Лекции по алгебре первого курса СП 2021

Преподаватель: Константин Михайлович Чепуркин

весна 2021

Лекция 14.02

1 Продолжение истории с матрицами

Наша текущая мотивация: компактно и точно описывать системы линейных уравнений(далее СЛУ) на языке матриц.

Для этого заметим, что в СЛУ каждая строчка имеет следующий вид: $a_1x_1 + \dots + a_nx_n$. Поэтому давайте заведём следующую операцию умножения для матриц $M_{1\times n}(R) \times M_{n\times 1}(R) \to R$(в данном контексте и далее R — произвольное кольцо), а именно:

$$\begin{pmatrix} a_1 & \dots & a_n \end{pmatrix} \times \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = a_1x_1 + \dots + a_nx_n$$

Определение (Вектор)**.** **Вектором** размера n будем называть матрицу $M_{n\times 1}$.

Теперь логично захотеть определить умножение матрицы на вектор $M_{m\times n} \times M_{n\times 1} \Rightarrow M_{m\times 1}$ таким образом, чтобы удобно было получать нечто похожее на СЛУ. Очевидно это можно сделать умножением каждой строчки на вектор следующим образом:

$$\begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix} \times \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{1,1}x_1 + \dots + a_{1,n}x_n \\ \vdots \\ a_{m,1}x_1 + \dots + a_{m,n}x_n \end{pmatrix}$$

После этого уже можно обобщить наше произведение на две матрицы. Для этого представим, что мы умножаем систему уравнений не на набор неизвестных, получая матрицу, похожую на систему уравнений, а на несколько наборов значений, ведь матрицу можно представить как упорядоченный набор векторов.

Определение (Произведение матриц)**.** Произведение матриц $A \in M_{m\times n}, B \in M_{n\times k}$ определим следующим образом:

$$A\times B = A\times\big(B_{1,*}, \dots, B_{k,*}\big) = \big(A\times B_{1,*}, \dots, A\times B_{k,*}\big) = \begin{pmatrix} a_{1,1}b_{1,1} + \dots + a_{1,n}b_{1,n} & \dots & a_{1,1}b_{k,1} + \dots + a_{1,n}b_{k,n} \\ \vdots & \ddots & \vdots \\ a_{m,1}b_{1,1} + \dots + a_{m,n}b_{1,n} & \dots & a_{m,1}b_{k,1} + \dots + a_{m,n}b_{k,n} \end{pmatrix}$$

Иначе говоря, если $A \times B = C$, тогда:

$$C_{i,j} = \sum_{k=0}^{n} A_{i,k}B_{k,j}$$

Замечание. (P.s знак $\times$ при умножении матриц и векторов в будущем часто будет опускаться)

Замечание. Произведение матриц не коммутативно:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}; \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}$$

Примеры. Давайте приведём несколько примеров использования введённой нами операции.

1. Для записи СЛУ в виде $Ax = b$, где A — матрица, а x, b — вектора.
2. Для записи скалярного произведения: a^Tx, где x, a — вектора, а a^T операция транспонирования матрицы, о которой будет сказано позже. Пока её можно воспринимать как переворот вектора в матрицу $M_{1\times n}$.
3. Для подсчёта количества путей размера k между любыми двумя вершинами ориентированного графа.

   Пусть G — ориентированный граф. Тогда его **матрицей смежности** $A(G)$ определим следующим образом:

   $$A(G)_{i,j} \begin{cases} 1, \text{если есть ребро } i \to j \\ 0, \text{иначе} \end{cases}$$

   Тогда легко показать, что $(A(G)_{i,j})^k$ — количество путей $i \to j$ длины k.

4. Для подсчёта суммы путей размера k между любыми двумя вершинами взвешенного ориентированного графа, где длинна пути считается как произведение весов рёбер на нём.

   Пример такой задачи: есть статистика по переселению людей между n городами в следующем виде: известно, что вероятность переезда человека из города i в город j равна весу ребра $i \to j$. Надо по этим данным научиться узнавать шанс того, что человек из города i через k лет будет жить в городе j.

   Для простоты будем считать, что сумма весов исходящих рёбер для каждой вершины равна 1. Если это не так, то мы можем это исправить, создав ребро $i \to i$ с нужным нам весом. В данной формулировке наиболее понятно, что шанс переезда человека, живущего в городе i, в город j через k лет будет равен сумме весов путей $i \to j$ длины k, если вес пути это произведение всех рёбер на нём. Таким образом, мы получили задачу похожую на предыдущую, за исключением того, что наш граф теперь взвешенный, а значит $(A(G)_{i,j})^k$ — искомая вероятность.

Свойства.

