$$E_A^0 = \{x \in E_A \mid x_i = 0 \text{ при } i > k\}$$

$$E_B^0 = \{x \in E_B \mid x_i = 0 \text{ при } i > k\}$$

То есть среди всех решений в E_A и E_B , соответственно, рассмотрим только те, у которых координаты с номерами больше k обращаются в ноль. Это не пустые подмножества, например, там есть нулевое решение. Если $E_A = E_B$, то и $E_A^0 = E_B^0$, так как последние задаются одинаковыми условиями. Значит, чтобы прийти к противоречию, достаточно показать, что в E_B^0 есть элемент, которого нет в E_A^0 .

Рассмотрим E_A^0 . Так как для $Ax = 0$ переменная x_k – главная, то она выражается через предыдущие. А значит, если предыдущие ноль, то и она ноль. Это значит, что для $x \in E_A^0$ автоматически $x_k = 0$. С другой стороны, для системы $Bx = 0$ переменная x_k является свободной. Тогда сделаем так: положим все свободные переменные кроме x_k равными нулю, а $x_k = 1$. Тогда все главные переменные правее x_k (с большими номерами) автоматически станут нулями. Таким образом мы получили точку $x \in E_B^0$, у которой $x_k \neq 0$. Последнее приводит к противоречию с предположением, что $E_A = E_B$. \square

Утверждение 4. Пусть $S_1 \in M_{mn}(\mathbb{R})$ и $S_2 \in M_{kn}(\mathbb{R})$ – произвольные матрицы в улучшенном ступенчатом виде. Если $S_1x = 0$ эквивалентно $S_2x = 0$, то $S_1 = S_2$.

Доказательство. Так как $S_1x = 0$ и $S_2x = 0$ эквивалентны между собой, то если мы возьмем любое уравнение l из системы $S_1x = 0$ и добавим его к системе $S_2x = 0$, получив систему $\begin{pmatrix} S_2 \\ l \end{pmatrix} x = 0$, то новая система будет эквивалентна всем трем. Аналогично, можно перекладывать уравнения из второй системы в первую, не меняя множества решений.

¹³Вот то место где мы пользуемся квадратностью матрицы.

¹⁴То есть имеют разное множество решений.

Пусть для определенности матрицы S_1 и S_2 имеют следующий вид:

$$S_1 = \begin{pmatrix} 1 & * & 0 & * & 0 & 0 & * & * & * \\ & & 1 & * & 0 & 0 & * & * & * \\ & & & & 1 & 0 & * & * & * \\ & & & & & & 1 & * & * \end{pmatrix} \quad S_2 = \begin{pmatrix} 1 & \bullet & \bullet & 0 & \bullet & \bullet & 0 & \bullet & \bullet \\ & & & 1 & \bullet & \bullet & 0 & \bullet & \bullet \\ & & & & & & 1 & \bullet & \bullet \end{pmatrix}$$

Они вообще говоря могут содержать разное количество ненулевых строк, пока мы ничего про это не знаем.

Давайте докажем, что в системах совпадают последние уравнения, потом следующие и так далее. Будем двигаться снизу вверх от коротких к более длинным. Нам надо показать три вещи: почему совпадают самые короткие уравнения, объяснить как показать совпадение для произвольного промежуточного уравнения и почему у одной из системы уравнения не закончатся раньше, чем у другой.

Пусть для определенности последнее уравнение S_2 не длиннее последнего уравнения S_1 , как на картинке. Добавим это уравнение к системе S_1 . Тогда возможны два случая: уравнение либо строго короче, либо имеет такую же длину. В первом случае получим две эквивалентные системы с матрицами

$$S_1 = \begin{pmatrix} 1 & * & 0 & * & 0 & 0 & * & * & * \\ & & 1 & * & 0 & 0 & * & * & * \\ & & & & 1 & 0 & * & * & * \\ & & & & & & 1 & * & * \end{pmatrix} \quad S'_1 = \begin{pmatrix} 1 & * & 0 & * & 0 & 0 & * & * & * \\ & & 1 & * & 0 & 0 & * & * & * \\ & & & & 1 & 0 & * & * & * \\ & & & & & & 1 & * & * \\ & & & & & & & 1 & \bullet \end{pmatrix}$$

Но по предыдущему утверждению это не возможно. Значит уравнения имеют одинаковую длину, потому эквивалентны системы

$$S_1 = \begin{pmatrix} 1 & * & 0 & * & 0 & 0 & * & * & * \\ & & 1 & * & 0 & 0 & * & * & * \\ & & & & 1 & 0 & * & * & * \\ & & & & & & 1 & * & * \end{pmatrix} \quad S'_1 = \begin{pmatrix} 1 & * & 0 & * & 0 & 0 & * & * & * \\ & & 1 & * & 0 & 0 & * & * & * \\ & & & & 1 & 0 & * & * & * \\ & & & & & & 1 & * & * \\ & & & & & & & 1 & \bullet \end{pmatrix}$$

В матрице S'_2 вычтем предпоследнее уравнение из последнего. Новая система $S''_2 x = 0$ будет эквивалентна $S_1 x = 0$. Если уравнения не совпадают, то разность даст новую ступеньку и по предыдущему утверждению системы не могут быть эквивалентными. Значит последние уравнения совпадают.

Теперь мы знаем, что матрицы S_1 и S_2 имеют вид (где треугольниками отмечены элементы одинаковых строк):

$$S_1 = \begin{pmatrix} 1 & * & 0 & * & 0 & 0 & * & * & * \\ & & 1 & * & 0 & 0 & * & * & * \\ & & & & 1 & 0 & * & * & * \\ & & & & & & 1 & \blacktriangle & \blacktriangle \end{pmatrix} \quad S_2 = \begin{pmatrix} 1 & \bullet & \bullet & 0 & \bullet & 0 & \bullet & \bullet & \bullet \\ & & & 1 & \bullet & 0 & \bullet & \bullet & \bullet \\ & & & & & & 1 & \blacktriangle & \blacktriangle \end{pmatrix}$$

Теперь посмотрим на следующую пару уравнений. Пусть для определенности уравнение в S_1 будет не длиннее, чем уравнение в S_2 . Добавим второе уравнение из S_1 в S_2 и получим эквивалентную систему. У нас как и выше два варианта: либо длина уравнения строго меньше, либо длины одинаковые. Рассмотрим случай первый:

$$S'_2 = \begin{pmatrix} 1 & \bullet & \bullet & 0 & \bullet & 0 & \bullet & \bullet & \bullet \\ & & & 1 & \bullet & 0 & \bullet & \bullet & \bullet \\ & & & & 1 & 0 & * & * & * \\ & & & & & & 1 & \blacktriangle & \blacktriangle \end{pmatrix} \quad S_2 = \begin{pmatrix} 1 & \bullet & \bullet & 0 & \bullet & 0 & \bullet & \bullet & \bullet \\ & & & 1 & \bullet & 0 & \bullet & \bullet & \bullet \\ & & & & & & 1 & \blacktriangle & \blacktriangle \end{pmatrix}$$

В этом случае по предыдущему утверждению системы не эквивалентны, чего быть не может. Значит у нас второй случай:

$$S'_2 = \begin{pmatrix} 1 & \bullet & \bullet & 0 & \bullet & 0 & \bullet & \bullet & \bullet \\ & & & 1 & \bullet & 0 & \bullet & \bullet & \bullet \\ & & & & 1 & * & 0 & * & * \\ & & & & & & 1 & \blacktriangle & \blacktriangle \end{pmatrix} \quad S_2 = \begin{pmatrix} 1 & \bullet & \bullet & 0 & \bullet & 0 & \bullet & \bullet & \bullet \\ & & & 1 & \bullet & 0 & \bullet & \bullet & \bullet \\ & & & & & & 1 & \blacktriangle & \blacktriangle \end{pmatrix}$$

Как и раньше, в S'_2 вычтем из нового уравнения вышестоящее. Предположим, что уравнения были разные и получилась ненулевая строка. Вопрос: где не может начинаться эта строка? Ответ, там где у обеих строк

были нули. Теперь воспользуемся тем, что все нижестоящие уравнения у нас одинаковые. Это значит, что нули у обеих строк в одних и тех же местах (это места где начинаются нижестоящие строки). Значит, может получиться что-то вроде

$$S_2'' = \begin{pmatrix} 1 & \bullet & \bullet & 0 & \bullet & 0 & \bullet & \bullet & \bullet \\ & & & 1 & \bullet & 0 & \bullet & \bullet & \bullet \\ & & & & * & 0 & * & * & * \\ & & & & & & 1 & \blacktriangle & \blacktriangle & \blacktriangle \end{pmatrix} \quad \text{или} \quad S_2'' = \begin{pmatrix} 1 & \bullet & \bullet & 0 & \bullet & 0 & \bullet & \bullet & \bullet \\ & & & 1 & \bullet & 0 & \bullet & \bullet & \bullet \\ & & & & & & * & * & * \\ & & & & & & & 1 & \blacktriangle & \blacktriangle & \blacktriangle \end{pmatrix} \quad \text{и т.д.}$$

Но по предыдущему утверждению такого опять быть не может, так как новая система не эквивалентна $S_2x = 0$. Продолжая аналогично, мы показываем, что все уравнения у систем совпадают.

Осталось объяснить почему уравнения в одной из систем не могут закончиться раньше, чем в другой. Но тогда у нас они обе в ступенчатом виде и одна получена из другой добавлением нескольких уравнений. Добавление одного уменьшает множество решений, как показано в предыдущем утверждении, а добавление нескольких – тем более. \square

Из этого утверждения следует, что матрица улучшенного ступенчатого вида для матрицы любой $A \in M_{m,n}(\mathbb{R})$ определена однозначно. Так как если матрица A приводится к двум разным ступенчатым видам, то их однородные системы эквивалентны, а значит они совпадают. Потому, говоря о матрице A , можно говорить и о ее улучшенном ступенчатом виде без какой-либо неоднозначности.

Классификация

Утверждение 5. Пусть $A, B \in M_{m,n}(\mathbb{R})$ и пусть $E_A, E_B \subseteq \mathbb{R}^n$ – множества решений систем $Ax = 0$ и $Bx = 0$, соответственно. Тогда следующее эквивалентно:

1. $E_A = E_B$, т.е. системы эквивалентны.
2. A приводится к B элементарными преобразованиями.
3. Существует обратимая $C \in M_m(\mathbb{R})$ такая, что $B = CA$.
4. Матрица улучшенного ступенчатого вида для A совпадает с матрицей улучшенного ступенчатого вида для B .

Доказательство. Мы все это уже доказали по сути, потому напомним, что откуда следует. $(2) \Rightarrow (1)$ Так как элементарные преобразования меняют систему на эквивалентную. $(1) \Rightarrow (4)$ Предыдущее утверждение. $(4) \Rightarrow (2)$ Если матрицы A и B приводятся элементарными преобразованиями к одной и той же матрице (улучшенного ступенчатого вида), то они переводятся и друг в друга. Эквивалентность $(2) \Leftrightarrow (3)$ следует из Утверждения 1 о том, что матрица обратима тогда и только тогда, когда она раскладывается в произведение элементарных. \square

Смысл этого утверждения в следующем. Возьмем множество всех однородных систем фиксированного размера, которое описывается матрицами $M_{m,n}(\mathbb{R})$. Тогда на этом множестве есть отношение эквивалентности: системы эквивалентны если они имеют одинаковое множество решений. Это полезное свойство, потому что нам не важно какую из систем решать среди эквивалентных. Однако, это свойство сложно проверяется. С другой стороны, у нас есть процедура изменения системы (элементарные преобразования), которая меняет системы на заведомо эквивалентные. Сделаем следующие замечания:

1. Утверждается, что эта процедура эффективная в том смысле, что если уж какие-то системы были эквивалентны, то мы обязательно от одной к другой сможем перейти элементарными преобразованиями.
2. Все то же самое верно и для второй процедуры – умножение на обратимую матрицу слева (потому что это по сути та же самая процедура).
3. Утверждается, что в каждом классе эквивалентных систем мы можем найти одну единственную матрицу улучшенного ступенчатого вида. То есть классов попарно неэквивалентных систем ровно столько же, сколько матриц улучшенного ступенчатого вида.
4. Последнее означает, что свойства системы с произвольной матрицей точно такие же, как у какой-то системы в улучшенном ступенчатом виде. Потому в абстрактных задачах про системы можно всегда предполагать, что система уже имеет улучшенный ступенчатый вид.

2.14 Полиномиальное исчисление от матриц

Обозначим множество всех многочленов с вещественными коэффициентами через $\mathbb{R}[x]$. Формально это значит: $\mathbb{R}[x] = \{a_0 + a_1x + \dots + a_nx^n \mid n \in \mathbb{Z}_+, a_i \in \mathbb{R}\}$. Аналогично можно обозначать многочлены с рациональными, целыми, комплексными и т.д. коэффициентами.

Подстановка матриц в многочлены Пусть $p(x) = a_0 + a_1x + \dots + a_nx^n$ — многочлен с вещественными коэффициентами, а $A \in M_n(\mathbb{R})$. Тогда можно определить $f(A) = a_0E + a_1A + \dots + a_nA^n \in M_n(\mathbb{R})$. Если определить $A^0 = E$, то формула становится более единообразной $f(A) = a_0A^0 + a_1A^1 + \dots + a_nA^n$. Однако, психологически проще думать так: вместо x подставляем A , а свободный член отождествляем со скалярными матрицами. Отметим что, если два многочлена равны, то и их значения на матрице A тоже равны.

Утверждение. Пусть $A \in M_n(\mathbb{R})$ и $f, g \in \mathbb{R}[x]$ — два произвольных многочлена, тогда:

1. $(f + g)(A) = f(A) + g(A)$.
2. $(fg)(A) = f(A)g(A)$.
3. $f(\lambda E) = f(\lambda)E$.
4. $f(C^{-1}AC) = C^{-1}f(A)C$ для любой обратимой $C \in M_n(\mathbb{R})$
5. Матрицы $f(A)$ и $g(A)$ коммутируют между собой.

Доказательство. Все это делается прямой проверкой по определению. Давайте объясним свойства (2) и (4).

(2) Пусть

$$f = \sum_{k=0}^n a_k x^k \text{ и } g = \sum_{k=0}^m b_k x^k$$

тогда

$$fg = \sum_{k=0}^{n+m} \left(\sum_{s+t=k} a_s b_t \right) x^k$$

Потому надо проверить равенство:

$$\left(\sum_{k=0}^n a_k A^k \right) \left(\sum_{k=0}^m b_k A^k \right) = \sum_{k=0}^{n+m} \left(\sum_{s+t=k} a_s b_t \right) A^k$$

которое следует из перестановочности A со своими степенями и коэффициентами.

(4) Заметим, что

$$(C^{-1}AC)^n = C^{-1}ACC^{-1}AC \dots C^{-1}AC = C^{-1}A^n C$$

Осталось воспользоваться дистрибутивностью умножения, т.е. $C^{-1}(A+B)C = C^{-1}AC + C^{-1}BC$. □

Обнуляющий многочлен

Утверждение 6. Пусть $A \in M_n(\mathbb{R})$, тогда:

1. Существует многочлен $f \in \mathbb{R}[x]$ не равный тождественно нулю степени не больше n^2 такой, что $f(A) = 0$.
2. Если для какого-то многочлена $g \in \mathbb{R}[x]$ имеем $g(A) = 0$, а для $\lambda \in \mathbb{R}$ имеем $g(\lambda) \neq 0$, то $A - \lambda E$ является обратимой матрицей.

Доказательство. (1) Давайте искать многочлен f с неопределенными коэффициентами в виде $f = a_0 + a_1x + \dots + a_nx^n$. Надо чтобы было выполнено равенство $a_0E + a_1A + \dots + a_nA^n = 0$. Последнее равенство означает равенство матрицы слева нулевой матрице справа. Это условие задается равенством всех n^2 ячеек матриц: $(a_0E + a_1A + \dots + a_nA^n)_{ij} = 0$ для всех i, j . Каждое из этих условий является линейным уравнением вида $a_0(E)_{ij} + a_1(A)_{ij} + \dots + a_n(A^n)_{ij} = 0$. То есть у нас есть система с n^2 уравнениями и $n^2 + 1$ неизвестной. А значит при приведении этой системы к ступенчатому виду у нас обязательно будет свободная переменная, а значит мы сможем найти ненулевое решение.

(2) Разделим многочлен g на $x - \lambda$ с остатком, получим $g(x) = h(x)(x - \lambda) + g(\lambda)$. Теперь в левую и правую часть равенства подставим A . Получим

$$0 = g(A) = h(A)(A - \lambda E) + g(\lambda)E$$

Перенесем $g(\lambda)E$ в другую сторону и поделим на $-g(\lambda)$, получим

$$E = -\frac{1}{g(\lambda)}h(A)(A - \lambda E)$$

То есть $-\frac{1}{g(\lambda)}h(A)$ является обратным к $A - \lambda E$. □

На самом деле можно показать, что найдется многочлен степени не больше n , зануляющий нашу матрицу. Однако, мы пока не в состоянии этого сделать.

Спектр Пусть $A \in M_n(\mathbb{R})$ определим вещественный спектр матрицы A следующим образом:

$$\text{спес}_{\mathbb{R}} A = \{\lambda \in \mathbb{R} \mid A - \lambda E \text{ не обратима}\}$$

Аналогично определяются спектры в рациональном, комплексном и прочих случаях.

Утверждение 7. Пусть $A \in M_n(\mathbb{R})$ и пусть $f \in \mathbb{R}[x]$ такой, что $f(A) = 0$. Тогда $|\text{спес}_{\mathbb{R}} A| \leq \deg f$. В частности спектр всегда конечен.

Доказательство. Покажем, что любой элемент спектра является корнем f . Для этого достаточно показать двойственное утверждение, если λ не корень, то λ не в спектре. Но это в точности Утверждение 6 пункт (2). □

Так как у нас для любой матрицы найдется многочлен степени n^2 ее зануляющий, то спектр всегда конечен и его размер не превосходит n^2 . Как говорилось выше, на самом деле, можно найти многочлен степени n , потому спектр всегда не превосходит по мощности n .

Примеры

1. Пусть $A \in M_n(\mathbb{R})$ – диагональная матрица с числами $\lambda_1, \dots, \lambda_n$ на диагонали, т.е.

$$A = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$$

Так как диагональные матрицы складываются и умножаются поэлементно

$$\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} + \begin{pmatrix} \mu_1 & & \\ & \ddots & \\ & & \mu_n \end{pmatrix} = \begin{pmatrix} \lambda_1 + \mu_1 & & \\ & \ddots & \\ & & \lambda_n + \mu_n \end{pmatrix}$$

$$\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \begin{pmatrix} \mu_1 & & \\ & \ddots & \\ & & \mu_n \end{pmatrix} = \begin{pmatrix} \lambda_1 \mu_1 & & \\ & \ddots & \\ & & \lambda_n \mu_n \end{pmatrix}$$

То для любого многочлена $f \in \mathbb{R}[x]$ верно

$$f \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} = \begin{pmatrix} f(\lambda_1) & & \\ & \ddots & \\ & & f(\lambda_n) \end{pmatrix}$$

То есть многочлен f зануляет A тогда и только тогда, когда он зануляет все λ_i . Например, в качестве такого многочлена подойдет $f(x) = (x - \lambda_1) \dots (x - \lambda_n)$.

Давайте покажем, что $\text{спес}_{\mathbb{R}} A = \{\lambda_1, \dots, \lambda_n\}$. Так как многочлен f зануляет A , утверждение 6 пункт (2) влечет, что спектр содержится среди его корней. Значит, надо показать, что $A - \lambda_i E$ необратим для любого i . Последнее легко видеть, так как $A - \lambda_i E$ содержит 0 на i -ом месте на диагонали.

2. Пусть $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{R})$. Прямое вычисление показывает, что $A^2 = -E$, то есть многочлен $f(x) = x^2 + 1$ зануляет A . Покажем, что $\text{спес}_{\mathbb{R}} A = \emptyset$. Действительно, по утверждению 6 пункт (2) спектр должен содержаться среди корней многочлена $f(x) = x^2 + 1$. Однако, этот многочлен не имеет вещественных корней. Этот пример объясняет, почему вещественных чисел иногда не достаточно и мы хотим работать с комплексными числами. Например, в комплексном случае $\text{спес}_{\mathbb{C}} A = \{i, -i\}$.

Минимальный многочлен Пусть $A \in M_n(\mathbb{R})$ – некоторая матрица. Рассмотрим множество всех ненулевых многочленов зануляющих A . Формально мы смотрим на множество

$$M = \{f \in \mathbb{R}[x] \mid f(A) = 0, f \neq 0\}$$

Пусть $f_{\min} \in M$ – многочлен самой маленькой степени и со старшим коэффициентом 1. Тогда он называется минимальным многочленом матрицы A .

Утверждение 8. Пусть $A \in M_n(\mathbb{R})$, тогда верны следующие утверждения:

1. Минимальный многочлен f_{\min} существует.
2. Минимальный многочлен делит любой другой многочлен зануляющий A .
3. Минимальный многочлен единственный.
4. $\lambda \in \text{спес}_{\mathbb{R}} A$ тогда и только тогда, когда $f_{\min}(\lambda) = 0$.

Доказательство. (1). По утверждению 6 пункт (1) у нас всегда найдется многочлен зануляющий A , а значит M не пусто. Так как степень не может убывать бесконечно, то мы обязательно найдем многочлен самой маленькой степени, который зануляет A . Осталось разделить его на старший коэффициент.

(2). Пусть $f \in M$ – произвольный многочлен, а f_{\min} – какой-то минимальный. Тогда разделим f на f_{\min} с остатком, получим

$$f(x) = h(x)f_{\min}(x) + r(x)$$

где $\deg r < \deg f_{\min}$. Подставим в это равенство матрицу A , получим

$$0 = f(A) = h(A)f_{\min}(A) + r(A) = r(A)$$

Значит мы нашли многочлен r , который зануляет A и меньше f_{\min} по степени. Такое может быть только если $r(x) = 0$.

(3). Пусть f_{\min} и f'_{\min} – два минимальных многочлена матрицы A . Тогда у них по определению одинаковая степень. Рассмотрим $r(x) = f_{\min}(x) - f'_{\min}(x)$. Многочлен $r(x)$ степени строго меньше, так как оба минимальных имеют старший коэффициент единица. Кроме того, $r(A) = f_{\min}(A) - f'_{\min}(A) = 0$. А значит $r(x) = 0$.

(4). Мы уже знаем, что $\text{спес}_{\mathbb{R}} A$ лежит среди корней f_{\min} (утверждение 6 пункт (2)). Осталось показать обратное включение. Предположим обратное, что есть $\lambda \in \mathbb{R}$ такое, что $f_{\min}(\lambda) = 0$, но $\lambda \notin \text{спес}_{\mathbb{R}} A$. Тогда $f_{\min}(x) = (x - \lambda)h(x)$. Подставим в это равенство матрицу A и получим

$$0 = f_{\min}(A) = (A - \lambda E)h(A)$$

Так как $\lambda \notin \text{спес}_{\mathbb{R}} A$, то матрица $A - \lambda E$ обратима, а значит на нее можно сократить, то есть $h(A) = 0$ и степень h строго меньше степени f_{\min} , хотя сам h – ненулевой многочлен. Последнее противоречит с нашим предположением о том, что $\lambda \notin \text{спес}_{\mathbb{R}} A$. \square

Поиск минимального многочлена Пусть задана матрица $A \in M_n(\mathbb{R})$. То мы знаем, что найдется многочлен $f \in \mathbb{R}[x]$ такой, что $f(A) = 0$. Кроме того, я сообщил, что $\deg f \leq n$. Давайте обсудим, как найти подобный многочлен. Будем искать его с неопределенными коэффициентами $f(x) = a_0 + a_1x + \dots + a_nx^n$. Подставим в многочлен матрицу A и приравняем результат к нулю.

$$f(A) = a_0E + a_1A + \dots + a_nA^n = 0$$

Тогда, то что написано является системой из n^2 уравнений, а именно

$$\{1 \leq i, j \leq n\} E_{ij}a_0 + A_{ij}a_1 + \dots + (A^n)_{ij}a_n = 0$$

Здесь через B_{ij} обозначены коэффициенты матрицы B , например, E_{ij} – это ij -ый коэффициент единичной матрицы, а $(A^n)_{ij}$ – ij -ый коэффициент матрицы A^n .

Теперь нас интересует ненулевое решение этой системы, у которого как можно больше нулей справа. Давайте поясню. Такое решение отвечает зануляющему многочлену. Мы хотим выбрать такой многочлен как можно меньшей степени. То есть мы хотим по возможности занулить a_n , потом a_{n-1} , потом a_{n-2} и так далее, пока находится ненулевое решение. Предположим, что мы привели систему к ступенчатому виду и a_k – самая левая свободная переменная. Я утверждаю, что k и будет степенью минимального многочлена, а чтобы его найти надо положить $a_k = 1$, а все остальные свободные переменные равными нулю.

Действительно, если мы сделали, как описано, то все главные переменные правее a_k тоже равны нулю, ибо они зависят от свободных переменных, стоящих правее, а они в нашем случае нулевые. То есть a_k будет старший ненулевой коэффициент в искомом многочлене, а значит k будет его степенью. Почему нельзя найти меньше. Чтобы найти меньше надо занулить еще и a_k . То есть все свободные переменные в этом случае будут нулевыми, а тогда и все главные будут нулевыми, а это даст нулевое решение, что противоречит нашим намерениям найти ненулевой многочлен.

Вычленение из какого-то зануляющего Предположим, что вы угадали какой-нибудь зануляющий многочлен для вашей матрицы $A \in M_n(\mathbb{R})$, а именно, нашли какой-то $f \in \mathbb{R}[x]$ такой, что $f(A) = 0$. Тогда можно попытаться найти минимальный многочлен среди делителей многочлена f . Эта процедура требует уметь искать эти самые делители. Но в некоторых ситуациях эта процедура тоже бывает полезна. Например, в случае большой блочной матрицы A бывает проще найти зануляющий многочлен.

Замечание о спектре Можно показать, что любой вещественный многочлен $f \in \mathbb{R}[x]$ единственным образом разваливается в произведение

$$f(x) = (x - \lambda_1) \dots (x - \lambda_k) q_1(x) \dots q_r(x)$$

где числа $\lambda_i \in \mathbb{R}$ могут повторяться, а $q_i(x)$ – многочлены второй степени с отрицательным дискриминантом (то есть без вещественных корней).

Пусть теперь f_{min} – минимальный многочлен некоторой матрицы A . Разложим его подобным образом. Тогда мы видим из предыдущего утверждения, что $\text{спес}_{\mathbb{R}} A$ помнит информацию только о первой половине сомножителей и теряет информацию о квадратичных многочленах. Однако, если бы мы рассмотрели f_{min} как многочлен с комплексными коэффициентами, то мы бы могли доразложить все $q_i(x)$ на линейные множители и $\text{спес}_{\mathbb{C}} A$ помнит информацию о всех сомножителях f_{min} . Еще надо понимать, что каждое $x - \lambda$ может несколько раз участвовать в разложении f_{min} , но спектр не помнит это количество, он лишь знает был ли там данный $x - \lambda$ или нет.

