Лекция 4
Линейные уравнения и матрицы

$\triangleright$Системы линейных уравнений, их матрицы и элементарные преобразования $\triangleright$Приведение матрицы над полем к строгому ступенчатому виду преобразованиями строк $\triangleright$Решение систем линейных уравнений над полем $\triangleright$Замены переменных и матрицы перехода $\triangleright$Сложение и умножение матриц $\triangleright$Аксиомы (некоммутативного) кольца с единицей $\triangleright$Элементарные матрицы $\triangleright$Отыскание обратной матрицы $\triangleright$Приведение матрицы над $\mathbb{Z}$ или $k[x]$ к диагональному виду преобразованиями строк и столбцов $\triangleright$Решение систем линейных уравнений над $\mathbb{Z}$ и $k[x]$

§1. Основные понятия

Система линейных уравнений — это одна из очень и очень немногих задач, допускающих полное и исчерпывающее решение, и принцип линеаризации, состоящий в том, что всякую вычислительную проблему, как правило, можно свести к линейным уравнениям, является излюбленным приёмом в алгебре, геометрии и анализе. Линейным уравнениям посвящены целая отрасль алгебры — *линейная алгебра*, и целая отрасль анализа — *линейный функциональный анализ.*

Как и всякую задачу, линейные уравнения можно решать на двух языках — геометрическом и алгебраическом. Первый сопоставляет задаче систему геометрических образов и исследует их взаимодействие, опираясь на интуицию картинок. Второй вводит удобную алгебраическую символику и аппелирует к интуиции формул. Геометрия линейных уравнений — это геометрия *векторных пространств*, или *модулей*. Алгебра линейных уравнений - это *алгебра матриц*. В этой лекции мы обсудим формально-алгебраическую сторону дела, а две следующие будут посвящены геометрическим аспектам.

1.1. Уравнения. Пусть требуется решить систему из m линейных уравнений с n неизвестными:

$$\begin{cases} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ & & & & \cdots & & & & \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m \end{cases} .$$

Это означает, что некотором коммутативном кольце R с единицей заданы mn чисел $\{a_{ij}\}$, называемых *коэффициентами* системы, и m чисел $\{b_i\}$, называемых *правыми частями* системы. Решить систему в некотором большем кольце $R_1 \supset R$, содержащем R в качестве подкольца, — это значит описать все возможные упорядоченные наборы $(c_1, c_2, \ldots, c_n) \in R_1 \times R_1 \times \cdots \times R_1$, которые при подстановке $x_i = c_i$, $(i = 1, 2, \cdots, n)$ превращают все уравнения системы в равенства, справедливые в кольце R_1. Каждый такой набор $(c_1, c_2, \ldots, c_n)$ называется *решением системы* в кольце $R_1 \supset R$.

Мы не будем в этих лекциях изучать системы уравнений в такой большой общности, а ограничимся случаями, когда $R = R_1$ будет (произвольным) полем k, кольцом целых чисел $\mathbb{Z}$ или кольцом многочленов $k[x]$.

1.2. Матрицы. Таблица коэффициентов из левых частей предыдущих уравнений

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

называется *матрицей системы*, а та же таблица, дополненная справа отдельной колонкой правых частей:

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right)$$

называется *расширенной матрицей системы*. Она содержит всю необходимую для решения системы информацию, если раз и навсегда условиться писать все уравнения так, чтобы неизвестные шли в фиксированном порядке $x_1, x_2, \ldots, x_n$.

Всюду далее, решая системы, мы будем работать исключительно только с их матрицами. Вообще же под $m \times n$*-матрицей над кольцом* R мы всегда будем понимать прямоугольную таблицу из m строк длины n, заполненную числами из R. При этом m мы будем называть *высотой*, а n — *шириной* матрицы.

Матрицы мы будем обозначать большими латинскими буквами A, B, и т.д. Элемент матрицы A, стоящий в пересечении i-той строчки и j-того столбца, мы будем обозначать через a_{ij}. Иногда для обозначения матрицы мы будем писать (a_{ij}) вместо A.

§2. Метод Гаусса над полем

2.1. Элементарные преобразования уравнений. Следуя школьной традиции, будем называть две системы уравнений *равнолсильными*, если их множества решений совпадают. Один из способов решения систем состоит в том, чтобы последовательно заменять их на более простые равносильные системы. Особенно удобны три простейших замены подобного рода, называемых *элементарными преобразованиями* (эп):

(эп-1) Элементарное преобразования *первого типа*: перемена каких-либо двух уравнений местами.

