Разбор билетов. Алгебра

(SE) Основная теорема арифметики. Малая теорема Ферма, функция Эйлера. Мультипликативность функции Эйлера. Теорема Эйлера.

Основная теорема арифметики.

Лемма. Если $x \cdot y$ делится на простое число p, то p делит x или y.

◀ Пусть x не делится на p, тогда найдутся числа u, v такие, что

$$xu + pv = 1.$$

Домножим обе части на y: $(xy)u + ypv = y$. Оба слагаемых в левой части делятся на p, поэтому y делится на p. Существование такой пары чисел u, v можно доказать с помощью алгоритма Евклида. ▶

Теорема. Основная теорема арифметики. Каждое натуральное число $n > 1$ представляется в виде $n = p_1 p_2 ... p_k$, где p_i — простое число. Такое представление единственно с точностью до порядка следования сомножителей.

◀ **Существование.** Пусть $n > 1$ — наименьшее число, неразложимое на простые множители. Тогда n не может быть простым, так как простое число очевидным образом раскладывается на простые. Если n — составное, то оно является произведением двух меньших натуральных чисел, каждое из которых можно разложить на простые множители. Тогда n можно представить как произведение всех простых. Противоречие.

Единственность. Пусть n — наименьшее натуральное число, допускающее два разных разложения на простые множители:

$$n = p_1 p_2 ... p_k = q_1 q_2 ... q_l.$$

Если множитель p_1 есть среди множества $\{q_1, ..., q_k\}$, то их можно сократить, тогда получим разные разложения меньшего числа. Противоречие. Если p_1 нет среди множителей $\{q_1, ..., q_k\}$, то левая часть не делится на p_1 по доказанной лемме. Противоречие. ▶

Функция Эйлера.

Определение. *Функция Эйлера* $\varphi(n)$ определяется как количество натуральных чисел, не превосходящих n и взаимно простых с n.

Формула для функции Эйлера.

Теорема. Функция Эйлера мультипликативна, то есть для любых двух взаимно простых чисел m, n выполняется соотношение $\varphi(nm) = \varphi(n)\varphi(m)$.

◀ Запишем $n \cdot m$ натуральных чисел в таблицу с n столбцами и m строками (см. ниже).

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{vmatrix}$$

Число, находящееся на месте (i, j) можно представить как $x = n(i - 1) + j$. Если x взаимно просто с n, то j взаимно просто с n. Значит весь столбец j взаимно прост с n. Так как внутри столбца остаток не меняется, то разные остатки при делении на n соответствуют разным столбцам, значит взаимно простых с n столбцов в таблице ровно $\varphi(n)$.

Числа внутри каждого столбца образуют геометрическую прогрессию с разностью $d = n$: $a,\ a + n,\ a + 2n,\ ...,\ a + (m - 1)n$. Если числа из одного столбца в строках k, l дают одинаковые остатки при делении на m, то $(k - l)n$ делится на m, при условии $(n, m) = 1$ это возможно только при $k = l$. Значит, числа в одном столбце образуют полную систему остатков по m. Таким образом, в каждом столбце ровно $\varphi(n)$ взаимно простых с m чисел. Следовательно, среди первых $n \cdot m$ чисел ровно $\varphi(n)\varphi(m)$ взаимно просты с $n \cdot m$. ▶

Теорема Эйлера. Пусть n и a — взаимно простые, тогда

$$a^{\varphi(n)} \equiv 1 \ (mod\ n).$$

Отношение сравнимости по модулю n — это отношение эквивалентности. Класс эквивалентности, содержащий число a называется *вычетом числа a по модулю n* и обозначается $[a]_n$. Вычет $[x]_n$ называется обратимым, если существует $[y]_n$ такой, что $[x]_n[y]_n \equiv 1 \ (mod\ n)$. Решение уравнения $[x]_n[y]_n - 1 = mn$ существует только при $(n, x) = 1$. Тогда у числа n ровно $\varphi(n)$ обратимых вычетов.

◀ Достаточно доказать теорему Эйлера только для вычетов. Рассмотрим вычеты по модулю n. Если $(a, n) = 1$, то вычет $[a]$ обратим. Пусть $[b_1], ..., [b_{\varphi(n)}]$ — все обратимые вычеты по модулю n. Тогда вычет $[b] = [b_1 \cdot ... \cdot b_{\varphi(k)}]$ тоже обратим. Тогда $[ab_1][ab_2]...[ab_{\varphi(n)}] = a^{\varphi(n)}[b] = [b]$, так как умножение всех вычетов $[b_i]$ на a просто меняет их порядок. Домножим обе части на $[b]^{-1}$, получим требуемое равенство $a^{\varphi(n)} \equiv 1$. ▶

Малая теорема Ферма после теоремы Эйлера доказывается легко. Очевидно, что $\varphi(p) = p - 1$ для любого простого p. Тогда для взаимно простых a и p справедливо соотношение $a^{\varphi(p)} \equiv 1 \ (mod\ p) \Rightarrow$

$$a^{p-1} \equiv 1 \ (mod\ p).$$

(YA, SE) Понятие линейного пространства (ЛП). Линейная зависимость и независимость. Базис и размерность ЛП, их связь. Координаты элемента ЛП в базисе. Замена базиса, матрица перехода, преобразование координат при замене базиса.

Определение. Пусть $\Re$ — произвольное поле. Векторным (или линейным) пространством над $\Re$ называется множество V, элементов (векторов), удовлетворяющее следующим аксиомам:

а) На V задана бинарная операция $V \times V \to V$, наделяющая V строением абелевой группы. Стало быть:

1. $x + y = y + x$ (*коммутативность*);
2. $(x + y) + z = x + (y + z)$ (*ассоциативность*);
3. в V существует *нулевой* вектор 0 такой, что $x + 0 = x$ для любого $x \in V$;
4. для каждого вектора x из V существует *обратный* $-x$ такой, что $x + (-x) = 0$;

б) На множестве $\Re \times V$ задано умножение векторов на скаляры из $\Re$ обладающее свойствами

1. $1 \cdot x = x$ (*унитарность*);
2. $(\alpha\beta)x = \alpha(\beta x)$ для всех $\alpha, \beta \in \Re$, и $x \in V$ (*ассоциативность*);
3. $(\alpha + \beta)x = \alpha x + \beta x$ (*дистрибутивность*);
4. $\alpha(x + y) = \alpha x + \alpha y$ (*дистрибутивность*).

Пусть имеется конечный набор скаляров $\lambda_1, ..., \lambda_n \in \Re$ и векторов $x_1, ..., x_n \in V$. Тогда выражение

$$\lambda_1 x_1 + ... + \lambda_n x_n = \sum_{i=1}^{n} \lambda_i x_i$$

называется *линейной комбинацией* векторов x_i с коэффициентами λ_i. При этом множество $\langle M \rangle_{\Re}$ всевозможных линейных комбинаций векторов $x_i \in M$ замкнуто относительно операций сложения векторов и умножения их на скаляры:

$$\lambda \in \Re,\ x, y \in \langle M \rangle \Rightarrow x + y \in \langle M \rangle,\ \lambda x \in \langle M \rangle.$$

Принято говорить, что $\langle M \rangle$ — *линейная оболочка* множества $M \subset V$.

Определение. Пусть V — векторное пространство над $\Re$, $U \subset V$ — его подмножество, являющееся аддитивной подгруппой V и переходящее в себя при умножении на скаляры. Тогда ограничение на U операций, определенных в V, наделяет U строением векторного пространства. Оно называется *векторным* (или *линейным*) *подпространством* в V.

