ЛЕКЦИЯ 12

ФОРМУЛА ОБРАТНОЙ МАТРИЦЫ

ФОРМУЛЫ КРАМЕРА

ОПРЕДЕЛИТЕЛЬ ВАНДЕРМОНДЫ

ПОЛУГРУППЫ, МОНОИДЫ, ГРУППЫ

СТЕПЕНЬ ЭЛЕМЕНТА ГРУППЫ, ЦИКЛИЧЕСКИЕ ГРУППЫ

ФОРМУЛА ОБРАТНОЙ МАТРИЦЫ

Мы уже проходили, что условие невырожденности матрицы эквивалентно условию ее обратимости.

Применяя это к соотношению

$$AA^{-1} = A^{-1}A = E,$$

мы получим

$$\det A \cdot \det A^{-1} = 1.$$

Значит, *определитель невырожденной матрицы отличен от нуля и*

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

Наряду с матрицей A рассмотрим ее *присоединенную* матрицу

$$A^{\,\mathrm{ad}} = \begin{pmatrix} A_{11} & \dots & A_{n1} \\ \dots\dots\dots\dots & & \\ A_{1n} & \dots & A_{nn} \end{pmatrix}.$$

У матрицы $A^{\,\mathrm{ad}}$ на месте (i, j) стоит алгебраическое к элементу a_{ji} транспонированной матрицы.

Теорема 1. *Матрица* $A \in M_n(\mathbb{R})$ *невырожденна (обратима) тогда и только тогда, когда* $\det A \neq 0$. *Если* $\det A \neq 0$, *то*

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

или, в более подробной записи,

$$\begin{pmatrix} a_{11} & \dots & a_{n1} \\ \dots & \dots & \dots \\ a_{1n} & \dots & a_{nn} \end{pmatrix}^{-1} = \begin{pmatrix} \frac{A_{11}}{\det A} & \dots & \frac{A_{n1}}{\det A} \\ \dots & \dots & \dots \\ \frac{A_{1n}}{\det A} & \dots & \frac{A_{nn}}{\det A} \end{pmatrix}.$$

Доказательству теоремы предпошлем лемму:

Лемма 1. *Пусть* $A \in M_n(\mathbb{R})$. *Имеют место соотношения*

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \dots + a_{in}A_{jn} = \delta_{ij} \det A,$$
$$a_{1i}A_{1j} + a_{2i}A_{2j} + \dots + a_{ni}A_{nj} = \delta_{ij} \det A,$$

где δ_{ij} *— символ Кронекера. При* $i \neq j$ *говорят о разложении определителя* $\det A$ *по чужой строке или чужому столбцу или о фальшивом разложении.*

Доказательство. при $i = j$ утверждение леммы уже доказывалось как обычное разложение определителя по строке или столбцу.

Поэтому остается рассмотреть случай $i \neq j$, когда $\delta_{ij} = 0$.

С этой целью введем матрицу

$$A' = [A_{(1)}, \ldots, A_{(i)}, \ldots, A_{(i)}, \ldots, A_{(n)} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{i1} & a_{i2} & \ldots & a_{in} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{i1} & a_{i2} & \ldots & a_{in} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix},$$

получающуюся из матрицы A заменой j-й строки на i-ую.

Как у всякой другой квадратной матрицы с двумя одинаковыми строками, $\det A' = 0$.

С другой стороны, алгебраическое дополнение A'_{jk}, $k = 1, \ldots, n$, образуется путем зачеркивания j-й строки $A'_{(j)} = A_{(i)}$ и k-го столбца определителя, так что $A'_{jk} = A_{jk}$.

Формальное разложение определителя матрицы $A' = (a'_{st})$ по j-й строке даст нам соотношение

$$0 = \det A' = \sum_{k=1}^{n} a'_{jk} A'_{jk} = \sum_{k=1}^{n} a_{ik} A_{jk},$$

что ровно и совпадает с соотношением в формулировке теоремы.