(эп-2) Элементарные преобразования *второго типа*: вместо одного из уравнений системы написать его сумму с уравнением, полученным в результате умножения обеих частей любого другого уравнения системы на произвольное число. (Подчеркнём, что изменяется ровно одно уравнение — то, к которому прибавляют. Вспомогательное уравнение, кратность которого прибавляется к изменяемому уравнению, должно быть переписано в преобразованную систему без изменений.)

(эп-3) Элементарные преобразования *третьего типа*: умножить обе части какого-либо уравнения на число, не являющемся делителем нуля.

2.1.1. Предложение. *Элементарные преобразования меняют систему на равносильную.*

Доказательство. Рассмотрим, к примеру, случай (эп-2). Пусть система $\mathfrak{S}_2$ получается из системы $\mathfrak{S}_1$ заменой уравнеия $\mathfrak{a}\in\mathfrak{S}_1$ на уравнение $\mathfrak{c} = \mathfrak{a} + \lambda\mathfrak{b}$, где $\mathfrak{b}\in\mathfrak{S}_1$, $\mathfrak{b} \neq \mathfrak{a}$.

Ясно, что всякое решение $\mathfrak{S}_1$ останется и решением $\mathfrak{S}_2$, ибо оно обращает и $\mathfrak{a}$ и $\mathfrak{b}$ в верные равенства.

Заметим теперь, что система $\mathfrak{S}_1$ также может быть получена из системы $\mathfrak{S}_2$ при помощи (эп-2), а именно, к уравнению $\mathfrak{c}\in\mathfrak{S}_2$ надо прибавить уравнение $\mathfrak{b}\in\mathfrak{S}_2$, умноженное на $(-\lambda)$. Но тогда всякое решение $\mathfrak{S}_2$ является решением и для $\mathfrak{S}_1$.

Задача 4.1. Убедитесь, что (эп-1) и (эп-3) также является равносильным преобразованием.

Задача 4.2. Приведите пример уравнения над кольцом вычетов $\mathbb{Z}/n\mathbb{Z}$, множество решений которого меняется при умножении на ненулевой вычет.

2.2. Элементарные преобразования матриц. При рассмотренных выше элементарных преобразований систем их матрицы также подвергаются элементарным преобразованиям:

(1-й тип) перемена двух строк местами;

(2-й тип) замена строки на ее поэлементную сумму с какой-либо другой строкой, умноженной (поэлементно) на любое число (при этом сама эта вторая строка остается в матрице системы без изменения);

(3-й тип) поэлементное умножение какой-либо строки на число, не являющееся делителем нуля.

2.3. Теорема. *Над любым полем k любая $m\times n$-матрица элементарными преобразованиями строк может быть приведена к так называемому строгому ступенчатому виду, который характеризуется тем, что в каждой строке самый левый ненулевой элемент:*

(1) равен 1;

(2) располагается строго правее, чем в предыдущей строке;

(3) является единственным ненулевым элементом своего столбца.

Доказательство. Процесс приведения будет состоять из n последовательных шагов (по количеству столбцов).

Перед выполнением k-ого шага предполагается, что та часть матрицы, которая расположена слева от k-ого столбца уже имеет нужный вид (в частности, может быть пустой или тождественно нулевой). Пусть в ней имеется s ненулевых строк. Отметим, что $0 \leq s \leq k-1$.

Сам k-ый шаг состоит в следующем.

Прежде всего в k-ом столбце в позициях строго ниже s-той выбирается ненулевой элемент (если его нет, то часть матрицы, расположенная слева от $(k+1)$-го столбца имеет нужный вид и можно сразу переходить к $(k+1)$-му шагу).

После того, как этот элемент выбран, строка, в которой он стоит, меняется местами с $(s+1)$-ой строкой, а затем умножается на элемент, обратный выбранному. В результате левые $k-1$ столбцов матрицы не изменяются, а $(s+1)$-ая строка приобретает вид

$$\underbrace{0\,0\,\ldots\,0\,0}_{k-1}\,1\,\underbrace{*\,*\,\ldots\,*\,*}_{n-k}\,.$$

В заключение к каждой строке, имющей в k-том столбце отличный от нуля элемент (кроме, разумеется, самой $(s+1)$-ой строки) прибавляется подходящая кратность $(s+1)$-ой строки так, чтобы этот ненулевой элемент занулился. Это опять не портит левой части матрицы и зануляет весь k-ый столбец за исключением единицы в $(s+1)$-ой строке. В результате мы попадаем в исходное положение для $(k+1)$-ого шага.
□