1. Ассоциативность произведения матриц в случае, где оба произведения определены: $(AB)C = A(BC)$. (Доказать самим)
2. Существование единичной матрицы $E_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$ Доказательство того, что она не изменяет умножаемую на неё, очевидно.
3. Обратный элемент существует не для любой матрицы. Приведём пример с $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$:

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Определение (Сложение матриц)**.** Введём очевидную операцию сложения матриц: $(A+B)_{i,j} = A_{i,j} + B_{i,j}$.

Свойства.

1. $A + B = B + A$
2. $(A + B) + C = A + (B + C)$
3. $\mathbf{0}_{m \times n} = \begin{pmatrix} 0 & \dots & 0 \\ 0 & \ddots & 0 \\ 0 & \dots & 0 \end{pmatrix}$
4. $\forall A \in M \exists (-A) : A + (-A) = \mathbf{0}$
5. $(A + B)C = AC + BC$
$C(A + B) = CA + CB$

Определение. Введём операцию умножения вектора на скаляр следующим образом:

$$\lambda \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}$$

Свойства.

1. $$\begin{pmatrix} \lambda & 0 & 0 & \dots \\ 0 & \lambda & 0 & \dots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \lambda \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix} = \lambda \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$
2. $$(\lambda\mu) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (\mu\lambda) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \lambda \left(\mu \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \right)$$

Определение. Введём операцию умножения матрицы на скаляр следующим образом:

$$\lambda A = \begin{pmatrix} \lambda & 0 & 0 & \dots \\ 0 & \lambda & 0 & \dots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \lambda \end{pmatrix} A$$

Свойства.

1. $$\lambda(AB) = (\lambda A)B = A(\lambda B)$$

Замечание. Исходя из введённых выше операций и их свойств становятся очевидными некоторые утверждения про решения СЛУ, перечислим их:

1. $$\begin{cases} Ax = b \\ Ay = c \end{cases} \Rightarrow A(x+y) = b + c$$

   Где x, y, b, c — вектора, а A — матрица системы.

2. Из предыдущего свойства:

   $$\begin{cases} Ax = b \\ Ax_0 = 0 \end{cases} \Rightarrow A(x + x_0) = b \Rightarrow A(x + kx_0) = b, \forall k \in \mathbb{N}$$

3. Пусть $L = \{x \mid Ax = 0\} \subset R^n$, тогда знаем следующие факты про $x_1, x_2 \in L, \lambda \in R$:

   (a) $x_1 + x_2 \in L$

   (b) $\lambda x_1 \in L$

2 Векторные пространства

2.1 Базовые понятия

Заметим, что полученные нами свойства не вписываются в изучаемые ранее структуры, из-за чего возникает желание завести новый объект.

Определение (Векторное пространство). **Векторным пространством** над полем K будем называть набор $(V, +, \cdot)$, удовлетворяющий свойствам ниже.

Свойства.

1. (a) Определена операция умножения вектора на скаляр $\cdot : K \times V \mapsto V$

   (b) Определена операция сложения векторов $+ : V \times V \mapsto V$

2. $(V, +)$ — абелева группа

3. $\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$

4. $(\lambda + \mu) \cdot v = \lambda v_1 + \lambda v_2$

5. $1 \cdot v = v$

6. $(\lambda\mu)v = \lambda(\mu v)$

Примеры.

1. K^n — векторное пространство над K.

2. $M_{m\times n}(K)$ — векторное пространство над K.

3. (a) $\mathbb{C}$ — векторное пространство над $\mathbb{R}$.

   (b) $\mathbb{R}$ — векторное пространство над $\mathbb{Q}$.

   (c) Таким образом можно показать, что если K является подполем L, то L — векторное пространство над K.

4. $C[a, b]$ — векторное пространство над $\mathbb{R}$.

5. $C'[a, b]$ — векторное пространство(далее ВП) над $\mathbb{R}$.

Определение (Подпространство). Если $W \subseteq V$, то W является **подпространством** при выполнении следующих условий:

1. $a + b \in W \quad \forall a, b \in W$.

2. $\lambda \cdot v \in W \quad \forall \lambda \in K, v \in W$.

3. $\overline{0} \in W$

Пример 1. $\{x \mid Ax = 0\}$ подпространство в K^n.

Определение (Линейная комбинация векторов). **Линейной комбинацией векторов** $v_1, \ldots, v_n \in V$ назовём: $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n$, где $\lambda_i \in K$.

Определение (Линейная зависимость). **Линейно зависимыми** назовём множество векторов такое, что любой вектор из множества записывается в виде линейной комбинации остальных. Иначе говоря, $v_1, \ldots, v_n$ — линейно зависимы если: $\exists \lambda_1, \ldots, \lambda_n \in K : \lambda_1 v_1 + \cdots + \lambda_n v_n = 0, \exists \lambda_j \neq 0$.