Ситуация со столбцами совершенно аналогична. □

Возвращаясь к доказательству теоремы, заметим, что левая часть соотношение из леммы есть не что иное как элемент матрицы $C = AA^{\,\mathrm{ad}}$:

$$\begin{pmatrix} c_{11} & \dots & c_{1n} \\ \dots & \dots & \dots \\ c_{n1} & \dots & c_{nn} \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} A_{11} & \dots & A_{n1} \\ \dots & \dots & \dots \\ A_{1n} & \dots & A_{nn} \end{pmatrix}.$$

Мы доказали, что

$$(c_{ij}) = (\delta_{ij} \det A) = (\det A)E.$$

Таким образом,

$$AA^{\,\mathrm{ad}} = (\det A)E,$$

откуда при $\det A \neq 0$ получаем

$$(\det A)^{-1}(AA^{\,\mathrm{ad}}) = A(\det A)^{-1}A^{\,\mathrm{ad}} = E.$$

Отсюда, очевидно,

$$A^{-1} = (\det A)^{-1}A^{\,\mathrm{ad}}.$$

Следствие 1. *Определитель равен нулю тогда и только тогда, когда его строки (или столбцы) линейно зависимы.*

Доказательство. Линейная зависимость строк (или столбцов) матрицы $A \in M_n(\mathbb{R})$ эквивалентна неравенству $\operatorname{rank} A < n$, то есть вырожденности матрицы A, что равносильно условию $\det A = 0$. □

ФОРМУЛЫ КРАМЕРА

Выведем теперь из всего уже доказанного формулы для решения системы из n линейных уравнений с n неизвестными.

Теорема 2 (Крамер)**.** *Если линейная система*

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n = b_n \end{cases}$$

имеет отличный от нуля определитель (то есть $\det(a_{ij}) \neq 0$*), то ее единственное решение задается формулами*

$$x_k^0 = \frac{\begin{vmatrix} a_{11} & \ldots & b_1 & \ldots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \ldots & b_n & \ldots & a_{nn} \end{vmatrix}}{\begin{vmatrix} a_{11} & \ldots & a_{1k} & \ldots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \ldots & a_{nk} & \ldots & a_{nn} \end{vmatrix}}, \quad k = 1, 2, \ldots, n.$$

Доказательство. Так как $\det A \neq 0$, то матрица (a_{ij}) обратима.

Поэтому, записав нашу систему в виде

$$AX = B,$$

мы будем иметь

$$\begin{pmatrix} x_1^0 \\ \vdots \\ x_k^0 \\ \vdots \\ x_n^0 \end{pmatrix} = A^{-1}B = \frac{1}{\det A} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix},$$

откуда

$$x_k^0 = \frac{1}{\det A} \sum_{i=1}^{n} A_{ik} b_i = \\ = \frac{1}{\det A}(b_1 A_{1k} + b_2 A_{2k} + \dots + b_n A_{nk}), \quad k = 1, 2, \dots, n.$$

Именно такое выражение мы получим, если разложим определитель из числителя формулы Крамера по k-му столбцу. $\square$

ОПРЕДЕЛИТЕЛЬ ВАНДЕРМОНДА

Рассмотрим матрицу

$$A = \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \dots & x_3^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{pmatrix}$$

и найдем ее определитель.

Из каждого столбца, начиная со второго, вычтем предыдущий столбец, умноженный на x_1. Получим матрицу

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & x_2 - x_1 & x_2(x_2 - x_1) & \dots & x_2^{n-2}(x_2 - x_1) \\ 1 & x_3 - x_1 & x_3(x_3 - x_1) & \dots & x_3^{n-2}(x_3 - x_1) \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_n - x_1 & x_n(x_n - x_1) & \dots & x_n^{n-2}(x_n - x_1) \end{pmatrix},$$

откуда видно, что этот определитель равен

$$(x_2 - x_1) \dots (x_n - x_1) \begin{vmatrix} 1 & x_2 & \dots & x_2^{n-2} \\ 1 & x_3 & \dots & x_3^{n-2} \\ \dots & \dots & \dots & \dots \\ 1 & x_n & \dots & x_n^{n-2} \end{vmatrix},$$

откуда, последовательно применяя те же соображения, получаем

$$|A| = \prod_{i,j=1, i<j}^{n} (x_j - x_i).$$

ПОЛУГРУППЫ И МОНОИДЫ

Бинарная операция $*$ на множестве X называется *ассоциативной*, если

$$(a * b) * c = a * (b * c)$$

для всех $a, b, c \in X$; она называется *коммутативной*, если

$$a * b = b * a.$$

Те же названия присваиваются и соответствующей алгебраической структуре $(X, *)$.

Требования ассоциативности и коммутативности независимы.

В самом деле, операция $*$ на $\mathbb{Z}$, заданная правилом

$$n * m = -n - m,$$

очевидно, коммутативна, но

$$(1 * 2) * 3 = (-1 - 2) * 3 = -(-1 - 2) - 3 = 0 \neq 4 = 1 * (2 * 3),$$

так что условие ассоциативности не выполняется. Далее, на множестве $M_n(\mathbb{R})$ всех квадратных матриц порядка $n > 1$ определена операция умножения — ассоциативная, но некоммутативная.