2.4. Решение системы линейных уравнений над полем методом Гаусса. состоит в том, что исходная система описанным выше путем преобразуется в равносильную систему, расширенная матрица которой имеет строго ступенчатый вид. Перенумеровав, если надо, переменные (т.е. переставив столбцы матрицы), мы можем считать, что итоговая расширенная матрица имеет вид:

$$
\begin{array}{|cccc|ccc|c|}
\hline
1 & & & & * & \cdots & * & b_1 \\
 & 1 & & 0 & * & \cdots & * & b_2 \\
0 & & \ddots & & \vdots & \vdots & \vdots & \vdots \\
 & & & 1 & * & \cdots & * & b_r \\
\hline
0 & 0 & \cdots & 0 & 0 & \cdots & 0 & b_{r+1} \\
\hline
0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\hline
\end{array}
$$

Такая система легко решается. Назовём первые r неизвестных $x_1, x_2, \dots, x_r$ *связанными*, а остальные неизвестные $x_{r+1}, \dots, x_n$ будем назвать *свободными*. Имеются, очевидно, две качественно разных возможности для последнего столбца.

Первая: $b_{r+1} = 1$, $b_1 = b_2 = \dots = b_r = 0$ (т.е. расширенная матрица имеет ровно на одну ненулевую строку больше, чем матрица коэффициентов). Это имеет место тогда и только тогда, когда система несовместна.

Вторая: $b_{r+1} = 0$, а остальные правые части $b_1, b_2, \dots, b_r$ – произвольны. Здесь любой набор из $(n-r)$ значений свободных неизвестных однозначно дополняется до решения системы, в котором значения связанных неизвестных вычисляются по формулам

$$x_s = b_s - \sum_{\nu=r+1}^{n} m_{s\nu} x_\nu \ , \quad s = 1, 2, \dots, r \ ,$$

где $m_{s\nu}$ – это элемент из s-той строки и ν-того столбца написанной выше матрицы. Таким образом, в этом случае все решения системы взаимно-однозначно линейно параметризуется $n-r$ "произвольными постоянными". В частности, при $n = r$ решение существует и единственно.

> Задача 4.3. Докажите, что две системы равносильны тогда и только тогда, когда их расширенные матрицы приводятся элементарными преобразованиями строк к одной и той же строго ступенчатой матрице.
>
> Указание. Проверьте, что разные строго ступенчатые матрицы задают системы с разными множествами решений.

2.4.1. Пример: однородные системы. Система линейных уравнений называется *однородной*, если все её правые части равны нулю. Однородная система, очевидно, остаётся таковой и после элементарных преобразований, и поэтому относится ко второму из рассмотренных выше типов. В частности, однородная ситема всегда имеет тривиальное *нулевое* решение. Непосредственно из предыдущего анализа вытекают

2.4.2. Следствие. *Однородная система m линейных уравнений от $n > m$ неизвестных всегда имеет ненулевое решение.*

2.4.3. Следствие. (Альтернатива Фредгольма.) *Система, в которой число уравнений равно числу неизвестных, либо имеет единственное решение при любых правых частях, либо имеет ненулевое решение при нулевых правых частях.*

§3. Алгебра матриц

Алгебраический матричный формализм служит для того,чтобы записывать преобразования систем линейных уравнений короткими алгебраическими формулами. В основе его лежат две операции над матрицами - сложение и умножение.

3.1. Определение. *Сумма $A + B$ двух матриц A и B определена для любых двух матриц одинакового размера и представляет собой матрицу того же размера, элементы которой суть суммы соответствующих элементов у A и B.*

Иными словами, если $A = (a_{ij})$, $B = (b_{ij})$, то $C = A + B$ имеет $c_{ij} = a_{ij} + b_{ij}$.

Задача 4.4. Докажите, что сложение матриц (с элементами из некоторого фиксированного кольца) коммутативно, ассоциативно, обладает нулем, а также что у каждой матрицы имеется единственная противоположная.

3.2. Определение. *Произведение AB определено тогда и только тогда, когда горизонтальный размер матрицы A равен вертикальному размеру матрицы B. Результатом произведения матрицы $A = (a_{ij})$ размера $m \times n$ и матрицы $B = (b_{ij})$ размера $n \times k$ является матрица $C = AB = (c_{ij})$ размера $m \times k$, элементы c_{ij} которой находятся по правилу:*

$$c_{ij} = \sum_{\nu=1}^{n} a_{i\nu} b_{\nu j} \ .$$

Иными словами, матрица-произведение имеет столько же строк, сколько первый сомножитель и столько же столбцов, сколько второй сомножитель, а для вычисления элемента, стоящего на пересечении i-ой строки и j-ого столбца надо взять i-ую строку первого сомножителя и j-ый столбец второго и "скалярно перемножить" их (т.е. умножить первый элемент на первый, второй на второй, и т. д., а затем сложить полученные n произведений).