Определение. Векторы $v_1, ..., v_n$ пространства V называются *линейно зависимыми*, если некоторая их нетривиальная линейная комбинация равна нулю, то есть найдутся такие скаляры $\alpha_1, ..., \alpha_n$, не все равные нулю, что

$$\alpha_1 v_1 + ... + \alpha_n v_n = 0.$$

В противном случае система векторов называется *линейно независимой*.

Определение. Число векторов, содержащихся в любой максимальной (не допускающей расширения до линейно независимой системы системы из большего числа векторов) линейно независимой подсистеме данной системы векторов, называется *рангом* системы.

Определение. Линейное пространство V, в котором существует n линейно независимых векторов, но нет линейно независимых систем большего ранга, называется *n-мерным* ($\dim V = n$). Если такого числа n нет, то векторное пространство называется *бесконечномерным*. Пример бесконечномерного пространства — множество всех непрерывных функций. Из него всегда можно выделить бесконечное число линейно независимых векторов $1,\ x,\ x^2, ..., x^n, ...$

Определение. Пусть V — n-мерное векторное пространство над полем $\Re$. Любая система из n независимых векторов $e_1, ..., e_n \in V$ называется (конечным линейным) *базисом* пространства V.

Теорема. Пусть V — векторное пространство над полем $\Re$ с базисом $(e_1, ..., e_n)$ тогда имеют место следующие утверждения:

1. каждый вектор $v \in V$ можно представить, и притом единственным образом, в виде линейно комбинации векторов $e_1, ..., e_n$;

2. всякую систему из $s \leq n$ линейно независимых векторов можно дополнить до базиса.

◀ 1) Присоединим к базису вектор v. По определению базиса система из векторов $(v, e_1, ..., e_n)$ линейно зависима, поэтому найдутся скаляры λ_i, $\lambda_0 \neq 0$ такие, что

$$\lambda_0 v + \lambda_1 e_1 + ... + \lambda_n e_n = 0,$$

тогда

$$v = (-\frac{\lambda_1}{\lambda_0})e_1 + ... + (-\frac{\lambda_n}{\lambda_0})e_n.$$

Если вектор v допускает два разложения по базису, то

$$\alpha_1 e_1 + ... + \alpha_n e_n = v = \beta_1 e_1 + ... + \beta_n e_n,$$

значит

$$(\alpha_1 - \beta_1)e_1 + ... + (\alpha_n - \beta_n)e_n = 0,$$

что по определению базиса возможно лишь при $\alpha_i = \beta_i$.

2) Пусть $f_1, ..., f_s$ — система линейно независимых векторов. Рассмотрим систему $f_1, ..., f_s, e_1, ..., e_n$. Удалим из нее все векторы, которые выражаются через предыдущие. Тогда по условию все векторы f_i останутся. Получаем

$$f_1, ..., f_s, e_{i_1}, ..., e_{i_t}.$$

Если теперь

$$\alpha_1 f_1 + ... + \alpha_s f_s + \beta_1 e_{i_1} + ... + \beta_t e_{i_t} = 0,$$

то существовал бы $\beta_k \neq 0$ с наибольшим номером k, значит e_{i_k} можно выразить через предыдущие, что исключено по построению. Значит такая система линейно независима. Очевидно, что через нее выражается любой вектор. Значит она максимальна, следовательно $f_1, ..., e_{i_k}$ образуют базис. ▶

В силу теоремы о единственности разложения вектора ЛП по базису имеет место следующее

Определение. Пусть $(e_1, ..., e_n)$ — базис векторного пространства V над $\Re$. Скаляры $\lambda_1, ..., \lambda_n \in \Re$, входящие в разложение

$$v = \lambda_1 e_1 + ... + \lambda_n e_n$$

называются *координатами* вектора $v \in V$ в данном базисе.

Если $x = \alpha_1 e_1 + ... + \alpha_n e_n$, $y = \beta_1 e_1 + ... + \beta_n e_n$, то $x + y = (\alpha_1 + \beta_1)e_1 + ... + (\alpha_n + \beta_n)e_n$ (коммутативность + дистрибутивность). При этом $\lambda x = \lambda(\alpha_1 e_1 + ... + \alpha_n e_n) \Rightarrow$ (дистрибутивность) $\Rightarrow \lambda x = \lambda\alpha_1 e_1 + ... + \lambda_n \alpha_n e_n$.

Замена базиса.

Пусть V — линейное пространство и $(e_1, ..., e_n)$, $(e'_1, ..., e'_n)$ — его базисы. Векторы одного базиса выражаются через векторы другого:

$$\begin{cases} e'_1 = a_{11}e_1 + a_{21}e_2 + ... + a_{n1}e_n \\ \dots \\ e'_n = a_{1n}e_1 + a_{2n}e_2 + ... + a_{nn}e_n. \end{cases}$$

Коэффициенты $a_{ij} \in \Re$ определяют матрицу

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}.$$

Важно! Координаты вектора e'_j составляют j-ый **столбец** матрицы A. Матрица A называется *матрицей перехода от базиса* $(e_1, ..., e_n)$ *к базису* $(e'_1, ..., e'_n)$.

Если вектор v задан в старом базисе координатами $[\lambda_1, ..., \lambda_n]$, то есть

$$v = \lambda_1 e_1 + ... + \lambda_n e_n,$$

то можно выразить его координаты через новый базис. Для этого нужно решить уравнение

$$X = AX'. \tag{1}$$

Здесь $X = [\lambda_1, ..., \lambda_n]$ — координаты вектора в старом базисе, A — матрица перехода от старого базиса к новому, $X' = [\lambda'_1, ..., \lambda'_n]$ — координаты вектора в новом базисе.

Данное уравнение не сложно получить, заменив старые базисные векторы на новые

$$v = \lambda_1'(a_{11}e_1 + ... + a_{n1}e_n) + ... + \lambda_n'(a_{1n}e_1 + ... + a_{nn}e_n) = \lambda_1 e_1 + ... + \lambda_n e_n.$$

Уравнение (1) можно переписать в виде $A^{-1}X = X'$. Итак, справедлива

Теорема. При переходе от базиса $(e_1, ..., e_n)$ пространства V к базису $(e_1', ..., e_n')$, определяемом матрицей A, координаты вектора в **новом** базисе выражаются через **старые** координаты при помощи обратимого линейного преобразования с матрицей A^{-1}.

Важно отметить, что старые координаты выражаются через новые естественным образом (зная X' легко получить X), в то время как получение новых координат через старые требует трудоемкой операции обращения матрицы перехода.

(SE) Системы линейных алгебраических уравнений. Теорема Кронекера-Капелли. Общее решение системы алгебраических уравнений.

В векторном пространстве $\mathbb{R}^m$ рассмотрим n векторов

$$A^{(j)} = [a_{1j}, a_{2j}, ..., a_{mj}], \quad j = 1, 2, ..., n,$$

и их линейную оболочку $V = \langle A^{(1)}, ..., A^{(n)} \rangle$. Пусть дан еще один вектор $B = [b_1, ..., b_m]$. Спрашивается, принадлежит ли B линейной оболочке $V \subset \mathbb{R}^m$, а если принадлежит, то как его координаты выражаются через координаты векторов $A^{(j)}$?