Элемент $e \in X$ называется *единичным* (или нейтральным), относительно рассматриваемой бинарной операции $*$, если

$$e * x = x * e = x$$

для всех $x \in X$.

Если e' — еще один единичный элемент, то, как следует из определения,

$$e' = e' * e = e.$$

Значит, в алгебраической структуре $(X, *)$ может существовать не более одного единичного элемента.

Множество X с заданной на нем бинарной ассоциативной операцией называется *полугруппой*.

Полугруппу с единичным (нейтральным) элементом принято называть еще *моноидом*.

Как и для всякого множества, мощность моноида $M = (M, *)$ обозначается символом $|M|$.

В случае конечности числа содержащихся в нем элементов говорят о конечном моноиде порядка $|M|$.

Пример 1. Пусть X — множество, $M(X)$ — множество всех его преобразований (отображений в себя) с операцией композиции (суперпозиции).

Ясно, что $M(X)$ — моноид.

СТЕПЕНЬ ЭЛЕМЕНТА

Благодаря тому, что от расстановки скобок в произведении результат вычислений не меняется, в полугруппе можно ввести понятие степени элемента.

Именно, для любого натурального числа $n \in \mathbb{N}$ и любого элемента $x \in X$ полугруппы n-ая степень этого элемента — это произведение n экземпляров x.

Если мы имеем дело с моноидом, то можно ввести нулевую степень любого элемента: $x^0 = e$.

Так введеная степени удовлетворяет двум самым основным обычным свойствам степени:

(1) для любого $x \in X$ и любых $n, m \in \mathbb{N}$ выполнено

$$(x^n)^m = x^{nm}.$$

(2) для любого $x \in X$ и любых $n, m \in \mathbb{N}$ выполнено

$$x^{n+m} = x^n x^m.$$

При этом привычное для нас свойство

$$x^n y^n = (xy)^n$$

выполняется тогда и только тогда, когда x и y коммутируют в полугруппе.

Если моноид коммутативен, то его принято записывать в аддитивной записи: вместо $\cdot$ пишут $+$, вместо e — 0.

В аддитивной записи выражение x^n записывают иначе — как $x + x + \cdots + x = nx$.

ОБРАТИМЫЕ ЭЛЕМЕНТЫ

Элемент x моноида $(X, \cdot)$ называется *обратимым*, если существует элемент $y \in X$ такой, что $xy = yx = e$.

Элемент y называется *обратным* к x и обозначается x^{-1}.

Понятно, что $(x^{-1})^{-1} = x$. Понятие обратимого элемента моноида служит, очевидно, естественным обобщением понятия обратимой матрицы в моноиде $(M_n(\mathbb{R}), \cdot, E)$.

Так как

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = e$$

и, аналогично,

$$(y^{-1}x^{-1})(xy) = e,$$

то

$$(xy)^{-1} = y^{-1}x^{-1},$$

то есть множество всех обратимых элементов моноида замкнуто относительно умножения, то есть само является моноидом.

Мы можем говорить о подмоноиде обратимых элементов моноида $(X, \cdot)$.

ГРУППЫ

Группой называется моноид, все элементы которого обратимы.

Иначе говоря, группа — это множество X с бинарной операцией $\cdot$, для которой выполнены свойства ассоциативности, наличия нейтрального элемента e и для каждого элемента x существует обратный x^{-1}.

Если умножение в группе коммутативно, то она называется *абелевой группой*.

Приведем несколько самых основных примеров групп.

Пример 2. Множество $\mathbb{Z}$ целых чисел по сложению является абелевой группой.

Действительно, операция сложения целых чисел ассоциативна и коммутативна, при этом нейтральным элементом выступает ноль, а обратным к числу x — противоположное число $-x$.

Пример 3. Также группами являются множества всех рациональных $\mathbb{Q}$ и всех действительных $\mathbb{R}$ чисел по сложению.

Нейтральный элемент — также ноль.

Если вместо операции сложения рассматривать умножение, то надо брать не все рациональные или действительные числа, а их же без нуля: $\mathbb{Q}^* = (\mathbb{Q} \setminus \{0\}, \cdot)$ и $\mathbb{R}^* = (\mathbb{R} \setminus \{0\}, \cdot)$.

Тогда нейтральным элементом в обеих группах будет сложить единица 1, а обратными — обычные обратные элементы.

Пример 4. Предыдущие группы были абелевыми, но пример неабелевой группы нам всем тоже уже известен — это группа S_n всех перестановок порядка n.

Заметим, что внутри нее живет еще одна группа — группа A_n четных перестановок порядка n.

Пример 5. Еще очень хороший пример группы — это группа вычетов по модулю n.