3.2.1. Замечание. Определение произведение *несимметрично*, и если AB определено, то BA может быть и не определено: AB и BA определены одновременно тогда и только тогда, когда при размере матрицы A равном $m \times n$ матрица B имеет "транспонированный" размер $n \times m$.

Более того, даже если A и B — это квадратные матрицы одинакового размера, произвендения AB и BA, как правило, не равны! Например:

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 10 \\ 12 & 15 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 0 \\ 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 4 & 23 \end{pmatrix}$$

3.2.2. Пример. Рассмотрим левую часть системы линейных уравнений как матрицу-столбец размера $m \times 1$:

$$\begin{pmatrix} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n \\ & & & \cdots & & & \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n \end{pmatrix} .$$

Тогда мы можем записать её как произведение

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

матрицы системы (её размер $m \times n$) и матрицы-столбца высоты n, составленного из неизвестных. Таким образом, система линейных уравнений

$$\begin{cases} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ & & & & \cdots & & & & \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m \end{cases} .$$

может быть записана в виде *одного линейного уравнения на матрицы*

$$Ax = b ,$$

где $A = (a_{ij})$ и $b = (b_j)$ — заданные матрицы, а $x = (x_i)$ — неизвестная матрица, подлежащая определению. Возникает естественное желание: чтобы найти x надо "разделить" обе части этого уравнения на матрицу A. Ниже в этой лекции мы объясним, что это означает.

3.2.3. Пример: линейные замены переменных. Помимо рассмотренного выше способа упрощения систем путём преобразования уравнений, из школы хорошо известен и другой способ — *замена переменных.* Он заключается в переходе от переменных (x_i) к новым переменным (y_ν) (возможно, в другом количестве). при помощи подстановки

$$x_i = \varphi_i(y_1, y_2, \ldots, y_k) ,$$

где справа стоят какие-то явные выражения x_i через $(y_1, y_2, \ldots, y_k)$. Искусно подобрав эти выражения, можно надеяться получить на (y_ν) более простые уравнения, чем на (x_i), решить их, а затем вернуться к исходным переменным.

Простейшие замены переменных — линейные. Они заключаются в подстановке:

$$x_i = c_{i1}y_1 + c_{i1}y_2 + \cdots + c_{ik}y_k = \sum_{\nu=1}^{k} c_{i\nu}y_\nu ,$$

где $i = 1, 2, \ldots, n$. При помощи умножения матриц это коротко записывается в виде

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = C \cdot \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{pmatrix} ,$$

где $C = (c_{ij})$ — матрица размера $n \times k$, называеиая *матрицей перехода* от x к y и обозначаемая (как правило) через C_{yx}.

Можно сказать,что данное выше определение произведения матриц в действительности *специально подгонялось* к тому, чтобы было выполнено свойство:

3.2.4. Предложение. *Пусть последовательно выполняются две линейных замены переменных:*

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} = C_{yx} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \qquad \text{и} \qquad \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_k \end{pmatrix} = C_{zy} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} \quad ,$$

где C_{yx} и C_{zy} — матрицы размеров $m \times n$ и $k \times m$ соответственно. Тогда

$$\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_k \end{pmatrix} = C_{zx} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} , \quad \text{где} \quad C_{zx} = C_{zy} \cdot C_{yz} \ .$$

Иными словами, матрица перехода для композиции двух линейных замен переменных равна произведению матриц перехода этих замен (в том же порядке).

Доказательство. Пусть $C_{zy} = A = (a_{ij})$ и $C_{zy} = B = (b_{ij})$. Тогда

$$z_i = \sum_{\nu=1}^{m} a_{i\nu} y_\nu = \sum_{\nu=1}^{m} a_{i\nu} \sum_{j=1}^{n} b_{\nu j} x_j \ .$$

Группируя вместе слагаемые с одинаковыми j и вынося x_j за скобку, получим:

$$z_i = \sum_{j=1}^{n} c_{ij} x_j \ , \quad \text{где} \quad c_{ij} = \sum_{\nu=1}^{m} a_{i\nu} b_{\nu j} \ ,$$

что и означает, что $C_{zx} = (c_{ij}) = A \cdot B = C_{zy} C_{yz}$.

3.3. Свойства действий над матрицами. Для того, чтобы введенные нами операции над матрицами превратились из удобных обозначений в эффективное вычислительное средство, необходимо выяснить, как они взаимодействуют между собой, т.е. описать "законы сложения и умножения".

3.3.1. Предложение. *Умножение матриц ассоциативно, т.е. всякий раз, как определена одна из матриц $(AB)C$ или $A(BC)$, вместе с ней определена и другая, причем $(AB)C = A(BC)$.*

Доказательство. Это немедленно следует из предыдущего предложения (ибо замена переменных, очевидно, ассоциативна). Для тех, кто не удовлетворён таким замечанием, приведём также и формальную выкладку.