Для этого составим уравнение с произвольными коэффициентами x_j :

$$x_1 A^{(1)} + ... + x_n A^{(n)} = B,$$

данное уравнение лишь иная запись системы из m линейных уравнений с n неизвестными

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n = b_2, \\ ... \\ a_{n1}x_1 + a_{n2}x_2 + ... + a_{nn}x_n = b_n. \end{cases} \tag{1}$$

Ранг матрицы

Определение. *Пространство столбцов матрицы* $A_{m\times n}$ — это линейная оболочка векторов, натянутая на векторы-столбцы: $V_{\text{в}} = \langle A^{(1)}, ..., A^{(n)}\rangle$.

Пространство строк матрицы — это линейная оболочка, натянутая на векторы-строки матрицы $V_{\text{г}} = \langle A_{(1)}, ..., A_{(m)}\rangle$.

Определение. Если $\{X_1, X_2, ...\}$ — какая-то, возможно, бесконечная, система векторов в пространстве $\mathbb{R}^n$, то ее *рангом* называют размерность линейной оболочки $\langle X_1, X_2, ...\rangle$:

$$\operatorname{rank}\{X_1, X_2, ...\} = \dim\langle X_1, X_2, ...\rangle.$$

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

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

Замечание. Применение элементарных преобразований не меняет ранги систем столбцов и строк матрицы.

Теорема. Для любой прямоугольной $m \times n$-матрицы A справедливо равенство $\operatorname{rank}_{\text{в}}(A) = \operatorname{rank}_{\text{г}}(A)$. Это число называется рангом матрицы A и обозначается rank A.

◀ Любую матрицу A' можно привести к ступенчатому виду A конечным числом элементарных преобразований.

$$A = \begin{pmatrix} a_{11} & ... & a_{1k} & ... & a_{1l} & ... & a_{1s} & ... & a_{1n} \\ 0 & ... & a_{2k} & ... & a_{2l} & ... & a_{2s} & ... & a_{2n} \\ 0 & ... & 0 & ... & a_{3l} & ... & a_{3s} & ... & a_{3n} \\ & & & & & & & & \\ 0 & ... & 0 & ... & 0 & ... & a_{rs} & ... & a_{rn} \\ 0 & ... & 0 & ... & 0 & ... & 0 & ... & 0 \\ & & & & & & & & \\ 0 & ... & 0 & ... & 0 & ... & 0 & ... & 0 \end{pmatrix}.$$

Важно! Ни один из элементов матрицы вида $a_{11}, a_{2k}, ..., a_{rs}$ не равен 0 по построению.

Так как элементарные преобразования не меняют рангов систем строк и столбцов, то достаточно доказать утверждение для матрицы ступенчатого вида.

Предположим наличие соотношения

$$\lambda_1 A^{(1)} + \lambda_k A^{(k)} + \lambda_l A^{(l)} ... + \lambda_s A^{(s)} = 0,$$

получаем $\lambda_s = 0 \Rightarrow \lambda_l = 0 \Rightarrow ... \Rightarrow \lambda_1 = 0$. Таким образом,

$$\dim\langle A^{(1)}, ..., A^{(n)}\rangle \geq \dim\langle A^{(1)}, A^{(k)}, ..., A^{(s)}\rangle = r.$$

При этом пространство $V_{\text{в}}$ отождествляется с пространством столбцов матрицы A, из которой удалили последние нулевые строки. Значит,

$$\dim\langle A^{(1)}, ..., A^{(n)}\rangle \leq \mathbb{R}^r = r.$$

Заметим, что все ненулевые строки матрицы A линейно независимы. Действительно, если

$$\lambda_1 A_{(1)} + ... + \lambda_r A_{(r)} = 0,$$

то $\lambda_1 a_{11} = 0 \Rightarrow \lambda_1 = 0 \Rightarrow \lambda_2 = ... = \lambda_r = 0$. Значит, $\dim\langle A_{(1)}, ..., A_{(r)}\rangle = r$. Стало быть $\operatorname{rank}_{\text{в}}(A) = \operatorname{rank}_{\text{г}}(A) = r$.▶

Критерий совместности.

Определение. Система линейных уравнений называется *совместной*, если у нее существует решение. В противном случае система называется *несовместной*.

Теорема (Кронекер-Капелли). Система линейных уравнений совместна тогда и только тогда, когда ранг ее матрицы совпадает с рангом расширенной матрицы.

◀ Вопрос существования решения системы можно трактовать как определение принадлежности вектора B линейной оболочке векторов $\langle A^{(1)}, ..., A^{(n)}\rangle$. Если вектор B можно представить в виде линейной комбинации векторов-столбцов, то

$$\operatorname{rank}\{A^{(1)}, ..., A^{(n)}\} = \operatorname{rank}\{A^{(1)}, ..., A^{(n)}, B\},$$

значит

$$\operatorname{rank} A = \operatorname{rank}_{\text{в}}(A) = \operatorname{rank}_{\text{в}}(A|B) = \operatorname{rank}\,(A|B).$$

Пусть теперь rank $A = \text{rank }(A|B) = r$. Значит среди столбцов матрицы A можно выделить r линейно независимых векторов $\{A^{(j_1)}, ..., A^{(j_r)}\}$. Добавление вектора B не изменяет размерность линейной оболочки, поэтому его можно выразить через базисные векторы $A^{(j)}$. ▶

Количество решений системы линейных уравнений.

Рассмотрим произвольную ступенчатую систему линейных уравнений. Пусть число ненулевых строк ее матрицы коэффициентов равно r, а число ненулевых строк расширенной матрицы равно $\overline{r}$. Очевидно, что $\overline{r} = r$ или $\overline{r} = r + 1$. Возможны три принципиально разных случая:

1. $\overline{r} = r + 1$. Тогда в системе есть строка вида

$$0 \cdot x_1 + ... + 0 \cdot x_n = b \neq 0.$$

   В этом случае система несовместна.

2. $\overline{r} = r = n$. В этом случае после отбрасывания нулевых уравнений получается строго треугольная система. Из последнего уравнения однозначно определяется x_n, тогда, подставляя его в предпоследнее уравнение, получаем x_{n-1} и т.д. Следовательно, система имеет единственное решение.

3. $r = \overline{r} < n$. Пусть в этом случае $j_1, ..., j_r$ — номера ведущих коэффициентов ненулевых уравнений системы. Неизвестные $x_{j_1}, ..., x_{j_r}$ назовем *главными*, а остальные — *свободными*. Выражаем главные неизвестные через свободные и получаем **общее решение** системы. Все решения системы получаются из общего подстановкой каких-то значений свободных неизвестных.

Определение. Совместная система линейных уравнений называется *определенной*, если она имеет единственное решение. В противном случае она называется *неопределенной*.

Теорема. Критерий единственности решения системы линейных уравнений. Система линейных уравнений имеет единственное решение тогда и только тогда, когда ранг основной матрицы равен рангу расширенной матрицы и равен числу переменных, то есть

$$\text{rank } A = \text{rank }(A|B) = n.$$

Теорема. 1) Совокупность всех решений системы однородных линейных уравнений с n неизвестными является подпространством пространства $\Re^n$.

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

◀ 1) Очевидно, что нулевая строка является решением системы однородных линейных уравнений. Пусть теперь строки $(u_1, ..., u_n)$, $(v_1, ..., v_n)$ являются ее решениями, тогда $a_{i1}(u_1 + v_1) + ... + a_{in}(u_n + v_n) = a_{i1}u_1 + a_{i1}v_1 + ... + a_{in}u_n + a_{in}v_n = 0 + 0 = 0$. Здесь $a_{i1}, ..., a_{in}$ — коэффициенты i-ой строки системы.