Рассмотрим числа $\{0, 1, 2, \ldots, n-1\}$, а на них введем операцию сложения по модулю n:

$$a \oplus b := a + b \mod n.$$

Очевидно, что сложение по модулю ассоциативно и коммутативно. Нейтральным элементов является ноль, а обратным элементом для $a \in \{0, 1, 2, \ldots, n-1\}$ служит число $n - a$.

Таким образом, для каждого $n \in \mathbb{N}$ мы получаем абелеву группу из n элементов, будем обозначать ее через $\mathbb{Z}_n$.

Пример 6. Если рассмотреть алгебру матриц $M_n(\mathbb{R})$ и выбрать из нее все обратимые матрицы, то мы получим группу $\mathrm{GL}_n(\mathbb{R})$ обратимых матриц порядка n, также называемую общей линейной группой.

Если внутри группы $\mathrm{GL}_n(\mathbb{R})$ рассмотреть только матрицы с определителем 1, то такое множество матриц будет замкнуто относительно умножения и взятия обратных матриц, поэтому такое множество матриц также будет является группой, ее обозначают через $\mathrm{SL}_n(\mathbb{R})$, называется она специальной линейной группой.

Заметим, что в случае группы понятие степени элемента расширяется: можно вводить не только натуральные степени элементов и нулевую, но и вообще любые целые степени.

Именно, для $n \in \mathbb{Z}$ и для $a \in G$

$$a^n = \begin{cases} a \cdot a \times \cdots \times a \ (n \text{ раз}) \text{ при } n > 0; \\ e \text{ при } n = 0; \\ a^{-1} \cdot a^{-1} \times \cdots \times a^{-1} \ (|n| \text{ раз}) \text{ при } n < 0. \end{cases}$$

Легко проверить, что выполняются те же самые соотношения, что и для натуральных степеней в моноиде/полугруппе.

ЦИКЛИЧЕСКИЕ ГРУППЫ

Пусть G — мультипликативная группа (то есть с операцией умножения), a — ее фиксированный элемент.

Если любой элемент $g \in G$ можно записать как a^n для некоторого целого n, то говорят, что $G = \langle a \rangle$ — *циклическая группа* с образующим a (или циклическая группа, порожденная элементом a).

Аналогично циклическая группа определяется в аддитивном случае:

$$\langle a \rangle = \{na \mid n \in \mathbb{Z}\}.$$

Это, конечно, не означает, что все элементы a^n попарно различны.

Простейшим примером циклической группы служит аддитивная группа целых чисел $(\mathbb{Z}, +)$, которая порождена обычной единицей 1 или -1.

Примером циклической группы из n элементов служит недавно введенная группа вычетов $\mathbb{Z}_n$. Она тоже порождается единицей 1, хотя может порождаться и другими элементами, в некоторых случаях — вообще любым ненулевым элементом.

Пусть снова G — произвольная группа, a — ее произвольный элемент. Имеются две возможности:

(1) Все степени элемента a различны, то есть

$$m \neq n \Longrightarrow a^m \neq a^n.$$

В этом случае говорят, что элемент a имеет *бесконечный порядок.*

(2) Имеются совпадения $a^m = a^n$ при некоторых $m \neq n$. Если, например, $m > n$, то $a^{m-n} = e$, то есть существует положительная степень элемента $a \in G$, равная единичному элементу.

Пусть q — наименьший положительный показатель, для которого $a^q = e$.

Тогда говорят, что a — элемент конечного порядка q.

В конечной группе G все элементы, естественно, будут иметь конечный порядок.

Теорема 3. *Порядок любого элемента $a \in G$ равен порядку группы $\langle a \rangle$.*

Если a — элемент конечного порядка q, то $\langle a \rangle = \{e, a, a^2, \ldots, a^{q-1}\}$,

$$a^k = e \Longleftrightarrow k = lq, \quad l \in \mathbb{Z}.$$

Доказательство. В случае элемента бесконечного порядка доказывать нечего.

Если a — элемент порядка q, то по определению все элементы $e, a, a^2, \ldots, a^{q-1}$ различны.

Любая другая степень a^k совпадает с одним из этих элементов, то есть

$$\langle a \rangle = \{e, a, \ldots, a^{q-1}\}.$$

В самом деле, воспользовавшись алгоритмом деления целых чисел с остатком, запишем показатель k в виде

$$k = lq + r, \quad 0 \leqslant r < k,$$

после чего получим

$$a^k = (a^q)^l a^r = ea^r = a^r.$$

В частности,

$$a^k = e \Longrightarrow r = 0 \Longrightarrow k = lq.$$

□