Пусть $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$ имеют размеры, соответственно, $m \times n$, $n \times k$, $k \times s$. Тогда (i, j)-тый элемент матрицы $F = (AB)C$ вычисляется по формуле

$$f_{ij} = \sum_{\nu=1}^{k} \Big(\sum_{\mu=1}^{n} a_{i\nu} b_{\nu\mu} \Big) c_{\mu j} = \sum_{\nu=1}^{k} \sum_{\mu=1}^{n} a_{i\nu} b_{\nu\mu} c_{\mu j} \quad .$$

Группируя вместе слагаемые с одинаковыми $a_{i\nu}$, получаем:

$$f_{ij} = \sum_{\nu=1}^{k} a_{i\nu}\Big(\sum_{\mu=1}^{n} b_{\nu\mu}c_{\mu j}\Big) = \sum_{\nu=1}^{k} a_{i\nu}g_{\nu j}\ .$$

Здесь $g_{\nu j} = \sum\limits_{\mu=1}^{n} b_{\nu\mu}c_{\mu j}$ является (ν, j)-м элементом матрицы BC, а значит, (f_{ij}) совпадает с (ij)-тым элементом матрицы $A(BC)$.
□

3.3.2. Предложение. *Сложение и умножение дистрибутивны друг относительно друга. Точнее, если определена одна из частей в равенствах:*

$$\begin{array}{rcll} A(B+C) & = & AB+AC & \text{(левая дистрибутивность)} \\ (A+B)C & = & AC+BC & \text{(правая дистрибутивность)} \end{array}$$

то определена и другая, а сами равенства верны.

Доказательство. Чтобы $A(B+C)$ (или $AB+AC$) имело смысл, размеры A, B, C должны иметь вид: $m \times n$, $n \times k$, $n \times k$. Если $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$, то (i, j)-тый элемент матрицы $F = A(B+C)$ есть

$$f_{ij} = \sum_{\nu=1}^{k} a_{i\nu}(b_{\nu j} + c_{\nu j} = \sum_{\nu=1}^{k} a_{i\nu}b_{\nu j} + \sum_{\nu=1}^{k} a_{i\nu}c_{\nu j}\ .$$

Справа стоит сумма (i, j)-того элемента матрицы AB с (i, j)-тым элементом матрицы AC, то есть (i, j)-ый элемент матрицы $AC + AB$. Это доказывает левую дистрибутивность.

Задача 4.5. Докажите праую дистрибутивность.

3.4. Определение. *Множество R с двумя бинарными операциями: сложением и умножением называется (некоммутативным) кольцом с единицей, если выполняются следующие*

Аксиомы (некоммутативного) ассоциативного кольца

1) Сложение коммутативно, ассоциативно, обладает нулем, и у каждого элемента есть противоположный.

2) Умножение ассоциативно и обладает двусторонней единицей; последнее означает, что

$$\exists E \in R: \quad AE = EA = A \qquad \forall A \in R\,.$$

3) Имеется левая и правая дистрибутивность:

$$A(B+C) = AB + AC \qquad \text{и} \qquad (A+B)C = AC + BC \qquad \forall\, A, B, C \in R\,.$$

3.4.1. Замечание. Отличие от аксиом коммутативного кольца — отсутствие коммутативности умножения — означает, неформально, что *умножение на A слева* и *умножение на A справа*— это две *разные* операции, имеющие, вообще говоря, разные свойства. Поэтому в теории некоммутативных колец свойства левого и правого умножений постоянно приходится рассматривать по отдельности, начиная уже с формулировок аксиом.

Задача 4.6. Докажите, что из аксиом кольца вытекает, что:
а) нулевой элемент $O \in R$ единственен;
б) $(-E)A = (-A) = A(-E)$;
в) $OA = AO = O \qquad \forall A \in R$.

3.5. Теорема. *Квадратные матрицы размера $n \times n$, элементы которых принадлежат фиксированному (возиожно, некоммутативному) кольцу R сами составляют кольцо*[1].

Доказательство. Легко видеть, что проделанные выше вычисления, доказывающие ассоциативность и дистрибутивность умножения, сохраняют смысл над любым (некоммутативным) кольцом R.

Единицей в $Mat_n(R)$ служит так называемая *единичная матрица*

$$E \stackrel{\text{def}}{=} \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ & 0 & & 1 \end{pmatrix},$$

на диагонали которой стоят единичные элементы кольца R, а в остальных местах - нули.

Задача 4.7. Проверьте, что $AE = EA = A \qquad \forall\, A \in Mat_n(R)$.