2) Пусть теперь $u \in \Re^n$ — фиксированное решение системы (1), тогда если $u_0 \in \Re$ — решение соответствующей системы однородных уравнений, то $u + u_0$ — решение системы (1). Пусть теперь u' — любое решение системы (1). Тогда $u' - u$ решение системы однородных уравнений, но $u' = u + (u' - u)$, значит u' получен из u и решения системы однородных уравнений. ▶

(YA, SE) Матрицы. Транспонированная матрица. Обратная матрица. Ранг матрицы, ранг произведения матриц, ранг транспонированной матрицы. Специальные виды матриц. Линейные и нелинейные операции над матрицами: сложение, умножение матрицы на число, умножение матриц, транспонирование матриц. Их свойства. Определитель матрицы. Определитель произведения.

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

Суммой матриц $A = (a_{ij})$, $B = (b_{ij})$ одинакового размера называется матрица

$$A + B = (a_{ij} + b_{ij}).$$

Произведением матрицы $A = (a_{ij})$ на элемент $\lambda \in K$ называется матрица

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

Относительно этих двух операций все матрицы размера $m \times n$ образуют векторное пространство, которое далее будет обозначаться $K^{m\times n}$.

Произведением матрицы $A = (a_{ij})$ размера $m\times n$ на матрицу $B = (b_{ij})$ размера $n \times p$ называется матрица $AB = (c_{ij})$ размера $m \times p$, элементы которой находятся по формуле

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

Замечение. На данный момент от элементов матрицы требовалась лишь принадлежность кольцу.

Умножение матриц *ассоциативно*:

$$(AB)C = A(BC),$$

если только размеры матриц A, B, C согласованы таким образом, что указанные произведения имеют смысл.

Определение. Матрица размера $n\times n$ называется *квадратной матрицей порядка n*.

Квадратная матрица имеет *главную* и *побочную диагональ*.

Квадратная матрица называется *диагональной*, если все элементы вне ее главной диагонали равны нулю.

Диагональная матрица, все ненулевые элементы которой равны единице называется *единичной* матрицей.

Следующие свойства связывают операцию умножения матриц с другими операциями:

$$A(B+C) = AB+AC, \quad (A+B)C = AC+BC, \quad (\lambda A)B = A(\lambda B) = \lambda(AB).$$

Перечисленные свойства показывают, что все квадратные матрицы порядка n образуют ассоциативную алгебру с единицей: $L_n(K)$.

Некоторые отрицательные свойства алгебры $L_n(K)$:

1. Алгебра $L_n(K)$ не коммутативна. То есть, вообще говоря,

$$AB \neq BA, \quad A, B \in L_n(K).$$

2. Алгебра $L_n(K)$ имеет делители нуля:

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

3. Не всякий ненулевой элемент алгебры $L_n(K)$ обратим. Пусть $AB = 0$, $A, B \neq 0$ и $\exists A^{-1}:\ A^{-1}A = 1$, тогда

$$B = 1 \cdot B = A^{-1}AB = A^{-1} \cdot 0 = 0.$$

Матрицы и отображения

Пусть $\mathbb{R}^n$, $\mathbb{R}^m$ — векторные пространства. Пусть далее $A = (a_{ij})$ — матрица размера $m \times n$. Определим отображение $\varphi_A : \mathbb{R}^n \to \mathbb{R}^m$, полагая для любого $X = [x_1, ..., x_n] \in \mathbb{R}^n$

$$\varphi_A(X) = x_1 A^{(1)} + x_2 A^{(2)} + ... + x_n A^{(n)}. \tag{1}$$

Результатом такой операции будет вектор столбец $Y = [y_1, ..., y_m]$. Более подробно (1) переписывается в виде

$$y_i = \sum_{k=1}^{n} a_{ik} x_k.$$

Несложно проверить, что если X', $X'' \in \mathbb{R}^n$, $\lambda \in \mathbb{R}$, то

1. $\varphi_A(X' + X'') = \varphi_A(X') + \varphi_A(X'')$;
2. $\varphi_A(\lambda X) = \lambda \varphi(X)$.

Обратно, предположим, что $\varphi : \mathbb{R}^n \to \mathbb{R}^m$ — отображение множеств, обладающее следующими свойствами:

1. $\varphi(X' + X'') = \varphi(X') + \varphi(X'')$ для всех $X', X'' \in \mathbb{R}^n$;
2. $\varphi(\lambda X) = \lambda \varphi(X)$ для всех $\lambda \in \mathbb{R}$, $X \in \mathbb{R}^n$.

Известно, что $\mathbb{R}^n = \langle E^{(1)}, ..., E^{(n)} \rangle$, тогда $\mathbb{R}^n \ni X = [x_1, ..., x_n] \Rightarrow$

$$X = \sum_{i=1}^{n} x_i E^{(i)}.$$

Используем свойства 1, 2 и получим

$$\varphi(X) = \varphi(x_1 E^{(1)} + ... + x_n E^{(n)}) = \varphi(x_1 E^{(1)}) + ... + \varphi(x_n E^{(n)}) =$$

$$= x_1 \varphi(E^{(1)}) + ... + x_n \varphi(E^{(n)}). \tag{2}$$

Таким образом, отображение φ_A полностью определяется своими значениями на базисных столбцах.

Пусть теперь отображение φ переводит каждый столбец $E^{(i)} \in \mathbb{R}^n$ в столбец $A^{(i)} \in \mathbb{R}^m$:

$$\varphi_A(E^{(i)}) = [a_{1i}, a_{2i}, ..., a_{ni}] = A^{(i)} \in \mathbb{R}^m.$$

В таком случае задание φ равносильно заданию прямоугольной матрицы $A = (a_{ij})$ размера $m \times n$, где i-й столбец указывает, во что переходит вектор $E^{(i)}$. В таком случае формулы (1), (2) и свойства совпадают, поэтому можно положить $\varphi = \varphi_A$.

Определение. Отображение $\varphi = \varphi_A : \mathbb{R}^n \to \mathbb{R}^m$, обладающее свойствами 1,2 называется *линейным отображением* из $\mathbb{R}^n$ в $\mathbb{R}^m$. Матрица A называется *матрицей линейного отображения* φ_A.

Фактически доказана

Теорема. Между линейными отображениями $\mathbb{R}^n$ в $\mathbb{R}^m$ и матрицами размера $n \times m$ существует взаимно однозначное соответствие.

Отметим важные свойства линейных отображений:

1. Если φ_A, $\varphi_B : \mathbb{R}^n \to \mathbb{R}^m$, α, $\beta \in \mathbb{R}$, то

$$\varphi = \alpha\varphi_A + \beta\varphi_B : \mathbb{R}^n \to \mathbb{R}^m.$$

2. Произведение $\varphi_A\varphi_B$ двух линейных отображений с матрицами A и B является линейным отображением с матрицей $C = AB$. Другими словами,

$$\varphi_A\varphi_B = \varphi_{AB}.$$

Транспонирование матриц

Определение. Будем говорить, что матрицы

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

размеров $m \times n$ и $n \times m$ соответственно получаются друг из друга *транспонированием* — заменой строк на столбцы, а столбцов на строки.

Видно, что

$$^t(^tA) = A, \quad ^t(A+B) = {}^tA + {}^tB, \quad ^t(\lambda A) = \lambda^t A.$$

Простая проверка показывает, что

$$^t(AB) =^t B \cdot {}^tA.$$

Утверждение о том, что $\text{rank}_{\text{в}}A = \text{rank}_{\text{г}}A$ доказывает, что

$$\text{rank}A = \text{rank}^t A.$$

Ранг матрицы смотри в билете выше.