Лекция 21.02

Определение (Линейная независимость). $v_1 \dots v_n$ — линейно независимы, если $\lambda_1 v_1 + \dots + \lambda_n v_n = 0 \Rightarrow \lambda_i = 0 \; \forall i$.

2.2 Базис

Определение (Стандартный базис). Для пространства K^n следующий набор назовём стандартным базисом:

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \dots \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

Очевидно, что этот набор линейно независим. Точно так же работает для матриц, один элемент главной диагонали которых единица.

Факт. Линейная зависимость в случае двух векторов $\Leftrightarrow$ вектора пропорциональны.

Факт. Есть у нас есть набор линейно независимых векторов $v_1, \dots v_n$, то новый набор век $v_1, \dots v_i, v_j + \lambda v_i, \dots v_n, i \neq j$ тоже линейно независим $\forall \lambda$.

Док-во: Обозначим новый набор векторов как v_i'. Рассмотрим $\sum_{k=1}^n \mu_k v_k' = 0$, надо понять существуют ли такие нетривиальные μ_k?

Раскрыв скобки, получим: $(\sum_{k=1}^n \mu_k v_k) + \mu_j \lambda v_i = 0 \Rightarrow \mu_k = 0 \forall k \neq i$ и $\mu_i + \mu_j \lambda = 0$ по линейной независимости векторов(а значит коэффициенты при всех векторах точно 0). Значит $\mu_i = 0$, так как $\mu_j \lambda = 0$.

Доказав факт выше мы получили что-то похожее на элементарное преобразование системы первого типа. Теперь давайте поймём что-то про размерность

Теорема 1 (О линейной зависимости линейной комбинации). Для произвольного набора векторов $v_1, \dots v_n \in V$, строим набор векторов такой, что каждый из $u_1, \dots u_m$ — линейная комбинация v. Тогда, если $m > n$, то набор векторов u линейно зависим.

Доказательство: Будем доказывать индукцией по n, считая что m у нас фиксировано.

База индукции:
$n = 1, m > 2$, все $u_i = \lambda_i \cdot v_1$, тогда по факту выше u линейно зависимы.

Индукционный переход: $n - 1 \to n$:
Определим $\lambda_{i,j}$ следующим образом: $u_i = \sum_{j=0}^n \lambda_{i,j} v_j$. Найдём вектор $u_k : \lambda_{k,n} \neq 0$, если такого нет, тогда оказывается, что v_n не участвует в разложении ни одного u_i, а значит можем воспользоваться шагом индукции.

Перейдём к доказательству случая, где u_k существует. Посмотрим на новый набор векторов $u' = \left\{ u_i - \frac{\lambda_{i,n}}{\lambda_{k,n}} u_k \mid i \neq k \right\}$. Тогда каждый u_i' выражается через $v_1, \dots, v_{n-1}$. То есть у нас есть $m - 1$ вектор, каждый из которых выражается через $n - 1$ вектор. А это значит, что данный набор $v_1', \dots, v_{m-1}'$ линейно зависим по предположению индукции.

Расписав по определению, получим $\sum_{i=0}^{m-1} \mu_i u_i' = 0$, где не все $\mu_i = 0$. Распишем то же самое, но через u_i: $\sum_{i=0}^{m-1} \mu_i u_i + (\sum \dots) u_m = 0$. Получается, что в этой линейной комбинации тоже не все коэффициенты равны нулю, а значит мы нашли нетривиальную линейную комбинацию. (Конец доказательства)

Для того, чтобы двигаться дальше дадим несколько определений.

Определение (Подпространство). Подпространством V для набора векторов $v_1, \dots, v_n \in V$ называется

$$\{\lambda_1 v_1 + \dots \lambda_n v_n \mid \lambda_i \in K\}$$

Причём, по теореме выше, это наименьшее подпространство содержащее $v_1, \dots, v_n$. Далее обозначается как $< v_1, \dots, v_n >$.

Определение (Порождающая система). Если $< v_1, \dots v_n >= V$, то набор векторов называется порождающей системой.

Определение (Базис). $v_1, \dots, v_n \in V$ — базис, если:

1. $v_1, \dots, v_n$ линейно независимы
2. $v_1, \dots, v_n$ — порождающая V

Утверждение 1. $v_1, \dots v_n \in V$ является базисом $\Leftrightarrow \forall v \in V \; \exists! \; \lambda_1, \dots, \lambda_n : \; v = \sum_{i=1}^n \lambda_i v_i$.