Выполнение аксиом сложения немедленно следует из их выполнения в R (ср. с зад.4.4).
□

3.5.1. Терминология. Диагонали $\begin{pmatrix} * & & \\ & * & \\ & & * \end{pmatrix}$ и $\begin{pmatrix} & & * \\ & * & \\ * & & \end{pmatrix}$ называются *главной* и *побочной*. Матрицы, под главной диагональю которых стоят нули, называются *верхнетреугольными*. Аналогично бывают и *нижнетреугольные* матрицы.

Задача 4.8. Докажите, что верхнетреугольные матрицы составляют подкольцо в $Mat_n(R)$.

Верхнетреугольная матрица с единицами на главной диагонали называется *верхней унитреугольной.*

Задача 4.9. Проверьте, что произведение любых двух верхних унитреугольных матриц снова будет верхней унитреугольной матрицей.

Задача 4.10. Докажите, что система линейных уравнений, матрица которой — квадратная верхняя унитреугольная, при любом столбце правых частей всегда имеет и притом единственное решение в любом (в том числе и некоммутативном) кольце.

3.6. Алгебраическая запись элементарных преобразований. Вернемся к элементарным преобразованиям строк. Мы собираемся реализовать их как умножения на подходящие *элементарные матрицы.* Чтобы найти эти матрицы мы применим элементарные преобразования к единичной матрице E. Полученные матрицы мы, как и выше, будем относить к трём типам:

(1 тип) получается переменой местами двух строк в матрице E;

(2 тип) получается прибавлением к одной из строк матрицы E какой-либо другой строки, умноженной на λ (или, что то же самое, заменой какого-то одного из нулей, стоящих вне главной диагонали на λ);

[1] Оно обозначается $Mat_n(R)$

(3 тип) получается умножением одной из строк матрицы E на λ (т. е. заменой на λ одной из стоящих на главной диагонали единиц).

3.6.1. Предложение. *При умножении слева на элементарную матрицу произвольная матрица подвергается элементарному преобразованию строк соответствующего типа.*

Задача 4.11. Докажите предложение проделав все необходимые выкладки.
Совет: на самом деле можно считать преобразуемую матрицу состоящей из одного столбца.

3.7. Элементарные преобразования столбцов. Введённые выше три типа элементарных преобразований можно применять не только к строкам, но и к столбцам матрицы. С точки зрения матричного умножения это означает следующее.

3.7.1. Лемма. *Умножение произвольной матрицы $A \in Mat_n(R)$ справа на элементарную матрицу 1-го, 2-го или 3-го типа приводит к соответствующему элементарному преобразованию столбцов этой матрицы.*

Задача 4.12. Проверьте лемму.

3.7.2. Пример: элементарные замены переменного. Если мы осуществляем линейную замену переменных в системе $A(x) = (b)$ при помощи подстановки $(x) = C_{xy}(y)$, то матрица системы уравнений на y будет получаться из исходной матрицы A умножением справа на матрицу перехода. Это немедленно следует из ассоциативности матричного умножения:

$$A(x) = (b) \iff A(C_{xy}(y)) = (AC_{xy})(y) = (b) \,.$$

Всякая элементарная матрица U порождает элементарную замену переменного $(x) = U(y)$. В каждом из случаев эти элементарные замены таковы:

$$(1) \qquad x_\nu = \begin{cases} y_j, & \text{при } \nu = i \\ y_i, & \text{при } \nu = j \\ y_\nu, & \text{при } \nu \neq i, j \end{cases},$$

$$(2) \qquad x_\nu = \begin{cases} y_i + \lambda y_j, & \text{при } \nu = i \\ y_\nu, & \text{при } \nu \neq i \end{cases},$$

$$(3) \qquad x_\nu = \begin{cases} \lambda y_i, & \text{при } \nu = i \\ y_\nu, & \text{при } \nu \neq i \end{cases}.$$

При подстановке $(x) = U(y)$ система уравнений $A(x) = (b)$ на (x) превращается в систему уравнений на (y) вида $B(y) = (b)$, где $B = AU$.

Таким образом при элементарных заменнах переменного матрица системы подвергается соответствующему элементарному преобразованию столбцов.

3.8. Обратная матрица. Теперь мы можем придать точный смысл фразе “разделим обе части равенства на матрицу A”. Заранее отметим, что из-за несимметричности левого и правого сомножителей в произведении нам, вообще говоря, придётся различать “деление слева” и “деление справа”.

3.8.1. Обратимость в некоммутативном кольце. Элемент A (некоммутативного) кольца R называется *обратимым справа*, если $\exists B \in R: \ AB = 1$. Аналогично, A называется *обратимым слева*, если $\exists C \in R: \ CA = 1$.