Теорема. Пусть A, B — произвольные матрицы размеров $m\times s$, $s\times n$. Тогда справедливо неравенство

$$\text{rank}(AB) \leq \min\{\text{rank}A, \text{rank}B\}.$$

◀ Имеем

$$C_{(i)} = A_{(i)}B, \quad C^{(i)} = AB^{(i)}.$$

Пусть $r_1 = \text{rank}A = \dim\langle A_{(1)}, ..., A_{(m)}\rangle$ и пусть строки $A_1, A_2, ..., A_{r_1}$ будут базисными, поскольку перестановка строк матрицы A точно так же переставит строки матрицы C, но перестановка строк на ранг не влияет. Теперь

$$A_{(k)} = \sum_{i=1}^{r_1} \lambda_i A_i, \quad r_1 \leq k \leq m,$$

то есть остальные строки с номерами $r_1+1, ..., m$ линейно выражаются через первые r_1 базисных строк. Воспользуемся тем, что $C_{(i)} = A_{(i)}B$, получим

$$C_{(k)} = A_{(k)}B = \left(\sum_{i=1}^{r_1} \lambda_i A_{(i)}\right) B.$$

Раскроем скобки, используя дистрибутивность и свойство умножения матриц на число

$$\left(\sum_{i=1}^{r_1} \lambda_i A_{(i)}\right) B = \sum_{i=1}^{r_1} (\left(\lambda_i A_{(i)}\right) B) = \sum_{i=1}^{r_1} \lambda_i \left(A_{(i)}B\right) = \sum_{i=1}^{r_1} \lambda_i C_{(i)}.$$

Таким образом, мы показали, что

$$C_{(k)} = \sum_{i=1}^{r_1} \lambda_i C_{(i)}, \quad r_1 \leq k \leq m.$$

Это значит, что если все строки матрицы A линейно выражаются через первые r_1 строк, то и строки матрицы C линейно выражаются через первые r_1 ее строки. Значит rank $C \leq$ rank A. Аналогично доказывается, что если все столбцы матрицы B линейно выражаются через первые r_2 столбца, то и столбцы матрицы C линейно выражаются через первые r_2 ее столбцов. Получаем, что rank $C \leq$ rank B ▶

Обратная матрица

Определение. Если для матрицы A из кольца $L_n(\mathbb{R})$ квадратных матриц порядка n существует матрица A' такая, что $AA' = E = A'A$, то матрица A' называется *обратной* к A (обозначение A^{-1}). Матрица A при этом называется *обратимой*.

Замечание. Если $A'A = AA'' = E$, то

$$A'' = EA'' = (A'A)A'' = A'(AA'') = A'E = A. \qquad (\bigstar)$$

Таким образом, если матрица $A' = A^{-1}$ существует, то она единственна.

Определение. Матрица $A \in L_n(\mathbb{R})$ называется невырожденной, если $\text{rank}(A) = n$, иначе матрица A называется вырожденной.

Теорема. Матрица $A \in L_n(\mathbb{R})$ обратима тогда и только тогда, когда A невырожденна.

◀ 1) Пусть матрица A вырождена. Заметим, что

$$n = \text{rank}(E) = \text{rank}(AA^{-1}) \leq \min\{\text{rank}(A), \text{rank}(A^{-1})\} \leq \text{rank}(A) < n.$$

Получаем противоречие.

2) Если $\text{rank}(A) = n$, то

$$\langle E^{(1)}, ..., E^{(n)} \rangle = \mathbb{R}^n = \langle A^{(1)}, ..., A^{(n)} \rangle.$$

Значит любой вектор $E^{(i)}$ линейно выражается через столбца матрицы A:

$$E^{(i)} = \sum_{k=1}^{n} b_{ki} A^{(i)}.$$

Нетрудно видеть, что матрица $B = (b_{ij})$ удовлетворяет условию $BA = E$.

По условию $\text{rank}(A) = n$, значит $\text{rank}(A^t) = n$. Поэтому найдется матрица C такая, что $CA^t = E$. Заметим, что $E = E^t = (CA^t)^t = (A^t)^t C^t = AC^t$. Имеем теперь

$$BA = E = AC^t.$$

При этом по (★) $B = C^t$. Таким образом, $B = A^{-1}$ ▶

Следствие 1 из теоремы. Если B — невырожденная квадратная матрица порядка m, A — произвольная $m \times n$-матрица, то $\text{rank}(BA) = \text{rank}A$.

◀ Известно, что $\text{rank}(BA) \le \min\{\text{rank}A, \text{rank}\ B\}$. Если $\text{rank}\ A \le \text{rank}\ B$, то $\text{rank}(BA) \le \text{rank}\ A$.

Пусть $\text{rank}\ A \ge \text{rank}\ B$, тогда

$$m = \text{rank}\ B \le \text{rank}\ A \le m,$$

так как ранг матрицы A не может превышать ее размеров. Следовательно, $\text{rank}(A) = m$, а значит

$$\text{rank}(BA) = \min\{m, m\} = m.$$

Таким образом, $\text{rank}(BA) \le \text{rank}\ A$.

Докажем теперь, что $\text{rank}\ A \le \text{rank}(BA)$. Действительно,

$$\text{rank}\ A = \text{rank}\ (B^{-1}B)A = \text{rank}\ B^{-1}(BA) \le$$

$$\le \min\{\text{rank}\ (BA),\ \text{rank}\ B^{-1}\} \le \text{rank}\ (BA) \ ▶$$

Следствие 2 из теоремы. Если $A, B, ..., C$ — невырожденные квадратные матрицы порядка n, то их произведение $AB...C$ невырожденно и

$$(AB...C)^{-1} = C^{-1} ... B^{-1}A^{-1}.$$

◀ Невырожденность произведения следует из следствия 1. Равенство $(AB...C)(C^{-1} ... B^{-1}A^{-1}) = E$ проверяется непосредственно исходя из ассоциативности умножения матриц ▶

Вычисление обратной матрицы требует порядка $O(n^3)$ операций. Пример того, как можно найти обратную матрицу приведен ниже.

Известно, что каждому элементарному преобразованию матриц соответствует специальная *элементарная матрица*. Так как любую невырожденную матрицу можно путем последовательного применения элементарных преобразований привести к единичной матрице, то с учетом того, что каждая элементарная матрица обратима, можно утверждать, что всякая невырожденная матрица записывается в виде произведения элементарных матриц. То есть если

$$P_k P_{k-1} ... P_1 A Q_1 Q_2 ... Q_l = E, \text{ то}$$

$$A = P_1^{-1} ... P_k^{-1} Q_l^{-1} ... Q_1^{-1}.$$

Здесь P_i, Q_j — некоторые элементарные матрицы.

Вычисление обратной матрицы

Пусть A — невырожденная квадратная матрица порядка n. Рассмотрим расширенную матрицу $(A|E)$. Возникает цепочка

$$(A|E) \xrightarrow{P_1} (P_1 A|P_1 E) \xrightarrow{P_2} ... \xrightarrow{P_k} (P_k ... P_1 A|P_k ... P_1 E) = (E|P_k ... P_1 E).$$

Матрица $P_k ... P_1$ по построению является обратной к A, то есть справа от черты получена матрица A^{-1}.