Замечание об арифметических свойствах матриц Если вы работаете с матрицами, то готовьтесь к тому, чтобы думать про них как про более сложную версию чисел. А значит, вы будете писать с ними различного рода алгебраические выражения. Например, для какой-нибудь матрицы $A \in M_n(\mathbb{R})$ можно написать $A^3 + 2A - 3E$. И предположим вы хотите упростить это выражение как-нибудь, не зная как именно выглядит ваша матрица A . Единственное, что вам поможет в этом случае – зануляющий многочлен. Пусть, например, $f(x) = x^2 - 3$ зануляет A . Это значит, что $A^2 = 3E$. Тогда выражение выше можно упростить так

$$A^3 + 2A - 3E = 3A + 2A - 3E = 5A - 3E$$

Роль минимального многочлена заключается в том, что это «самый лучший» многочлен, который помнит как можно больше соотношений на матрицу A , чтобы можно было упрощать выражения. Более того, минимальный многочлен автоматически говорит, когда можно делить на выражение от матрицы, а когда нет. Например, на $A - E$ поделить можно, так как 1 не является корнем f , с другой стороны на матрицы $A \pm \sqrt{3}E$ делить нельзя.

Обратимость и минимальный многочлен Обратимость матрицы по определению равносильна тому, что в ее спектре нет нуля, а это то же самое, что у минимального многочлена свободный член отличен от нуля. В этом случае мы можем явно выразить обратную матрицу через исходную. Действительно, пусть $f_{min} = a_0 + a_1x + \dots + a_mx^m$ для некоторой матрицы $A \in M_n(\mathbb{R})$. Тогда

$$a_0E + a_1A + \dots + a_mA^m = 0 \quad \Rightarrow \quad A(a_1E + \dots + a_mA^{m-1}) = -a_0E \quad \Rightarrow \quad A \left(-\frac{a_1}{a_0}E - \dots - \frac{a_m}{a_0}A^{m-1} \right) = E$$

То есть по определению

$$A^{-1} = -\frac{a_1}{a_0}E - \dots - \frac{a_m}{a_0}A^{m-1}$$

Обратите внимание, что данная формула работает при условии, что $a_0 \neq 0$. Эта процедура похожа на процедуру избавления от иррациональности в знаменателе дробей или от избавления от мнимой части в знаменателе в комплексных дробях. Это не спроста, это в точности тот же самый метод.

3 Перестановки

3.1 Отображения множеств

Пусть X, Y – некоторые множества, а $\varphi: X \rightarrow Y$ – отображение. Тогда φ называется *инъективным*, если оно «не склеивает точки», т.е. для любых $x, y \in X$ из условия $x \neq y$ следует $\varphi(x) \neq \varphi(y)$. Отображение φ называется *сюръективным*, если в любой элемент что-то переходит, т.е. для любого $y \in Y$ существует $x \in X$ такой, что $\varphi(x) = y$. Отображение φ называется *биективным*, если оно одновременно инъективно и сюръективно.¹⁵

Свойства отображения можно подчеркивать видом стрелки. Например, инъективное отображение обычно обозначается $\varphi: X \hookrightarrow Y$, сюръективное – $\varphi: X \twoheadrightarrow Y$, а биективное – $\varphi: X \xrightarrow{\sim} Y$.

Для любого множества X отображение $\text{Id}: X \rightarrow X$ заданное по правилу $\text{Id}(x) = x$ называется *тождественным*. Пусть $\varphi: X \rightarrow Y$ – некоторое отображение. Тогда $\psi: Y \rightarrow X$ называется *левым обратным* (соответственно *правым обратным*) к φ , если $\psi\varphi = \text{Id}$ ($\varphi\psi = \text{Id}$).¹⁶ Левых и правых обратных для φ может быть много. Однако, если есть оба обратных и ψ_1 – левый обратный, а ψ_2 – правый обратный, то они совпадают, так как $\psi_1 = \psi_1(\varphi\psi_2) = (\psi_1\varphi)\psi_2 = \psi_2$. А следовательно совпадают все левые обратные со всеми правыми и такой единственный элемент называют *обратным* и обозначают φ^{-1} , а φ называют *обратимым*. Легко проверить следующее.

Утверждение. Пусть $\varphi: X \rightarrow Y$ – некоторое отображение. Тогда

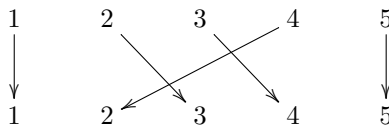
1. φ инъективно тогда и только тогда, когда φ обладает левым обратным.
2. φ сюръективно тогда и только тогда, когда φ обладает правым обратным.
3. φ биективно тогда и только тогда, когда φ обратимо.

3.2 Перестановки

Пусть $X_n = \{1, \dots, n\}$ – конечное множество из n занумерованных элементов.¹⁷ *Перестановкой* называется биективное отображение $\sigma: X_n \rightarrow X_n$. Множество всех перестановок на n элементном множестве будем обозначать через S_n .

Как задавать перестановки Как только вам встречается новый объект, первый важный вопрос – а как подобные объекты вообще задавать? Для перестановок есть три способа:

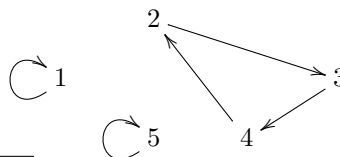
1. Задать стрелками соответствие на элементах



2. С помощью таблицы значений (графика). Здесь под каждым элементом пишется его образ:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$$

3. Графически в виде действия на элементах



¹⁵В теории множеств, множества – это мешки с элементами, а отображения «сравнивают» эти мешки между собой. Биекция, между множествами говорит, что это по сути одно и то же множество, но по разному заданное. Потому на биекцию между X и Y можно смотреть не как на отображение между разными множествами, а как на правило «переименовывающее» элементы на одном и том же множестве.

¹⁶Легко проверить, что существование левого обратного никак не связано с существованием правого обратного и наоборот.

¹⁷Формально говоря, это множество из n элементов и фиксированный линейный порядок на нем.

Все эти виды записи однозначно задают перестановку. Самым популярным методом в литературе является второй способ. В общем виде для перестановки $\sigma \in S_n$ табличная запись выглядит следующим образом:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Заметим, что, если записать элементы $1, \dots, n$ в другом порядке, скажем, i_1, \dots, i_n , то перестановка σ запишется в виде¹⁸

$$\begin{pmatrix} i_1 & i_2 & \dots & i_n \\ \sigma(i_1) & \sigma(i_2) & \dots & \sigma(i_n) \end{pmatrix}$$

Из однозначности табличной записи получаем следующее.

Утверждение. Количество перестановок на n элементах есть $n!$, т.е. $|S_n| = n!$.

3.3 Операция на перестановках

Так как перестановки являются отображениями, а на отображениях есть операция композиции, то и на перестановках появляется операция. Пусть $\sigma, \tau \in S_n$ – две произвольные перестановки, определим $\sigma\tau$ как композицию, т.е. $\sigma\tau(k) = \sigma(\tau(k))$. На языке диаграмм

$$\begin{array}{ccccc} X_n & \xrightarrow{\tau} & X_n & \xrightarrow{\sigma} & X_n \\ & \searrow & & \nearrow & \\ & & \sigma\tau & & \end{array}$$

Важно Обратите внимание, что перестановки применяются к элементам справа налево. Это связано с тем, что они являются отображениями, а когда вы считаете композицию отображений, то вы сначала применяете к аргументу самое правое, потом следующее за ним и так далее.

Давайте посмотрим как выглядит произведение двух перестановок в табличной записи. Пусть даны перестановки

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \text{ и } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

То перестановки $\sigma\tau$ и $\tau\sigma$ имеют вид

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ и } \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Свойства умножения

- Если $\sigma, \tau, \rho \in S_n$ – произвольные перестановки, то как легко видеть по определению $(\sigma\tau)\rho = \sigma(\tau\rho)$. То есть в выражениях составленных из перестановок и произведений не важно в каком порядке расставлять скобки. Потому скобки обычно опускаются.
- Умножение перестановок не коммутативно, то есть вообще говоря $\sigma\tau \neq \tau\sigma$.¹⁹
- Тожественное отображение Id является нейтральным элементом для умножения перестановок в том смысле, что верно $\text{Id}\sigma = \sigma\text{Id} = \sigma$ для любой перестановки σ . В табличной записи Id имеет вид

$$\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

- Обратное отображение к σ будем обозначать через σ^{-1} . Оно будет обратным элементом относительно операции в том смысле, что $\sigma\sigma^{-1} = \sigma^{-1}\sigma = \text{Id}$. В табличной записи обратное отображение можно записать так

$$\begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix}$$

¹⁸Заметим, что в этой записи можно произвольным образом перемешивать столбцы, это никак не изменит задаваемую перестановку.

¹⁹Один пример мы уже видели, еще один будет в разделе «Циклические перестановки».

3.4 Переименование элементов

В нашем определении перестановка – это биекция на множестве X_n . Однако, элементы X_n имеют конкретные имена – это числа от 1 до n . А что произойдет, если мы сменим имена элементов? Как изменится табличная запись перестановки?

В начале надо понять, что значит переименование элементов. Во-первых, у нас есть запас старых имен $\{1, \dots, n\}$, во-вторых, у нас должен быть список новых имен, скажем, $\{“1”, \dots, “n”\}$ и, в-третьих, у нас должно быть соответствие, которое по старым именам строит новые, т.е. $\tau: \{1, \dots, n\} \rightarrow \{“1”, \dots, “n”\}$. Потому, если мысленно убрать кавычки, то на переименование можно смотреть как на перестановку $\tau: X_n \rightarrow X_n$.

Пусть теперь у нас есть перестановка $\sigma: X_n \rightarrow X_n$. Ее можно записать в табличном виде в старых и новых именах. Чтобы различать эти таблицы мы будем использовать обозначения $\sigma_{\text{стар}}$ и $\sigma_{\text{нов}}$ для них соответственно. Тогда мы можем записать связь между ними с помощью следующей диаграммы:

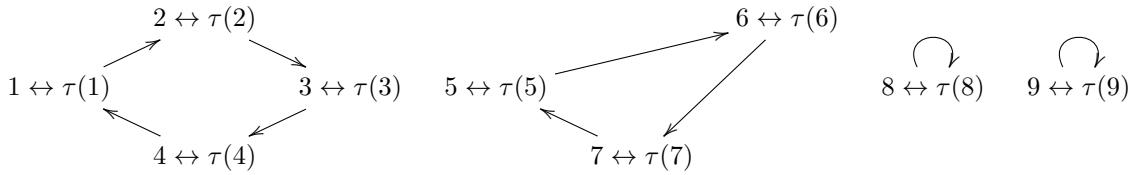
$$\begin{array}{ccc} \{1, \dots, n\} & \xrightarrow{\tau} & \{“1”, \dots, “n”\} \\ \sigma_{\text{стар}} \downarrow & & \downarrow \sigma_{\text{нов}} \\ \{1, \dots, n\} & \xrightarrow{\tau} & \{“1”, \dots, “n”\} \end{array}$$

Если вспомнить, что $\{“1”, \dots, “n”\} = \{\tau(1), \dots, \tau(n)\}$, то действие $\sigma_{\text{нов}}$ в новых именах устроено так: мы берем произвольный элемент с новым именем $\tau(k)$, находим его старое имя – k , на старом имени можем подействовать $\sigma_{\text{стар}}$, которое есть $\sigma(k)$, а теперь надо найти новое имя для образа, что есть $\tau(\sigma(k))$.

Подытожим, что $\sigma_{\text{нов}} = \tau \sigma_{\text{стар}} \tau^{-1}$. В табличной записи перестановки выглядят так

$$\sigma_{\text{стар}} = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \quad \sigma_{\text{нов}} = \begin{pmatrix} \tau(1) & \tau(2) & \dots & \tau(n) \\ \tau(\sigma(1)) & \tau(\sigma(2)) & \dots & \tau(\sigma(n)) \end{pmatrix}$$

Хорошо еще иметь перед глазами следующую картинку:



Здесь в вершинах подписаны и старые и новые имена, а перестановка одна и та же.

3.5 Циклы

Пусть $\sigma \in S_n$ действует следующим образом. Для некоторого множества i_1, \dots, i_k ($k \geq 2$) выполнено

$$\sigma(i_1) = i_2, \dots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1,$$

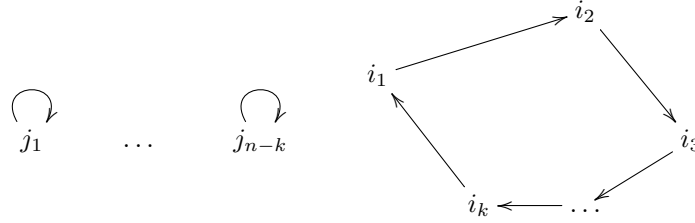
а все остальные элементы остаются на месте под действием σ . Тогда σ называется *циклом* длины k . Такая перестановка для краткости обозначается (i_1, \dots, i_k) . Заметим, что такая запись не единственная, например можно сказать $\sigma = (i_2, \dots, i_k, i_1)$.²⁰ Стоит отметить, что если в определении выше выбрать $k = 1$, то перестановка обозначаемая (i_1) совпадает с тождественной перестановкой. Потому циклов длины 1 просто не существует. Однако, в некоторых случаях сама запись (i_1) является удобным обозначением для единообразия в формулах. Потому такие «циклы» принято называть тривиальными (подразумевая не цикл, а обозначение), а настоящие циклы – нетривиальными.

Таблицей цикл задается следующим образом

$$\begin{pmatrix} i_1 & \dots & i_{k-1} & i_k & j_1 & \dots & j_{n-k} \\ i_2 & \dots & i_k & i_1 & j_1 & \dots & j_{n-k} \end{pmatrix}$$

²⁰Как легко видеть, другой неоднозначности в записи цикла нет.

где $\{1, \dots, n\} = \{i_1, \dots, i_k\} \sqcup \{j_1, \dots, j_{n-k}\}$. Графически этот цикл выглядит так



Цикл длины 2 называется *транспозицией*, т.е. транспозиция (i, j) – это перестановка двух элементов i и j . Два цикла (i_1, \dots, i_k) и (j_1, \dots, j_m) называются *независимыми*, если множества $\{i_1, \dots, i_k\}$ и $\{j_1, \dots, j_m\}$ не пересекаются, т.е. множества действительно перемещаемых элементов не пересекаются. Заметим, что независимые циклы коммутируют друг с другом, а зависимые нет, как показывает следующий пример: $(12)(23) = (123)$, а $(23)(12) = (321)$.²¹

Утверждение 9. Пусть $\rho = (i_1, \dots, i_k) \in S_n$ – некоторый цикл длины k и $\tau \in S_n$ – произвольная перестановка, тогда

$$\tau(i_1, \dots, i_k)\tau^{-1} = (\tau(i_1), \dots, \tau(i_k))$$

Доказательство. Есть два способа понять это равенство. Первый – посмотреть на τ как на переименование элементов. Тогда справа написан цикл по элементам с новыми именами, а слева – правило переименования.

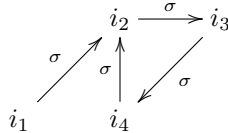
Второй способ – проверка в лоб. Надо проверить, что и левая и правая часть одинаково действуют на всех элементах вида $\tau(i)$. Возьмем элемент $\tau(i_1)$, тогда правая часть его переводит в $\tau(i_2)$. Посмотрим, что с ним делает левая часть. Вначале, мы переходим в i_1 , потом в i_2 , а потом в $\tau(i_2)$. Получили то же самое. Аналогично проверяется, что $\tau(i)$ остается на месте, если i не совпадает ни с одним из i_s . \square

Теперь мы готовы доказать структурный результат о перестановках.

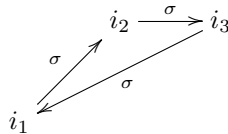
Утверждение 10. Пусть $\sigma \in S_n$ – произвольная перестановка. Тогда

1. Перестановку σ можно представить в виде $\sigma = \rho_1 \dots \rho_k$, где ρ_i – независимые циклы. Причем это представление единственное с точностью до перестановки сомножителей.
2. Пусть $\rho \in S_n$ – произвольный цикл длины k , тогда его можно представить в виде $\rho = \tau_1 \dots \tau_{k-1}$, где τ_i – транспозиции.²²

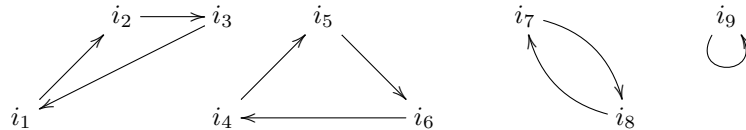
Доказательство. (1) Пусть $i_1 \in X_n$ – произвольный элемент. Подействуем на него σ , получим $i_2 = \sigma(i_1)$ и т.д. Так как X_n конечно, то мы в какой-то момент повторимся, например $i_5 = i_2$, как на рисунке ниже



На этой картинке видно, что $\sigma(i_1) = \sigma(i_4)$, но σ инъективно, потому $i_1 = i_4$. То есть правильная картинка следующая



Далее возьмем элемент, который не попал на этот цикл и повторим рассуждение для него. Так найдем другой цикл и т.д. В итоге картинка будет приблизительно такая



Значит перестановка выше раскладывается в циклы $\sigma = (i_1, i_2, i_3)(i_4, i_5, i_6)(i_7, i_8)$.²³

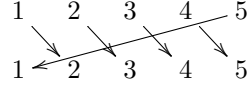
²¹Проверьте это.

²²Это представление уже не единственное.

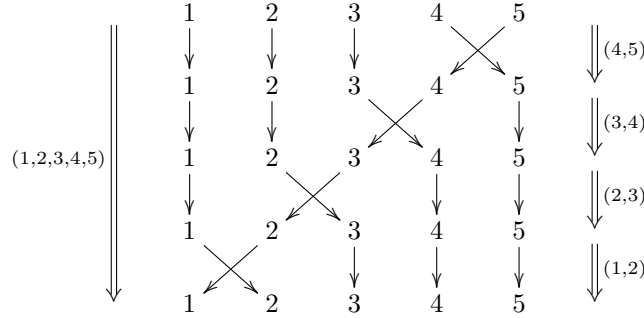
²³Цикл (i_9) здесь не используется, так как он совпадает с тождественной перестановкой Id , как и любой другой цикл длины 1.

Единственность такого разложения следует из метода пристального взгляда на картинку и наше рассуждение. Если нужно формальное объяснение, то нужно делать так. Пусть $\sigma = \rho_1 \dots \rho_k$ и пусть $\rho_1 = (i_1, \dots, i_s)$. Подействуем σ на элемент i_1 . Так как циклы справа независимы, то только ρ_1 действует на i_1 и значит $\sigma(i_1) = \rho_1 \dots \rho_k(i_1) = i_2$. То есть i_2 однозначно определено. Продолжая в том же духе, мы видим, что все циклы однозначно определяются через σ .

(2) Пусть цикл σ действует как на картинке ниже



Нам надо использовать $k - 1$ (на рисунке 4 транспозиции), чтобы результат был перестановкой элементов по кругу. Сделаем это следующим образом



То есть в общем случае $(1, 2, \dots, k) = (1, 2)(2, 3) \dots (k - 2, k - 1)(k - 1, k)$.

□

Давайте поймем, почему представление во втором случае не единственное. Рассмотрим перестановку $(12)(23)$. Тогда

$$(12)(23) = (12)(23)(12)^{-1}(12) = (13)(12)$$

здесь в первом равенстве мы поделили и домножили на (12) , а во втором воспользовались утверждением 9.

3.6 Знак перестановки

Рассмотрим произвольное отображение

$$\phi: S_n \rightarrow \{\pm 1\}$$

удовлетворяющее следующим двум свойствам:

1. $\phi(\sigma\tau) = \phi(\sigma)\phi(\tau)$ для любых $\sigma, \tau \in S_n$.²⁴
2. $\phi \neq 1$, т.е. ϕ не равно тождественно 1.

Заметим, что несложно найти отображение удовлетворяющее только первому свойству, например, $\phi(\sigma) = 1$ для любого σ , что не интересно. Наша основная задача доказать следующее.

Утверждение 11. *Существует единственное отображение $\phi: S_n \rightarrow \{\pm 1\}$ обладающее свойствами (1) и (2).*

В этом случае такое отображение обозначается $\text{sgn}: S_n \rightarrow \{\pm 1\}$ и называется знаком. Значение $\text{sgn}(\sigma)$ называется знаком перестановки $\sigma \in S_n$. Перестановка называется четной, если знак 1 и нечетной, если -1 .

²⁴Здесь справа стоит произведение чисел вида 1 или -1 .

Существование Обычно знак перестановки σ определяют в виде $(-1)^{d(\sigma)}$, где $d(\sigma)$ – некоторая целочисленная характеристика перестановки σ . Классическим определением является *число беспорядков*.²⁵

Пусть $\sigma \in S_n$ – некоторая перестановка и $i, j \in X_n$ – пара различных элементов. Тогда эта пара называется *инверсией*, если « σ меняет характер монотонности», т.е. $i < j$ влечет $\sigma(i) > \sigma(j)$, а $i > j$ влечет $\sigma(i) < \sigma(j)$. Если использовать запись перестановки в виде

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \swarrow & \searrow & \swarrow & \downarrow \\ 1 & 2 & 3 & 4 & 5 \end{array}$$

то инверсия соответствует пересечению стрелок. Определим число $d_{ij}(\sigma) = 1$, если пара i, j образует инверсию и 0, если не образуют. Тогда число всех инверсий для всевозможных пар это $d(\sigma) = \sum_{i < j} d_{ij}(\sigma)$. Определим отображение $\text{sgn}: S_n \rightarrow \{\pm 1\}$ по правилу $\text{sgn}(\sigma) = (-1)^{d(\sigma)}$. Для доказательства существования, надо проверить, что sgn обладает указанными свойствами (1) и (2), то есть надо доказать следующее.

Утверждение. Пусть $\sigma, \tau \in S_n$ – произвольные перестановки, тогда

$$\text{sgn}(\sigma\tau) = \text{sgn}(\sigma) \text{sgn}(\tau) \quad \text{и} \quad \text{sgn}(1, 2) = -1$$

Доказательство. Второе утверждение очевидно, в перестановке $(1, 2)$ всего одна инверсия, а значит $\text{sgn}(1, 2) = -1$.

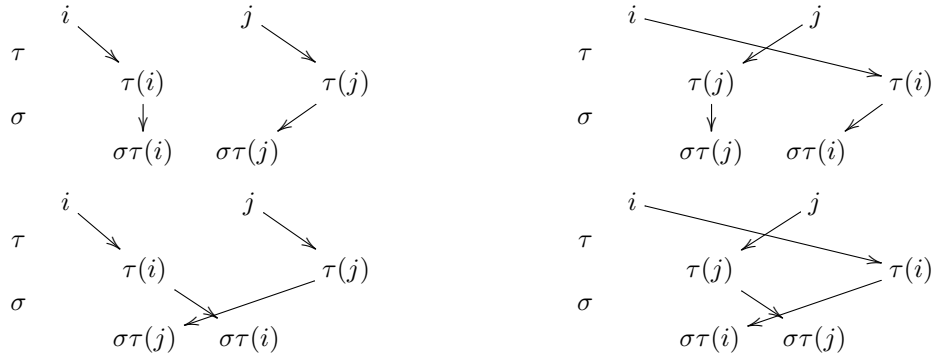
Для доказательства первого надо показать, что

$$d(\sigma) + d(\tau) = d(\sigma\tau) \pmod{2}$$

Давайте фиксируем пару i, j и докажем следующее равенство

$$d_{ij}(\tau) + d_{\tau(i)\tau(j)}(\sigma) = d_{ij}(\sigma\tau) \pmod{2}$$

Возможны следующие 4 случая:



Занесем результаты в таблицу

$d_{ij}(\tau)$	0	1	0	1
$d_{\tau(i)\tau(j)}(\sigma)$	0	0	1	1
$d_{ij} + d_{\tau(i)\tau(j)}(\sigma)$	0	1	1	2
$d_{ij}(\sigma\tau)$	0	1	1	0

Что доказывает равенство

$$d_{ij}(\tau) + d_{\tau(i)\tau(j)}(\sigma) = d_{ij}(\sigma\tau) \pmod{2}$$

Теперь сложим его для всех пар $i < j$. Получим

$$\sum_{i < j} d_{ij}(\tau) + \sum_{i < j} d_{\tau(i)\tau(j)}(\sigma) = \sum_{i < j} d_{ij}(\sigma\tau) \pmod{2}$$

Откуда

$$d(\tau) + \sum_{i < j} d_{\tau(i)\tau(j)}(\sigma) = d(\sigma\tau) \pmod{2}$$

Так как $\tau: X_n \rightarrow X_n$ – биекция, то если (i, j) пробегает все разные пары, то и $(\tau(i), \tau(j))$ пробегает все разные пары. Значит оставшаяся сумма равна $d(\sigma)$, что завершает доказательство. \square

²⁵Оно же *число инверсий*.

Единственность

Утверждение. Пусть $\phi: S_n \rightarrow \{\pm 1\}$ обладает свойством (1). Тогда

1. $\phi(\text{Id}) = 1$
2. $\phi(\sigma^{-1}) = \phi(\sigma)^{-1}$
3. Значение ϕ совпадает на всех транспозициях.

Доказательство. (1) Рассмотрим цепочку равенств

$$\phi(\text{Id}) = \phi(\text{Id}^2) = \phi(\text{Id})\phi(\text{Id})$$

Так как это числовое равенство (все числа ± 1), то можно сократить на $\phi(\text{Id})$ и получим требуемое.

(2) Рассмотрим цепочку равенств

$$1 = \phi(\text{Id}) = \phi(\sigma\sigma^{-1}) = \phi(\sigma)\phi(\sigma^{-1})$$

Значит число $\phi(\sigma^{-1})$ является обратным к $\phi(\sigma)$.²⁶

(3) Заметим, что для любых различных $i, j \in X_n$ у нас обязательно существует перестановка $\tau \in S_n$ такая, что $\tau(1) = i$ и $\tau(2) = j$.²⁷ Тогда по утверждению 9 получаем $(i, j) = \tau(1, 2)\tau^{-1}$. А значит

$$\phi(i, j) = \phi(\tau(1, 2)\tau^{-1}) = \phi(\tau)\phi(1, 2)\phi(\tau^{-1}) = \phi(1, 2)\phi(\tau)\phi(\tau^{-1}) = \phi(1, 2)$$

В предпоследнем равенстве мы воспользовались тем, что числа можно переставлять. Следовательно, значение на любой транспозиции равно значению на фиксированной транспозиции $(1, 2)$. То есть значение на всех транспозициях одинаковое. \square

Теперь давайте докажем единственность. Пусть у нас существует два таких отображения $\phi, \psi: S_n \rightarrow \{\pm 1\}$ удовлетворяющие свойствам (1) и (2). Давайте покажем, что $\phi(\sigma) = \psi(\sigma)$ для любой $\sigma \in S_n$. Из утверждения 10 следует, что σ представляется в виде $\sigma = \tau_1 \dots \tau_r$, где τ_i – транспозиции.