Если элемент A обратим и слева и справа, скажем $CA = AB = 1$, то левый и правый обратные к A элементы C и B совпадают, ибо

$$C = C \cdot 1 = CAB = 1 \cdot B = B$$

Такие элементы A называются просто *обратимыми*, а (двусторонне) обратный к A элемент обозначается A^{-1}.

Задача 4.13. Докажите, что двусторонне обратный элемент единственен (если существует).

3.8.2. Пример. Элементарные матрицы первого и второго типов обратимы в кольце $Mat_n(R)$ над любым кольцом R. Действительно, обратной (и слева и справа) к элементарной матрице первого типа будет она же сама, а обратной (и слева и справа) к элементарной матрице второго типа будет матрица, отличающаяся от исходной заменой знака у λ.

Задача 4.14. Обязательно убедитесь в этом!

3.8.3. Пример. Элементарная матрица третьего типа обратима в кольце матриц над полем. Обратная матрица получается из исходной заменой λ на λ^{-1}.

3.8.4. Решение системы в терминах матричной алгебры. Если квадратная матрица $A \in Mat_n(R)$ обратима, то система $A(x) = (b)$ (где (x) и (b) – столбцы высоты n, состоящие, соответственно, из неизвестных и правых частей) имеет и притом единственное решение при любом столбце правых частей.

Действительно, если $(x) = (c)$ — решение, то умножая обе части матричного равенства $A(c) = (b)$ слева на A^{-1}, получим $(c) = A^{-1}(b)$, т.е. (c) однозначно восстанавливается по (b).

Наоборот, полагая $(x) = A^{-1}(b)$, мы получим решение системы.

3.9. Отыскание обратной матрицы над полем. Пусть $R = k$ — произвольное поле. Как показывает метод Гаусса, в этом случае квадратная матрица A обратима тогда и только тогда, когда она приводится элементарными преобразованиями к строго ступенчатому виду

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

Пусть последовательность элементарных преобразований, превращающая A в E, состоит в умножению A слева на элементарные матрицы $U_1, U_2, \ldots, U_s$. Это записывается равенством

$$U_s \cdot U_{s-1} \cdot \cdots \cdot U_2 \cdot U_1 \cdot A = E .$$

Поскольку все U_ν обратимы в $Mat_n(k)$, мы можем умножить обе части этого равенства слева на

$$U_1^{-1} U_2^{-1} \cdots U_s^{-1} .$$

Получим, что $A = U_1^{-1} U_2^{-1} \cdots U_s^{-1} \cdot E$, откуда $A^{-1} = U_s U_{s-1} \cdots U_2 U_1$, что можно переписать в виде

$$A^{-1} = U_s U_{s-1} \cdots U_2 U_1 \cdot E$$

и воспринимать как результат воздействия на матрицу E ровно той же последовательности элементарных преобразований строк, которая превращает A в E. Мы получаем

3.9.1. Предложение. *Пусть $A \in Mat_n(k)$ — произвольная квадратная матрица над полем. Если приписать к ней справа матрицу E и привести полученную $n \times 2n$-матрицу (AE) к строгому ступенчатому виду элементарными преобразованиями срок, то либо в результате получится матрица, содержащая по меньшей мере одну нулевую строку (что равносильно необратимости A), либо — матрица (EA^{-1}).*

§4. Метод Гаусса над евклидовым кольцом

До конца этого параграфа мы будем считать, что R – это *евклидово кольцо* (см. начало лекции 3). Основными примерами, которые читателю рекомендуется держать в голове, являются $R = \mathbb{Z}$ или $R = k[x]$, где k – произвольное поле.

4.1. Обратимые элементарные преобразования. Условимся называть элементарное преобразование *обратимым*, если оно задаётся умножением на обратимую элементарную матрицу. Отметим, что элементарные преобразования первых двух типов обратимы всегда (и над любым кольцом). Элементарное преобразование третьего типа обратимо тогда и только тогда, когда λ — обратимый элемент (т. е. ± 1 для $R = \mathbb{Z}$ и любая ненулевая константа для $R = k[x]$). Мы собираемся выяснить, до какой степени можно упростить прямоугольную матрицу над R при помощи обратимых элементарных преобразований строк и столбцов. Окончательный вид матрицы , к которому мы стремимся, мы будем называть *строгим диагональным*.

4.2. Строгий диагональный вид. Прямоугольную матрицу над R будем называть *диагональный* если она имеет вид

$$D = \begin{pmatrix} d_1 & & & & \\ & d_2 & & 0 & \\ & & \ddots & & \\ & & & d_s & \\ & 0 & & 0 & \\ & & & & \ddots \end{pmatrix},$$

в котором все ненулевые элементы исчерпываются числами $d_1, d_2, \dots, d_s$, расположенными в верхней части главной диагонали[2].