Пространство решений Пусть A — $m \times n$-матрица, X — вектор-столбец размера n. Необходимо решить уравнение

$$AX = B, \quad \text{где } B \in \mathbb{R}^m.$$

Обозначим через V_A *пространство решений* ЛОС $AX = 0$:

$$V_A = \langle X \in \mathbb{R}^n | AX = 0 \rangle \subset \mathbb{R}^n.$$

Теорема. rank $A = n - \dim V_A$.

◀ Пусть $s = \dim V_A$. Выберем базис $X^{(1)}, ..., X^{(s)}$ линейной оболочки V_A и дополним его до базиса $X^{(1)}, ..., X^{(s)}, X^{(s+1)}, ..., X^{(n)}$ всего пространства $\mathbb{R}^n$. Заметим, что $X^{(s+1)}, ..., X^{(n)}$ линейно независимы (как подмножество некоторого базиса). Рассмотрим произвольный вектор $X \in \mathbb{R}^n$. Заметим, что

$$AX = A\left(\sum_{i=1}^{n} \alpha_i X^{(i)}\right) = A\left(\sum_{i=1}^{s} \alpha_i X^{(i)}\right) + A\left(\sum_{i=s+1}^{n} \alpha_i X^{(i)}\right) =$$

$$= 0 + A\left(\sum_{i=s+1}^{n} \alpha_i X^{(i)}\right).$$

Таким образом пространство столбцов $\langle AX \mid X \in \mathbb{R}^n \rangle$ матрицы A совпадает с линейной оболочкой $\langle AX^{(s+1)}, ..., AX^{(n)} \rangle$. Это означает, что

$$\text{rank } A = \dim \langle AX^{(s+1)}, ..., AX^{(n)} \rangle.$$

При этом из независимости векторов $X^{(s+1)}, ..., X^{(n)}$ следует, что размер оболочки натянутой на векторы $AX^{(s+1)}, ..., AX^{(n)}$ равен $n - s$ ▶

Замечание. В терминах линейных отображений пространство столбцов матрицы и пространство решений системы можно обозначить как образ и ядро отображения $\varphi_A : \mathbb{R}^n \to \mathbb{R}^m$:

$$V_A = \langle X \in \mathbb{R}^n | AX = 0 \rangle = \text{Ker}_{\varphi_A},$$

$$\langle A^{(1)}, ..., A^{(n)} \rangle = \text{Im}_{\varphi_A}.$$

Любой базис пространства решений однородной системы $AX = 0$ называется *фундаментальной системой решений.*

Определитель

Геометрическая мотивировка

Определение. Квадратной матрице $A = (a_{ij})$ порядка n поставим в соответствие *параллелепипед*

$$\Pi(A) = \Pi(A^{(1)}, ..., A^{(n)}),$$

ребра которого задаются столбцами матрицы $A^{(1)}, ..., A^{(n)}$, то есть точками $A(i) = [a_{i1}, ..., a_{in}] \in \mathbb{R}^n$.

Определение. *Объем* $v(\Pi(A))$ n-мерного параллелепипеда определяется по индукции как произведение объема $v(\Pi(A^{(1)}, ..., A^{(n-1)}))$ $(n-1)$-мерного основания в $\mathbb{R}^n$ и длины h перпендикуляра $A^{(n)}P$ опущенного из точки $A^{(n)}$.

Замечание. Для удобного обращения с формулой определителя необходимо ввести понятие *ориентированного* объема. Для $\Pi(A^{(1)}, A^{(2)})$ объем берется со знаком плюс, если пара векторов $(A^{(1)}, A^{(2)})$ задает ту же ориентацию плоскости, что и базисная пара векторов (e_1, e_2).

При таком понимании естественно считать при любом n определителем det A матрицы A ориентированный объем параллелепипеда:

$$\det\ A = v(\Pi(A)).$$

Комбинаторно-аналитический подход

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

$$\det A = \sum_{\sigma \in S_n} \varepsilon_\sigma a_{1\sigma_1} a_{2\sigma_2} ... a_{n\sigma_n}.$$

Здесь S_n — группа перестановок на n элементах, $\varepsilon_\sigma = 1$, если перестановка σ четная, иначе $\varepsilon_\sigma =$ -1. Перестановка называется *четной* (*нечетной*), если число инверсий в ней четно (нечетно).

Далее будем считать, что $A_{(i)}$ — i-я строка матрицы A, $A^{(i)}$ — i-й столбец данной матрицы. Теперь мы хотим изучить определитель $\det A$ матрицы A как функцию от ее строк или столбцов.

Определение. Произвольную функцию

$$D : [A_{(1)}, ..., A_{(n)}] \mapsto D(A_{(1)}, ..., A_{(n)})$$

будем называть *полилинейной*, если она линейна по каждому аргументу, то есть

$$D(A_{(1)}, ..., \alpha A'_{(i)} + \beta A''_{(i)}, ..., A_{(n)}) =$$
$$= \alpha D(A_{(1)}, ..., A'_{(i)}, ..., A_{(n)}) + \beta D(A_{(1)}, ..., A''_{(i)}, ..., A_{(n)}).$$

Определение. Полилинейную функцию

$$D : [A_{(1)}, ..., A_{(n)}] \mapsto D(A_{(1)}, ..., A_{(n)})$$

будем называть *кососимметрической*, если для всех i

$$D(A_{(1)}, ..., A_{(i)}, A_{(i+1)}, ..., A_{(n)}) = -D(A_{(1)}, ..., A_{(i+1)}, A_{(i)}, ..., A_{(n)}).$$

Замечание.

1. Функция полилинейна ровно тогда, когда при фиксированных $A_{(1)}, ..., A_{(i-1)}, A_{(i+1)}, ...A_{(n)}$ и при $A_{(i)} = X = (x_1, ..., x_n)$ имеется соотношение
$$D(A_{(1)}, ..., A_{(n)}) = \alpha_1 x_1 + ... + \alpha_n x_n,$$
где α_j — скаляр, не зависящий от X.

2. Кососимметричность функции эквивалентна соотношению
$$D(...X, X...) = 0.$$

То есть, если две два аргумента равны, то кососимметрическая функция обращается в нуль. Действительно, если $X' = X''$, то

$$D(...X'', X'...) = D(...X', X''...) = -D(..., X'', X'...) = 0.$$

Обратно. Пусть $D(...X, X..) = 0$, тогда

$$D(...X, Y...) + D(...Y, X...) = D(...X + Y, X + Y...) = 0.$$

3. При перестановке любых двух аргументов кососимметрическая функция меняет знак на противоположный.

Теорема. Свойства определителя. Функция $\det : A \mapsto \det A$ на множестве $L_n(\mathbb{R})$ (квадратных матриц порядка n) обладает следующими свойствами.