Значение ϕ одно и то же на всех транспозициях: либо 1 либо -1 . Предположим, что значение равно 1. Тогда $\phi(\sigma) = \phi(\tau_1 \dots \tau_r) = \phi(\tau_1) \dots \phi(\tau_r) = 1$ для всех $\sigma \in S_n$, что противоречит свойству (2). А значит $\phi(\tau) = -1$ для любой транспозиции τ . Аналогично, $\psi(\tau) = -1$ для любой транспозиции τ . А следовательно

$$\phi(\sigma) = \phi(\tau_1 \dots \tau_r) = \phi(\tau_1) \dots \phi(\tau_r) = (-1)^r = \psi(\tau_1) \dots \psi(\tau_r) = \psi(\tau_1 \dots \tau_r) = \psi(\sigma)$$

То есть, на самом деле, все определяется значением на транспозиции.

3.7 Подсчет знака

Декремент Декремент перестановки $\sigma \in S_n$ – это

$$\text{dec}(\sigma) = n - \text{«количество нетривиальных циклов»} - \text{«количество неподвижных точек»}$$

Если рассматривать все неподвижные точки как тривиальные «циклы», то формула превращается в

$$\text{dec}(\sigma) = n - \text{«количество циклов»}$$

Декремент можно описать еще так: каждая перестановка σ определяет граф на множестве вершин X_n , где (i, j) – ребро, если $\sigma(i) = j$. Тогда

$$\text{dec}(\sigma) = \text{«количество вершин»} - \text{«количество компонент графа»}$$

Утверждение 12. Пусть $\sigma \in S_n$, тогда $\text{sgn}(\sigma) = (-1)^{\text{dec}(\sigma)}$.

²⁶Так как все наши числа ± 1 , то можно было бы сказать $\phi(\sigma^{-1}) = \phi(\sigma)$. Но в указанной форме равенство лучше запоминается и встретится вам еще не раз.

²⁷Я оставляю это как упражнение.

Доказательство. Действительно, разложим перестановку σ в произведение независимых циклов $\sigma = \rho_1 \dots \rho_k$. Пусть длины циклов d_1, \dots, d_k , соответственно. Тогда

$$\text{sgn}(\sigma) = (-1)^{d_1-1} \dots (-1)^{d_k-1} = (-1)^{\sum_i d_i - k}$$

Пусть s – количество неподвижных точек. Тогда

$$\text{sgn}(\sigma) = (-1)^{(\sum_i d_i + s) - k - s} = (-1)^{n - k - s} = (-1)^{\text{dec}(\sigma)}$$

□

При подсчета знака перестановки надо пользоваться декрементом. То есть, надо разложить перестановку в произведение независимых циклов и сложить их длины без единицы. Например:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 8 & 2 & 3 & 7 & 1 & 5 & 9 & 6 \end{pmatrix}$$

Теперь видим, что

$$\begin{aligned} 1 &\rightarrow 4 \rightarrow 3 \rightarrow 2 \rightarrow 8 \rightarrow 9 \rightarrow 6 \rightarrow 1 \\ 5 &\rightarrow 7 \rightarrow 5 \end{aligned}$$

Значит $\sigma = (1, 4, 3, 2, 8, 9, 6)(57)$, а значит $\text{dec}(\sigma) = 6 + 1 = 7$ и $\text{sgn}(\sigma) = -1$.

3.8 Возведение в степень

Прежде всего сделаем два простых наблюдения:

1. Пусть $\sigma, \tau \in S_n$ – две коммутирующие перестановки, тогда $(\sigma\tau)^m = \sigma^m \tau^m$.
2. Пусть $\rho \in S_n$ – цикл длины d , тогда d совпадает с наименьшим натуральным числом k таким, что $\rho^k = \text{Id}$.

Пусть теперь $\sigma \in S_n$ – произвольная перестановка. Мы можем разложить ее в произведение независимых циклов $\sigma = \rho_1 \dots \rho_k$ с длинами d_1, \dots, d_k , соответственно. Тогда

$$\sigma^m = \rho_1^m \dots \rho_k^m = \rho_1^{m \pmod{d_1}} \dots \rho_k^{m \pmod{d_k}}$$

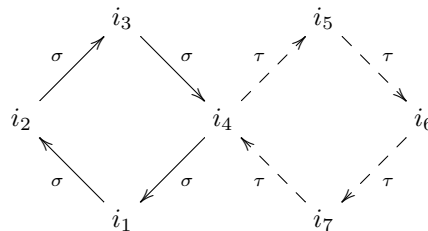
Таким образом, расчет произвольной степени перестановки σ сводится к возведению циклов в степень не большую их длины.

Оставим еще одно замечание в качестве упражнения. Если $\sigma = \rho_1 \dots \rho_k$ – разложение в произведение независимых циклов длин d_1, \dots, d_k , соответственно, то наименьшее натуральное r такое, что $\sigma^r = \text{Id}$, равно наименьшему общему кратному чисел d_1, \dots, d_k .

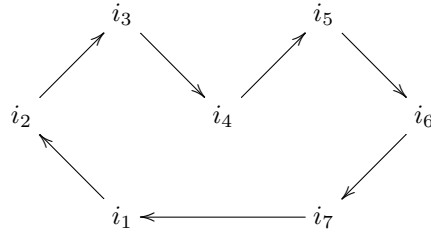
3.9 Произведение циклов

В этом разделе я приведу несколько примеров того, как перемножаются между собой зависимые циклы.

Два цикла Пусть $\sigma, \tau \in S_n$ циклы зацепляющиеся по одному элементу, как на рисунке ниже

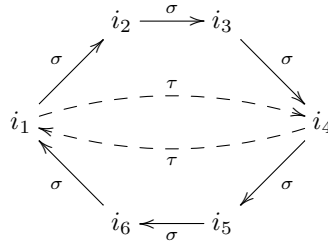


Надо найти произведение $\sigma\tau$. На рисунке ниже показано как выглядит произведение

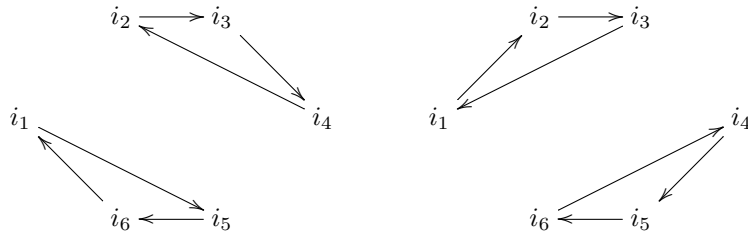


Таким образом, мы получили формулу $(i_1, \dots, i_k)(i_k, \dots, i_n) = (i_1, \dots, i_n)$.

Цикл и транспозиция Пусть $\sigma, \tau \in S_n$, где σ – цикл, а τ – транспозиция, переставляющая два элемента цикла σ как на рисунке ниже.



Вот так выглядят композиции для $\sigma\tau$ и $\tau\sigma$ соответственно

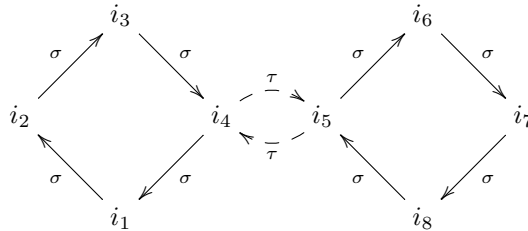


Таким образом общее правило выглядит так

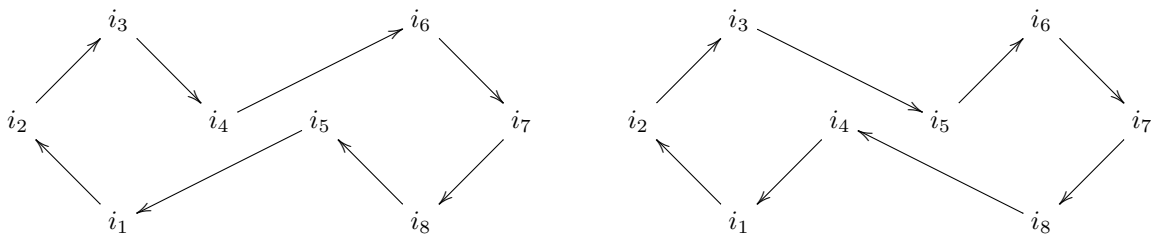
$$(i_1, \dots, i_n)(i_1, i_k) = (i_1, i_{k+1}, \dots, i_n)(i_2, \dots, i_k)$$

$$(i_1, i_k)(i_1, \dots, i_n) = (i_1, \dots, i_{k-1})(i_k, \dots, i_n)$$

Пара циклов и транспозиция Пусть $\sigma, \tau \in S_n$, причем, σ – произведение двух независимых циклов, а τ – транспозиция, переставляющая две вершины из разных циклов как на рисунке ниже.



Произведения $\sigma\tau$ и $\tau\sigma$ имеют вид



Таким образом общее правило выглядит так

$$\begin{aligned}(i_1, \dots, i_k)(i_{k+1}, \dots, i_n)(i_k, i_{k+1}) &= (i_1, \dots, i_k, i_{k+2}, \dots, i_n, i_{k+1}) \\ (i_k, i_{k+1})(i_1, \dots, i_k)(i_{k+1}, \dots, i_n) &= (i_k, i_1, \dots, i_{k-1}, i_{k+1}, \dots, i_n)\end{aligned}$$

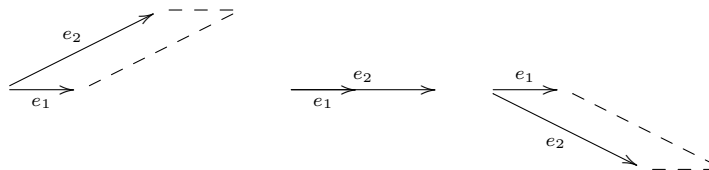
4 Определитель

4.1 Философия

Сейчас я хочу обсудить «ориентированный объем» на прямой, плоскости и в пространстве.

Прямая На прямой мы можем выбрать «положительное» направление. Обычно на рисунке выбирают слева направо. Тогда длина вектора, который смотрит слева направо, считается положительной, а справа налево – отрицательной.

Плоскость Здесь объем будет задаваться парой векторов, то есть некоторой квадратной матрицей размера 2, где вектора – это ее столбцы. Основная идея такая: пусть мы хотим посчитать площадь между двумя векторами на плоскости, точнее площадь параллелограмма натянутого на вектора e_1 и e_2 как на первом рисунке ниже.

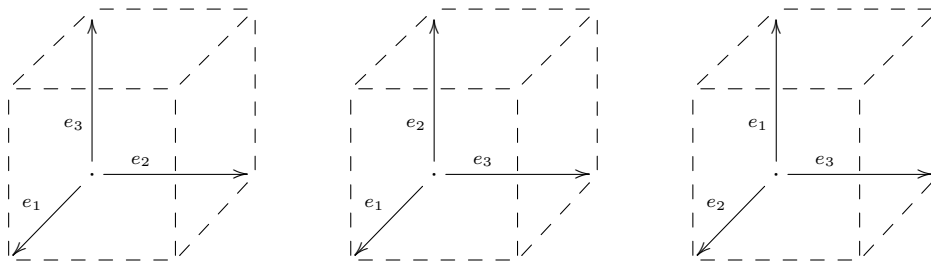


Давайте двигать вектор e_2 к вектору e_1 . Тогда площадь будет уменьшаться и когда вектора совпадут, она будет равна нулю. Однако, если мы продолжим двигать вектор e_2 , то площадь между векторами опять начнет расти и картинка в конце концов станет симметрична исходной, а полученный параллелограмм равен изначальному. Однако, эта ситуация отличается от предыдущей и вот как можно понять чем. Предположим, что между векторами была натянута хорошо сжимаемая ткань, одна сторона которой красная, другая зеленая. Тогда в самом начале на нас смотрит красная сторона этой ткани, но как только e_2 прошел через e_1 на нас уже смотрит зеленая сторона. Мы бы хотели научиться отличать эти две ситуации с помощью знака, если на нас смотрит красная сторона – знак положительный, если зеленая – отрицательный.

Еще один способ думать про эту ситуацию. Представим, что плоскость – это наш стол, а параллелограмм вырезан из бумаги. Мы можем положить параллелограмм на стол двумя способами: лицевой стороной вверх или же вниз. В первом случае мы считаем площадь положительной, а во втором – отрицательной. Возможность определить лицевую сторону связана с тем, что мы знаем, где у стола верх, а где низ. Это возможно, потому что наша плоскость лежит в трехмерном пространстве и мы можем глядеть на нее извне. Однако, если бы мы жили на плоскости и у нас не было бы возможности выглянуть за ее пределы, то единственный способ установить «какой стороной вверх лежит параллелограмм» был бы с помощью порядка векторов.

Еще одно важное замечание. Если мы берем два одинаковых параллелограмма на нашем столе, которые лежат лицевой стороной вверх, то мы можем передвинуть один в другой, не отрывая его от стола. А вот если один из параллелограммов имеет положительный объем, а другой отрицательный, то нельзя перевести один в другой, не отрывая от стола. То есть, если вы живете на плоскости, то вам не получится переместить положительный параллелограмм в отрицательный, не сломав или не разобрав его.

Пространство В пространстве дело с ориентацией обстоит абсолютно аналогично. Мы хотим уже считать объемы параллелепипедов натянутых на три вектора. И мы так же хотим, чтобы эти объемы показывали «с какой стороны» мы смотрим на параллелепипед.



Здесь знак объема определяется по порядку векторов, как знак перестановки. На рисунке объемы первого и третьего положительные, а у второго отрицательный. Если вы сделаете модельки этих кубиков из подписан-

ных спичек, то третий кубик – это первый, но лежащий на другой грани. А вот второй кубик получить из первого вращениями не получится. Надо будет его разобрать и присобачить ребра по-другому.

Как и в случае с плоскостью, если бы мы могли выйти за пределы нашего трехмерного пространства, то у нас появилась бы лицевая и тыльная сторона, как у стола. И тогда первый и третий кубики лежали бы лицевой стороной вверх, а второй – вниз. Мы, конечно же, так сделать не сможем и никогда в жизни не увидим подобное, но думать про такое положение вещей по аналогии с плоскостью можем и эта интуиция бывает полезна.

Пояснение планов В текущей лекции я не собираюсь обсуждать объемы, а всего лишь хочу коснуться некоторой техники, которая используется для работы с ориентированными объемами. Чтобы начать честный рассказ про сами объемы (который обязательно будет, но позже), нам надо поговорить о том, что такое векторное пространство и как в абстрактном векторном пространстве мерить расстояния и углы. Потому, пока мы не покроем эти темы, всерьез говорить про настоящие объемы мы не сможем.

4.2 Три разных определения

Начнем с классического определения в виде явной формулы.

Определитель (I) Рассмотрим отображение $\det: M_n(\mathbb{R}) \rightarrow \mathbb{R}$ задаваемое следующей формулой: для любой матрицы $A \in M_n(\mathbb{R})$ положим

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

Данное отображение называется *определителем*, а его значение $\det A$ на матрице A называется определителем матрицы A .

Давайте неформально обсудим, как считается выражение для определителя. Как мы видим определитель состоит из суммы некоторых произведений. Каждое произведение имеет вид $a_{1\sigma(1)} \dots a_{n\sigma(n)}$ умноженное на $\operatorname{sgn}(\sigma)$. Здесь из каждой строки матрицы A ²⁸ выбирается по одному элементу так, что никакие два элемента не лежат в одном столбце (это гарантировано тем, что σ – перестановка и потому $\sigma(i)$ не повторяются). Заметим, что слагаемых ровно столько, сколько перестановок – $n!$ штук. Из этих слагаемых половина идет со знаком плюс, а другая – со знаком минус.

Нормированные полилинейные кососимметрические отображения (II) Пусть $\phi: M_n(\mathbb{R}) \rightarrow \mathbb{R}$ – некоторое отображение и $A \in M_n(\mathbb{R})$. Тогда про матрицу A можно думать, как про набор из n столбцов: $A = (A_1 | \dots | A_n)$. Тогда функцию $\phi(A) = \phi(A_1, \dots, A_n)$ можно рассматривать как функцию от n столбцов.

В обозначениях выше рассмотрим отображения $\phi: M_n(\mathbb{R}) \rightarrow \mathbb{R}$ удовлетворяющие следующим свойствам:

1. $\phi(A_1, \dots, A_i + A'_i, \dots, A_n) = \phi(A_1, \dots, A_i, \dots, A_n) + \phi(A_1, \dots, A'_i, \dots, A_n)$ для любого i .
2. $\phi(A_1, \dots, \lambda A_i, \dots, A_n) = \lambda \phi(A_1, \dots, A_i, \dots, A_n)$ для любого i и любого $\lambda \in \mathbb{R}$.
3. $\phi(A_1, \dots, A_i, \dots, A_j, \dots, A_n) = -\phi(A_1, \dots, A_j, \dots, A_i, \dots, A_n)$ для любых различных i и j .
4. $\phi(E) = 1$.

Первые два свойства вместе называются *полилинейностью* ϕ по столбцам, т.е. это уважение суммы и умножения на скаляр. Третье свойство называется *кососимметричностью* ϕ по столбцам. Последнее условие – это условие нормировки. Данный набор свойств можно заменить эквивалентным с переформулированным третьим свойством:

1. $\phi(A_1, \dots, A_i + A'_i, \dots, A_n) = \phi(A_1, \dots, A_i, \dots, A_n) + \phi(A_1, \dots, A'_i, \dots, A_n)$ для любого i .
2. $\phi(A_1, \dots, \lambda A_i, \dots, A_n) = \lambda \phi(A_1, \dots, A_i, \dots, A_n)$ для любого i и любого $\lambda \in \mathbb{R}$.
3. $\phi(A_1, \dots, A', \dots, A', \dots, A_n) = 0$, т.е. если есть два одинаковых столбца, то значение ϕ равно нулю.
4. $\phi(E) = 1$.

²⁸Первый индекс – индекс строки.

Действительно, обозначим $\Phi(a, b) = \phi(A_1, \dots, a, \dots, b, \dots, A_n)$. Тогда Φ полилинейная функция двух аргументов.²⁹ И нам надо показать, что $\Phi(a, a) = 0$ для любого $a \in \mathbb{R}^n$ тогда и только тогда, когда $\Phi(a, b) = -\Phi(b, a)$ для любых $a, b \in \mathbb{R}^n$. Для \Rightarrow подставим $b = a$, получим $\Phi(a, a) = -\Phi(a, a)$. Для обратного \Leftarrow подставим $a + b$, получим $\Phi(a + b, a + b) = 0$. Раскроем скобки: $\Phi(a, a) + \Phi(a, b) + \Phi(b, a) + \Phi(b, b) = 0$. Откуда следует требуемое.

Пример На всякий случай поясню все свойства выше на примерах:

1. $\phi \begin{pmatrix} 1 & 3 \\ 2 & 7 \end{pmatrix} = \phi \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix} \middle| \begin{pmatrix} 3 \\ 7 \end{pmatrix} \right) = \phi \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix} \middle| \begin{pmatrix} 1 \\ 3 \end{pmatrix} + \begin{pmatrix} 2 \\ 4 \end{pmatrix} \right) = \phi \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} + \phi \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$
2. $\phi \begin{pmatrix} 1 & 3 \\ 2 & 9 \end{pmatrix} = 3\phi \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$
3. $\phi \begin{pmatrix} 1 & 3 \\ 2 & 7 \end{pmatrix} = -\phi \begin{pmatrix} 3 & 1 \\ 7 & 2 \end{pmatrix}$
- 3'. $\phi \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix} = 0$

Везде далее будем упоминать отображения с такими свойствами, как отображения со свойством (II).

Нормированные полилинейные кососимметрические отображения (II') Аналогично (II) можно рассмотреть полилинейные кососимметрические отображения по строкам матрицы A вместо столбцов. Тогда можно рассматривать отображения $\phi': M_n(\mathbb{R}) \rightarrow \mathbb{R}$ с аналогами четырех свойств выше: полилинейность, кососимметричность, значение 1 на единичной матрице. Такие отображения мы будем называть, как отображения со свойствами (II').

Специальные мультипликативные отображения (III) Рассмотрим множество отображений $\psi: M_n(\mathbb{R}) \rightarrow \mathbb{R}$ удовлетворяющие следующими свойствам:

1. $\psi(AB) = \psi(A)\psi(B)$ для любых $A, B \in M_n(\mathbb{R})$.
2. $\psi \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & d \end{pmatrix} = d$ для любого ненулевого $d \in \mathbb{R}$.

Всюду ниже будем упоминать отображения с такими свойствами, как отображения со свойством (I).³⁰

План дальнейших действий Наша задача показать, что, во-первых, определитель обладает свойствами (II), (II') и (III), а, во-вторых, что кроме определителя никакое другое отображение не удовлетворяет этим свойствам. То есть все три определения между собой эквивалентны. Самое сложное будет показать, что (III) влечет остальные два определения. Это означает, что (III) легко проверять, но из него сложно выводить какие-либо свойства. Самые полезные с вычислительной точки зрения – определения (II) и (II').

4.3 Явные формулы для определителя

Подсчет в малых размерностях

1. Если $A \in M_1(\mathbb{R}) = \mathbb{R}$, то $\det A = A$.
2. Если $A \in M_2(\mathbb{R})$ имеет вид $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, то $\det A = ad - bc$. Графически: главная диагональ минус побочная.

²⁹Такие отображения называются билинейными.

³⁰Обратите внимание, что существует много отображений со свойством (1), не удовлетворяющих свойству (2). Действительно, если ψ – мультипликативное отображение, то есть удовлетворяет только свойству (1), то $\gamma_n(A) = \psi(A)^n$ – тоже мультипликативное отображение для любого натурального $n \in \mathbb{N}$. Кроме того, $\delta_\alpha(A) = |\psi(A)|^\alpha$ тоже является мультипликативным отображением для любого положительного $\alpha \in \mathbb{R}$.

3. Если $A \in M_3(\mathbb{R})$ имеет вид $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, то определитель получается из 6 слагаемых три из них с + три с -. Графически слагаемые можно изобразить так:

$$\det A = + \left(\begin{array}{c} \diagdown \\ \diagup \end{array} \right) + \left(\begin{array}{c} \diagup \\ \diagdown \end{array} \right) + \left(\begin{array}{c} \diagdown \\ \diagdown \end{array} \right) - \left(\begin{array}{c} \diagup \\ \diagup \end{array} \right) - \left(\begin{array}{c} \diagdown \\ \diagup \end{array} \right) - \left(\begin{array}{c} \diagup \\ \diagdown \end{array} \right)$$

Точная формула³¹

$$\det A = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}$$

Треугольные матрицы

Утверждение 13. Для любых верхне и нижне треугольных матрицы верны следующие формулы:

$$\det \begin{pmatrix} \lambda_1 & \dots & * \\ & \ddots & \vdots \\ & & \lambda_n \end{pmatrix} = \lambda_1 \dots \lambda_n \quad \det \begin{pmatrix} \lambda_1 & & \\ \vdots & \ddots & \\ * & \dots & \lambda_n \end{pmatrix} = \lambda_1 \dots \lambda_n$$

В частности $\det E = 1$.

Доказательство. Я докажу утверждение для верхнетреугольных матриц, нижнетреугольный случай делается аналогично. Для доказательства надо посчитать определитель по определению и увидеть, что только одно слагаемое соответствующее тождественной перестановке является не нулем. Действительно, рассмотрим выражение $a_{1\sigma(1)} \dots a_{n\sigma(n)}$. Посмотрим когда это выражение не ноль. Последний множитель $a_{n\sigma(n)}$ лежит в последней строке и должен быть не ноль. Для этого должно выполняться $\sigma(n) = n$. Теперь $a_{n-1\sigma(n-1)}$ должен быть не ноль. Так как $\sigma(n) = n$, то $\sigma(n-1) \neq n$. А значит, чтобы $a_{n-1\sigma(n-1)}$ был не ноль, остается только один случай $\sigma(n-1) = n-1$. Продолжая аналогично, мы видим, что $\sigma(i) = i$ для всех строк i . \square

4.4 Свойства определителя

Определитель и транспонирование Прежде чем перейти к доказательству следующего утверждения сделаем одно полезное наблюдение. Если мы возьмем две произвольные перестановки $\sigma, \tau \in S_n$ и матрицу $A \in M_n(\mathbb{R})$, то выражения $a_{\tau(1)\sigma(\tau(1))} \dots a_{\tau(n)\sigma(\tau(n))}$ совпадает с выражением $a_{1\sigma(1)} \dots a_{n\sigma(n)}$ с точностью до перестановки сомножителей. Это делается методом пристального взгляда: замечаем что каждый сомножитель одного выражения ровно один раз встречается в другом и наоборот.

Утверждение 14. Пусть $A \in M_n(\mathbb{R})$, тогда $\det A = \det A^t$.

Доказательство. Посчитаем по определению $\det A^t$, получим

$$\det A^t = \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n} = \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{\sigma(1)\sigma^{-1}(\sigma(1))} \dots a_{\sigma(n)\sigma^{-1}(\sigma(n))}$$

Теперь применим наше замечание перед доказательством:

$$a_{\sigma(1)\sigma^{-1}(\sigma(1))} \dots a_{\sigma(n)\sigma^{-1}(\sigma(n))} = a_{1\sigma^{-1}(1)} \dots a_{n\sigma^{-1}(n)}$$

Значит

$$\det A^t = \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{1\sigma^{-1}(1)} \dots a_{n\sigma^{-1}(n)}$$

Вспомним, что $\text{sgn}(\sigma) = \text{sgn}(\sigma^{-1})$. Следовательно:

$$\det A^t = \sum_{\sigma \in S_n} \text{sgn}(\sigma^{-1}) a_{1\sigma^{-1}(1)} \dots a_{n\sigma^{-1}(n)}$$

³¹Для больших размерностей чем 3 на 3 явная формула не пригодна из-за слишком большого числа слагаемых. Даже с вычислительной точки зрения.

Теперь, если σ пробегает все перестановки, то σ^{-1} тоже пробегает все перестановки, так как отображение $S_n \rightarrow S_n$ по правилу $\sigma \mapsto \sigma^{-1}$ является биекцией.³² То есть мы можем сделать замену $\tau = \sigma^{-1}$ и приходим к выражению

$$\det A^t = \sum_{\tau \in S_n} \operatorname{sgn}(\tau) a_{1\tau(1)} \dots a_{n\tau(n)}$$

Последнее в точности совпадает с определением $\det A$. □

Отметим, что если мы доказали какое-то свойство определителя для столбцов, то это утверждение автоматически гарантирует, что такое же свойство выполнено и для строк. И наоборот, если что-то сделано для строк, то это автоматически следует для столбцов.

4.5 Полилинейность и кососимметричность определителя

Сейчас мы докажем, что определитель обладает всеми свойствами (II) и (II'). В силу утверждения 14 нам достаточно показать только (II).

Утверждение 15. *Отображение $\det: M_n(\mathbb{R}) \rightarrow \mathbb{R}$ рассматриваемое как отображение столбцов матрицы является полилинейным и кососимметричным, т.е. удовлетворяет следующим свойствам:*

1. $\det(A_1, \dots, A_i + A'_i, \dots, A_n) = \det(A_1, \dots, A_i, \dots, A_n) + \det(A_1, \dots, A'_i, \dots, A_n)$ для любого i .
2. $\det(A_1, \dots, \lambda A_i, \dots, A_n) = \lambda \det(A_1, \dots, A_i, \dots, A_n)$ для любого i и любого $\lambda \in \mathbb{R}$.
3. $\det(A_1, \dots, A_i, \dots, A_j, \dots, A_n) = -\det(A_1, \dots, A_j, \dots, A_i, \dots, A_n)$ для любых различных i и j .
4. $\det E = 1$.