Доказательство:
$\Leftarrow$:

1. Пусть набор v линейно зависим, тогда: $\exists \mu : \sum_{i=1}^n \mu_i v_i = 0, \exists \mu_j \neq 0$. Тогда расписав любой вектор, воспользовавшись условием, получим $v = \sum_{i=1}^n \lambda_i v_i = \sum_{i=1}^n (\lambda_i + \mu_i) v_i$. То есть мы нашли второе разложение v как линейную комбинацию v_i, что противоречит с единственностью λ. Значит v линейно независим.

2. $v_1, \dots, v_n$ — порождающая V просто так как любой вектор из V выражается линейной комбинацией векторов из v.

$\Rightarrow$:

$\exists \lambda_i \sum_{i=1}^{n} \lambda_i v_i = V$ Пусть есть две линейные комбинации, дающие v. $\sum_{i=1}^{n} \lambda_i v_i = \sum_{i=1}^{n} \mu_i v_i = v$. Можем вычесть одну из другой, тогда $\sum_{i=1}^{n}(\lambda_i - \mu_i)v_i = 0 \Rightarrow \lambda_i - \mu_i = 0 \ \forall i \Rightarrow \lambda_i = \mu_i \ \forall i$. (Конец доказательства)

Пример 2 (Бесконечный базис)**.** $1, x, x^2, \ldots, x^n, \ldots$ — базис $K[x]$. Проблема бесконечного базиса в том, что многие факты доказываются сильно сложнее. Поэтому полноценно работать с пространствами, которые имеют бесконечный базис, в рамках этого курса мы не будем, но иногда будем приводить примеры таковых.

Теорема 2. $u_1, \ldots, u_m \in V$ — порождающий набор в V. $v_1, \ldots, v_n \in V$ — линейно независимый. Тогда $v_1, \ldots, v_n$ можно дополнить до базиса добавив какие-то вектора из $u_1 \ldots, u_m$.

Доказательство:
Идея банальна: добавляем по одному и в какой-то момент мы достигнем того, что набор линейно независимым, но ни один вектор из u мы не можем добавить не сделав набор линейно зависимым.

Посмотрим на количество векторов из $u_1, \ldots, u_m$, которые не лежат в линейной комбинации в пространстве, порождённом $< v_1, \ldots, v_n >$. $v_1, \ldots, v_n, u_1, \ldots, u_k$ набор векторов в момент остановки. Хотим понять, что мы получили базис. Заметим, что в $< v_1, \ldots, v_n, u_1, \ldots, u_k >$ нельзя добавить ни одно u_i $i > k$, а значит любое u_i выражается через вектора из нашего множества(очевидно). Тогда мы получили следующую цепочку:

$$V \supseteq < v_1, \ldots, v_n, u_1, \ldots, u_k > \supseteq < u_1, \ldots, u_m > = V$$

(Конец доказательства)

Следствие 1. $v_1, \ldots, v_n$ — пуст $\Rightarrow$ в любом векторном пространстве есть базис.

Теорема 3. $V = < u_1, \ldots, u_m > \Rightarrow$ размер любых двух базисов V одинаков и конечен.
Доказательство: $e_1, \ldots, e_n$, $f_1, \ldots, f_\alpha$ — базисы. Знаем, что все f_j выражаются через e_i и все e_i выражаются через f_j. Допустим $\alpha > n$, тогда $f_1, \ldots, f_\alpha$ линейно зависимы(по **теореме 1**), а значит f не базис. Для случая $\alpha < n$ всё аналогично. (Конец доказательства)

Определение (Размерность пространства)**.** V — век. пространство $dimV$ = количество векторов в базисе V.

Определение. V — конечномерное, если $V = < u_1, \ldots, u_m >$.

Замечание. Если V — конечномерное $U \leq V$, более того $dimU \leq dimV$, причём $dimU = dimV \Leftrightarrow U = V$.
Доказательство: Возьмём $u_1, \ldots, u_k \in U$, $K \leq dimV$. TODO()

2.3 Алгебраические и трансцендентные числа

Определение. $\alpha \in \mathbb{C}$, α — алгебраическое, если $\exists p(x) \neq 0 \in \mathbb{Q}[x] p(\alpha) = 0$. Иначе α — трансцендентное.

Если α — алгебраическое, $f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$ Вопрос: $f(\alpha)$ — алгебраическое или нет? Ответ: α — алгебраическое $\Rightarrow f(a)$ — алгебраическое.

2.4 Связь с теорией множеств

Определение. $U_1, U_2 \leq V \Rightarrow U_1 \cap U_2 \leq V$ и $U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1; u_2 \in U_2\} \in V$

Теорема 4 (Формула Грассмана)**.** V — конечномерно. $U_1, U_2 \leq V$. $dimU_1 + dimU_2 = dim(U_1 + U_2) + dim(U_1 \cap U_2)$

Замечание. Для трёх подпространств и более она **не работает** по аналогии с формулой включений исключений.