D1) $\det A$ — **кососимметрическая функция строк матрицы** A**.** При перестановке любых двух строк матрицы определитель меняет знак на противоположный. ◀ Пусть A' получена из A перестановкой пары строк с номерами s и t. Тогда произвольную перестановку π можно записать как $\pi = \sigma \circ (s, t) = \sigma\tau$. Тогда

$$\det A' = \sum_{\pi \in S_n} \varepsilon_\pi a'_{1\pi_1}, ..., a'_{s\pi_s}, ..., a'_{t\pi_t}, ..., a'_{n\pi_n} =$$

$$= \sum_{\sigma \in S_n} \varepsilon_{\sigma\tau} a_{1\sigma_1}, ..., a_{t\sigma_t}, ..., a_{s\sigma_s}, ..., a_{n\sigma_n} = -\sum_{\sigma \in S_n} \varepsilon_\sigma a_{1\sigma_1}, ..., a_{n\sigma_n} = -\det A \;▶$$

D2) $\det A$ — **полилинейная функция строк матрицы** A**.** То есть определитель матрицы является линейной функцией элементов любой ее строки. ◀ Доказывается на основе замечания 1. Видно, что

$$\det A = \sum_{j=1}^{n} \alpha_j a_{ij},$$

где a_{ij} — элементы i-й строки, α_i — скаляры, которые не зависят от $A^{(i)}$ ▶

D3) $\det E = 1$. ◀ Все слагаемые кроме одного в формуле определителя равны 0, оставшееся равно 1. Ему соответствует перестановка $\mathrm{id} \in S_n$, которая очевидно четная ▶

D4) Пусть $A \in L_n(\mathbb{R})$, $\lambda \in \mathbb{R}$. Тогда $\det \lambda A = \lambda^n \det A$. ◀ Доказательство очевидно следует из формулы определителя. Пусть $A = (a_{ij})$, тогда

$$\det \lambda A = \sum_{\sigma \in S_n} \varepsilon_\sigma (\lambda a_{1\sigma_1}) ... (\lambda a_{n\sigma_n}) = \lambda^n \sum_{\sigma \in S_n} \varepsilon_\sigma a_{1\sigma_1} ... a_{n\sigma_n} \blacktriangleright$$

D5) **Определитель с нулевой строкой равен нулю**. ◀ Если в матрице A есть строка $A_{(i)} = (0, 0, ..., 0)$, то в каждое слагаемое умножается на 0, поэтому вся сумма равна нулю ▶

D6) **Если в определителе две строки совпадают, то он равен нулю.** ◀ Доказательство опирается на тот факт, что определитель — кососимметрическая функция строк матрицы, а замечание 2 доказывает, что любая кососимметрическая функция на наборе аргументов с парой совпадающих значений равна нулю ▶

D7) **Добавление к некоторой строке матрицы A другой строки, умноженной на $\lambda \in \mathbb{R}$ не меняет определителя матрицы.** ◀

$$\det(A_{(1)}, ..., A_{(i)} + \lambda A_{(j)}, ..., A_{(j)}, ..., A_{(n)}) =$$

в силу полилинейности

$$= \det(A_{(1)}, ..., A_{(i)}, ..., A_{(j)}, ..., A_{(n)}) + \lambda \det(A_{(1)}, ..., A_{(j)}, ..., A_{(j)}, ..., A_{(n)}) =$$

в силу свойства D6)

$$= \det(A_{(1)}, ..., A_{(i)}, ..., A_{(j)}, ..., A_{(n)}) + 0 = \det\ A \blacktriangleright$$

D8) Определитель не меняется при транспонировании матрицы. $\det A^t = \det A$. ◀ Пусть $\pi \in S_n$ — некоторая перестановка, π^{-1} — обратная ей перестановка. Пусть $A = (a_{ij})$, $A^t = (a'_{ij})$. Заметим, что

$$a'_{1\pi_1} ... a'_{n\pi_n} = a'_{\pi^{-1}1}, ..., a'_{\pi^{-1}n,n} = a_{1\pi^{-1}}, ..., a_{n\pi^{-1}n}.$$

Поскольку $\pi \mapsto \pi^{-1}$ — биекция, то по формуле определителя получаем требуемое равенство ▶

Теорема. Матрица $A \in L_n(\mathbb{R})$ невырождена ($\mathrm{rank}(A) = n$) тогда и только тогда, когда $\det A \neq 0$.

◀ Приведем матрицу A к ступенчатому виду A' с помощью элементарных преобразований. Если $\det A = 0$, то $\det A' = 0$, так как элементарные преобразования либо не изменяют определитель, либо меняют его знак, либо умножают на отличное от нуля число. По этой же причине если $\det A \neq 0$, то и $\det A' \neq 0$. Матрица A является невырожденной тогда и только тогда, когда она является строго треугольной. При этом произведение диагональных элементов матрицы A' равно ее определителю. Следовательно, матрица A' строго треугольная тогда и только тогда, когда ее определитель отличен от нуля ▶

Определение. Определитель матрицы, получающейся из $A = (a_{ij})$ вычеркиванием i-й строки и j-го столбца, обозначается M_{ij} и называется *минором* матрицы A.

Определение. Величина $(-1)^{i+j} M_{ij}$ называется *алгебраическим дополнением* элемента a_{ij}.

Лемма. Пусть

$$A = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ 0 & a_{22} & ... & a_{2n} \\ 0 & ... & & ... \\ ... & ... & ... & ... \\ 0 & a_{n2} & ... & a_{nn} \end{pmatrix}, \qquad (\diamondsuit)$$

тогда $\det A = a_{11} M_{11} = a_{11} A_{11}$.

◀ Рассмотрим произвольную перестановку $\pi \in S_n$. Заметим, что слагаемое вида $a_{1\pi_1} a_{2\pi_2} ... a_{n\pi_n} = 0$ если $\pi(1) \neq 1$. При этом совокупность всех перестановок, оставляющих на месте 1 соответствует группе перестановок S_{n-1} на множестве $\{2, 3, ..., n\}$. Значит

$$\det A = \sum_{\pi \in S_n, \pi(1)=1} \varepsilon_\pi a_{11} a_{2\pi_2} ... a_{n\pi_n} =$$

$$= a_{11} \sum_{\sigma \in S_{n-1}} \varepsilon_\sigma a_{2\sigma_2} ... a_{n\sigma_n} = a_{11} M_{11} \text{ ▶}$$

Эта лемма позволяет вычислять значение определителя матрицы. А именно необходимо привести исходную матрицу к виду $(\diamondsuit)$ с помощью элементарных преобразований. Так как элементарное преобразование $(..., A_{(i)}, ..., A_{(j)}, ...) \to (..., A_{(i)} + \lambda A_{(j)}, ..., A_{(j)}, ...)$ не меняет определителя необходимо лишь запомнить сколько раз мы поменяли строки местами. Тогда $\det \overline{A} = (-1)^q \det A$, где $\overline{A}$ определитель полученной диагональной матрицы, который легко найти по формуле

$$\det \overline{A} = \overline{a}_{11} ... \overline{a}_{nn},$$

а q — количество элементарных преобразований-перестановок строк.

Разложение определителя по элементам строки или столбца

Теорема. Пусть $A = (a_{ij}) \in L_n(\mathbb{R})$. Справедливы следующие формулы

$$\det A = \sum_{i=1}^{n} a_{ij} A_{ij} \quad \text{— разложение определителя по элементам столбца;}$$

$$\det A = \sum_{j=1}^{n} a_{ij} A_{ij} \quad \text{— разложение определителя по элементам строки.}$$

◀ Распишем определитель матрицы A специальным образом (из соображений полилинейности):

$$\det A = \begin{vmatrix} a_{11} & ... & a_{1j} & ... & a_{1n} \\ a_{21} & ... & a_{2j} & ... & a_{2n} \\ ... & ... & ... & ... & ... \\ a_{n1} & ... & a_{nj} & ... & a_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} a_{11} & ... & a_{1j} & ... & a_{1n} \\ a_{21} & ... & 0 & ... & a_{2n} \\ ... & ... & ... & ... & ... \\ a_{n1} & ... & 0 & ... & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & ... & 0 & ... & a_{1n} \\ a_{21} & ... & a_{21} & ... & a_{2n} \\ ... & ... & ... & ... & ... \\ a_{n1} & ... & 0 & ... & a_{nn} \end{vmatrix} + ... + \begin{vmatrix} a_{11} & ... & 0 & ... & a_{1n} \\ a_{21} & ... & 0 & ... & a_{2n} \\ ... & ... & ... & ... & ... \\ a_{n1} & ... & a_{nj} & ... & a_{nn} \end{vmatrix}.$$