Доказательство. Мы знаем, что

$$\det A = \det A^t = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(i)i} \dots a_{\sigma(n)n}$$

Проверим свойство (1):

$$\begin{aligned} \det(A_1, \dots, A_i + A'_i, \dots, A_n) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \dots (a_{\sigma(i)i} + a'_{\sigma(i)i}) \dots a_{\sigma(n)n} = \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(i)i} \dots a_{\sigma(n)n} + \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \dots a'_{\sigma(i)i} \dots a_{\sigma(n)n} = \\ &= \det(A_1, \dots, A_i, \dots, A_n) + \det(A_1, \dots, A'_i, \dots, A_n) \end{aligned}$$

Теперь свойство (2):

$$\det(A_1, \dots, \lambda A_i, \dots, A_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \dots (\lambda a_{\sigma(i)i}) \dots a_{\sigma(n)n} = \lambda \det(A_1, \dots, A_i, \dots, A_n)$$

Для проверки свойства (3) введем следующее обозначение. Пусть $\tau \in S_n$ обозначает транспозицию (i, j) . Тогда посчитаем определитель с переставленными столбцами i и j местами:

$$\begin{aligned} \det(A_1, \dots, A_j, \dots, A_i, \dots, A_n) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(i)j} \dots a_{\sigma(j)i} \dots a_{\sigma(n)n} = \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1)\tau(1)} \dots a_{\sigma(i)\tau(i)} \dots a_{\sigma(j)\tau(j)} \dots a_{\sigma(n)\tau(n)} = \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(\tau^{-1}(1))1} \dots a_{\sigma(\tau^{-1}(n))n} = - \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma\tau^{-1}) a_{\sigma(\tau^{-1}(1))1} \dots a_{\sigma(\tau^{-1}(n))n} \end{aligned}$$

³² Оно биекция, так как имеет обратное – оно само.

Здесь при переходе от второй строчки к третьей мы воспользовались замечанием перед упражнением 14. Так как отображение $S_n \rightarrow S_n$ по правилу $\sigma \mapsto \sigma\tau^{-1}$ является биекцией, то если σ пробегает все перестановки, то и $\sigma\tau^{-1}$ пробегает все перестановки. А значит, делая замену $\rho = \sigma\tau^{-1}$, получаем

$$- \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma\tau^{-1}) a_{\sigma(\tau^{-1}(1))1} \dots a_{\sigma(\tau^{-1}(n))n} = -\det(A_1, \dots, A_i, \dots, A_j, \dots, A_n)$$

(4) Это непосредственно следует из определения, либо если хотите, то можно сослаться на утверждение 13. \square

Утверждение. Если $A \in M_n(\mathbb{R})$ имеет нулевой столбец или нулевую строку, то $\det A = 0$.

Доказательство. Пусть A имеет нулевой столбец. Мы знаем, что \det – полилинейная функция. Значит, если мы умножим нулевой столбец на -1 , определитель должен поменять знак. С другой стороны, если мы умножим нулевой столбец на любое число, он не поменяется и определитель не должен поменяться. Значит по безысходности определитель должен быть 0. \square

Определитель от элементарных матриц

Утверждение 16. Верны следующие утверждения:

1. $\det(S_{ij}(\lambda)) = 1$, где $S_{ij}(\lambda) \in M_n(\mathbb{R})$ – матрица элементарного преобразования первого типа.
2. $\det(U_{ij}) = -1$, где $U_{ij} \in M_n(\mathbb{R})$ – матрица элементарного преобразования второго типа.
3. $\det(D_i(\lambda)) = \lambda$, где $D_i(\lambda) \in M_n(\mathbb{R})$ – матрица элементарного преобразования третьего типа.

Доказательство. (1) Является следствием для случая верхне- и нижнетреугольных матриц.

(2) Так как U_{ij} получается из единичной матрицы перестановкой i -го и j -го столбцов, то результат следует из кососимметричности определителя.

(3) Следует из полилинейности определителя – свойство (II) (2). \square

4.6 Полилинейные кососимметрические отображения

Все утверждения в этом разделе доказываются для строк. Соответствующие утверждения для столбцов доказываются аналогично. Их формулировки и доказательства я оставляю в качестве упражнения.

Утверждение 17. Пусть $\phi: M_n(\mathbb{R}) \rightarrow \mathbb{R}$ – полилинейное кососимметрическое отображение по строкам матриц, т.е. удовлетворяет следующим свойствам.³³

1. $\phi(A_1, \dots, A_i + A'_i, \dots, A_n) = \phi(A_1, \dots, A_i, \dots, A_n) + \phi(A_1, \dots, A'_i, \dots, A_n)$ для любого i .
2. $\phi(A_1, \dots, \lambda A_i, \dots, A_n) = \lambda \phi(A_1, \dots, A_i, \dots, A_n)$ для любого i и любого $\lambda \in \mathbb{R}$.
3. $\phi(A_1, \dots, A_i, \dots, A_j, \dots, A_n) = -\phi(A_1, \dots, A_j, \dots, A_i, \dots, A_n)$ для любых различных i и j .

Тогда $\phi(UA) = \det(U)\phi(A)$ для любой матрицы $A \in M_n(\mathbb{R})$ и любой элементарной матрицы $U \in M_n(\mathbb{R})$.

Доказательство. Случай $U = S_{ij}(\lambda)$.

$$\begin{aligned} \phi(S_{ij}(\lambda)A) &= \phi(A_1, \dots, A_i + \lambda A_j, \dots, A_j, \dots, A_n) = \\ &= \phi(A_1, \dots, A_i, \dots, A_j, \dots, A_n) + \lambda \phi(A_1, \dots, A_j, \dots, A_j, \dots, A_n) = \phi(A) = \det(S_{ij}(\lambda))\phi(A) \end{aligned}$$

Случай $U = U_{ij}$.

$$\phi(U_{ij}A) = \phi(A_1, \dots, A_j, \dots, A_i, \dots, A_n) = -\phi(A_1, \dots, A_i, \dots, A_j, \dots, A_n) = -\phi(A) = \det(U_{ij})\phi(A)$$

Случай $U = D_i(\lambda)$.

$$\phi(D_i(\lambda)A) = \phi(A_1, \dots, \lambda A_i, \dots, A_n) = \lambda \phi(A_1, \dots, A_i, \dots, A_n) = \lambda \phi(A) = \det(D_i(\lambda))\phi(A)$$

\square

³³Здесь через A_i обозначаются строки матрицы A идущие сверху вниз.

Определитель и элементарные матрицы Заметим, что по утверждению 15, определитель тоже является полилинейной и кососимметрической функцией. Потому доказанное утверждение в частности означает, что $\det(UA) = \det(U)\det(A)$ для любой матрицы $A \in M_n(\mathbb{R})$ и любой элементарной матрицы $U \in M_n(\mathbb{R})$.

Подсчет определителя Предыдущее замечание позволяет дать эффективный способ вычисления определителя методом Гаусса. Мы берем матрицу A и приводим ее к ступенчатому виду попутно запоминая как изменился определитель по сравнению с определителем изначальной матрицы. Если же мы будем использовать только элементарные преобразования первого типа, то определитель вовсе меняться не будет. Ступенчатый вид матрицы всегда верхне треугольный. Там определитель считается как произведение диагональных элементов.

Следствия утверждения 17

Утверждение 18 (Единственность для полилинейных кососимметричных). Пусть $\phi: M_n(\mathbb{R}) \rightarrow \mathbb{R}$ – полилинейное кососимметрическое отображение по строкам матриц. Тогда $\phi(X) = \det(X)\phi(E)$. В частности, если $\phi(E) = 1$, то $\phi = \det$.

Доказательство. Пусть $X \in M_n(\mathbb{R})$ – произвольная матрица, тогда ее можно элементарными преобразованиями строк привести к улучшенному ступенчатому виду. Последнее означает, что $X = U_1 \dots U_k S$, где S – матрица улучшенного ступенчатого вида, а U_i – матрицы элементарных преобразований. Применим к этому равенству отдельно ϕ и отдельно \det , получим

$$\begin{aligned}\phi(X) &= \det(U_1) \dots \det(U_k) \phi(S) \\ \det(X) &= \det(U_1) \dots \det(U_k) \det(S)\end{aligned}$$

Теперь для матрицы S у нас есть два варианта: либо S единичная, либо содержит нулевую строку.

Пусть $S = E$, тогда

$$\begin{aligned}\phi(X) &= \det(U_1) \dots \det(U_k) \phi(E) \\ \det(X) &= \det(U_1) \dots \det(U_k)\end{aligned}$$

Откуда и получаем требуемое $\phi(X) = \det(X)\phi(E)$.

Пусть теперь S имеет нулевую строку. Тогда из полилинейности определителя и ϕ следует, что $\phi(S) = 0 = \det(S)$.³⁴ Что тоже влечет равенство $\phi(X) = \det(X)\phi(E)$. \square

Утверждение 19 (Мультипликативность определителя). Пусть $A, B \in M_n(\mathbb{R})$ – произвольные матрицы. Тогда $\det(AB) = \det(A)\det(B)$.

Доказательство. Фиксируем матрицу $B \in M_n(\mathbb{R})$ и рассмотрим отображение $\gamma: M_n(\mathbb{R}) \rightarrow \mathbb{R}$ по правилу $A \mapsto \det(AB)$. Если A_1, \dots, A_n – строки матрицы A , то A_1B, \dots, A_nB – строки матрицы AB . Из этого легко видеть, что γ – полилинейна и кососимметрическая функция по строкам матрицы A . Значит по утверждению 18 $\gamma(A) = \det(A)\gamma(E)$. Но последнее равносильно $\det(AB) = \det(A)\det(B)$. \square

Утверждение 20 (Определитель с углом нулей). Пусть $A \in M_n(\mathbb{R})$ и $B \in M_m(\mathbb{R})$. Тогда

$$\det \begin{pmatrix} A & * \\ 0 & B \end{pmatrix} = \det \begin{pmatrix} A & 0 \\ * & B \end{pmatrix} = \det(A) \det(B)$$

Доказательство. Рассмотрим функцию $\phi: M_n(\mathbb{R}) \rightarrow \mathbb{R}$ по правилу

$$\phi(X) = \det \begin{pmatrix} X & * \\ 0 & B \end{pmatrix}$$

Заметим, что эта функция является полилинейной и кососимметричной по столбцам матрицы X . В этом случае по утверждению 18 о единственности для полилинейных кососимметрических отображений она имеет вид $\phi(X) = \det(X)\phi(E)$, то есть

$$\det \begin{pmatrix} A & * \\ 0 & B \end{pmatrix} = \det A \det \begin{pmatrix} E & * \\ 0 & B \end{pmatrix}$$

³⁴При умножении на -1 нулевой строки с одной стороны функция должна поменять знак, а с другой не измениться.

Теперь рассмотрим функцию $\psi: M_n(\mathbb{R}) \rightarrow \mathbb{R}$ по правилу

$$\psi(X) = \det \begin{pmatrix} E & * \\ 0 & X \end{pmatrix}$$

Заметим, что эта функция является полилинейной и кососимметричной по строкам матрицы X . В этом случае по утверждению 18 о единственности для полилинейных кососимметрических отображений она имеет вид $\psi(X) = \det(X)\psi(E)$, то есть

$$\det \begin{pmatrix} E & * \\ 0 & B \end{pmatrix} = \det B \det \begin{pmatrix} E & * \\ 0 & E \end{pmatrix}$$

Последний определитель равен 1, так как по утверждению 13 определитель верхнетреугольной матрицы равен произведению ее диагональных элементов. Теперь собираем вместе доказанные факты и получаем требуемый результат. \square

Заметим, что таким образом мы можем считать определитель для блочно верхнетреугольных матриц и для блочно нижнетреугольных матриц с любым количеством блоков. Формулы тогда будут выглядеть так

$$\det \begin{pmatrix} A_1 & * & \dots & * \\ & A_2 & \dots & * \\ & & \ddots & \vdots \\ & & & A_k \end{pmatrix} = \det \begin{pmatrix} A_1 & & & \\ * & A_2 & & \\ \vdots & \vdots & \ddots & \\ * & * & \dots & A_k \end{pmatrix} = \det A_1 \dots \det A_k$$

где $A_i \in M_{n_i}(\mathbb{R})$ – обязательно квадратные матрицы. Это правило является обобщением утверждения о вычислении определителя для треугольных матриц.

4.7 Мультипликативные отображения

Давайте подытожим, что мы показали. Утверждение 15 вместе с утверждением 14 объясняют почему определитель является полилинейной кососимметрической функцией как строк, так и столбцов. Далее утверждение 18 доказывает, что любая полилинейная кососимметричная функция по строкам, принимающая значение 1 на единичной матрице, должна быть определителем. С помощью утверждения 14 мы получаем аналогичный результат для столбцов. Таким образом мы показали эквивалентность подхода (I) подходам (II) и (II').

Теперь, утверждение 19 показывает, что определитель обязательно мультипликативен, а свойство (III) (2) следует из явных вычислений для элементарных матриц. Тем самым мы показали, что (I) и (II) влекут (III). Осталось показать, что (III) влечет (I), т.е. что определитель является единственной функцией с такими свойствами.

Утверждение 21. Пусть $\psi: M_n(\mathbb{R}) \rightarrow \mathbb{R}$ – отображение удовлетворяющее свойствам:

1. $\psi(AB) = \psi(A)\psi(B)$ для любых $A, B \in M_n(\mathbb{R})$.

2. $\psi \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & d \end{pmatrix} = d$ для любого ненулевого $d \in \mathbb{R}$.

Тогда $\psi = \det$.

Доказательство этого утверждения разобьем в несколько этапов. В начале докажем элементарные свойства мультипликативных отображений.

Утверждение 22. Пусть $\psi: M_n(\mathbb{R}) \rightarrow \mathbb{R}$ отображение со свойством $\psi(AB) = \psi(A)\psi(B)$ для всех $A, B \in M_n(\mathbb{R})$. Тогда

1. Если $P \in M_n(\mathbb{R})$ такая что $P^2 = P$, то $\psi(P)$ равно либо 0 либо 1.
2. В частности, значение $\psi(0)$ и $\psi(E)$ равно либо 0 либо 1.
3. Если $\psi(E) = 0$, то $\psi(A) = 0$ для любой матрицы $A \in M_n(\mathbb{R})$.

4. Если $\psi(0) = 1$, то $\psi(A) = 1$ для любой матрицы $A \in M_n(\mathbb{R})$.

5. Если $\psi(E) = 1$, то $\psi(A^{-1}) = \psi(A)^{-1}$ для любой обратимой матрицы $A \in M_n(\mathbb{R})$.

Доказательство. (1) Применим ψ к тождеству $P^2 = P$, получим $\psi(P) = \psi(P) = \psi(P)\psi(P)$. То есть число $\psi(P)$ в квадрате равно самому себе. Значит либо $\psi(P) = 0$, либо $\psi(P) = 1$.

(2) Заметим, что $E^2 = E$ и $0^2 = 0$ и воспользуемся предыдущим пунктом.

(3) Применим ψ к тождеству $A = AE$, получим $\psi(A) = \psi(A)\psi(E) = 0$.

(4) Применим ψ к тождеству $0 = A0$, получим $\psi(0) = \psi(A)\psi(0)$. И так как $\psi(0) = 1$ по предположению, то $\psi(A) = 1$.

(5) Применим ψ к тождеству $AA^{-1} = E$, получим $1 = \psi(E) = \psi(AA^{-1}) = \psi(A)\psi(A^{-1})$. Значит число $\psi(A^{-1})$ является обратным к числу $\psi(A)$, что и требовалось показать. \square

Утверждение 23. Пусть $\psi: M_n(\mathbb{R}) \rightarrow \mathbb{R}$ – отображение удовлетворяющее свойствам:

1. $\psi(AB) = \psi(A)\psi(B)$ для любых $A, B \in M_n(\mathbb{R})$.

2. $\psi(D_n(\lambda)) = \lambda$ для любого ненулевого $\lambda \in \mathbb{R}$.

Тогда

1. $\psi(S_{ij}(\lambda)) = 1 = \det(S_{ij}(\lambda))$.

2. $\psi(U_{ij}) = -1 = \det(U_{ij})$.

3. $\psi(D_i(\lambda)) = \lambda = \det(D_i(\lambda))$.

Доказательство. В начале заметим, что $\psi(E) = 1$. Потому что иначе $\psi(A) = 0$ для любой матрицы, что противоречит второму свойству. А раз $\psi(E) = 1$, то можно пользоваться пунктом (4) предыдущего утверждения.

(1) Для доказательства воспользуемся следующим замечанием: если $A, B \in M_n(\mathbb{R})$ – произвольные обратимые матрицы, то $\psi(ABA^{-1}B^{-1}) = 1$. Действительно,

$$\psi(ABA^{-1}B^{-1}) = \psi(A)\psi(B)\psi(A)^{-1}\psi(B)^{-1} = \psi(A)\psi(A)^{-1}\psi(B)\psi(B)^{-1} = 1$$

Для доказательства нам достаточно представить $S_{ij}(\lambda)$ в таком виде. Давайте проверим, что

$$S_{ij}(\lambda) = D_i(2)S_{ij}(\lambda)D_i^{-1}(2)S_{ij}(\lambda)^{-1}$$

Это равенство проверяется непосредственно глядя на матрицы. Давайте для простоты проверим в случае 2 на 2, когда все наглядно:

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2\lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

(3) Для доказательства этого пункта воспользуемся следующим наблюдением: если $A, B \in M_n(\mathbb{R})$ причем A обратима, тогда $\psi(ABA^{-1}) = \psi(B)$. Действительно,

$$\psi(ABA^{-1}) = \psi(A)\psi(B)\psi(A)^{-1} = \psi(B)\psi(A)\psi(A)^{-1} = \psi(B)$$

Мы уже знаем, что $\psi(D_n(\lambda)) = \lambda$ по условию. Надо лишь доказать, что для всех i выполнено $\psi(D_i(\lambda)) = \lambda$. Для этого достаточно представить $D_i(\lambda) = AD_{i+1}(\lambda)A^{-1}$. Возьмем в качестве $A = U_{i,i+1}$ элементарную матрицу переставляющую i и $i+1$ строки. Тогда $A^{-1} = A$. Более того, легко видеть, что $D_i(\lambda) = U_{i,i+1}D_{i+1}(\lambda)U_{i,i+1}^{-1}$. Действительно, умножение на $U_{i,i+1}$ слева – переставляет i и j строки, а умножение на $U_{i,i+1}$ справа равносильно умножению на $U_{i,i+1}^{-1}$ и оно переставляет i и j столбцы. Для наглядности двумерный случай:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$$

(2) Здесь мы воспользуемся тем, что элементарные преобразования второго типа можно выразить через элементарные преобразования первого и третьего типа, а именно, давайте проверим, что

$$U_{ij} = D_i(-1)S_{ji}(1)S_{ij}(-1)S_{ji}(1)$$

Применив ψ к этому равенству и воспользовавшись предыдущими двумя пунктами, мы получаем требуемое. Однако, остается законный вопрос: а как вообще можно догадаться до такого и проверить? Вот вам рассуждение приводящее к такому ответу. Давайте последовательно применять элементарные преобразования первого и третьего типа к единичной матрице, пока не получим из нее матрицу U_{ij} . Написанное равенство означает, что надо сделать так: (1) прибавить i строку к j , (2) вычесть j строку из i , (3) прибавить i строку к j , (4) умножить i строку на -1 . Давайте для наглядности это сделаем на матрицах 2 на 2. Ниже мы последовательно умножаем матрицу с левой стороны на матрицу написанную над стрелкой:

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

□

Утверждение 24. Пусть $\psi: M_n(\mathbb{R}) \rightarrow \mathbb{R}$ – отображение удовлетворяющее свойствам:

1. $\psi(AB) = \psi(A)\psi(B)$ для любых $A, B \in M_n(\mathbb{R})$.
2. $\psi(D_n(\lambda)) = \lambda$ для любого ненулевого $\lambda \in \mathbb{R}$.

И пусть $P_k \in M_n(\mathbb{R})$ – диагональная матрица, у которой k единиц на диагонали и $n - k$ нулей, причем $k < n$. Тогда $\psi(P_k) = 0$.

Доказательство. Я приведу два доказательства. Первое будет супер коротким, а второе будет годиться в более общей ситуации.³⁵

Доказательство I. Заметим, что $D_n(\lambda)P_k = P_k$ при $k < n$ и любом ненулевом $\lambda \in \mathbb{R}$. Применим к этому равенству ψ и получим

$$\lambda\psi(P_k) = \psi(D_n(\lambda))\psi(P_k) = \psi(P_k)$$

Выберем любое ненулевое число λ отличное от 1, тогда получим, что $\psi(P_k)$ обязано быть нулем.³⁶

Доказательство II. В начале покажем, что $\psi(0) = 0$. Мы уже знаем, что $\psi(0)$ либо 0 либо 1. Предположим, что $\psi(0) = 1$. Применим ψ к тождеству $0 = A0$, получим $\psi(0) = \psi(A)\psi(0)$. А следовательно $\psi(A) = 1$ для любого $A \in M_n(\mathbb{R})$, что противоречит второму свойству.

Теперь докажем, что $\psi(P_k) = 0$. Заметим, что $P_k^2 = P_k$. Значит $\psi(P_k)$ либо 0, либо 1. Давайте предположим, что $\psi(P_k) = 1$. Теперь покажем, что из равенства $\psi(P_k) = 1$ следует равенство $\psi(P_{k-1}) = 1$ для любого $k < n$. Если это так, то применив это соображение k раз, мы получим $\psi(P_0) = 1$, но $P_0 = 0$, а $\psi(0) = 0$.

Теперь мы боремся за то, чтобы из равенства $\psi(P_k) = 1$ вывести равенство $\psi(P_{k-1}) = 1$ для любого $k < n$. Рассмотрим следующие матрицы³⁷

$$P_k = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 0 & \\ & & & & & \ddots \end{pmatrix} \quad \text{и} \quad U_{k,k+1}P_kU_{k,k+1}^{-1} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & \\ & & & & 1 & \\ & & & & & \ddots \end{pmatrix}$$

Тогда ясно, что $P_{k-1} = P_kU_{k,k+1}P_kU_{k,k+1}^{-1}$. А значит, если мы применим ψ к последнему равенству, то получим

$$\psi(P_{k-1}) = \psi(P_k)\psi(U_{k,k+1})\psi(P_k)\psi(U_{k,k+1}^{-1}) = \psi(P_k)^2 = 1$$

Что и требовалось. □

³⁵Имеется в виду случай матриц над произвольным полем, если вы знаете, что это такое. Позже мы с этим познакомимся.

³⁶Для тех, кто уже знает о том, что бывают разные поля. Обратите внимание, что это доказательство не работает, если в поле нет элементов кроме 0 и 1, то есть в случае \mathbb{Z}_2 .

³⁷Здесь $U_{k,k+1}$ – матрица перестановки k и $k + 1$ строк. Именно в этом месте мы пользуемся тем, что $k < n$.

Доказательство Утверждения 21. В начале пусть $A \in M_n(\mathbb{R})$ – невырожденная матрица. Тогда мы знаем, что она является произведением элементарных матриц $A = U_1 \dots U_k$. Применим ψ к этому равенству, получим $\psi(A) = \psi(U_1) \dots \psi(U_k)$. С другой стороны по утверждению 23 получаем $\psi(A) = \det(U_1) \dots \det(U_k)$. А из мультипликативности определителя, следует, что правая часть равна $\det A$.

Теперь покажем, что ψ совпадает с \det на всех матрицах. Пусть $A \in M_n(\mathbb{R})$ – произвольная матрица. Тогда элементарными преобразованиями строк она приводится к ступенчатому виду, то есть A можно представить в виде TB , где T – обратимая, а B имеет улучшенный ступенчатый вид. После этого к B можно применить элементарные преобразования столбцов и привести к виду P_k . То есть B представляется в виде $P_k D$, где D – обратимая матрица.³⁸ То есть любая матрица A представляется в виде $A = TP_k D$, где $T, D \in M_n(\mathbb{R})$ – обратимые матрицы. Тогда, применим к этому равенству ψ , получим

$$\psi(A) = \psi(T)\psi(P_k)\psi(D) = 0$$

Последнее равенство в силу $\psi(P_k) = 0$ из утверждения 24. В свою очередь, так как A необратима, то $\det(A) = 0$ тоже. \square

4.8 Миноры и алгебраические дополнения

Определения Пусть $B \in M_n(\mathbb{R})$ – некоторая матрица с b_{ij} . Рассмотрим матрицу $D_{ij} \in M_{n-1}(\mathbb{R})$ полученную из B вычеркиванием i -ой строки и j -го столбца. Определитель матрицы D_{ij} обозначается M_{ij} и называется *минором* матрицы B или i j -минором для определенности. Число $A_{ij} = (-1)^{i+j} M_{ij}$ называется *алгебраическим дополнением* элемента b_{ij} или i j -алгебраическим дополнением матрицы B .

Покажем как это все выглядит на картинках. Если мы представим матрицу B в виде

$$B = \left(\begin{array}{ccc|ccc} & & & * & & \\ & X_{ij} & & \vdots & & Y_{ij} \\ & & & \vdots & & \\ * & \dots & & b_{ij} & \dots & * \\ & & & \vdots & & \\ Z_{ij} & & & * & & W_{ij} \end{array} \right)$$

Тогда

$$D_{ij} = \begin{pmatrix} X_{ij} & Y_{ij} \\ Z_{ij} & W_{ij} \end{pmatrix}, \quad M_{ij} = \det \begin{pmatrix} X_{ij} & Y_{ij} \\ Z_{ij} & W_{ij} \end{pmatrix} \quad \text{и} \quad A_{ij} = (-1)^{i+j} \det \begin{pmatrix} X_{ij} & Y_{ij} \\ Z_{ij} & W_{ij} \end{pmatrix}$$

Присоединенная матрица \hat{B} для B определяется как

$$\hat{B} = \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix}$$

То есть надо в матрице B каждый элемент b_{ij} заменить на его алгебраическое дополнение A_{ij} , а потом полученную матрицу транспонировать. Полезно держать перед глазами формулу для элемента присоединенной матрицы $\hat{B}_{ij} = A_{ji}$.

Формула разложения по строке

Утверждение 25. Пусть $B \in M_n(\mathbb{R})$ – произвольная матрица. Тогда³⁹

1. Для любой строки i верно разложение

$$\det B = \sum_{j=1}^n b_{ij} A_{ij}$$

³⁸Обратите внимание, что k – наш старый знакомый, а именно – количество главных переменных в системе $Ax = 0$.

³⁹Всюду в формулах A_{ij} обозначает алгебраическое дополнение.