Мы называем диагональную матрицу *строгой диагональной*, если её ненулевые элементы $d_1, d_2, \dots, d_s$ таковы, что каждое d_i делится в R на все предыдущие d_j с $j < i$.

4.3. Теорема. *Любая прямоугольная матрица A с коэффициентами из R обратимыми элементарными преобразованиями строк и столбцов приводится к строго диагональному виду.*

Доказательство. Пусть $R \xrightarrow{\lambda} \mathbb{N} \cup 0$ – высота в евклидовом кольце R (т. е. модуль целого числа для $R = \mathbb{Z}$ и степень многочлена для $R = k[x]$). Будем преобразовывать строки и столбцы матрицы A с таким расчётом, чтобы высота элемента, стоящего в левом верхнем углу уменьшалась. Поскольку натуральные числа нельзя уменьшать безгранично, в какой-то момент дальнейшее уменьшение $\lambda(a_{11})$ станет невозможным. Я утверждаю, что в этот момент все элементы матрицы обязаны будут нацело делиться на a_{11}.

[2] Для прямоугольной неквадратной матрицы A мы понимаем под "главной диагональю" совокупность элементов вида a_{ii} (которая диагональю в строгом смысле и не является, ибо начавшись в левом верхнем углу, кончается где придётся).

Действительно, пусть в первом столбце есть элемент a_{k1}, не делящийся нацело на a_{11}. Деление с остатком даёт $a_{k1} = qa_{11} + r$, где $\lambda(r) < \lambda(a_{11})$. Следовательно, если отнять из k-ой строки первую, умноженную на q, а затем поменять местами первую строку с k-ой, в верхнем левом углу возникнет элемент r, высота которого меньше, чем высота a_{11}.

Меняя в только что проделанном рассуждении строки и столбцы ролями, мы видим, что вся первая строка также делится на a_{11}.

Наконец, пусть элемент a_{ij}, не делящийся на a_{11}, найдется где-либо вне первых строки и столбца. Отнимая из всех строк и всех столбцов подходящие кратные первых строки и столбца, можно добиться того, чтобы первые строка и столбец обнулились вне a_{11}. К элементу a_{ij} при этом прибавится нечто кратное a_{11}, а значит он по прежнему не будет делится на a_{11}. Прибавив в полученной новой матрице к первому столбцу j-ый, я получу матрицу, содержащую a_{ij} в первом столбце, после чего a_{11} можно будет уменьшить так, как это уже было описано выше.

Итак, за конечное число обратимых элементарных преобразований я могу привести матрицу A к виду

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix},$$

где через B обозначена $(m-1)\times(n-1)$-матрица, все элементы которой нацело делятся на d_1. Далее продолжаем по индукции.

Теорема доказана.

4.3.1. Следствие. *Пусть A - матрица размера $m \times n$ над R. Тогда существуют обратимые над R $m \times m$-матрица U и $n \times n$-матрица V, такие что $D = UAV$ имеет строгий диагональный вид.*

> Задача 4.15. Докажите, что эти матрицы U и V можно явно отыскать так: припишем к матрице A справа и снизу единичные матрицы размеров $m \times m$ и $n \times n$ соответственно, так чтобы получилась Г-образная таблица вида $\begin{matrix} A & E \\ E & \end{matrix}$; затем элементарными преобразованиями строк и столбцов этой таблицы добьёмся того, чтобы угловой блок A приобрёл строгий диагональный вид D, и в этот момент вся таблица приобретёт вид $\begin{matrix} D & U \\ V & \end{matrix}$ с искомыми U и V.

4.3.2. Следствие. *Всякая система уравнений $A(x) = (b)$ с коэффициентами из R при помощи обратимой линейной замены переменного $(x) = V(y)$ может быть преобразована в систему, равносильную системе*

$$\begin{cases} d_1 y_1 &= c_1 \\ d_2 y_2 &= c_2 \\ & \dots \\ d_k y_k &= c_k \end{cases},$$

в которой каждое d_j делит все последующие d_i с $i > j$.

Эти следствия и задача дают вполне исчерпывающий алгоритм для решения систем линейных уравнений над евклидовыми кольцами.

4.3.3. Замечание. В действительности диагональные элементы $d_1, d_2, \ldots, d_s$ с точностью до умножения на обратимые элементы кольца R не зависят от того способа, которым матрица A приводилась к строгому диагональному виду. Мы докажем это в лекции 7, а пока лишь отметим, что элементы d_ν называются *инвариантными множителями* матрицы A, а их количество – *рангом* матрицы A.