Далее каждую из этих матриц необходимо привести к виду ($\Diamond$). Столбцы в каждой матрице мы поменяем $(j-1)$ раз, строки в i-й по порядку матрице поменяются $i-1$ раз, поэтому

$$\begin{vmatrix} a_{11} & ... & 0 & ... & a_{1n} \\ a_{21} & ... & 0 & ... & a_{2n} \\ ... & ... & ... & ... & ... \\ a_{i1} & ... & a_{ij} & ... & a_{in} \\ ... & ... & ... & ... & ... \\ a_{n1} & ... & 0 & ... & a_{nn} \end{vmatrix} = (-1)^{(j-1)+(i-1)} \times \begin{vmatrix} a_{ij} & a_{i1} & ... & a_{in} \\ 0 & a_{11} & ... & a_{2n} \\ ... & ... & ... & ... \\ 0 & a_{n1} & ... & a_{nn} \end{vmatrix} = a_{ij} A_{ij}.$$

Суммирование всех таких определителей и дает нужный результат ▶

Теорема. Для любых двух квадратных матриц A, B выполняется соотношение $\det AB = \det A \det B$.

◀ Зафиксируем матрицу B и положим, что для любой матрицы A

$$D_B(A) = \det AB.$$

Тогда функция $D_B(A)$ — кососимметрическая и полилинейная функция от строк матрицы A. Значит, функция $D_B(A)$ может быть представлена в виде $D_B(A) = D_B(E) \det A$. $D_B(E) = \det(EB) = \det B$. Отсюда следует, что $\det AB = D_B(A) = \det B \det A$ ▶

Критерий невырожденности матрицы

Теорема. Определитель невырожденной матрицы отличен от нуля и $\det(A^{-1}) = (\det A)^{-1}$.

◀ Невырожденность матрицы эквивалентна ее обратимости, поэтому если A невырождена, то существует A^{-1}. Тогда $1 = \det E = \det(AA^{-1}) = \det A \cdot \det A^{-1}$, значит

$$(\det A)^{-1} = \det A^{-1} \text{ ▶}$$

Лемма. Пусть $A \in L_n(\mathbb{R})$. Тогда имеет место соотношение

$$a_{i1}A_{j1} + a_{i2}A_{j2} + ... + a_{in}A_{jn} = \delta_{ij} \det A, \qquad (\heartsuit)$$

где $\delta_{ij} = 0$ при $i \neq j$, иначе $\delta_{ij} = 1$.

◀ При $i = j$ это формула разложения определителя. Пусть $i \neq j$. Рассмотрим матрицу

$$A' = [A_{(1)}, ..., A_{(i)}, ..., A_{(i)}, ..., A_{(n)}],$$

полученную заменой строки $A_{(j)}$ строкой $A_{(i)}$. Распишем определитель матрицы A' по элементам j-ой строки.

$$\det A' = \sum_{k=1}^{n} a'_{jk}A'_{jk} = \sum_{k=1}^{n} a_{ik}A_{jk}$$

Последняя сумма есть сумма из условия, а $\det A' = 0$ в силу того, что матрица A' содержит одинаковые строки ▶

Теорема. Матрица $A \in L_n(\mathbb{R})$ невырожденна (обратима) тогда и только тогда, когда $\det A \neq 0$. Если $\det A \neq 0$, то

$$A^{-1} = (\det A)^{-1} A^{\triangle},$$

где

$$A^{\triangle} = \begin{vmatrix} A_{11} & A_{21} & ... & A_{n1} \\ A_{12} & A_{22} & ... & A_{n2} \\ ... & ... & ... & ... \\ A_{1n} & A_{2n} & ... & A_{nn} \end{vmatrix}$$

◀ Рассмотрим матрицу $C = AA^{\triangle}$. Согласно вышедоказанной лемме $c_{ij} = \delta_{ij} \det A$, значит

$$AA^{\triangle} = (\det A)E.$$

При $\det A \neq 0$ получаем $(\det A)^{-1} AA^{\triangle} = A(\det A)^{-1} A^{\triangle} = E \Rightarrow$

$$(\det A)^{-1} A^{\triangle} = A^{-1} \blacktriangleright$$

Замечание. Сначала мы показали, что если матрица невырожденна, то ее определитель не равен нулю. Затем предположили, что определитель матрицы отличен от нуля, что позволило написать явную формулу для обратной матрицы.

Формулы Крамера

Теорема (Крамер). Пусть $A \in L_n(R)$, $X \in \mathbb{R}^n$, $B \in \mathbb{R}^n$, а $\det A \neq 0$. Тогда система

$$AX = B$$

имеет единственное решение, которое задается формулами

$$x_k = \frac{\det[A_{(1)}, ..., A_{(k-1)}, B, A_{(k+1)} ..., A_{(n)}]}{\det A}. \tag{$\clubsuit$}$$

◀ Так как $\det A \neq 0$, то матрица A обратима, значит система имеет решение

$$X = A^{-1} B.$$

Запишем явную формулу матрицы A^{-1}:

$$X = \frac{1}{\det A} \begin{vmatrix} A_{11} & ... & A_{n1} \\ ... & ... & ... \\ A_{1n} & ... & A_{nn} \end{vmatrix} \cdot \begin{vmatrix} b_1 \\ ... \\ b_n \end{vmatrix},$$

откуда

$$x_k = \frac{1}{\det A} \sum_{i=1}^{n} A_{ik} b_i.$$

Заметим, что именно такое выражение мы получим, разложив числитель дроби (♣) по k-му столбцу. Выполнение всех преобразований в обратном порядке показывает, что набор $(\frac{D_1}{\det A}, ..., \frac{D_n}{\det A})$ действительно удовлетворяет всем условиям ▶

(YA) Евклидовы и унитарные пространства. Свойства скалярного произведение, неравенство Коши-Буняковского. Норма, ортонормированный базис. Разложение пространства в прямую сумму подпространства и его ортогонального дополнения.

(YA) Понятие линейного оператора, матрицы линейного оператора, нормы. Преобразование матрицы при замене базиса, характеристический многочлен. Собственные векторы и собственные значения, геометрический смысл.

(YA) Квадратичные формы, их знакоопределенность и канонический вид. Унитарные и нормальные операторы.

Вопросы из программы НОД-ВШЭ.

Линейная зависимость системы векторов. Базис линейного пространства. Скалярное произведение.

Определитель квадратной матрицы. Вычисление определителей. Разложение определителя по строке и по столбцу.

Транспонированная матрица. Обратная матрица. Ранг матрицы. Специальные виды матриц.

Системы линейных уравнений. Метод Крамера. Метод Гаусса. Фундаментальная система решений.

Линейные преобразования векторных пространств и их матрицы. Изменение матриц линейного пространства и квадратичной формы при смене базиса.

Собственные числа и собственные векторы матрицы. Собственные и инвариантные подпространства.

Характеристический многочлен. Аннулирующий и минимальный многочлены. Теорема Гамильтона-Кэли.

Квадратичные формы. Матрица квадратичной формы. Условие положительной (отрицательной) определенности квадратичной формы. Критерий Сильвестра. Индексы инерции квадратичных форм.