2. Для любого столбца j верно разложение

$$\det B = \sum_{i=1}^n b_{ij} A_{ij}$$

Доказательство. Мы докажем формулу для строки, для столбца она получается аналогично либо применением транспонирования к матрице. Рассмотрим i -ю строку в матрице B

$$B = \begin{pmatrix} X_{ij} & \vdots & Y_{ij} \\ b_{i1} & \dots & b_{ij} & \dots & b_{in} \\ Z_{ij} & \vdots & W_{ij} \end{pmatrix}$$

Эту строку можно разложить в сумму следующих строк

$$(b_{i1}, \dots, b_{in}) = \sum_{j=1}^n (0, \dots, 0, b_{ij}, 0, \dots, 0)$$

Теперь вычислим определитель B пользуясь линейностью по i -ой строке

$$\det B = \sum_{j=1}^n \det \begin{pmatrix} X_{ij} & \begin{matrix} * \\ \vdots \end{matrix} & Y_{ij} \\ 0 & \dots & b_{ij} & \dots & 0 \\ Z_{ij} & \begin{matrix} \vdots \\ * \end{matrix} & W_{ij} \end{pmatrix}$$

Теперь отдельно посчитаем следующий определитель

$$\det \begin{pmatrix} X_{ij} & \begin{matrix} * \\ \vdots \end{matrix} & Y_{ij} \\ 0 & \dots & b_{ij} & \dots & 0 \\ Z_{ij} & \begin{matrix} \vdots \\ * \end{matrix} & W_{ij} \end{pmatrix} = (-1)^{j-1} \det \begin{pmatrix} \begin{matrix} * \\ \vdots \end{matrix} & X_{ij} & Y_{ij} \\ b_{ij} & \dots & 0 \\ \begin{matrix} \vdots \\ * \end{matrix} & Z_{ij} & W_{ij} \end{pmatrix} = (-1)^{j-1} (-1)^{i-1} \det \begin{pmatrix} b_{ij} & \dots & 0 \\ \vdots & X_{ij} & Y_{ij} \\ * & Z_{ij} & W_{ij} \end{pmatrix}$$

В первом равенстве мы переставили j -ый столбец $j-1$ раз, чтобы переместить его на место первого столбца. Во втором равенстве мы переставили i -ю строку $i-1$ раз, чтобы переставить ее на место первой строки. Последняя матрица является блочно нижнетреугольной, а следовательно, равенство можно продолжить так

$$(-1)^{i+j} b_{ij} \det \begin{pmatrix} X_{ij} & Y_{ij} \\ Z_{ij} & W_{ij} \end{pmatrix} = b_{ij} (-1)^{i+j} M_{ij} = b_{ij} A_{ij}$$

□

Явные формулы для обратной матрицы

Утверждение 26. Для любой матрицы $B \in M_n(\mathbb{R})$ верно

$$\hat{B}B = B\hat{B} = \det(B)E$$

Доказательство. Нам надо отдельно доказать два равенства $\hat{B}B = \det(B)E$ и $B\hat{B} = \det(B)E$. Давайте докажем второе равенство, а первое показывается аналогично (или через трюк с транспонированием).

Для доказательства $B\hat{B} = \det(B)E$ нам надо показать две вещи: (1) все диагональные элементы матрицы $B\hat{B}$ равны $\det(B)$, (2) все внедиагональные элементы равны нулю.

(1) Рассмотрим i диагональный элемент в матрице $B\hat{B}$:

$$(B\hat{B})_{ii} = \sum_{j=1}^n b_{ij} \hat{B}_{ji} = \sum_{j=1}^n b_{ij} A_{ij} = \det(B)$$

Последняя формула является разложением определителя $\det(B)$ по i -ой строке из утверждения 25.

(2) Рассмотрим элемент на позиции $i j$ для $i \neq j$:

$$(B\hat{B})_{ij} = \sum_{k=1}^n b_{ik} \hat{B}_{kj} = \sum_{k=1}^n b_{ik} A_{jk}$$

Нам надо показать, что последнее выражение равно нулю. Давайте рассмотрим матрицу B и заменим в ней j -ю строку на i -ю, все остальные оставим нетронутыми. Обозначим полученную матрицу через B' . Тогда

$$B' = \begin{pmatrix} * & \dots & * & \dots & * \\ \boxed{b_{i1} \quad \dots \quad b_{ik} \quad \dots \quad b_{in}} \\ * & \dots & * & \dots & * \\ \boxed{b_{i1} \quad \dots \quad b_{ik} \quad \dots \quad b_{in}} \\ * & \dots & * & \dots & * \end{pmatrix}$$

Давайте посчитаем определитель B' двумя способами. С одной стороны $\det(B') = 0$ так как в матрице есть две одинаковые строки. С другой стороны, давайте разложим определитель $\det(B')$ по j -ой строке

$$\det(B') = \sum_{k=1}^n b_{ik} A_{jk}$$

Что и требовалось доказать. □

В качестве непосредственного следствия этого утверждения получаем явные формулы обратной матрицы.⁴⁰

Утверждение 27 (Явные формулы обратной матрицы). Пусть $B \in M_n(\mathbb{R})$ – обратимая матрица, тогда

$$B^{-1} = \frac{1}{\det(B)} \hat{B}$$

Заметим, что в случае матрицы 2 на 2 формулы принимают следующий вид

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

4.9 Формулы Крамера

Пусть $A \in M_n(\mathbb{R})$ – произвольная матрица и $b \in \mathbb{R}^n$ – столбец. Рассмотрим систему линейных уравнений $Ax = b$. Давайте в матрице A i -ый столбец заменим на b , а остальные столбцы оставим как есть. Обозначим полученную матрицу через \bar{A}_i . Определим $\Delta = \det(A)$ и $\Delta_i = \det(\bar{A}_i)$.

Мы знаем, что данная система имеет единственное решение для любого b тогда и только тогда, когда матрица A обратима. Следующее утверждение дает явные формулы для координат решения системы в этом случае.

Утверждение 28 (Формулы Крамера). Пусть $A \in M_n(\mathbb{R})$, $x, b \in \mathbb{R}^n$ и выполнено равенство $Ax = b$. Тогда $\Delta x_i = \Delta_i$ для любого i .⁴¹

⁴⁰Заметим, что для формулы требуется условие $\det(B) \neq 0$. Однако, матрица обратима тогда и только тогда, когда $\det(B) \neq 0$. Один из способов это показать – применить \det к равенству $BB^{-1} = E$ и увидеть, что $\det(B) \det(B^{-1}) = 1$. А в обратную сторону – явные формулы.

⁴¹Здесь x_i – координаты вектора x .

Доказательство. Возьмем в матрице A заменим i -ый столбец на столбец b . Обозначим результирующую матрицу через \bar{A}_i . Рассмотрим матрицу A как строку из столбцов $A = (A_1 | \dots | A_n)$, где A_i – столбцы матрицы A . Тогда равенство $Ax = b$, пользуясь блочными формулами, можно переписать так $x_1 A_1 + \dots + x_n A_n = b$. Давайте посчитаем определитель \bar{A}_i , пользуясь последним равенством.

$$\det(\bar{A}_i) = \det(A_1 | \dots | b | \dots | A_n) = \det(A_1 | \dots | \sum_{k=1}^n x_k A_k | \dots | A_n) = \sum_{k=1}^n x_k \det(A_1 | \dots | A_k | \dots | A_n)$$

В последней формуле, если $k \neq i$, то слагаемое имеет два одинаковых столбца A_i . Потому остается только одно слагаемое для $k = i$. Получаем

$$\det(\bar{A}_i) = x_i \det(A_1 | \dots | A_i | \dots | A_n) = x_i \det(A)$$

Что и требовалось. \square

Заметим, что если $\Delta = \det(A) \neq 0$, то имеется единственное решение системы $Ax = b$ для любой правой части b и координаты этого решения заданы по формулам $x_i = \frac{\Delta_i}{\Delta}$. Однако, если $\Delta = \det(A) = 0$, то либо решений бесконечное число, либо их вообще нет. В этом случае единственная информация из формул Крамера это: $\Delta_i = 0$.

4.10 Характеристический многочлен

Пусть $A \in M_n(\mathbb{R})$ – произвольная квадратная матрица и $\lambda \in \mathbb{R}$. Рассмотрим функцию $\chi_A(\lambda) = \det(\lambda E - A)$.

Утверждение 29. Пусть $A \in M_n(\mathbb{R})$. Тогда верно

1. Функция $\chi_A(\lambda)$ является многочленом степени n со старшим коэффициентом 1.
2. Для произвольного числа λ верно, что $\lambda \in \text{spec}_{\mathbb{R}} A$ тогда и только тогда, когда $\chi_A(\lambda) = 0$.⁴²

Доказательство. (1) Давайте посмотрим на явную формулу определителя

$$\det B = \sum_{\sigma \in S_n} \text{sgn}(\sigma) b_{1\sigma(1)} \dots b_{n\sigma(n)}$$

Заметим, что данное выражение является многочленом от коэффициентов матрицы A , причем все его слагаемые имеют степень n . Теперь, когда мы считаем характеристический многочлен, мы находим $\det(\lambda E - A)$. То есть вместо b_{ii} мы должны подставить $\lambda - a_{ii}$, а вместо b_{ij} взять $-a_{ij}$ (при $i \neq j$). То есть мы в многочлен от многих переменных подставляем либо числа, либо линейный многочлен от λ . Понятно, что результат будет многочлен от λ причем степени уж точно не больше n . Теперь давайте поймем какая будет у него степень и старший коэффициент.

$$\lambda E - A = \begin{pmatrix} \lambda - a_{11} & \dots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_{n1} & \dots & \lambda - a_{nn} \end{pmatrix}$$

Ясно, что максимальная степень по λ может вылезти только из слагаемого являющегося произведением диагональных элементов – $(\lambda - a_{11}) \dots (\lambda - a_{nn})$. А его старший член λ^n . Вот и все.

(2) Вспомним, что $\lambda \in \text{spec}_{\mathbb{R}} A$ тогда и только тогда, когда $A - \lambda E$ – необратимая матрица или что то же самое, $\lambda E - A$ – необратимая матрица. Матрица необратима тогда и только тогда, когда ее определитель ноль. Потому $\lambda \in \text{spec}_{\mathbb{R}} A$ тогда и только тогда, когда $\det(\lambda E - A) = 0$, то есть $\chi_A(\lambda) = 0$. Что и требовалось. \square

Определение 30. Для произвольной матрицы $A \in M_n(\mathbb{R})$ многочлен $\chi_A(\lambda)$ называется *характеристическим многочленом* матрицы A .

⁴² Аналогичное утверждение верно и для $\text{spec}_{\mathbb{C}} A$.

Явные формулы для коэффициентов характеристического многочлена Вначале давайте введем некоторые обозначения. Пусть $A \in M_n(\mathbb{R})$ – некоторая матрица. Рассмотрим произвольное k элементное подмножество в множестве чисел от 1 до n заданное в виде i_1, \dots, i_k ⁴³ Вычеркнем из матрицы A столбцы и строки с этими номерами и обозначим полученную матрицу через R_{i_1, \dots, i_k} . Графически эта процедура выглядит так:

$$\begin{array}{c} i_1 \\ \vdots \\ i_k \end{array} \begin{pmatrix} & \begin{array}{c} i_1 \\ \vdots \\ a_{i_1 1} \end{array} & \dots & \begin{array}{c} i_k \\ \vdots \\ a_{i_k 1} \end{array} & \\ \begin{array}{c} R_{11} \\ \vdots \\ a_{i_1 1} \end{array} & \begin{array}{c} a_{1i_1} \\ \vdots \\ a_{i_1 i_1} \end{array} & \dots & \begin{array}{c} a_{1i_k} \\ \vdots \\ a_{i_1 i_k} \end{array} & \begin{array}{c} R_{1k+1} \\ \vdots \\ a_{i_1 k+1} \end{array} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \begin{array}{c} a_{i_k 1} \\ \vdots \\ R_{k+1 1} \end{array} & \begin{array}{c} a_{i_k i_1} \\ \vdots \\ a_{n i_1} \end{array} & \dots & \begin{array}{c} a_{i_k i_k} \\ \vdots \\ a_{n i_k} \end{array} & \begin{array}{c} R_{k+1 k+1} \\ \vdots \\ R_{k+1 n} \end{array} \end{pmatrix} \mapsto R_{i_1, \dots, i_k} = \begin{pmatrix} R_{11} & \dots & R_{1k+1} \\ \vdots & \ddots & \vdots \\ R_{k+1 1} & \dots & R_{k+1 k+1} \end{pmatrix} \in M_{n-k}(\mathbb{R})$$

Пользуясь этими обозначениями покажем следующее.

Утверждение 31. Пусть $A \in M_n(\mathbb{R})$ и его характеристический многочлен имеет вид

$$\chi_A(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \dots + a_1\lambda + a_0$$

Тогда

1. В обозначениях выше, для коэффициентов a_k верна следующая формула⁴⁴

$$a_k = (-1)^{n-k} \left(\sum_{i_1 < \dots < i_k} \det R_{i_1, \dots, i_k} \right)$$

2. $a_0 = (-1)^n \det A$.

3. $a_{n-1} = -\text{tr } A$.

Доказательство. (1) Введем обозначения для столбцов матрицы $A = (A_1 | \dots | A_n)$ и пусть $e_i \in \mathbb{R}^n$ – столбец, у которого i -я координата равна 1, а все остальные 0. Нам надо посчитать $\det(\lambda E - A) = (-1)^n \det(A - \lambda E)$. Тогда,

$$\det(A - \lambda E) = \det(A_1 - \lambda e_1 | \dots | A_n - \lambda e_n)$$

Теперь надо раскрыть последний определитель по полилинейности.⁴⁵ Всего у нас будет 2^n слагаемых, каждое из которых – это определитель матрицы состоящей из столбцов A_i или $-\lambda e_j$, стоящих вперемешку.

Давайте для определенности считать, что у нас $n = 5$, тогда мы считаем

$$\det(A_1 - \lambda e_1 | A_2 - \lambda e_2 | A_3 - \lambda e_3 | A_4 - \lambda e_4 | A_5 - \lambda A_5)$$

Среди слагаемых давайте посмотрим на слагаемое, содержащее 2 столбца матрицы A и 3 столбца вида $-\lambda e_i$, например, такое

$$\det(A_1 | -\lambda e_2 | A_3 | -\lambda e_4 | -\lambda e_5) = \det \begin{pmatrix} a_{11} & 0 & a_{13} & 0 & 0 \\ a_{21} & -\lambda & a_{23} & 0 & 0 \\ a_{31} & 0 & a_{33} & 0 & 0 \\ a_{41} & 0 & a_{43} & -\lambda & 0 \\ a_{51} & 0 & a_{53} & 0 & -\lambda \end{pmatrix}$$

⁴³Здесь предполагается, что $i_1 < \dots < i_k$.

⁴⁴Заметим, что эта формула также имеет смысл при $k = 0$ и при $k = n$. Если $k = 0$, то множество индексов пусто \emptyset и $R_\emptyset = A$, потому формула превращается в равенство $a_0 = (-1)^n \det A$. При условии $k = n$, мы вычеркиваем все строки из матрицы и в этом случае $R_{i_1, \dots, i_n} \in M_0(\mathbb{R})$. Такого объекта не существует, но мы можем для удобства считать, что в этом случае формула означает $\det R_{i_1, \dots, i_n} = 1$.

⁴⁵Думать про это выражение надо так: надо мысленно заменить вертикальные черточки умножением и считать, что мы раскрываем скобки в произведении.

Давайте последовательно разлагать этот определитель по 2-ому, 4-ому и 5-ому столбцам. Обратим внимание, что $-\lambda$ всегда будут стоять на диагонали, потому что знаки всех алгебраических дополнений будут положительными:

$$\det \begin{pmatrix} a_{11} & 0 & a_{13} & 0 & 0 \\ a_{21} & -\lambda & a_{23} & 0 & 0 \\ a_{31} & 0 & a_{33} & 0 & 0 \\ a_{41} & 0 & a_{43} & -\lambda & 0 \\ a_{51} & 0 & a_{53} & 0 & -\lambda \end{pmatrix} = (-\lambda) \det \begin{pmatrix} a_{11} & a_{13} & 0 & 0 \\ a_{31} & a_{33} & 0 & 0 \\ a_{41} & a_{43} & -\lambda & 0 \\ a_{51} & a_{53} & 0 & -\lambda \end{pmatrix} = (-\lambda)^2 \det \begin{pmatrix} a_{11} & a_{13} & 0 \\ a_{31} & a_{33} & 0 \\ a_{51} & a_{53} & -\lambda \end{pmatrix} = (-\lambda)^3 \det \begin{pmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{pmatrix}$$

В общем случае слагаемое с k столбцами вида $-\lambda e_i$ является определителем матрицы вида

$$\begin{matrix} & & i_1 & \dots & i_k & & \\ & & \boxed{0} & \dots & \boxed{0} & & \\ & R_{11} & \vdots & \dots & \vdots & R_{1\ k+1} & \\ i_1 & \boxed{a_{i_1 1} \dots -\lambda} & & & & \dots & a_{i_1 n} \\ \vdots & \vdots & & \ddots & & \vdots & \\ i_k & \boxed{a_{i_k 1} \dots} & & & \boxed{-\lambda} & \dots & a_{i_k n} \\ & R_{k+1\ 1} & \vdots & \dots & \vdots & R_{k+1\ k+1} & \\ & & \boxed{0} & & \boxed{0} & & \end{matrix} = I_{i_1, \dots, i_k}$$

Раскладывая этот определитель по столбцам i_1, \dots, i_k мы получаем

$$\det I_{i_1, \dots, i_k} = (-\lambda)^k \det R_{i_1, \dots, i_k}$$

Слагаемые при λ^k вылезут, когда ровно k столбцов имеют вид $-\lambda e_i$. Остается не забыть, что мы считали $(-1)^n \chi_A(\lambda)$.

(2) Свободный член многочлена $\chi_A(\lambda)$ всегда равен $\chi_A(0) = \det(0E - A) = \det(-A) = (-1)^n \det(A)$, что и требовалось.

(3) Для подсчета a_{n-1} воспользуемся формулой, получим⁴⁶

$$a_{n-1} = (-1)^{n-(n-1)} \sum_{i=1}^n \det R_{1, \dots, \hat{i}, \dots, n}$$

Но заметим, что $R_{1, \dots, \hat{i}, \dots, n} = a_{ii}$, а значит предыдущее равенство превращается в

$$a_{n-1} = (-1)^{n-(n-1)} \sum_{i=1}^n a_{ii} = -\operatorname{tr} A$$

□

Примеры

1. Если $A \in M_1(\mathbb{R})$, то есть $A = a \in \mathbb{R}$ – число, то $\chi_A(\lambda) = \lambda - a$.
2. Если $A \in M_2(\mathbb{R})$, то $\chi_A(\lambda) = \lambda^2 - \operatorname{tr} A \lambda + \det A$.
3. Если $A \in M_3(\mathbb{R})$, то $\chi_A(\lambda) = \lambda^3 - \operatorname{tr} A \lambda^2 + a_1 \lambda - \det A$, где

$$a_1 = \det \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} + \det \begin{pmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{pmatrix} + \det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Стоит отметить, что считать характеристические многочлены от матриц большего размера через эти формулы практически не целесообразно. Максимальный разумный размер – матрица 4 на 4. Самый быстрый способ остается алгоритм Гаусса для подсчета определителя $\det(\lambda E - A)$ с символьными коэффициентами.

⁴⁶Здесь \hat{i} означает, что индекс i пропущен.

4.11 Теорема Гамильтона-Кэли

Многочлены с матричными коэффициентами Обозначим через $M_n(\mathbb{R})[t]$ множество многочленов от переменной t имеющих матричные коэффициенты из $M_n(\mathbb{R})$, т.е.

$$M_n(\mathbb{R})[t] = \{A_0 + A_1t + \dots + A_k t^k \mid A_i \in M_n(\mathbb{R})\}$$

здесь t – формальная переменная, которая представляет собой неизвестное число. Про эти многочлены надо думать как про картинки. Такие картинки можно складывать и умножать по формулам известным для многочленов с обычными числовыми коэффициентами:

- Сумма.

$$\left(\sum_i A_i t^i\right) + \left(\sum_j B_j t^j\right) = \sum_i (A_i + B_i) t^i$$

- Произведение.

$$\left(\sum_i A_i t^i\right) \left(\sum_j B_j t^j\right) = \sum_k \left(\sum_{s+t=k} A_s B_t\right) t^k$$

Надо лишь отметить, что в произведении нельзя переставлять местами A_s и B_t , так как матрицы вообще говоря не перестановочны.

Подстановка матрицы в многочлен Теперь для произвольного многочлена $f \in M_n(\mathbb{R})[t]$ и матрицы $D \in M_n(\mathbb{R})$ определим подстановку матрицы D в многочлен f справа:

$$f(D) = A_0 + A_1 D + \dots + A_k D^k$$

т.е. мы вместо t подставляем всюду матрицу D . Аналогично, можно определить левую подстановку:

$$(D)f = A_0 + D A_1 + \dots + D^k A_k$$

Надо отметить, что вообще говоря $f(D) \neq (D)f$. Мы всегда будем пользоваться только правой подстановкой.

Свойства подстановки Пусть $f, g \in M_n(\mathbb{R})[t]$ – два многочлена и $D \in M_n(\mathbb{R})$ – некоторая матрица. Сделаем следующие замечания:

1. Всегда верно равенство

$$f(D) + g(D) = (f + g)(D)$$

2. Для произведения вообще говоря выполнено

$$f(D)g(D) \neq (fg)(D)$$

Действительно, возьмем $f(t) = t$, $g(t) = Bt$, тогда $(fg)(t) = Bt^2$. В этом случае $f(D)g(D) = DBD$, а $(fg)(D) = BDD$. Вообще говоря, имеем $DBD \neq BDD$ если матрицы B и D не коммутируют.

3. Если D коммутирует со всеми коэффициентами матрицы g , то верно равенство

$$f(D)g(D) = (fg)(D)$$

Это видно непосредственно из определения умножения и подстановки.

Теорема Теперь мы готовы к формулировке и доказательству полезного результата.

Утверждение 32 (Теорема Гамильтона-Кэли). Пусть $A \in M_n(\mathbb{R})$. Тогда $\chi_A(A) = 0$.

Прежде чем доказывать теорему, давайте объясним в чем сложность и почему дурацкие доказательства не работают. Смотрите, у нас $\chi_A(\lambda) = \det(\lambda E - A)$. Хочется подставить вместо λ матрицу A и сказать, что определитель нулевой матрицы равен 0. В этом рассуждении есть лажа. Давайте продемонстрируем ее на матрице 2 на 2. Пусть

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Тогда

$$\det(A - \lambda E) = \det\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} - \lambda E\right) = \det\begin{pmatrix} a_{11} - \lambda & a_{12} \\ a_{21} & a_{22} - \lambda \end{pmatrix}$$

Так вот, последнее равенство верно если λ является числом. Если же λ является матрицей, то оно непонятно, что значит. Можно понимать правую часть как блочную матрицу 2 на 2 из блоков 2 на 2 (т.е. всего 4 на 4), но тогда это просто не верное равенство. Это рассуждение можно докрутить до верного, но тогда в правой части надо использовать вместо определителя более хитрую его версию. Подобное рассуждение растет из коммутативной алгебры, где доказательство естественным образом сводится к формулам Крамера, но для его освоения надо знать, что такое кольца и модули. Мы же пойдем чуть более простым путем.

Доказательство. Рассмотрим матрицу $\lambda E - A$, где λ – неизвестное число. Введем следующее обозначение $R(\lambda) = \widehat{\lambda E - A}$.

Заметим, что каждый коэффициент $R(\lambda)$ является многочленом от λ , т.е. $R(\lambda) = (r_{ij}(\lambda))$ и $r_{ij}(\lambda)$ – многочлен. То есть $r_{ij}(\lambda) = \sum_k r_{ijk} \lambda^k$. Тогда $R(\lambda) = \sum_k R_k \lambda^k$, где $R_k = (r_{ijk})$. То есть $R(\lambda) \in M_n(\mathbb{R})[\lambda]$. Для ясности, давайте проиллюстрируем сказанное на следующем примере.

$$\begin{pmatrix} 5 - \lambda + 2\lambda^2 & 3 \\ 4 - \lambda & 2 + \lambda \end{pmatrix} = \begin{pmatrix} 5 & 3 \\ 4 & 2 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \lambda + \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \lambda^2$$

Теперь применим формулы для перемножения матрицы с ее присоединенной из утверждения 26 для матрицы $\lambda E - A$, получим

$$(\lambda E - A)R(\lambda) = R(\lambda)(\lambda E - A) = \det(\lambda E - A)E = \chi_A(\lambda)E$$

Нас интересует только равенство

$$R(\lambda)(\lambda E - A) = \chi_A(\lambda)E$$

Тогда рассмотрим многочлены $f(\lambda) = R(\lambda)$, $g(\lambda) = \lambda E - A$. В этом случае $(fg)(\lambda) = \chi_A(\lambda)E$. Возьмем в качестве матрицы D матрицу A . Заметим, что она коммутирует с коэффициентами g , потому что это E и $-A$. Значит верно равенство $f(D)g(D) = (fg)(D)$. Последнее означает

$$0 = R(A)(AE - A) = \chi_A(A)E = \chi_A(A)$$

Что и требовалось доказать. □

5 Комплексные числа

5.1 Идея

Почему нам вдруг не хватает вещественных чисел? Давайте вспомним, а откуда получились вещественные числа? Для начала у нас есть натуральные числа: $\mathbb{N} = \{1, 2, 3, \dots\}$. Которые мы беззаботно складывали и умножали. Но как только нам захотелось посчитать $5 - 8$, как нам понадобились другие числа – целые $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. И мы опять жили долго и счастливо, пока на не пришлось делить $2/3$ и тут пришлось построить рациональные числа $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\}$. Вещественные нам пригодились, когда надо было решить уравнение $x^2 = 2$. Тогда пришлось добавить $\sqrt{2}$, а заодно и кучу других полезных чисел. Однако, этого опять оказалось мало и уравнение $x^2 + 1 = 0$ не решается в вещественных числах. При этом давайте заметим, что добавляя новые числа, операции над старыми мы не меняли. Мы добавили целые, рациональные, вещественные, а натуральные как складывались и умножались по старым правилам, так и продолжают складываться и умножаться.

А какие-же числа мы хотим получить в идеале. Прежде всего хочется решать уравнения вида $f(x) = 0$, где $f \in \mathbb{R}[x]$, всегда, когда это возможно. Например, если $f = 1$, то решить такое уравнение по понятным причинам не возможно, но вот если $\deg f > 0$, то очень хочется иметь решение. Новые числа должны содержать все вещественные как подмножество. Но кроме этого, мы хотим уметь делать все арифметические операции с новыми числами, да еще так, чтобы старые операции не изменились. И еще хочется по возможности быть экономными. Вдруг, можно построить много разных лишних чисел (например, когда нам понадобились рациональные числа, мы могли по наивности и безрассудству сразу же построить вещественные, но обошлись более экономным вариантом в виде рациональных чисел).

Для того, чтобы формализовать идеи выше, нам надо строго сказать, а какой математической структурой должны являться новые числа. Такими структурами являются поля. Потом надо объяснить как правильно обращаться с полями, что с ними можно делать, как их сравнивать между собой. И как только у нас появился зверинец полей, мы можем найти в нем поле комплексных чисел, как самое лучшее, которое только возможно среди тех, что удовлетворяют нашим запросам.

Сейчас нас ждет очередное абстрактное определение. Напомню, что оно всегда состоит из двух частей: в первой части сказано какие у нас данные, а во второй – каким аксиомам эти данные подчиняются.

Определение 33 (Поле). Поле это следующий набор данных: $(F, +, \cdot)$, где

- F – некоторое множество. Элементы этого множества называются числами.
- $+$: $F \times F \rightarrow F$, $(x, y) \mapsto x + y$ – некоторая операция называемая сложением.
- \cdot : $F \times F \rightarrow F$, $(x, y) \mapsto xy$ – некоторая операция называемая умножением.

Эти данные должны подчиняться следующим десяти аксиомам:

1. **Ассоциативность сложения** Для любых элементов $x, y, z \in F$ выполнено $x + (y + z) = (x + y) + z$.
2. **Существования нейтрального по сложению** Существует такой элемент $0 \in F$ такой, что для любого $x \in F$ верно $x + 0 = 0 + x = x$. Такой элемент называется нулем.
3. **Существование обратного по сложению** Для любого $x \in F$ существует элемент $-x \in F$ такой, что $x + (-x) = (-x) + x = 0$. Такой элемент называется противоположным.
4. **Коммутативность сложения** Для любых элементов $x, y \in F$ верно $x + y = y + x$.
5. **Ассоциативность умножения** Для любых элементов $x, y, z \in F$ верно $x(yz) = (xy)z$.
6. **Существование нейтрального по умножению** Существует такой элемент $1 \in F$, что для любого $x \in F$, верно $x1 = 1x = x$. Такой элемент называется единицей.
7. **Существование обратного по умножению** Для любого элемента $x \in F \setminus \{0\}$ существует элемент $x^{-1} \in F$ такой, что $xx^{-1} = x^{-1}x = 1$. Такой элемент называется обратным к x .
8. **Коммутативность умножения** Для любых элементов $x, y \in F$ верно $xy = yx$.
9. **Дистрибутивность** Для любых элементов $x, y, z \in F$ верно $x(y + z) = xy + xz$ и $(x + y)z = xz + yz$.
10. **Нетривиальность** $0 \neq 1$.

Замечания Давайте сделаем несколько полезных замечаний.

1. Аксиомы сгруппированы следующим образом: (1–4) аксиомы на сложение, (5–8) аксиомы на умножение, (9) связь между сложением и умножением, (10) нетривиальность. Причем аксиомы (1–4) и (5–8) идут по одному и тому же шаблону: ассоциативность, нейтральный элемент, обратный, коммутативность. НО стоит отметить важную разницу между аксиомами (3) и (7). По сложению обратный должен быть для любого элемента, по умножению только для ненулевого. В частности, аксиому (7) нельзя сформулировать без аксиомы (2).
2. В аксиомах (2) и (6) не требуется единственность нуля и единицы. Однако, можно показать, что если ноль существует, то он обязательно единственный, аналогично с единицей. Действительно, если у нас есть два нуля 0_1 и 0_2 , то рассмотрим их сумму $0_1 + 0_2$. Так как 0_1 является нулем, то $0_1 + 0_2 = 0_2$. Так как 0_2 является нулем, то $0_1 + 0_2 = 0_1$. Значит оба нуля совпадают. Аналогично проверяется единственность единицы. Потому в силу однозначности эти элементы обозначаются 0 и 1.
3. В аксиомах (3) и (7) не требуется единственность обратного. Однако, можно показать, что для любого x существует единственный $-x$ и единственный x^{-1} . Действительно, если для элемента $x \in F$ есть два элемента $y, z \in F$ таких, что

$$x + y = y + x = 0 \quad \text{и} \quad x + z = z + x = 0$$

Тогда рассмотрим выражение

$$(y + x) + z = y + (x + z)$$

Его левая часть вычисляется в $0 + z = z$, а правая вычисляется в $y + 0 = y$. А значит y и z совпадают. То есть обратный по сложению будет один, аналогично с обратным по умножению. Именно по причине однозначности им даются такие имена. В частности однозначно определено число -1 .

4. Мы привыкли к всяким замечательным свойствам, которым подчиняются числа 0 и 1. Например: $x0 = 0$ или $(-1)x = -x$ для любого x . Оказывается, что их можно доказать пользуясь аксиомами. Попробуйте сделать это.
5. Давайте рассмотрим множество $F = \{\cdot\}$ состоящее из одной точки. Тогда на таком множестве существует единственная операция, положим сложение и умножение равными ей. Тогда данный набор данных удовлетворяет всем аксиомам поля кроме последней. Здесь ноль равен единице и вообще все элементы равны друг другу и ничего кроме нуля (единицы) у нас нет. На самом деле, если ноль равен единице, то никаких других структур мы не построим. Действительно, предположим $(F, +, \cdot)$ удовлетворяет всем аксиомам с первой по девятую, а вместо десятой – ее отрицание $1 = 0$. Тогда для любого элемента $a \in F$ имеем $a = a \cdot 1 = a \cdot 0$. Давайте покажем, что $a \cdot 0 = 0$ для любого $a \in F$. Рассмотрим равенство $0 + 0 = 0$, которое следует из определения нуля. Умножим его на a , получим $a \cdot (0 + 0) = a \cdot 0$. Раскроем скобки и получим $a \cdot 0 + a \cdot 0 = a \cdot 0$. Теперь прибавим к обеим частям равенства элемент $-(a \cdot 0)$. Получим

$$a \cdot 0 + a \cdot 0 + -(a \cdot 0) = a \cdot 0 + -(a \cdot 0)$$

Что равносильно $a \cdot 0 + 0 = 0$, а значит $a \cdot 0 = 0$, что и требовалось. Потому последняя аксиома нужна для того, чтобы исключить именно этот дурацкий пример.

Примеры Как только вам скормили абстрактное определение, первым делом нужны примеры. Он помогут по-новому взглянуть на старых знакомых и разобраться с тем, а как вообще задавать эти самые новые объекты.

1. Рациональные и вещественные числа \mathbb{Q} и \mathbb{R} с обычными операциями.
2. Множество $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ с обычными операциями является примером поля, которое лежит между \mathbb{Q} и \mathbb{R} .
3. Рациональные функции $\mathbb{R}(x) = \{\frac{f}{g} \mid f, g \in \mathbb{R}[x]\}$. Давайте думать про рациональные функции как про картинки. Тогда на них определены формальные операции сложения и умножения. Относительно этих операций они являются полем.

4. Теперь время экзотики $\mathbb{F}_2 = \{0, 1\}$, а операции берутся по модулю 2. Можно проверить, что и этот товарищ является полем. Это очень важное поле для computer science. Оно и его аналоги используются в теории кодирования, восстановления сигнала, архивирования и т.д.

Определение 34 (Подполе). Пусть K и L – два поля причем $K \subseteq L$. Тогда K называется подполем в L , если операции сложения и умножения из L ограниченные на K дают сложение и умножение на K соответственно. Более подробно, пусть $+_L$ и \cdot_L – сложение и умножение на L , а $+_K$ и \cdot_K – сложение и умножение на K . Тогда для любых элементов $x, y \in K$ верно: $x +_L y = x +_K y$ и $x \cdot_L y = x \cdot_K y$.

По простому подполе – это подмножество чисел в нашем поле, которое само является полем относительно операций из большего поля. То есть нет никакой разницы какие операции использовать в подполе K : операции из K или операции из L , так как между ними нет разницы.

5.2 Абстрактное определение комплексных чисел

Определение 35. Пусть поле \mathbb{C} обладает следующими свойствами:

1. $\mathbb{R} \subseteq \mathbb{C}$ – подполе, т.е. поле \mathbb{C} содержит вещественные числа и операции сложения и умножения ограничиваются на \mathbb{R} в обычные операции сложения и умножения.⁴⁷
2. Для любого не константного многочлена $f \in \mathbb{C}[x]$ существует корень $\alpha \in \mathbb{C}$, т.е. $f(\alpha) = 0$.
3. Поле \mathbb{C} является минимальным полем, удовлетворяющим предыдущим свойствам, т.е. для любого поля F такого что $\mathbb{R} \subseteq F \subseteq \mathbb{C}$ если F обладает двумя предыдущими свойствами, то $F = \mathbb{C}$.

Тогда оно называется полем комплексных чисел.

Стоит сделать важное замечание. Из определения вообще говоря не следует, что подобное поле существует, но даже если оно и существует, то не понятно, вообще говоря, единственно ли оно. Как можно ожидать, такое поле обязательно существует и оказывается, что оно единственно в некотором естественном смысле. Потому идейно к определению выше надо относиться так: это набросок тех свойств, которые мы хотели бы получить от нашего поля, а дальше вся работа заключается в том, чтобы показать, во-первых, что таких свойств добиться можно и построить необходимое поле, а во-вторых, что как бы мы ни построили поле комплексных чисел, всегда получится одно и то же.

Как вы понимаете построить поле удовлетворяющее свойству (2) – не простая задача. Потому обычно поступают по-другому. Мы построим поле с более слабым свойством, что существует решение только у уравнения $x^2 + 1 = 0$. А уже потом покажем, что подобное поле удовлетворяет более сильному условию (2) из определения. Единственность мы с вами доказывать не будем в силу того, что эта тема будет затронута в курсе алгебры в общем виде.

5.3 Две модели комплексных чисел

В этом разделе я построю две модели комплексных чисел. Для того чтобы различать эти модели, я для начала буду обозначать их \mathbb{C}_1 и \mathbb{C}_2 . Но как только мы поймем, что это одно и то же, мы будем опускать индекс и обозначать построенное поле через \mathbb{C} .

Символьная модель Пусть \mathbb{C}_1 – это множество картинок вида $a + bi$, где $a, b \in \mathbb{R}$ – вещественные числа, а i и $+$ – картинки. Множество мы определили, теперь надо определить операции сложения и умножения. Сумму картинок определим покомпонентно:

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \quad \text{где } a, b, c, d \in \mathbb{R}$$

Умножение определим исходя из соображений $i^2 = -1$. Тогда

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i, \quad \text{где } a, b, c, d \in \mathbb{R}$$

На этом этапе необходимые данные для определения поля нами построены. Осталось дело за малым – проверить все 10 аксиом. Эту интереснейшую задачу я оставлю в качестве упражнения, но обязательно проверьте эти аксиомы.

⁴⁷В терминологии ниже вложение $\mathbb{R} \rightarrow \mathbb{C}$ является гомоморфизмом полей.

Теперь \mathbb{C}_1 является полем. Вещественные числа в него вкладываются так: число $r \in \mathbb{R}$ идет в картинку $r + 0i \in \mathbb{C}_1$. Теперь надо проверить что сложить два вещественных числа – это все равно, что сложить их как два комплексных числа. Аналогично, умножить два вещественных числа – это все равно, что умножить их как два комплексных числа. Напоследок заметим, что число комплексное число i выбрано так, чтобы оно являлось решением уравнения $x^2 + 1 = 0$.

Матричная модель Пусть \mathbb{C}_2 – это множество матриц вида $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in M_2(\mathbb{R})$. Множество построено, теперь дело за операциями. Придумывать их не надо, это будут обычные матричные сложение и умножение, единственное, что надо проверить, что сумма и произведение матриц из \mathbb{C}_2 остаются в \mathbb{C}_2 .⁴⁸

Как и с первой моделью, мы только что построили все необходимые данные для определения поля, теперь надо проверить аксиомы. И тут нам очень пригождаются матрицы. Почти все аксиомы будут автоматически следовать из соответствующих свойств матричных операций. Единственное, что надо проверить: коммутативность умножения и что любой ненулевой элемент обратим. Я сейчас опять поступлю не очень честно и попрошу жаждущего до знаний читателя все проверить самостоятельно.⁴⁹

Вещественные числа вкладываются в \mathbb{C}_2 в виде скалярных матриц, то есть $r \in \mathbb{R}$ идет в $rE \in \mathbb{C}_2$. Как мы знаем при этом операции матричного сложения и умножения превращаются в операции сложения и умножения вещественных чисел. Осталось найти решение уравнения $x^2 + 1 = 0$. Для этого заметим, что матрица $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ удовлетворяет этому уравнению.

Сравнение полей Для того чтобы сравнить различные поля и сказать, что они одинаковые или различные нам потребуется понятие изоморфизма полей.

Определение 36. Пусть F_1 и F_2 поля. Отображение $\varphi: F_1 \rightarrow F_2$ называется гомоморфизмом полей, если

1. $\varphi(x + y) = \varphi(x) + \varphi(y)$ для любых $x, y \in F_1$.
2. $\varphi(xy) = \varphi(x)\varphi(y)$ для любых $x, y \in F_1$.
3. $\varphi(1) = 1$.

Если φ является биекцией, то оно называется изоморфизмом.

Стоит отметить, что гомоморфизм полей всегда инъективен. Попробуйте доказать это. Кроме того, если отображение φ инъективно, то достаточно лишь проверить первые два свойства гомоморфизма, т.е. единица автоматически перейдет в единицу.⁵⁰

Мы будем говорить что два поля изоморфны, если между ними существует изоморфизм. Про изоморфные поля надо думать, как про одинаковые поля. Действительно, что значит, что между множествами есть биекция. Это значит, что это на самом деле одно и то же множество, а биекция лишь переопределяет имена, которыми называются наши элементы. Изоморфизм кроме всего прочего сохраняет операции, это значит, что отождествив элементы наших полей, мы не различаем проделанных операций. Так как поле для нас – это множество с операциями, то значит мы не увидим никакой разницы, между полями, если в них одинаковые операции.

Задачи 37. Пусть $\varphi: K \rightarrow L$ – гомоморфизм полей. Покажите, что выполнены следующие вещи:

1. $\varphi(0) = 0$.
2. $\varphi(-x) = -\varphi(x)$ для любого $x \in K$.
3. Если в определении гомоморфизма оставить только свойства 1 и 2, то $\varphi(1)$ либо 0, либо 1. В частности, если φ инъективно, то $\varphi(1) = 1$.
4. $\varphi(x^{-1}) = \varphi(x)^{-1}$ для любого ненулевого $x \in K$.

⁴⁸Это, пусть и легкое, упражнение мы оставляем на совести читателя.

⁴⁹На самом деле я всего лишь полу-честен с вами ибо чуть ниже будут проведены все соответствующие проверки.

⁵⁰Догадливый читатель уже сообразил, что в этом месте будет фраза: «Проверьте это».

Сравнение моделей комплексных чисел Прежде чем объяснить, что \mathbb{C}_1 и \mathbb{C}_2 – это одно и то же. Нам понадобится еще одно определение. Дело в том, что в наших полях лежат дополнительно вещественные числа и мы, когда будем сравнивать эти два поля, хотим чтобы это сравнение было согласовано в каком-то смысле с вещественными числами.

Определение 38. Пусть F_1 и F_2 – два поля, содержащие поле вещественных чисел \mathbb{R} , то есть $\mathbb{R} \subseteq F_1$ и $\mathbb{R} \subseteq F_2$ и операции с F_i ограничиваются на соответствующие операции на вещественных числах. Будем говорить, что $\varphi: F_1 \rightarrow F_2$ является изоморфизмом над \mathbb{R} , если

1. φ является изоморфизмом.
2. $\varphi(r) = r$ для любого вещественного числа $r \in \mathbb{R}$.

Давайте построим изоморфизм над \mathbb{R} между \mathbb{C}_1 и \mathbb{C}_2 . А именно: $\varphi: \mathbb{C}_1 \rightarrow \mathbb{C}_2$ будет действовать по правилу $a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. По построению очевидно, что данное отображение является биекцией. Кроме того, очевидно, что оно переводит сумму в сумму. Методом пристального взгляда проверяем, что φ сохраняет умножение. Вещественное число $r = r + 0i$ переходит в матрицу $\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} = rE$. С учетом нашего отождествления вещественных чисел с подмножествами в \mathbb{C}_1 и \mathbb{C}_2 последнее означает, что $\varphi(r) = r$ для любого $r \in \mathbb{R}$. То есть нет никакой разницы между этими двумя моделями. Причем на столько нет разницы, что при нашем отождествлении все новые числа в одной модели имеют ровно те же отношения со старыми числами, что и в другой (это по сути философия изоморфизма над \mathbb{R}). С этого момента мы будем обозначать любую из этих двух моделей через \mathbb{C} .

5.4 Простейшие свойства и операции

Комплексное сопряжение Определим следующую операцию $\bar{\cdot}: \mathbb{C} \rightarrow \mathbb{C}$ по правилу $z = a + bi \mapsto \bar{z} = a - bi$. На языке матричной модели эта операция соответствует транспонированию. Мы знаем, что транспонирование переводит сумму в сумму, а на произведении действует так $(AB)^t = B^t A^t$, но так как \mathbb{C}_2 коммутативно, то для матриц из \mathbb{C}_2 мы имеем $(AB)^t = A^t B^t$. Кроме того сопряжение биективно, как видно из построения и переводит вещественные числа в вещественные. Значит сопряжение является изоморфизмом \mathbb{C} на \mathbb{C} над \mathbb{R} .

Сделаем еще одно полезное замечание, на матричном языке сопряжение так же совпадает с вычислением присоединенной матрицы. Действительно,

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}^t = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{-b} \\ \overline{b} & \overline{a} \end{pmatrix}$$

У последнего замечания есть интересное философское следствие. Заметим, что сопряжение переводит i в $-i$. А так как оно является изоморфизмом, то это означает, что между i и $-i$ нет никакой разницы. То есть если мы внезапно обозначим $-i$ за j , то i превратится в $-j$ и все комплексные числа будут иметь вид $a + bj$ и в этой новой форме никто не догадается, что j это была $-i$, а не опечатка наборщика перепутавшего буквы i и j . То есть в поле комплексных чисел есть небольшая свобода выбора. Мы случайно выбрали один из корней уравнения $x^2 + 1 = 0$ за i и на самом деле нет никакой разницы какой из его корней мы так обозначим.

Вещественная и мнимая части Когда комплексное число записано в виде $z = a + bi$, где $a, b \in \mathbb{R}$, мы говорим, что это его алгебраическая форма. В таком случае число a называется его вещественной частью и обозначается $\operatorname{Re} z$, а b называется мнимой частью z и обозначается $\operatorname{Im} z$. Числа с нулевой мнимой частью – это вещественные числа, а числа с нулевой вещественной частью называются чисто мнимыми.

Заметим, что для любого числа $z \in \mathbb{C}$ верно

1. $z \in \mathbb{R}$ тогда и только тогда, когда $\bar{z} = z$.
2. $z \in i\mathbb{R}$ тогда и только тогда, когда $\bar{z} = -z$.

5.5 Геометрическая модель

Комплексные числа \mathbb{C} можно отождествить с вещественной плоскостью \mathbb{R}^2 , а именно $a + bi$ соответствует вектору на плоскости $\begin{pmatrix} a \\ b \end{pmatrix}$. Таким образом про каждое комплексное число можно думать геометрически как про вектора. При этом сложение комплексных чисел соответствует сложению векторов на плоскости.

У каждого вектора есть длина $|z| = \sqrt{a^2 + b^2}$ – эта величина называется модулем комплексного числа. В матричной модели у нас определитель, легко увидеть, что $\det z = |z|^2$. Перечислим свойства модуля в следующем утверждении.

Утверждение. Модуль комплексного числа обладает следующими свойствами:

1. $|-|: \mathbb{C} \rightarrow \mathbb{R}_+$ является нормой, то есть
 - $|z| \geq 0$ для любого $z \in \mathbb{C}$, причем равенство нулю достигается тогда и только тогда, когда $z = 0$.
 - $|\lambda z| = |\lambda||z|$ для любого $\lambda \in \mathbb{R}$ и $z \in \mathbb{C}$.
 - $|z + w| \leq |z| + |w|$ для любых $z, w \in \mathbb{C}$.
2. $z\bar{z} = |z|^2$ для любого $z \in \mathbb{C}$.
3. $|zw| = |z||w|$ для любых $z, w \in \mathbb{C}$.
4. $z^{-1} = \frac{\bar{z}}{|z|^2}$.

Доказательство. Проверку (1) я оставляю на совести читателя. (2) – это явная формула. (3) доказывается с использованием (2). А вот (4) – это явная формула для обратной матрицы, потому что в матричной модели \bar{z} – это сопряженная матрица, а $|z|^2$ – это $\det(z)$. \square

Тригонометрическая форма Пусть $z \in \mathbb{C}$ и пусть $z \neq 0$. Тогда мы можем сделать следующее

$$z = a + bi = \sqrt{a^2 + b^2} \left(\frac{a}{\sqrt{a^2 + b^2}} + \frac{b}{\sqrt{a^2 + b^2}} i \right)$$

У числа в скобках вещественная и мнимая часть после возведения в квадрат в сумме дают единицу, а значит они являются косинусом и синусом некоторого числа φ , а значит, z можно переписать в следующей форме

$$z = |z|(\cos \varphi + i \sin \varphi)$$

Такая запись комплексного числа называется тригонометрической. Число φ определено с точностью до $2\pi n$, $n \in \mathbb{Z}$ и называется аргументом комплексного числа. Геометрически φ – это угол между осью OX и вектором проходящим из нуля в z . Угол отсчитывается против часовой стрелки. Существует следующее удобное соглашение

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

Оказывается, что при таком определении экспонента обладает всеми знакомыми нам свойствами.⁵¹ В этом случае тригонометрическую форму можно записать так

$$z = |z|e^{i\varphi} = e^{\ln|z| + i\varphi}$$

Алгебраическая форма записи комплексного числа хорошо согласована со сложением, а тригонометрическая – с умножением, о чем говорит следующее.

Утверждение. Для комплексных чисел в тригонометрической форме верны следующие формулы

1. Пусть $z_1 = r_1(\cos \varphi + i \sin \varphi)$ и $z_2 = r_2(\cos \psi + i \sin \psi)$ – два ненулевых комплексных числа, тогда

$$z_1 z_2 = r_1 r_2 (\cos(\varphi + \psi) + i \sin(\varphi + \psi))$$

2. Пусть $z_1 = r_1(\cos \varphi + i \sin \varphi)$ и $z_2 = r_2(\cos \psi + i \sin \psi)$ – два ненулевых комплексных числа, тогда

$$\frac{z_1}{z_2} = \frac{r_1}{r_2} (\cos(\varphi - \psi) + i \sin(\varphi - \psi))$$

3. **Формулы Муавра** Пусть $z = r(\cos \varphi + i \sin \varphi)$ ненулевое комплексное число, тогда

$$z^n = r^n (\cos(n\varphi) + i \sin(n\varphi))$$

⁵¹Если заглянуть чуть глубже в большую науку, то окажется, что вас ждет некоторый набор чудес. Окажется, что в комплексном мире очень мало гладких функций и они очень жесткие. Это значит, что для любой вещественной гладкой функции $f: \mathbb{R} \rightarrow \mathbb{R}$ существует не более одной комплексной гладкой функции $\tilde{f}: \mathbb{C} \rightarrow \mathbb{C}$, продолжающей f , в том смысле, что $\tilde{f}(r) = f(r)$ для любой $r \in \mathbb{R}$. Потому как бы мы не продолжили нашу вещественную экспоненту в комплексный мир, все эти способы дают одно и то же.

Доказательство. 1) По определению

$$r_1(\cos \varphi + i \sin \varphi)r_2(\cos \psi + i \sin \psi) = r_1r_2(\cos \varphi \cos \psi - \sin \varphi \sin \psi + i(\sin \varphi \cos \psi + \sin \psi \cos \varphi)) = \\ r_1r_2(\cos(\varphi + \psi) + i \sin(\varphi + \psi))$$

2) Можно проверить двумя способами. Либо воспользоваться тем, что $1/z_2 = \bar{z}_2/|z_2|^2$, либо домножить требуемое равенство на z_2 и тогда проверка сводится к первому пункту.

3) Это непосредственное следствие первого пункта. \square

5.6 Основная теорема алгебры

Определение 39. Поле F называется алгебраически замкнутым, если для любого многочлена $f \in F[x] \setminus F$ существует корень $\alpha \in F$, то есть $f(\alpha) = 0$.

Утверждение 40 (Основная теорема алгебры). *Поле \mathbb{C} построенное в разделе 5.3 алгебраически замкнуто.*

План доказательства Доказательство основной теоремы алгебры проведем следующим образом. Нам надо будет показать, что верны следующие утверждения:

1. Пусть $p \in \mathbb{C}[x]$ – произвольный многочлен отличный от константы. Тогда для любой константы $c > 0$ найдется $r > 0$ такое, что для любого $z \in \mathbb{C}$ с условием $|z| > r$ выполнено $|p(z)| > c$.⁵²
2. Пусть $p \in \mathbb{C}[x]$ – произвольный многочлен, тогда отображение $|p|: \mathbb{C} \rightarrow \mathbb{R}$ заданное по правилу $z \mapsto |p(z)|$ достигает минимума, то есть найдется такая точка $z_0 \in \mathbb{C}$, что $|p(z_0)| \leq |p(z)|$ для любого $z \in \mathbb{C}$.
3. Пусть $p \in \mathbb{C}[x]$ – не константный многочлен и пусть $z \in \mathbb{C}$ такая точка, что $p(z) \neq 0$. Тогда найдется точка $z_1 \in \mathbb{C}$ такая, что $|p(z_1)| < |p(z)|$.

Первое утверждение нужно для доказательства второго. В свою очередь второе утверждение и третье дадут доказательство теоремы. В начале я покажу, как из утверждений два и три вытекает основная теорема.

Доказательство основной теоремы алгебры. Возьмем произвольный неконстантный многочлен $p \in \mathbb{C}[x]$. Мы должны показать, что он имеет хотя бы один корень в \mathbb{C} . Предположим противное, пусть у него нет корней. По второму пункту мы знаем, что найдется точка минимума $z_0 \in \mathbb{C}$ для отображения $|p|: \mathbb{C} \rightarrow \mathbb{R}$. То есть для любой точки $z \in \mathbb{C}$ будет выполнено $|p(z_0)| \leq |p(z)|$. Так как по предположению у нас нет корней у многочлена p , то $p(z_0) \neq 0$. А значит по третьему пункту мы можем найти точку $z_1 \in \mathbb{C}$ такую, что $|p(z_1)| < |p(z_0)|$, что противоречит тому, что z_0 была точкой минимума. Противоречие получилось из нашего предположения, что p не имело корней. \square

Теперь для завершения доказательства нам надо лишь показать истинность утверждений два и три выше. Однако, для доказательства второго мне понадобится первое утверждение.

Утверждение 41. Пусть $p \in \mathbb{C}[x]$ – произвольный многочлен отличный от константы. Тогда для любого $c > 0$ найдется $r > 0$, что $|p(z)| > c$ при $|z| > r$.

Доказательство. Пусть $p(z) = a_0 + a_1z + \dots + a_nz^n$ и $a_n \neq 0$. Тогда

$$p(z) = a_nz^n \left(1 + \frac{a_{n-1}}{a_nz} + \dots + \frac{a_0}{a_nz^n} \right) = a_nz^n(1 + \omega(z))$$

Фиксируем произвольное положительное число $r > 1$ и рассмотрим $|z| > r$. Тогда

$$|\omega(z)| \leq \left| \frac{a_{n-1}}{a_nz} \right| + \dots + \left| \frac{a_0}{a_nz^n} \right| \leq \left| \frac{a_{n-1}}{a_n} \right| \frac{1}{r} + \dots + \left| \frac{a_0}{a_n} \right| \frac{1}{r^n} \leq \left(\left| \frac{a_{n-1}}{a_n} \right| + \dots + \left| \frac{a_0}{a_n} \right| \right) \frac{1}{r}$$

Последнее выражение обозначим за $\delta(r)$, оно идет к нулю при $r \rightarrow \infty$. Давайте теперь оценим вне этого диска значение $|p(z)|$:

$$|p(z)| = |a_nz^n(1 + \omega(z))| = |a_n||z|^n|1 + \omega(z)| \geq |a_n||z|^n(1 - |\omega(z)|) \geq |a_n||r|^n(1 - \delta(r)) \rightarrow \infty, \text{ при } r \rightarrow \infty$$

То есть мы сможем найти r при котором вне диска $\{z \in \mathbb{C} \mid |z| \leq r\}$ будет выполняться $|p(z)| > c$. \square

⁵²То есть для z больших по модулю значения модуля многочлена тоже большие.

Утверждение 42. Пусть $p \in \mathbb{C}[x]$ – произвольный многочлен, тогда отображение $|p|: \mathbb{C} \rightarrow \mathbb{R}$ заданное по правилу $z \mapsto |p(z)|$ достигает минимума, то есть найдется такая точка $z_0 \in \mathbb{C}$, что $|p(z_0)| \leq |p(z)|$ для любого $z \in \mathbb{C}$.

Доказательство. Идея доказательства этого утверждения следующая. Пусть $c = |p(0)|$. Если это ноль, то мы нашли наш минимум. Пусть $c \neq 0$, тогда давайте найдем диск $D_r(0)$ с центром в нуле и радиуса r такой, что $|p(z)| > c$ для всех $z \notin D_r(0)$. Тогда, по предыдущему утверждению 41 мы можем найти диск $D_r(0) = \{z \in \mathbb{C} \mid |z| \leq r\}$, вне которого $|p(z)| > c$. А значит, если мы найдем минимум для $|p(z)|$ на диске $D_r(0)$ он автоматически будет минимумом в \mathbb{C} . Действительно, внутри диска в этой точке мы будем принимать наименьшее значение, в частности значение не будет больше c . Но вне диска мы не можем принять значение меньше, так как там мы строго больше c .

Теперь надо найти минимум внутри диска $D_r(0)$. Давайте я приведу два доказательства: идейное и доказательство в лоб. Идейное доказательство такое. Функция $\phi: \mathbb{C} \rightarrow \mathbb{R}$ по правилу $z \mapsto |p(z)|$ есть композиция двух отображений: полиномиального $p: \mathbb{C} \rightarrow \mathbb{C}$ и модуля $|\cdot|: \mathbb{C} \rightarrow \mathbb{R}$ по правилу $z \mapsto |z|$. Оба эти отображения непрерывны, а значит и отображение $z \mapsto |p(z)|$ тоже непрерывно. Кроме того, диск $D_r(0)$ является компактом, а любое непрерывное отображение на компакте достигает минимума.⁵³ \square

Минимум на диске (по простому?) Чтобы найти минимум на диске, мне придется пользоваться фактами из математического анализа, ведь свойства комплексных чисел должны зависеть от особенностей их природы, которая не чисто алгебраическая. Нам понадобится следующий факт.⁵⁴

Утверждение (БД). У любой последовательности на отрезке найдется сходящаяся подпоследовательность. То есть для любой $a_n \in [a, b]$ найдется подпоследовательность a_{n_k} такая, что существует

$$\lim_{k \rightarrow \infty} a_{n_k} \in [a, b]$$

Рассмотрим функцию $f = |p|: D_r(0) \rightarrow \mathbb{R}$ по правилу $f(z) = |p(z)|$. Так как эта функция ограничена снизу нулем, то существует нижняя грань

$$a = \inf_{z \in D_r(0)} f(z)$$

По определению нижней грани, мы можем выбрать последовательность $z_n \in D_r(0)$ такую, что $f(z_n) \rightarrow a$. Такая последовательность обязательно имеет вид $z_n = a_n + ib_n$, где $a_n, b_n \in [-r, r]$ – последовательности вещественных чисел на отрезке. Из них мы по очереди можем выбрать сходящиеся подпоследовательности a_{n_k} и b_{n_k} , так что последовательность z_{n_k} сходится в $D_r(0)$ к какой-то точке z_0 . А значит

$$a = \lim_{k \rightarrow \infty} f(z_{n_k}) = \lim_{k \rightarrow \infty} |p(z_{n_k})| = \left| \lim_{k \rightarrow \infty} p(z_{n_k}) \right| = \left| p \left(\lim_{k \rightarrow \infty} z_{n_k} \right) \right| = |p(z_0)|$$

Давайте объясним все переходы. Первый – это определение нашей последовательности, мы по ней подбираем к инфимуму. Второй – это непрерывность модуля, то есть для комплексного числа верно $\lim_{n \rightarrow \infty} |z_n| = |\lim_{n \rightarrow \infty} z_n|$. Действительно, ведь $|a + bi| = \sqrt{a^2 + b^2}$ и функция корня от суммы квадратов непрерывна, то есть предел в точке равен ее значению в точке. Третий переход следует из непрерывности многочлена $p(z)$. Действительно, такой многочлен – это сумма произведений мнимых и вещественных частей с коэффициентами, а в таких функциях мы тоже умеем переходить к пределу. Последнее равенство – это возможность взять предел у выбранной подпоследовательности. Таким образом в точке z_0 достигается нижняя грань на диске $D_r(0)$, а значит это точка минимума.

Минимум обязан быть нулем Теперь осталось доказать утверждение (3), что минимум для функции $|p(z)|$ (если p не константа) обязательно должен быть нулем. Точнее мы покажем, что если $|p(z)| \neq 0$, то обязательно найдется точка с еще меньшим модулем, то есть найдется $z' \in \mathbb{C}$, что $|p(z')| < |p(z)|$. Но в начале нам понадобится следующий пример.

Пример 43 (V.I.P. пример). Рассмотрим $p(z) = z^d$ и посмотрим на функцию $p: \mathbb{C} \rightarrow \mathbb{C}$ по правилу $z \mapsto p(z) = z^d$. Давайте рассмотрим окружность $z(t) = re^{2\pi it}$ для $t \in [0, 1]$. Когда t пробегает от 0 до 1, то $z(t) = re^{2\pi it}$ пробегает по окружности радиуса r один оборот против часовой стрелки. Давайте посмотрим на образ этой окружности под действием p , получим $p(z(t)) = r^d e^{2\pi i d t}$. То есть теперь, когда t пробегает от 0 до 1 мы пробегаем окружность радиуса r^d но уже d раз против часовой стрелки (делаем d оборотов вместо одного).

⁵³Если вы сейчас пребываете в шоке, то это нормально. Сейчас я исправлюсь и напишу простое доказательство, но он будет несколько длиннее.

⁵⁴Искренне надеюсь, что с ним вы знакомы. Его можно считать одной из аксиом вещественных чисел.

Утверждение 44. Пусть $p \in \mathbb{C}[x]$ – произвольный не константный многочлен и $z_0 \in \mathbb{C}$ такая точка, что $p(z_0) \neq 0$. Тогда найдется точка $z_1 \in \mathbb{C}$ такая, что $|p(z_1)| < |p(z_0)|$.

Доказательство. Рассмотрим отображение $|p|: \mathbb{C} \rightarrow \mathbb{R}$. По предыдущему утверждению, у него есть точка минимума z_0 . Давайте определим многочлен $g(z) = p(z_0 + z)$. Тогда у многочлена $g(z)$ то же множество значений, что и у $p(z)$, но у него точка 0 является точкой минимума. В свою очередь g представляется в виде

$$g(z) = a_0 + a_r z^r + a_{r+1} z^{r+1} + \dots + a_n z^n$$

Здесь выше a_0 – это значение многочлена g в нуле, которое по условию не ноль. Число a_r – это первый ненулевой коэффициент после a_0 в многочлене g . Учтите, что r может быть 1, а может быть больше 1. Давайте перепишем многочлен g следующим образом:

$$g(z) = a_0 + a_r z^r \left(1 + \frac{a_{r+1}}{a_r} z + \dots + \frac{a_n}{a_r} z^{n-r} \right) = a_0 + a_r z^r (1 + \omega(z))$$

где

$$\omega(z) = \frac{a_{r+1}}{a_r} z + \dots + \frac{a_n}{a_r} z^{n-r}$$

Давайте в начале посмотрим на многочлен $h(z) = a_0 + a_r z^r$ и покажем что для него найдется точка z_1 такая, что $|h(z_1)| < |h(z_0)|$. Если $|z| = \delta$, то z^r описывает окружность радиуса δ^r вокруг нуля и делает r оборотов. Выражение $a_r z^r$ описывает окружность радиуса $|a_r| \delta^r$ вокруг нуля и делает r оборотов.⁵⁵ А значит $h(z) = a_0 + a_r z^r$ описывает окружность радиуса $|a_r| \delta^r$ вокруг точки a_0 и делает r оборотов. При малых δ эта окружность пересекается с радиус вектором a_0 в некоторой точке m . Тогда решая уравнение $m = a_0 + a_r z^r$,⁵⁶ мы найдем точку z_1 такую, что $h(z_1) = m$. Но по построению точка m ближе к нулю, чем a_0 , а это и значит, что $|h(z_1)| < |h(z_0)|$.

Теперь давайте посмотрим, что происходит с функцией g . Давайте для начала оценим $\omega(z)$, когда $|z| = \delta < 1$:

$$|\omega(z)| \leq \left| \frac{a_{r+1}}{a_r} \right| \delta + \dots + \left| \frac{a_n}{a_r} \right| \delta^{n-r} \leq \left(\left| \frac{a_{r+1}}{a_r} \right| + \dots + \left| \frac{a_n}{a_r} \right| \right) \delta = C\delta$$

Последнее неравенство следует из того, что $\delta < 1$. А через C мы обозначили полученную константу. Тогда при $|z| = \delta$ имеем⁵⁷

$$|g(z) - h(z)| = |a_{r+1} z^{r+1} + \dots + a_n z^n| = |a_r| \delta^r |\omega(z)| \leq |a_r| \delta^r C\delta = RC\delta$$

где за R мы обозначили радиус окружности описываемой $h(z)$ при $|z| = \delta$. Таким образом мы видим, что при малых δ выполнено $|g(z_1) - h(z_1)| < RC\delta$.⁵⁸ Но тогда

$$|g(z_1)| \leq |h(z_1)| + RC\delta$$

Но по построению

$$|h(z_1)| = |m| = |a_0| - R$$

Значит

$$|g(z_1)| \leq |h(z_1)| + RC\delta = |a_0| - R(1 - C\delta) < |a_0|$$

где последнее неравенство выполнено при малых δ , когда $C\delta < 1$. □

5.7 Многочлены

В этом разделе я хочу сказать пару слов про многочлены. Пусть F – некоторое поле. Тогда многочлен над полем F – это картинка вида $f = a_0 + a_1 x + \dots + a_n x^n$, где $a_i \in F$. Формально, такая картинка – это конечная последовательность чисел (a_0, \dots, a_n) , но психологически лучше и правильнее думать именно про картинки. Еще можно для краткости писать $f = \sum_{k \geq 0} a_k x^k$, подразумевая, что в этой сумме только конечное число

⁵⁵Начальная точка для окружности имеет аргумент равный аргументу a_r .

⁵⁶Это мы можем сделать, так как тут задача про извлечение корня из числа $(m - a_0)/a_r$.

⁵⁷Давайте я объясню смысл этой оценки. Мы видим, что при $|z| = \delta$ функция $h(z)$ описывает окружность вокруг точки a_0 радиуса R . Полученная оценка показывает, что функция $g(z)$ отличается от $h(z)$ на величину εR , то есть лежит в кольце возле этой окружности. А значит, $g(z)$ пересечет вектор a_0 в точке близкой к m – точке пересечения вектора a_0 с $h(z)$.

⁵⁸Здесь z_1 – точка такая, что $h(z_1)$ пересекает вектор a_0 .

ненулевых коэффициентов. Это удобное соображение позволяет удобно записать правила для сложения и умножения многочленов, которые определяются следующим образом

$$\left(\sum_{k \geq 0} a_k x^k\right) + \left(\sum_{k \geq 0} b_k x^k\right) = \sum_{k \geq 0} (a_k + b_k) x^k \quad \text{и} \quad \left(\sum_{k \geq 0} a_k x^k\right) \left(\sum_{k \geq 0} b_k x^k\right) = \sum_{k \geq 0} \left(\sum_{m+n=k} a_m b_n\right) x^k$$

Таким образом многочлен – это не функция, а картинка. Однако, каждый многочлен $f \in F[x]$ задает функцию $F \rightarrow F$ по правилу $x \mapsto f(x)$. Но в случае конечных полей (то есть полей из конечного числа элементов) разные многочлены могут давать одни и те же функции. Напомню, что степень многочлена f – это наибольший номер n , что коэффициент $a_n \neq 0$.⁵⁹

Пример

- Пример конечного поля.

Пусть $p \in \mathbb{Z}$ – некоторое простое число. Обозначим через \mathbb{Z}_p множество остатков по этому числу, то есть $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$. Введем на этом множестве операции сложения и умножения по модулю простого числа p , то есть

$$a + b = a + b \pmod{p} \quad \text{и} \quad ab = ab \pmod{p}$$

Тогда можно проверить, что \mathbb{Z}_p является полем, где числа 0 и 1 являются нулем и единицей поля. Единственная аксиома, которая требует усилий – показать, что любой ненулевой элемент \mathbb{Z}_p обратим. Давайте возьмем произвольный ненулевой элемент $a \in \mathbb{Z}_p$. Так как $a < p$ и p – простое число, то $(a, p) = 1$. По расширенному алгоритму евклида найдутся целые числа $u, v \in \mathbb{Z}$ такие, что $1 = ua + vp$. Рассмотрим это равенство по модулю простого числа p и получим, что $ua = 1 \pmod{p}$, а это и означает, что u является обратным к a по умножению.

- Пример, когда разные многочлены дают одну и ту же функцию.

Рассмотрим многочлены $\mathbb{Z}_2[x]$. Тогда \mathbb{Z}_2 состоит только из 0 и 1. В этом случае все многочлены x^n задают одну и ту же функцию.

Определение 45. Пусть F – произвольное поле и $f \in F[x]$ – некоторый многочлен. Если число $a \in F$ является его корнем, то f делится на $x - a$, а значит представляется в виде $f(x) = (x - a)g(x)$ для некоторого $g \in F[x]$. Аналогично, если a является корнем g , то можно выделить $(x - a)$ и в g и так далее. В итоге можно найти разложение $f(x) = (x - a)^k g(x)$, где $g(a) \neq 0$. В этом случае говорят, что k – это кратность корня a в многочлене f . Корень кратности 1 называется простым.

Определение 46. Пусть $f \in F[x]$ имеет вид $f = a_0 + a_1 x + \dots + a_n x^n$. Определим формальную производную следующим образом $f' = a_1 + 2a_2 x + \dots + na_n x^{n-1}$ или по-другому $f' = \sum_{k \geq 0} ka_k x^{k-1}$.

Несложно убедиться, что, определив таким образом производную, она удовлетворяет всем естественным свойствам, к которым мы привыкли в анализе. В качестве упражнения предлагается проверить следующее.

Утверждение 47. Пусть F – произвольное поле. Для формальной производной выполнены следующие свойства:

1. $(f + g)' = f' + g'$ для любых $f, g \in F[x]$.
2. $(\lambda f)' = \lambda f'$ для любых $\lambda \in F$ и $f \in F[x]$.
3. $(fg)' = f'g + fg'$ для любых $f, g \in F[x]$.
4. $f(g(x))' = f'(g(x))g'(x)$ для любых $f, g \in F[x]$.

С помощью формальной производной можно проверить кратность корня в произвольном многочлене. Для начала нам нужно следующее вспомогательное утверждение.

Утверждение 48. Пусть F – произвольное поле, $f \in F[x]$ – некоторый многочлен и $a \in F$ – его корень кратности k . Тогда

⁵⁹По-хорошему надо еще аккуратно определить степень нулевого многочлена. Но ее обычно определяют по ситуации так, как удобнее. Например можно положить -1 или $-\infty$ и есть еще пара способов. Но об этом можно особенно не запариваться.

1. Число a является корнем кратности хотя бы $k - 1$ в многочлене f' .

2. Если число $k \neq 0$ в F , то a является корнем кратности в точности $k - 1$ в многочлене f' .

Доказательство. 1) По определению имеем $f = (x - a)^k g(x)$ причем $g(a) \neq 0$. Возьмем производную от f , получим

$$f' = k(x - a)^{k-1}g(x) + (x - a)^k g'(x) = (x - a)^{k-1}(kg(x) + (x - a)g'(x))$$

и мы видим, что у производной a имеет кратность хотя бы $k - 1$.

2) Давайте поймем, когда кратность может вырасти. Только если множитель $(kg(x) + (x - a)g'(x))$ зануляется в a . Если подставить a , то получим $kg(a)$. Число $g(a) \neq 0$ по выбору, но если $k \neq 0$, то и их произведение не ноль в поле F , а это будет означать, что кратность корня в точности $k - 1$. \square

Примеры и замечания

- Давайте продемонстрируем ситуацию, когда кратность корня может возрасти. Например, выберем $F = \mathbb{Z}_p$ и в качестве многочлена h рассмотрим $x^p - 1$. Тогда $h' = 0$. Теперь положим $f = xh(x) = x^{p+1} - x$. Тогда $f' = h(x) = x^p - 1$. С другой стороны $x^p - 1 = (x - 1)^p$, а значит 1 имеет кратность p в многочлене f . Но и в многочлене f' 1 имеет кратность p .
- Если для любого натурального числа $k \in \mathbb{N}$ в поле F выполнено, $k \neq 0$, то можно следующим образом проверить корень многочлена $f \in F[x]$ на кратность. Если $a \in F$ — некоторый корень. Надо посмотреть на $f'(a)$. Если это число ноль, то a корень кратности больше 1, а если не ноль, то кратности в точности 1.
- Если F произвольное поле, то общий алгоритм проверки корня на простоту следующий. Надо взять многочлен $f \in F[x]$, для которого a является корнем. Посчитать производную f' , потом посчитать нод $d(x) = (f, f')$. Если $d(a) = 0$, то a кратный корень, если $d(a) \neq 0$, то это корень кратности 1.⁶⁰

⁶⁰Я не буду останавливаться на доказательствах этих фактов. Все они вам встретятся в курсе алгебры.

6 Векторные пространства

6.1 Идея и определение

Идея Мы с вами до этого изучали много разных объектов, которые не сильно похожи друг на друга. Например, вектор-столбцы F^n , матрицы $M_{m,n}(F)$, функции $f: X \rightarrow F$, многочлены $F[x]$. Все эти товарищи нам постоянно встречаются и каждый раз приходится для каждого из них все доказывать заново и во время доказательств мы видим, что наши рассуждения повторяются. Это означает, что на самом деле у всех этих объектов есть некий общий интерфейс, через который мы на самом деле с ним работаем. Самое главное в этом интерфейсе то, что мы можем брать элементы из этих объектов, умножать эти элементы на числа и складывать между собой. Абстрактное векторное пространство как раз и формализует идею такого общего интерфейса, через который в множестве можно складывать элементы и умножать на числа.

У такого подхода есть несколько плюсов. Во-первых, формальное удобство, как только вы что-то сделали для абстрактного векторного пространства и увидели, что что-то конкретное является таковым, то все ваши достижения автоматом применимы в этой конкретной ситуации. Общий алгоритм для векторного пространства будет одинаково хорошо работать и для столбцов, и для матриц, и для функций и т.д. Во-вторых, есть менее очевидный бонус. Когда мы доказываем что-то про абстрактное векторное пространство, то про него надо думать как про F^n . Это поможет вам не потеряться в формализме и догадаться, что откуда берется. Неформально это означает, что если вы что-то умеете делать для F^n , то это автоматически верно для любого векторного пространства! Формально это не совсем правда, но в классе хороших пространств это так.⁶¹ Тем не менее, даже в классе всех пространств, интуиция из F^n очень полезна.

Определение Следующее определение – это пример определения с контекстом. Это означает, что прежде, чем его дать, вы должны зафиксировать некоторую информацию, которая необходима для вашего определения и без этой информации оно – бессмысленный мусор. У определения векторного пространства в качестве такого контекста выступает некоторое поле F . Это значит, что пока вы не зафиксировали какое-то поле, вы не можете говорить о векторных пространствах над полем F , а «просто векторных пространств» без указания какого-либо поля не существует.

Определение 49. Пусть F – некоторое фиксированное поле. Тогда векторное пространство над полем F – это следующий набор данных $(V, +, \cdot)$, где

- V – множество. Элементы этого множества будут называться векторами.
- $+: V \times V \rightarrow V$ – бинарная операция, то есть правило действующее так $(v, u) \mapsto v + u$, где $u, v \in V$.
- $\cdot: F \times V \rightarrow V$ – бинарная операция, то есть правило действующее так $(\alpha, v) \mapsto \alpha v$, где $\alpha \in F$ и $v \in V$.

При этом эти данные удовлетворяют следующим 8 аксиомам:

1. **Ассоциативность сложения** Для любых векторов $u, v, w \in V$ верно $(u + v) + w = u + (v + w)$.
2. **Существование нулевого вектора** Существует такой вектор $0 \in V$, что для любого $v \in V$ выполнено $0 + v = v + 0 = v$.
3. **Существование противоположного вектора** Для любого вектора $v \in V$ существует вектор $-v \in V$ такой, что $v + (-v) = (-v) + v = 0$.
4. **Коммутативность сложения** Для любых векторов $u, v \in V$ верно $u + v = v + u$.
5. **Согласованность умножения со сложением векторов** Для любого числа $\alpha \in F$ и любых векторов $u, v \in V$ верно $\alpha(v + u) = \alpha v + \alpha u$.
6. **Согласованность умножения со сложением чисел** Для любых чисел $\alpha, \beta \in F$ и любого вектора $v \in V$ верно $(\alpha + \beta)v = \alpha v + \beta v$.
7. **Согласованность умножения с умножением чисел** Для любых чисел $\alpha, \beta \in F$ и любого вектора $v \in V$ верно $(\alpha\beta)v = \alpha(\beta v)$.
8. **Нетривиальность** Для любого $v \in V$ верно $1v = v$.⁶²

⁶¹Под хорошими тут подразумеваются конечно мерные.

⁶²Здесь $1 \in F$.

Примеры

1. Поле F (или кто больше привык к вещественным числам \mathbb{R}) является векторным пространством над F (соответственно над \mathbb{R}).
2. Более обще, множество вектор-столбцов F^n является векторным пространством над F .
3. Множество матриц $M_{mn}(F)$ является векторным пространством над F .
4. Пусть X – произвольное множество, тогда множество функций $F(X, F) = \{f: X \rightarrow F\}$ является векторным пространством над F . Надо лишь объяснить как складывать функции и умножать на элементы F . Операции поточечные, пусть $f, g: X \rightarrow F$, тогда функция $(f + g): X \rightarrow F$ действует по правилу $(f + g)(x) = f(x) + g(x)$. Если $\alpha \in F$, то функция $(\alpha f): X \rightarrow F$ действует по правилу $(\alpha f)(x) = \alpha f(x)$.
5. Множество многочленов $F[x] = \{a_0 + a_1x + \dots + a_nx^n \mid a_i \in F, n \in \mathbb{Z}_{\geq 0}\}$. Тут надо обратить внимание, что мы подразумеваем под многочленом. Для нас многочлен – это НЕ функция, многочлен – это картинка вида $a_0 + a_1x + \dots + a_nx^n$.⁶³ Складываются и умножаются эти картинки по одинаковым правилам. Важно, что две такие картинки равны тогда и только тогда, когда у них равные коэффициенты. Множество всех многочленов $F[x]$ является векторным пространством над F .

Замечание Стоит отметить, что в обычных векторных пространствах мы привыкли к некоторым свойствам, которые бы хотелось иметь и в общем случае. Например, в F^n есть единственный нулевой вектор, а аксиомы в общем случае говорят, что нулевой вектор лишь существует. Однако, можно показать, что нулевой вектора автоматически единственный. Давайте перечислим некоторые непосредственные следствия из аксиом, которые я оставляю в качестве упражнения:

1. Нулевой вектор единственный.
2. Для любого $v \in V$ существует единственный $-v$.
3. Для любого вектора $v \in V$ верно $-v = (-1)v$.
4. Для любого вектора $v \in V$ имеем $0v = 0$.
5. Для любого числа $\alpha \in F$ верно $\alpha 0 = 0$.

6.2 Подпространство

Пусть V – векторное пространство над F . Тогда непустое подмножество $U \subseteq V$ называется подпространством, если на него можно ограничить операции $+$ и \cdot и относительно них оно является векторным пространством. Давайте определим подпространство формально.

Определение 50. Пусть V – векторное пространство над полем F . Тогда подмножество $U \subseteq V$ называется подпространством, если

1. U не пусто.⁶⁴
2. Для любых векторов $u, u' \in U$ верно, что $u + u' \in U$.
3. Для любого скаляра $\alpha \in F$ и вектора $u \in U$ верно, что $\alpha u \in U$.

Если U – подпространство в V , то на U можно корректно ограничить операции сложения и умножения на скаляр из исходного пространства V . Таким образом у нас получается набор данных $(U, +, \cdot)$ и теперь надо, чтобы выполнялись все аксиомы векторного пространства для них. Оказывается, что все аксиомы будут выполняться автоматически! Например, почему у нас будет $0 \in U$. Потому что если мы возьмем любой вектор $u \in U$, то $0 = 0u \in U$. Остальное я оставлю в качестве упражнения.

⁶³Для любителей формализма, можете считать, что многочлен – это конечная последовательность элементов F вида (a_0, \dots, a_n) , но длина последовательности может быть любой, включая нулевую.

⁶⁴При наличии свойства (3) это свойство эквивалентно тому, что нулевой вектор V попадает в U . Действительно, если он попадает, то U не пусто. Наоборот, если $u \in U$ – какой-то вектор, то $0 = 0u \in U$ по третьему свойству.

Примеры

1. Для любого векторного пространства V подмножества 0 и V всегда являются подпространствами.
2. Множество $\{y \in F^n \mid Ay = 0\} \subseteq F^n$, где $A \in M_{m,n}(F)$, является векторным подпространством в F^n .
3. Множество многочленов $\mathbb{R}[x]$ является подпространством в пространстве $F(\mathbb{R}, \mathbb{R})$ – всех функций на прямой.

Обратите внимание, что подпространство из второго примера кажется устроено сложнее, чем векторное пространство, в котором оно лежит F^n . Однако, окажется, что взаимодействие с ними через абстрактный интерфейс векторного пространства происходит абсолютно одинаков. То есть на самом деле подпространство устроено не сложнее, чем исходное пространство. Об этом речь пойдет после того, как мы узнаем, что такое базисы и что значит, что какие-то векторные пространства одинаковые.

6.3 Линейные комбинации

Мотивация Пусть у нас есть векторное пространство V над полем F . Давайте поймем, а что вообще с ним можно делать? Во-первых, V – это множество. Значит из него можно брать элементы. Во-вторых, там есть операция умножения на числа, то есть любой вектор можно умножить на какое-то число. В-третьих, у нас вектора можно складывать. Все это означает, что все что можно делать с векторным пространством, это набрать каких-то векторов из него v_1, \dots, v_n и написать выражение вида $\alpha_1 v_1 + \dots + \alpha_n v_n$, для произвольных $\alpha_i \in F$. Это выражение будет задавать нам какой-то вектор из V . Как мы видим, особенно не разбежишься с разнообразием действий. Однако, важно, что с помощью подобных выражений можно вытащить абсолютно всю информацию из векторных пространств, которую только возможно. Именно поэтому все наше внимание будет посвящено выражениям такого вида, так как из них получится узнать все, что только можно про векторные пространства.

Линейные комбинации

Определение 51. Пусть V – некоторое векторное пространство над полем F и пусть $v_1, \dots, v_n \in V$ – некоторый набор векторов. Тогда выражение вида $\alpha_1 v_1 + \dots + \alpha_n v_n$, где $\alpha_i \in F$, называется линейной комбинацией v_1, \dots, v_n . Линейная комбинация называется тривиальной, если все $\alpha_i = 0$. В противном случае она называется нетривиальной.

Определение 52. Вектора $v_1, \dots, v_n \in V$ называются линейно зависимыми, если существует их нетривиальная линейная комбинация равная нулю, то есть для каких-то $\alpha_i \in F$ (так что хотя бы один не равен нулю) выражение $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$. Подчеркнем, что вектора линейно независимы, если из равенство $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$ следует, что все $\alpha_i = 0$.

Примеры

1. Вектор 0 всегда линейно зависим.
2. Вектор $v \in V$ линейно зависим тогда и только тогда, когда он равен нулю.
3. Вектора $v_1, v_2 \in V$ линейно зависимы тогда и только тогда, когда они пропорциональны (то есть один из них равен другому умноженному на элемент поля).

Заметим, что если множество векторов v_1, \dots, v_k линейно независимо, то и любое его подмножество тоже линейно независимо. Потому интересно не уменьшать, а увеличивать линейно независимые подмножества векторов. Линейно независимое множество векторов v_1, \dots, v_k называется максимальным, если при добавлении к нему любого вектора, оно становится линейно зависимым.

Линейная оболочка

Определение 53. Пусть $E \subseteq V$ – некоторое подмножество в векторном пространстве V над полем F . Тогда обозначим через $\langle E \rangle$ множество всех линейных комбинаций векторов из E , то есть

$$\langle E \rangle = \{\alpha_1 v_1 + \dots + \alpha_n v_n \mid \alpha_i \in F, v_i \in E, n \in \mathbb{N}\}$$

Сделаем важное замечание, если $E = \emptyset$ пусто, то $\langle \emptyset \rangle$ полагаем равным нулевому подпространству (подпространству состоящему только из нуля). Это полезное и удобное соглашение можно понимать так: если берется линейная комбинация с нулевым числом слагаемых, то она равна нулю.

Заметим, что $\langle E \rangle$ является наименьшим векторным подпространством содержащим E . Потому, для любого подпространства $U \subseteq V$ верно $\langle U \rangle = U$.

Пример Полезно держать перед глазами следующий пример. Пусть $V = \mathbb{R}^3$ – пространство, $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$ три вектора вдоль координатных осей. Тогда $\langle e_1 \rangle$, $\langle e_2 \rangle$ и $\langle e_3 \rangle$ – это в точности координатные оси. Подпространства $\langle e_1, e_2 \rangle$, $\langle e_1, e_3 \rangle$ и $\langle e_2, e_3 \rangle$ – это плоскости содержащие пары координатных осей, $\langle e_1, e_2, e_3 \rangle$ будет совпадать со всем пространством \mathbb{R}^3 .

Порождающее подмножество

Определение 54. Пусть V – векторное пространство над полем K , тогда подмножество $E \subseteq V$ называется порождающим, если $\langle E \rangle = V$.

Другими словами, E является порождающим если любой вектор из V является линейной комбинацией векторов из E . Отметим, что V целиком всегда является порождающим. Если $E \subseteq E' \subseteq V$ и подмножество E является порождающим, то и E' тоже порождающее. Потому порождающее семейство всегда можно увеличить и это не интересно, интереснее попытаться его уменьшить и сделать более экономным. Порождающее множество E называется минимальным, если любое строго меньшее подмножество E уже не порождающее. Для этого достаточно проверить, что для любого $v \in E$ множество $E \setminus \{v\}$ уже не порождающее.

6.4 Базис

Подмножество $E \subseteq V$ называется порождающим, если $\langle E \rangle = V$. Другими словами, E является порождающим если любой вектор из V является линейной комбинацией векторов из E . Отметим, что V целиком всегда является порождающим. Если $E \subseteq E' \subseteq V$ и подмножество E является порождающим, то и E' тоже порождающее. Потому порождающее семейство всегда можно увеличить и это не интересно, интереснее попытаться его уменьшить и сделать более экономным. Порождающее множество E называется минимальным, если любое строго меньшее подмножество E уже не порождающее. Для этого достаточно проверить, что для любого $v \in E$ множество $E \setminus \{v\}$ уже не порождающее.

Подмножество $E \subseteq V$ называется линейно независимым, если любое конечное подмножество векторов E линейно независимо. Если $E' \subseteq E \subseteq V$ и E является линейно независимым, то E' тоже будет линейно независимым. Потому линейно независимое подмножество можно всегда уменьшать⁶⁵ и это не интересно, интереснее попытаться его увеличить и сделать наиболее большим. Линейно независимое подмножество E называется максимальным, если любое строго содержащее его подмножество является линейно зависимым. Для этого достаточно проверить, что для любого $v \in V \setminus E$ множество $E \cup \{v\}$ является линейно зависимым.

Утверждение 55. Пусть V – некоторое векторное пространство над некоторым полем F . Тогда следующие условия на подмножество $E \subseteq V$ эквивалентны:

1. E – минимальное порождающее подмножество.
2. E – максимальное линейно независимое подмножество.
3. E – одновременно порождающее и линейно независимое подмножество.

Доказательство. Будем доказывать по схеме $(1) \Leftrightarrow (3) \Leftrightarrow (2)$.

$(1) \Rightarrow (3)$. Пусть E – минимальное порождающее, нам надо показать, что оно будет линейно независимым. Предположим противное, пусть найдется вектора $v_1, \dots, v_n \in E$ и числа $\alpha_1, \dots, \alpha_n \in F$, так что не все из них равны нулю, что выполнено $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$. Мы можем предположить, что $\alpha_1 \neq 0$. Тогда $v_1 = \beta_2 v_2 + \dots + \beta_n v_n$ для некоторых $\beta_i \in F$. Давайте покажем, что тогда $E \setminus \{v_1\}$ тоже является порождающим, что будет противоречить минимальности E . Действительно, пусть $v \in V$ – произвольный вектор. Так как E – порождающее, то v выражается через вектора из E , $v = \sum_i \alpha'_i v'_i$. Если среди v'_i нет вектора v_1 то мы выразили v через $E \setminus \{v_1\}$, если есть то подставим вместо него выражение $\beta_2 v_2 + \dots + \beta_n v_n$ и получим выражение v только через вектора из $E \setminus \{v_1\}$, что и требовалось.

⁶⁵ Вопрос линейной независимости пустого множества оставим на совести строгой аксиоматической теории множеств и не будем его касаться, чтобы не обжечься о всякий формальный гемморрой.

(3) \Rightarrow (1). Пусть E одновременно порождающее и линейно независимое, нам надо показать, что оно минимальное порождающее. Достаточно проверить, что для любого $v \in E$ вектор v не лежит в $\langle E \setminus \{v\} \rangle$. Действительно, пусть лежит, тогда найдутся вектора $v_1, \dots, v_n \in E \setminus \{v\}$ и числа $\alpha_i \in F$ такие, что $v = \alpha_1 v_1 + \dots + \alpha_n v_n$, то тогда $(-1)v + \alpha_1 v_1 + \dots + \alpha_n v_n = 0$ – нетривиальная линейная комбинация разных элементов E , что противоречит линейной независимости E .

(2) \Rightarrow (3). Пусть E – максимальное линейно независимое, нам надо показать, что оно будет порождающим. Нам надо показать, что $\langle E \rangle = V$. Пусть пусть это не так, возьмем $v \in V \setminus \langle E \rangle$, тогда множество $E \cup \{v\}$ строго больше, а значит линейно зависимо. То есть для каких-то $v_1, \dots, v_n \in E \cup \{v\}$ и чисел $\alpha_i \in F$ (так что не все из них нули) выполнено $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$. Выкинув все нулевые слагаемые, можем считать, что на самом деле все α_i не равны нулю. Если среди v_i нет v , то значит все они из E . Тогда это означает, что E линейно зависимо, что неправда. Значит один из v_i – это v . Будем считать, что $v_1 = v$. Так как по нашему предположению все коэффициенты не нулевые, то $v = v_1$ выражается через остальные v_2, \dots, v_n . Но это означает, что $v \in \langle E \rangle$, противоречие с выбором v .

(3) \Rightarrow (2). Пусть E одновременно порождающее и линейно независимое, нам надо показать, что оно максимальное линейно независимое. Для этого возьмем любой вектор $v \in V \setminus E$ и покажем, что $E \cup \{v\}$ линейно зависимо. Действительно, мы знаем, что E порождающее, значит v представляется в виде линейной комбинации векторов из E , то есть $v = \alpha_1 v_1 + \dots + \alpha_n v_n$ для некоторых $v_i \in E$ и $\alpha_i \in F$. Но тогда $(-1)v + \alpha_1 v_1 + \dots + \alpha_n v_n = 0$ – нетривиальная линейная комбинация векторов из $E \cup \{v\}$, то есть последнее множество линейно зависимо, что и требовалось. \square

Пусть V – векторное пространство над некоторым полем F , тогда подмножество $E \subseteq V$ удовлетворяющее одному из трех эквивалентных условий предыдущего утверждения называется базисом V .

Примеры

1. Пусть $V = F^n$, тогда вектора

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, v_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

являются базисом. Очевидно, что эти вектора линейно независимы и любой вектор через них выражается.

2. Пусть $V = F[x]$ – множество многочленов, тогда в качестве базиса можно взять $E = \{1, x, x^2, \dots, x^n, \dots\}$ – множество всех степеней x . Заметим, что в данном случае базис получается бесконечным.
3. Пусть X – произвольное множество и $V = \{f: X \rightarrow F\}$ – множество всех функций на X со значениями в F . Тогда это векторное пространство над F с очень любопытным свойством.

Ситуация с базисами тут устроена так. Чтобы работать с бесконечными множествами нам нужно использовать аккуратно определенную теорию множеств. Я не буду вдаваться в подробности, что там да как строится, но важно понимать, что в теории множеств вообще говоря не всякое утверждение является доказуемым или опровергаемым. Подобные утверждения можно включить в качестве дополнительных аксиом, а можно их отрицания использовать в качестве таких же законных аксиом и будут получаться совершенно разные теории множеств. Есть такая популярная аксиома «аксиома выбора», которую очень любят включать в список стандартных.

Если вы используете аксиому выбора, то можно доказать, что всякое векторное пространство имеет базис. Если же вы не используете аксиому выбора, то нельзя ни доказать, ни опровергнуть существования базиса уже в пространстве V из этого примера. Оказывается, что факт существования базиса является более слабым утверждением, чем аксиома выбора. Кроме того, если базис существует по аксиоме выбора, то это значит, что не существует никакой процедуры, которая бы помогла вам описать этот базис, потому что существование подобной процедуры дало бы вам доказательство существования базиса без аксиомы выбора.

Замечания

- Пусть V – некоторое векторное пространство и $E' \subseteq V$ – произвольное линейно независимое подмножество. Тогда его всегда можно дополнить до базиса $E \supseteq E'$, потому что базис – это максимальное линейно независимое подмножество. В случае, если существует конечный базис, это просто. А если конечного не существует, то тут придется обращаться к аккуратной формулировке аксиоматики теории множеств.
- Пусть V – некоторое векторное пространство и $E'' \subseteq V$ – произвольное порождающее множество, тогда из него всегда можно выбрать базис $E \subseteq E''$. Как и в предыдущем случае, если существует конечный базис, то это просто. А если нет конечного базиса, то это требует аккуратной аксиоматики теории множеств.

6.5 Удобный формализм

Пусть V – некоторое векторное пространство над некоторым полем F . Возьмем некоторые вектора $v_1, \dots, v_n \in V$ и набор чисел $x_1, \dots, x_n \in F$. Тогда можно составить строку из векторов v_i и столбец из чисел x_i и перемножить в следующем порядке

$$(v_1 \quad v_2 \quad \dots \quad v_n) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = x_1 v_1 + \dots + x_n v_n$$

Таким образом мы можем записывать линейные комбинации с помощью матричных объектов, когда матрицы состоят не только из чисел, но и из векторов. Если при этом ввести обозначения

$$v = (v_1 \quad v_2 \quad \dots \quad v_n) \quad \text{и} \quad x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

то линейную комбинацию можно записать как vx . Если $w \in V$ – некоторый вектор, то тот факт, что он линейно выражается через v_i тогда записывается так $w = vx$ для некоторого $x \in F^n$. Пусть теперь у нас есть несколько векторов $w_1, \dots, w_m \in V$ и каждый из них выражается через вектора v_1, \dots, v_n , тогда

$$w_1 = (v_1 \quad v_2 \quad \dots \quad v_n) A_1, \dots, w_m = (v_1 \quad v_2 \quad \dots \quad v_n) A_m$$

где $A_i \in F^n$. Тогда составим из A_i матрицу $A \in M_{nm}(F)$ и получим запись

$$(w_1 \quad w_2 \quad \dots \quad w_m) = (v_1 \quad v_2 \quad \dots \quad v_n) A$$

6.6 Размерность

Наша задача сейчас показать, что в векторном пространстве любые два базиса имеют одинаковое количество элементов. Однако, обсуждать как сравнивать бесконечные множества между собой я не очень хочу, потому мы с этого момента ограничимся случаями конечных базисов. Для начала нам надо показать, что если векторное пространство имеет хотя бы один конечный базис, то все его базисы конечны и имеют одинаковое количество элементов.

Утверждение 56. Пусть V – некоторое векторное пространство над полем F и пусть $\{e_1, \dots, e_n\} \subseteq V$ – базис V . Тогда если $E \subseteq V$ – некоторый базис V , то $|E| = n$.

Доказательство. Нам достаточно показать, что $|E| \leq n$. Тогда базис E становится конечным и мы можем поменять местами два базиса и применить это же утверждение для доказательства обратного неравенства.

Предположим, что это не верно, тогда в E есть хотя бы $n + 1$ элемент v_1, \dots, v_{n+1} . Так как e_1, \dots, e_n – базис, то каждый v_i линейно выражается через этот базис. Значит можно найти матрицу $A \in M_{n, n+1}(F)$ такую, что

$$(v_1 \quad v_2 \quad \dots \quad v_{n+1}) = (e_1 \quad e_2 \quad \dots \quad e_n) A$$

Рассмотрим систему $Ax = 0$, где $x \in F^{n+1}$. В этой системе количество столбцов больше, чем количество строк. Значит обязательно существует ненулевое решение $x \in F^{n+1}$. Тогда умножим на него предыдущее равенство слева, получим

$$(v_1 \ v_2 \ \dots \ v_{n+1})x = (e_1 \ e_2 \ \dots \ e_n)Ax = 0$$

То есть мы нашли нетривиальную линейную комбинацию векторов v_1, \dots, v_{n+1} . Но по определению E в нем не должно быть линейно зависимых векторов, противоречие. \square

Пусть V – векторное пространство над полем F , тогда размерностью V называется число элементов в любом из его базисов.⁶⁶ Размерность V будем обозначать через $\dim V$ или $\dim_F V$, если надо подчеркнуть, какое поле F имеется в виду.

Утверждение 57. Пусть $U \subseteq V$ – подпространство в векторном пространстве над полем F . Тогда

1. $\dim U \leq \dim V$.
2. $\dim U = \dim V$ тогда и только тогда, когда $U = V$.

Доказательство. (1) В начале сделаем замечание. Пусть $E \subseteq V$ – какое-то линейно независимое подмножество V . Так как базис – это максимальное линейно независимое подмножество, то $|E| \leq \dim V$.

Пусть $E \subseteq U$ – базис U . Тогда E – линейно независимое подмножество U , а значит и V . Но тогда из замечания выше $|E| \leq \dim V$. А по определению $\dim U = |E|$.

(2) Теперь сделаем еще одно замечание. Пусть $E \subseteq V$ – некоторое линейно независимое подмножество V . Как понять, что оно максимальное? Достаточно, проверить, что в нем $\dim V$ элементов. Действительно, если бы при этом оно было не максимальным, то в максимальном было бы больше $\dim V$ элементов, что противоречит определению размерности.

Теперь пусть $E \subseteq U$ – базис U и пусть $\dim U = \dim V$. Мы хотим показать, что $U = V$. Тогда E – это линейно независимое подмножество в V и в нем $|E| = \dim U = \dim V$ элементов. Но тогда по замечанию выше оно является базисом в V . Так как E – базис в U , то $U = \langle E \rangle$, а так как E – базис в V , то $V = \langle E \rangle$, то есть $U = V$. Утверждение в обратную сторону очевидно. \square

6.7 Конкретные векторные пространства

Пусть V – векторное пространство над некоторым полем F . Вообще говоря, в этом случае элементы V могут быть чем угодно (функции, вектор-столбцы, матрицы, отображения и т.д.), но если в нем можно выбрать конечный базис, то оно автоматически превратится в пространство F^n . Сейчас я хочу обсудить все этапы этого магического превращения.

Пусть $e_1, \dots, e_n \in V$ – некоторый базис пространства V . Тогда можно рассмотреть отображение

$$\begin{aligned} F^n &\rightarrow V \\ x &\mapsto ex \end{aligned}$$

где $e = (e_1, \dots, e_n)$, $x \in F^n$. Так как e порождает V , то это отображение сюръективно. С другой стороны из линейной независимости следует инъективность: если $ex = ey$ для $x, y \in F^n$, то $e(x - y) = 0$, а значит $x - y = 0$. Таким образом мы получаем, что каждый вектор-столбец длины n однозначно соответствует некоторому вектору из V . Кроме того, если присмотреться внимательно, то мы увидим, что сложение столбцов соответствует сложению векторов и то же самое верно для умножения на скаляр. Таким образом, мы видим, что между этими пространствами нет никакой разницы. Изучать одно из них – это все равно, что изучать другое. По-другому, можно думать еще так: если вам дали произвольное конечномерное пространство, то всегда можно считать, что это F^n (для этого нужно всего лишь выбрать базис).

Координаты Если вектор $v \in V$ разложен по некоторому базису $e = (e_1, \dots, e_n)$ пространства V , то есть представлен в виде $v = ex$, где $x \in F^n$, то столбец $x = (x_1, \dots, x_n)$ называют координатами вектора v в базисе e_1, \dots, e_n .

⁶⁶Корректность этого определения следует из предыдущей леммы в случае существования хотя бы одного конечного базиса. Однако, если бы мы были знакомы с теорией мощности для произвольных множеств, то мы бы показали, что количество элементов в базисе не зависит от базиса всегда. Потому можно говорить о размерности даже для бесконечно мерных пространств. Например, размерность многочленов $F[x]$ счетная, а для бесконечного множества X размерность пространства F^X совпадает с $|F^X|$, то есть она зависит от мощности поля.

Смена базиса Так как базис в пространстве выбирается не единственным образом, то в конструкции выше у нас есть некоторая свобода. Давайте проследим, что и как меняется при замене одного базиса другим.

Утверждение 58. Пусть V – некоторое векторное пространство над полем F и пусть $e_1, \dots, e_n \in V$ – какой-нибудь базис этого пространства. Тогда

1. Для любой обратимой матрицы $C \in M_n(F)$ набор векторов $(e_1, \dots, e_n)C$ тоже является базисом.
2. Если $f_1, \dots, f_n \in V$ – любой другой базис V , то найдется единственная обратимая матрица $C \in M_n(F)$ такая, что $(f_1, \dots, f_n) = (e_1, \dots, e_n)C$.

Доказательство. (1) Заметим, что набор $(e_1, \dots, e_n)C$ является линейно независимым и состоит из $n = \dim V$ элементов, а значит автоматом максимальный линейно независимый набор. Для проверки линейной независимости рассмотрим линейную комбинацию $(e_1, \dots, e_n)Cx = 0$, где $x \in F^n$. Тогда $Cx = 0$ так как e_i базис. А следовательно $x = 0$, так как C обратима.

(2) Так как e_i – базис, то любой вектор однозначно раскладывается по этому базису, например, каждый f_i имеет представление $f_i = (e_1, \dots, e_n)C_i$, где $C_i \in F^n$. Тогда все эти равенства вместе можно записать так $(f_1, \dots, f_n) = (e_1, \dots, e_n)C$, где $C = (C_1 | \dots | C_n) \in M_n(F)$ – квадратная матрица составленная из столбцов C_i . То есть такая матрица найдется, а ее единственность следует из того, что любой вектор однозначно раскладывается по базису.

Теперь осталось доказать обратимость матрицы C . Применив, то же самое рассуждение но для базисов в обратном порядке, мы найдем матрицу $B \in M_n(F)$ такую, что $(e_1, \dots, e_n) = (f_1, \dots, f_n)B$. Тогда получаем

$$(e_1, \dots, e_n) = (f_1, \dots, f_n)B = (e_1, \dots, e_n)CB$$

А значит $(e_1, \dots, e_n)(E - CB) = 0$. Из линейной независимости базиса следует, что $E = CB$. Аналогично доказывается $BC = E$, то есть B является обратной к C , что и требовалось. \square

Если e_1, \dots, e_n и f_1, \dots, f_n – два базиса пространства V , то матрица $C \in M_n(F)$ такая, что $(f_1, \dots, f_n) = (e_1, \dots, e_n)C$ называется матрицей перехода от базиса e_i к базису f_i . Таким образом у нас есть, вообще говоря бесконечный, граф с вершинами пронумерованными базисами пространства V , а ребра соответствуют матрицам перехода C от базиса e_i к базису f_i , если $(f_1, \dots, f_n) = (e_1, \dots, e_n)C$. Предыдущее утверждение говорит, что этот граф связный и между любыми двумя вершинами есть ровно одно ребро.⁶⁷

Смена координат Пусть теперь у нас $v \in V$ – некоторый вектор. Тогда мы его можем разложить по одному базису $v = ex$ с координатами $x \in F^n$ и по другому базису $v = fy$ с координатами $y \in F^n$. Пусть C – матрица перехода от базиса e к базису f , то есть $f = eC$. Тогда координаты x в старом базисе e связаны с новыми координатами в базисе f следующим образом: $x = Cy$. Действительно, с одной стороны $v = ex$, а с другой $v = fy = eCy$. Но так как разложение по базису однозначно, получаем, что $x = Cy$. Запоминать это правило надо так: если от базиса e к базису f мы перешли с помощью умножения справа на матрицу C , то на координатах у нас отображение в обратную сторону с помощью умножения на матрицу C слева (то есть тоже с другой стороны). Еще полезно держать перед глазами вот эту таблицу.

базис	новый \xleftarrow{C} старый
координаты	новые \xrightarrow{C} старые

6.8 Подпространства в F^n

Давайте посмотрим как можно задавать подпространства в F^n . Существует два способа

Явный	Неявный
Если $v_1, \dots, v_k \in V$, тогда $U = \langle v_1, \dots, v_k \rangle$	Если $A \in M_{m \times n}(F)$, тогда $U = \{y \in F^n \mid Ay = 0\}$

По-хорошему, хочется научиться пересчитывать векторное пространство заданное в одной из этих форм в другую. Мы разберем пока только одну из этих задач. А именно, пусть подпространство задано неявно в виде системы, то как найти его базис?

Если подпространство $U \subseteq F^n$ задано в виде $U = \{y \in F^n \mid Ay = 0\}$ для некоторой матрицы $A \in M_{m \times n}(F)$, то любой базис пространства U будем называть фундаментальной системой решений (ФСР). Ниже мы разберем задачу построения какого-нибудь ФСР для однородной системы линейных уравнений.

⁶⁷Кстати между вершиной и ей самой тоже есть ребро-петля, соответствующая единичной матрице.

Нахождение ФСР однородной СЛУ В начале мы приведем алгоритм находящий ФСР, а потом объясним почему он работает.

Дано Система однородных линейных уравнений $Ax = 0$, где $A \in M_{m \times n}(F)$ и $x \in F^n$.

Задача Найти ФСР системы $Ax = 0$.

Алгоритм

1. Привести матрицу A элементарными преобразованиями строк к улучшенному ступенчатому виду. Например

$$A' = \begin{pmatrix} 1 & 0 & a_{31} & 0 & a_{51} \\ 0 & 1 & a_{32} & 0 & a_{52} \\ 0 & 0 & 0 & 1 & a_{53} \end{pmatrix}$$

2. Пусть k_1, \dots, k_r – позиции свободных переменных. Если положить одну из этих переменных равной 1, а все остальные нулями, то существует единственное решение, которое мы обозначим через u_i (всего r штук). Например, для матрицы A' выше свободные переменные имеют номера 3 и 5. Тогда вектора (записанные в строку)

$$u_1 = (-a_{31} \quad -a_{32} \quad 1 \quad 0 \quad 0), u_2 = (-a_{51} \quad -a_{52} \quad 0 \quad -a_{53} \quad 1)$$

являются ФСР.

Доказательство корректности алгоритма поиска ФСР. Пусть в общем виде, ступенчатый вид матрицы A выглядит так

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

Тогда построенные вектора имеют вид

$$\begin{array}{ccccccccc} & & k_1 & & k_2 & & \dots & \dots & k_r \\ u_1 & (* & 1 & 0 & 0 & 0 & 0 & 0 & 0) \\ u_2 & (* & 0 & * & 1 & 0 & 0 & 0 & 0) \\ \vdots & (* & 0 & * & 0 & * & 1 & 0 & 0) \\ \vdots & (* & 0 & * & 0 & * & 0 & 1 & 0) \\ u_r & (* & 0 & * & 0 & * & 0 & 0 & 1) \end{array}$$

В начале проверим, что u_i линейно независимы. Действительно, тогда линейная комбинация $\alpha_1 u_1 + \dots + \alpha_r u_r$ имеет вид

$$(* \quad \alpha_1 \quad * \quad \alpha_2 \quad * \quad \dots \quad \dots \quad * \quad \alpha_r)$$

Если эта линейная комбинация равна нулю, то значит и все α_i равны нулю.

Теперь пусть v – произвольное решение системы $Ax = 0$. Посмотрим на его координаты в свободных позициях

$$(* \quad v_1 \quad * \quad v_2 \quad * \quad \dots \quad \dots \quad * \quad v_r)$$

Теперь рассмотрим вектор $w = v - v_1 u_1 - \dots - v_r u_r$. С одной стороны это решение системы $Ax = 0$. С другой стороны у этого решения все свободные переменные равны нулю. А значит автоматически и все главные переменные равны нулю, что означает, что $w = 0$. То есть $v = v_1 u_1 + \dots + v_r u_r$, что и требовалось. \square

Замечание

- Обратите внимание, что ФСР – это любой базис в пространстве $\{y \in F^n \mid Ay = 0\}$, а не только тот, который построен по алгоритму.
- В алгоритме выше, мы могли бы вместо 1 и 0 расставить любой набор из r линейно независимых векторов длины r в позиции со свободными переменными. Это тоже дало бы базис. Однако, у построенного ФСР именно по алгоритму выше есть одно важное преимущество: в нем легко считать координаты. Действительно, для любого вектора из пространства решений его свободные переменные – это и есть координаты в построенном базисе.